AWS Well-Architected Framework

Pilar de seguridad

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Pilar de seguridad: AWS Well-Architected Framework

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

Resumen e introducción 1
Introducción 1
Aspectos básicos de seguridad 3
Principios de diseño 3
Definición 4
Responsabilidad compartida 4
Gobernanza 7
AWSAdministración y separación de cuentas de 8
SEC01-BP01 Separación de cargas de trabajo con cuentas 10
SEC01-BP02 Protección del usuario raíz y las propiedades de la cuenta 13
Funcionamiento seguro de las cargas de trabajo 18
SEC01-BP03 Identificación y validación de los objetivos de control 20
SEC01-BP04 Actualización constante de las amenazas y recomendaciones de seguridad 23
SEC01-BP05 Reducción del alcance de la administración de la seguridad 25
SEC01-BP06 Automatización de la implementación de controles de seguridad estándares ... 27
SEC01-BP07 Identificación de amenazas y priorización de mitigaciones con un modelo de amenazas 31
SEC01-BP08 Evaluación e implementación de nuevos servicios y características de seguridad de forma periódica 35
Identity and Access Management 38
Administración de identidades 38
SEC02-BP01 Uso de mecanismos de inicio de sesión sólidos 39
SEC02-BP02 Uso de credenciales temporales 43
SEC02-BP03 Almacenamiento y uso seguros de secretos 47
SEC02-BP04 Uso de un proveedor de identidades centralizado 53
SEC02-BP05 Auditoría y rotación periódicas de las credenciales 58
SEC02-BP06 Uso de grupos y atributos de usuarios 60
Administración de permisos 64
SEC03-BP01 Definición de los requisitos de acceso 66
SEC03-BP02 Concesión de acceso con privilegios mínimos 70
SEC03-BP03 Establecimiento de un proceso de acceso de emergencia 74
SEC03-BP04 Reducción continua de los permisos 82
SEC03-BP05 Definición de las barreras de protección de los permisos para una organización 85

SEC03-BP06 Administración del acceso en función del ciclo de vida 89
SEC03-BP07 Análisis del acceso público y entre cuentas 92
SEC03-BP08 Uso compartido de recursos de forma segura en su organización 94
SEC03-BP09 Uso compartido seguro de recursos con terceros 99
Detección 104
SEC04-BP01 Configuración del registro de servicios y aplicaciones 105
Guía para la implementación 10
Recursos 12
SEC04-BP02 Recopilación de registros, resultados y métricas en ubicaciones estandarizadas 110
Guía para la implementación 10
Pasos para la implementación 22
Recursos 12
SEC04-BP03 Correlación y enriquecimiento de las alertas de seguridad 114
Guía para la implementación 10
Recursos 12
SEC04-BP04 Inicio de correcciones para recursos no conformes 117
Guía para la implementación 10
Recursos 12
Protección de la infraestructura 122
Protección de redes 123
SEC05-BP01 Creación de capas de red 124
SEC05-BP02 Control del flujo de tráfico dentro de las capas de red 127
SEC05-BP03 Implementación de una protección basada en la inspección 130
SEC05-BP04 Automatización de la protección de la red 134
Protección de la computación 137
SEC06-BP01 Administración de las vulnerabilidades 137
SEC06-BP02 Aprovisionamiento de computación a partir de imágenes reforzadas 141
SEC06-BP03 Reducción de la administración manual y el acceso interactivo 144
SEC06-BP04 Validación de la integridad del software 147
SEC06-BP05 Automatización de la protección de computación 149
Protección de los datos 153
Clasificación de datos 153
SEC07-BP01 Comprensión del esquema de clasificación de datos 153
SEC07-BP02 Aplicación de controles de protección de datos según la confidencialidad de los datos 156

SEC07-BP03 Automatización de la identificación y la clasificación 159
SEC07-BP04 Definición de la administración escalable del ciclo de vida de los datos 162
Protección de los datos en reposo 165
SEC08-BP01 Implementación de una administración de claves segura 166
SEC08-BP02 Aplicación del cifrado en reposo 170
SEC08-BP03 Automatización de la protección de los datos en reposo 173
SEC08-BP04 Aplicación del control de acceso 177
Protección de los datos en tránsito 180
SEC09-BP01 Implementación de la administración segura de claves y certificados 181
SEC09-BP02 Aplicación del cifrado en tránsito 185
SEC09-BP03 Autenticación de las comunicaciones de red 187
Respuesta a incidentes 192
AWSRespuesta frente a incidencias de 192
Diseño de objetivos de respuesta en la nube 193
Preparación 195
SEC10-BP01 Identificación del personal clave y los recursos externos 195
SEC10-BP02 Desarrollo de planes de administración de incidentes 199
SEC10-BP03 Preparación de las capacidades forenses 204
SEC10-BP04 Desarrollo y prueba de manuales de estrategias de respuesta a incidentes de seguridad 207
SEC10-BP05 Aprovisionamiento previo del acceso 209
SEC10-BP06 Implementación de las herramientas con anticipación 213
SEC10-BP07 Ejecución de simulaciones 216
Operaciones 218
Actividad posterior al incidente 219
SEC10-BP08 Establecimiento de un marco de trabajo para aprender de los incidentes 220
Seguridad de las aplicaciones 223
SEC11-BP01 Formación en seguridad de las aplicaciones 224
Guía para la implementación 10
Recursos 12
SEC11-BP02 Automatización de las pruebas a lo largo del ciclo de vida de desarrollo y lanzamiento 228
Guía para la implementación 10
Recursos 12
SEC11-BP03 Pruebas de penetración periódicas 232
Guía para la implementación 10

Recursos 12
SEC11-BP04 Revisiones del código de conducta 234
Guía para la implementación 10
Recursos 12
SEC11-BP05 Centralización de servicios para paquetes y dependencias 238
Guía para la implementación 10
Recursos 12
SEC11-BP06 Implementación de software mediante programación 240
Guía para la implementación 10
Recursos 12
SEC11-BP07 Evaluación periódica de las propiedades de seguridad de las canalizaciones 244
Guía para la implementación 10
Recursos 12
SEC11-BP08 Creación de un programa que integre la propiedad de la seguridad en los equipos de la carga de trabajo 246
Guía para la implementación 10
Recursos 12
Conclusión 250
Colaboradores 251
Documentación adicional 253
Revisiones del documento 254
Avisos 258
Glosario de AWS 259

Pilar de seguridad: Marco de AWS Well-Architected

Fecha de publicación: 6 de noviembre de 2024 (Revisiones del documento)

Este documento se centra en el pilar de seguridad del Marco de AWS Well-Architected. Proporciona orientación para ayudarle a aplicar las prácticas recomendadas y las recomendaciones actuales en el diseño, la entrega y el mantenimiento de las cargas de trabajo seguras de AWS.

Introducción

El Marco de AWS Well-Architected le ayuda a comprender las ventajas y desventajas de las decisiones que toma al crear cargas de trabajo en AWS. Mediante el uso del marco, aprenderá prácticas recomendadas de arquitectura actuales para diseñar y operar cargas de trabajo fiables, eficaces, rentables y sostenibles en la nube. Proporciona una forma de medir sus cargas de trabajo de forma coherente en función de las prácticas recomendadas y de identificar áreas de mejora. Creemos que contar con cargas de trabajo de Well-Architected aumenta en gran medida la probabilidad de éxito empresarial.

El marco se basa en seis pilares:

- Excelencia operativa
- Seguridad
- Fiabilidad
- Eficacia del rendimiento
- Optimización de costes
- Sostenibilidad

El presente documento se centra en el pilar de seguridad. Le ayudará a cumplir los requisitos empresariales y normativos mediante recomendaciones actuales de AWS. Está destinado a aquellos que ocupan puestos relacionados con la tecnología, como directores de tecnología (CTO), directores de seguridad de la información (CSO o CISO), arquitectos, desarrolladores y miembros del equipo de operaciones.

Después de leer este documento, comprenderá mejor las prácticas recomendadas y estrategias actuales de AWS que puede utilizar cuando diseñe arquitecturas en la nube teniendo en cuenta la seguridad. En este documento no se proporcionan detalles de implementación ni patrones de

arquitectura, pero se incluye referencias a los recursos adecuados para obtener esta información. Al adoptar las prácticas incluidas en este documento, puede crear arquitecturas que protejan datos y sistemas, controlen el acceso y respondan automáticamente a eventos de seguridad.

Aspectos básicos de seguridad

En el pilar de seguridad, se describe cómo aprovechar las tecnologías en la nube para proteger los datos, los sistemas y los activos de una manera que pueda mejorar su posición de seguridad. En este documento se incluyen consejos detallados y de prácticas recomendadas para el diseño de cargas de trabajo seguras en AWS.

Principios de diseño

Hay una serie de principios en la nube que pueden ayudarle a fortalecer la seguridad de la carga de trabajo:

- Implementación de sólidas bases de identidad: implemente un principio de privilegios mínimos y aplique una separación de tareas con la autorización adecuada para cada interacción con los recursos de AWS. Centralice la administración de identidades y busque eliminar la dependencia de las credenciales a largo plazo.
- Mantenimiento de la trazabilidad: supervise, audite y alerte de acciones y cambios en el entorno en tiempo real. Integre la recopilación de registros y métricas con sistemas para investigar y tomar medidas automáticamente.
- Aplicación de la seguridad en todas las capas: aplique un enfoque de defensa en profundidad con múltiples controles de seguridad. Impleméntelo en todas las capas (por ejemplo, red periférica, VPC, equilibrio de carga, cada instancia y servicio de computación, sistema operativo, aplicación y código).
- Automatización de las prácticas recomendadas de seguridad: los mecanismos automatizados de seguridad basados en software mejoran la capacidad de escalar de forma más segura, rápida y rentable. Cree arquitecturas seguras, como la implementación de controles definidos y administrados como código en plantillas controladas por versión.
- Protección de datos en tránsito y en reposo: clasifique los datos por niveles de confidencialidad y use mecanismos como el cifrado, la tokenización y el control de acceso cuando corresponda.
- Alejamiento de las personas respecto a los datos: use mecanismos y herramientas para reducir o eliminar la necesidad de acceder directamente a los datos o procesarlos manualmente. De esta forma, se reducen los errores humanos y el riesgo de una mala gestión o modificación al gestionar información confidencial.
- Preparación para eventos de seguridad: para prepararse para un incidente, tenga a su disposición procesos y políticas de investigación y administración de incidentes que se ajusten a los requisitos

de su organización. Ejecute simulaciones de respuesta frente a incidencias y use herramientas con automatización para aumentar la velocidad de detección, investigación y recuperación.

Definición

La seguridad en la nube consta de siete áreas:

- Aspectos básicos de seguridad
- Identity and Access Management
- Detección
- Protección de la infraestructura
- Protección de los datos
- Respuesta frente a incidencias
- Seguridad de las aplicaciones

Responsabilidad compartida

Los asuntos relacionados con la seguridad y la conformidad son una responsabilidad compartida entre AWS y el cliente. Este modelo compartido puede aliviar la carga operativa del cliente, ya que AWS opera, administra y controla los componentes del sistema operativo host y la capa de virtualización con el fin de ofrecer seguridad física en las instalaciones en las que operan los servicios. Por otra parte, el cliente asume la responsabilidad y la administración del sistema operativo invitado (incluidas las actualizaciones y los parches de seguridad), de cualquier otro software de aplicaciones asociadas y de la configuración del firewall del grupo de seguridad que ofrece AWS. Los clientes deben pensar detenidamente en los servicios que eligen, ya que las responsabilidades varían en función de los servicios que utilicen, la integración de estos en su entorno de TI, y la legislación y los reglamentos aplicables. La naturaleza de esta responsabilidad compartida también ofrece la flexibilidad y la posibilidad de que el cliente pueda controlar la implementación. Tal y como se muestra en el siguiente gráfico, esta diferenciación de responsabilidad suele denominarse Seguridad “de” la nube en comparación con Seguridad “en” la nube.

Responsabilidad de AWS respecto a la “Seguridad en la nube”: AWS es responsable de proteger la infraestructura que ejecuta todos los servicios que se ofrecen en la nube de AWS. Esta infraestructura está conformada por el hardware, el software, las redes y las instalaciones que ejecutan los servicios de la nube de AWS.

Responsabilidad del cliente respecto a la “Seguridad en la nube”: la responsabilidad del cliente vendrá determinada por los servicios en la nube de AWS que seleccione el cliente. Esto determina la cantidad de trabajo de configuración que el cliente debe llevar a cabo como parte de sus responsabilidades de seguridad. Por ejemplo, un servicio como Amazon Elastic Compute Cloud (Amazon EC2) se categoriza como infraestructura como servicio (IaaS) y, como tal, requiere que el cliente lleve a cabo todas las tareas necesarias de administración y configuración de seguridad. Los clientes que implementan una instancia de Amazon EC2 son responsables de administrar el sistema operativo invitado (incluidas las actualizaciones y los parches de seguridad), todo el software de la aplicación o las utilidades que instale el cliente en las instancias y la configuración del firewall proporcionado por AWS (conocido como grupo de seguridad) en cada instancia. En el caso de los servicios abstractos, como Amazon S3 y Amazon DynamoDB, AWS se encarga de gestionar la capa de infraestructura, el sistema operativo y las plataformas, mientras que los clientes acceden a los puntos de conexión para guardar y recuperar información. Los clientes son responsables de administrar sus datos (incluidas las opciones de cifrado), clasificar sus recursos y utilizar herramientas de IAM para aplicar los permisos adecuados.

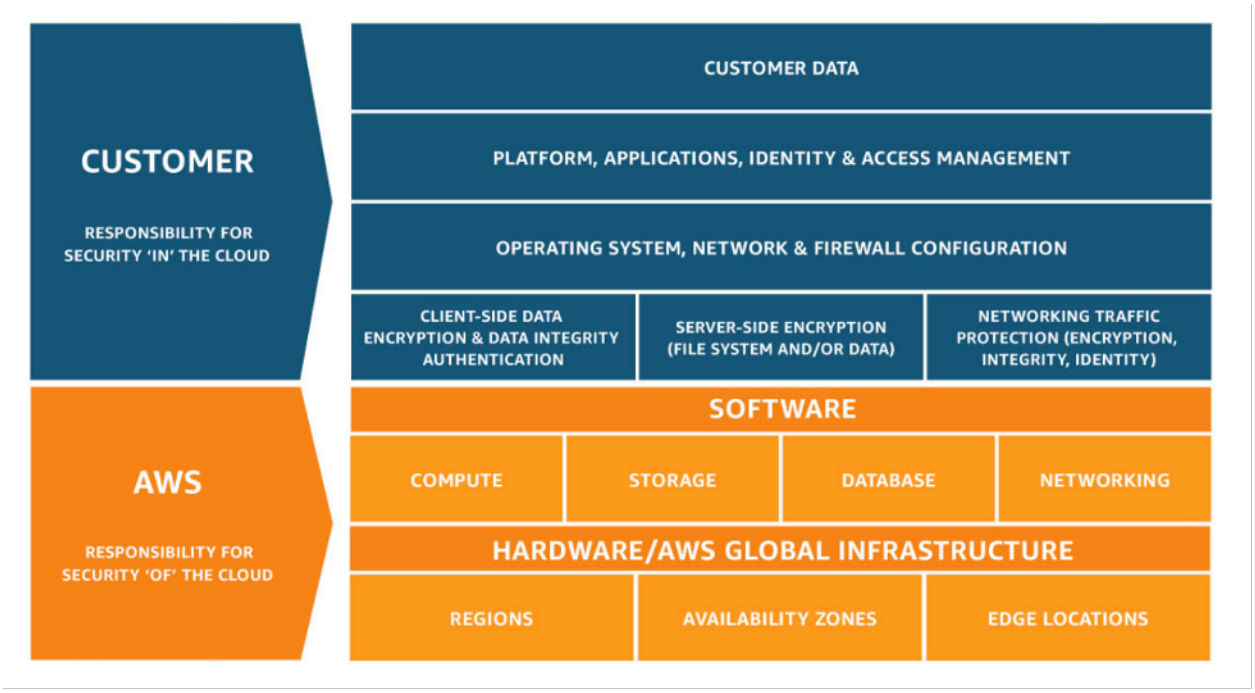


Figura 1: Modelo de responsabilidad compartida de AWS.

Este modelo de responsabilidad compartida entre el cliente y AWS también abarca los controles de TI. De la misma forma que AWS y sus clientes comparten la responsabilidad de operar el entorno de TI, también la comparten en lo referente a la administración, operación y verificación de los controles de TI. AWS puede ayudar a aliviar la carga que supone para los clientes operar los controles mediante la administración de los controles asociados con la infraestructura física implementada

en el entorno de AWS, de cuya administración se encargaba el cliente anteriormente. Como la implementación de cada cliente se lleva a cabo de manera diferente en AWS, los clientes tienen la oportunidad de migrar a AWS la administración de determinados controles de TI para así obtener un entorno de control distribuido (nuevo). Los clientes pueden utilizar la documentación de conformidad y control de AWS disponible para llevar a cabo sus procedimientos de evaluación y verificación de control según sea necesario. Los siguientes son ejemplos de controles administrados por AWS, los clientes de AWS o por ambos.

Controles heredados: controles que un cliente hereda completamente de AWS.

- Controles ambientales y físicos

Controles compartidos: controles que se aplican tanto a la capa de infraestructura como a la del cliente, pero en perspectivas o contextos distintos. En un control compartido, AWS proporciona los requisitos para la infraestructura y el cliente debe proporcionar su propia implementación de control en el uso que se haga de los servicios de AWS. Entre los ejemplos se incluyen:

- Administración de parches: AWS es responsable de la aplicación de parches y de la solución de defectos en la infraestructura, pero los clientes son responsables de la aplicación de parches en las aplicaciones y el sistema operativo invitado.
  - En el caso de los servicios administrados por AWS que funcionan en arquitecturas de un solo inquilino (como Amazon ElastiCache, Amazon RDS y Amazon OpenSearch Service), la responsabilidad de la administración de los parches se comparte de la siguiente manera:
    - Responsabilidad de AWS: identificar las vulnerabilidades, desarrollar y validar los parches, publicar los parches dentro del SLA de aplicación de parches del servicio y notificar a los clientes las actualizaciones disponibles mediante el mecanismo de notificación documentado del servicio.
    - Responsabilidad del cliente: revisar las actualizaciones disponibles y facilitar la aplicación de los parches seleccionando los periodos de mantenimiento, aplicando las actualizaciones del servicio o programando los reinicios necesarios dentro de los plazos indicados por AWS.
  - En el caso de los servicios administrados por AWS que funcionan en arquitecturas de varios inquilinos (como Amazon ElastiCache sin servidor, Amazon DynamoDB y Amazon S3), la responsabilidad de la administración de los parches se comparte de la siguiente manera:
    - Responsabilidad de AWS: aplicar los parches sin que sea necesaria la intervención del cliente.
    - Responsabilidad del cliente: consultar la documentación de mantenimiento y aplicación de parches de cada servicio administrado por AWS que utilice para conocer los mecanismos de

notificación específicos, las opciones de plazos de mantenimiento y actualizar los procesos de aplicaciones disponibles.

- Administración de la configuración: AWS mantiene la configuración de sus dispositivos de infraestructura, pero los clientes son responsables de la configuración de sus propios sistemas operativos invitados, bases de datos y aplicaciones.
- Concienciación y formación: AWS imparte formación a los empleados de AWS, pero los clientes deben formar a sus propios empleados.

Específicos del cliente: controles que son responsabilidad exclusiva del cliente en función de la aplicación que esté implementando en los servicios de AWS. Entre los ejemplos se incluyen:

- Protección de comunicaciones y servicios o seguridad de zona, que pueden requerir que un cliente dirija o especifique datos de zona en entornos de seguridad específicos.

Gobernanza

La gobernanza de seguridad, como un subconjunto del enfoque general, se utiliza para cumplir los objetivos empresariales mediante la definición de políticas y objetivos de control con el fin de gestionar el riesgo. Gestione el riesgo con un enfoque por capas en relación con los objetivos de control de seguridad: cada capa se basa en la anterior. Comprender el modelo de responsabilidad compartida de AWS es la capa fundamental. Al conocer este modelo, podrá establecer con claridad sus responsabilidades en lo que respecta al cliente y las que ha heredado de AWS. Un recurso beneficioso es AWS Artifact, que le ofrece acceso bajo demanda a los informes de cumplimiento y seguridad de AWS y a determinados acuerdos en línea.

Logre la mayoría de sus objetivos de control en la próxima capa. Esta capa es la que proporciona la capacidad a toda la plataforma. Por ejemplo, esta capa incluye el proceso de aprovisionamiento de cuentas de AWS, la integración con un proveedor de identidades, como AWS IAM Identity Center, y los controles habituales de detección. Aquí también se incluyen algunos de los resultados del proceso de gobernanza de la plataforma. Cuando quiera comenzar a usar un nuevo servicio de AWS, actualice las políticas de control de servicio (SCP) en el servicio de AWS Organizations para proporcionar las barreras de protección durante el uso inicial del servicio. Puede utilizar otras SCP para implementar objetivos comunes de control de seguridad que, a menudo, se denominan invariables de seguridad. Se trata de objetivos de control o configuración que puede aplicar a varias cuentas, unidades organizativas o toda la organización de AWS. Ejemplos típicos de esto son limitar las regiones en las que se ejecuta la infraestructura o impedir que se desactiven los controles de

detección. Esta capa intermedia también incluye políticas codificadas, como, por ejemplo, reglas de configuración o comprobaciones en las canalizaciones.

En la capa superior es donde los equipos de productos logran los objetivos de control. Esto se debe a que la implementación se lleva a cabo en las aplicaciones que estos equipos controlan. Esto podría hacerse mediante la implementación de la validación de entrada en una aplicación o al garantizar que la identidad se transfiere correctamente entre los microservicios. Aunque el equipo de productos sea el propietario de la configuración, sus miembros pueden seguir heredando cierta capacidad de la capa intermedia.

Cada vez que implemente el control, el objetivo es el mismo: gestionar el riesgo. Una selección de marcos de gestión de riesgos se aplica a determinados, sectores, regiones o tecnologías. Su objetivo principal: destacar el riesgo en función de su probabilidad y consecuencia. Este es el riesgo inherente. Puede definir un objetivo de control que reduzca tanto la probabilidad como la consecuencia, o ambas opciones. Luego, con un control establecido, puede ver cuál es el riesgo probable. Este es el riesgo residual. Los objetivos de control pueden aplicarse a una o varias cargas de trabajo. En el siguiente diagrama se muestra una matriz típica de riesgos. La probabilidad se basa en la frecuencia de incidencias anteriores y la consecuencia en los costos financieros, relacionados con la reputación y con el tiempo invertido del evento.

Likelihood	Risk Level				
Very Likely	Low	Medium	High	Critical	Critical
Likely	Low	Medium	Medium	High	Critical
Possible	Low	Low	Medium	Medium	High
Unlikely	Low	Low	Medium	Medium	High
Very unlikely	Low	Low		Medium	High
Consequence	Minimal	Low	Medium	High	Severe

Figura 2: Matriz de probabilidad de nivel de riesgo

AWSAdministración y separación de cuentas de

Le recomendamos que organice cargas de trabajo en cuentas distintas y las agrupe según su función, requisitos de conformidad o un conjunto común de controles, en lugar de crear una réplica de la estructura de informes de la organización. En AWS, las cuentas tienen un límite bien definido. Por ejemplo, se recomienda encarecidamente la separación de nivel de cuenta para aislar cargas de trabajo de producción de las de desarrollo y prueba.

Administración centralizada de las cuentas: AWS Organizations automatiza la creación y la gestión de cuentas de AWS, así como el control de esas cuentas una vez creadas. Al crear una cuenta a través de AWS Organizations, es importante que tenga en cuenta la dirección de correo electrónico que utilice, ya que esta será el usuario raíz que permita el restablecimiento de la contraseña. Organizations le permite agrupar cuentas en unidades organizativas (OU), que pueden representar diferentes entornos en función de los requisitos y el propósito de la carga de trabajo.

Definición de controles centralizados: para controlar lo que pueden hacer las cuentas de AWS, permita únicamente servicios, regiones y acciones de servicios específicos en el nivel adecuado. AWS Organizations le permite utilizar políticas de control de servicio (SCP) para aplicar barreras de protección de permiso en la organización, unidad organizativa o nivel de cuenta, que se aplicarán a todos los usuarios y roles de AWS Identity and Access Management (IAM). Por ejemplo, puede aplicar una SCP que no permita a los usuarios iniciar recursos en regiones que no se hayan permitido explícitamente. AWS Control Tower ofrece una forma simplificada de configurar y controlar varias cuentas. Automatiza la configuración de las cuentas en su AWS Organization, automatiza el aprovisionamiento, aplica barreras de protección (que incluyen la prevención y la detección) y le proporciona un panel de control para mayor visibilidad.

Configuración de los servicios y los recursos centralizada: AWS Organizations le ayuda a configurar los servicios de AWS que se aplican a todas sus cuentas. Por ejemplo, puede configurar el registro central de todas las acciones hechas en la organización con AWS CloudTrail e impedir que las cuentas de los miembros desactiven los registros. También puede agregar datos de forma centralizada para las reglas que haya definido con AWS Config, lo que le permitirá auditar sus cargas de trabajo para comprobar su conformidad y reaccionar rápidamente ante los cambios. AWS CloudFormation StackSets le permite administrar de forma centralizada pilas de AWS CloudFormation en las cuentas y las OU de la organización. Esto le permite aprovisionar automáticamente una cuenta nueva para cumplir con los requisitos de seguridad.

Utilice la característica de administración delegada de los servicios de seguridad para separar las cuentas utilizadas para la administración de la cuenta de facturación (administración) de la organización. Algunos servicios de AWS, como GuardDuty, Security Hub y AWS Config, admiten integraciones con AWS Organizations, incluida la designación de una determinada cuenta para funciones administrativas.

Prácticas recomendadas

- SEC01-BP01 Separación de cargas de trabajo con cuentas
- SEC01-BP02 Protección del usuario raíz y las propiedades de la cuenta

SEC01-BP01 Separación de cargas de trabajo con cuentas

Establezca barreras de protección y medidas de aislamiento comunes entre los entornos (por ejemplo, producción, desarrollo y pruebas) y las cargas de trabajo mediante una estrategia de varias cuentas. Es muy recomendable que la separación se haga en la cuenta, ya que así se consigue una barrera de aislamiento sólida para gestionar la seguridad, la facturación y el acceso.

Resultado deseado: una estructura de cuentas que aísla las operaciones en la nube, las cargas de trabajo no relacionadas y los entornos en cuentas independientes, lo que aumenta la seguridad en toda la infraestructura de la nube.

Patrones comunes de uso no recomendados:

- Colocar en la misma cuenta varias cargas de trabajo no relacionadas con diferentes niveles de confidencialidad de los datos.
- Definir de manera insuficiente la estructura de la unidad organizativa (OU).

Beneficios de establecer esta práctica recomendada:

- Menor alcance del impacto si se accede inadvertidamente a una carga de trabajo.
- Gobernanza central del acceso a los servicios, recursos y regiones de AWS.
- Mantenimiento de la seguridad de la infraestructura en la nube con políticas y una administración centralizada de los servicios de seguridad.
- Proceso automatizado de creación y mantenimiento de las cuentas.
- Auditoría centralizada de la infraestructura para los requisitos de conformidad y reglamentarios.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Las Cuentas de AWS proporcionan una barrera de aislamiento de seguridad entre cargas de trabajo o recursos que operan con distintos niveles de confidencialidad. AWS ofrece herramientas para administrar las cargas de trabajo en la nube a escala mediante una estrategia de varias cuentas para aprovechar esta barrera de aislamiento. Para obtener orientación sobre los conceptos, los patrones y la implementación de una estrategia de varias cuentas en AWS, consulte Organizing Your AWS Environment Using Multiple Accounts.

Cuando tenga varias Cuentas de AWS con una administración central, las cuentas deben organizarse en una jerarquía definida por capas de unidades organizativas (OU). Luego, pueden organizarse y aplicarse controles de seguridad a las OU y a las cuentas miembro mediante el establecimiento de controles preventivos uniformes en las cuentas miembros de la organización. Los controles de seguridad se heredan, lo que permite filtrar los permisos disponibles para las cuentas miembros situadas en niveles inferiores de una jerarquía de OU. Un buen diseño aprovecha esta herencia para reducir el número y la complejidad de las políticas de seguridad necesarias para lograr los controles de seguridad deseados para cada cuenta miembro.

AWS Organizations y AWS Control Tower son dos servicios que puede utilizar para implementar y administrar esta estructura de varias cuentas en el entorno de AWS. AWS Organizations le permite organizar las cuentas en una jerarquía definida por una o más capas de unidades organizativas, y cada unidad organizativa contiene varias cuentas miembro. Las políticas de control de servicio (SCP) permiten al administrador de la organización establecer controles preventivos detallados en las cuentas miembro, y AWS Config se puede utilizar para establecer controles proactivos y de detección en las cuentas miembro. Muchos servicios de AWS se integran en AWS Organizations para proporcionar controles administrativos delegados y llevar a cabo tareas específicas del servicio en todas las cuentas miembro de la organización.

Además de AWS Organizations, AWS Control Tower ofrece una configuración de prácticas recomendadas con un solo clic para un entorno de AWS de varias cuentas con una zona de aterrizaje. La zona de aterrizaje es el punto de entrada al entorno de varias cuentas que se establece por medio de Control Tower. Control Tower ofrece varias ventajas frente a AWS Organizations. Estas son tres ventajas que mejoran la gobernanza de las cuentas:

- Controles de protección de seguridad obligatorios integrados que se aplican automáticamente a las cuentas que se admiten en la organización.
- Controles de protección opcionales que pueden activarse o desactivarse para un conjunto determinado de OU.
- AWS Control Tower Account Factory ofrece una implementación automatizada de cuentas que contienen bases de referencia y opciones de configuración previamente aprobadas dentro de su organización.

Pasos para la implementación

1. Diseño de una estructura de unidades organizativas: una estructura de unidades organizativas bien diseñada reduce la carga administrativa necesaria para crear y mantener las políticas de

control de servicios y otros controles de seguridad. La estructura de la unidad organizativa debe estar alineada con las necesidades empresariales, la confidencialidad de los datos y la estructura de las carga de trabajo.

2. Creación de una zona de aterrizaje para el entorno de varias cuentas: una zona de aterrizaje proporciona una base de seguridad e infraestructura coherente a partir de la cual la organización puede desarrollar, lanzar e implementar cargas de trabajo rápidamente. Puede utilizar una zona de aterrizaje hecha a medida o AWS Control Tower para organizar el entorno.
3. Establecimiento de barreras de protección: implemente barreras de protección de seguridad uniformes para el entorno a través de la zona de aterrizaje. AWS Control Tower proporciona una lista de controles obligatorios y opcionales que se pueden implementar. Los controles obligatorios se implementan automáticamente al implementar Control Tower. Revise la lista de los controles más recomendables y opcionales, e implemente los controles que sean adecuados a sus necesidades.
4. Restricción del acceso a las regiones recién agregadas: en el caso de las nuevas Regiones de AWS, los recursos de IAM, como los usuarios y roles, solo se propagan a las regiones que especifique. Esta acción se puede llevar a cabo a través de la consola cuando se utiliza Control Tower o mediante el ajuste de las políticas de permisos de IAM en AWS Organizations.
5. Consideración de uso AWS CloudFormation StackSets: StackSets le ayuda a implementar recursos que incluyen políticas, roles y grupos de IAM en diferentes regiones y Cuentas de AWS a partir de una plantilla aprobada.

Recursos

Prácticas recomendadas relacionadas:

- SEC02-BP04 Uso de un proveedor de identidades centralizado

Documentos relacionados:

- AWS Control Tower
- AWS Directivas de auditoría de seguridad de
- Prácticas recomendadas de IAM
- Use CloudFormation StackSets to provision resources across multiple Cuentas de AWS and regions
- Preguntas frecuentes sobre Organizations

- AWS Organizations Terminología y conceptos de
- Best Practices for Service Control Policies in an AWS Organizations Multi-Account Environment
- AWS Account Management Reference Guide
- Organización de su entorno de AWS con varias cuentas

Videos relacionados:

- Enable AWS adoption at scale with automation and governance
- Security Best Practices the Well-Architected Way
- Building and Governing Multiple Accounts using AWS Control Tower
- Enable Control Tower for Existing Organizations

SEC01-BP02 Protección del usuario raíz y las propiedades de la cuenta

El usuario raíz es el usuario con más privilegios de una Cuenta de AWS. Tiene acceso administrativo completo a todos los recursos de la cuenta y, en algunos casos, no se puede limitar con políticas de seguridad. Deshabilitar el acceso programático al usuario raíz, establecer controles apropiados para este usuario y evitar su uso rutinario ayuda a reducir el riesgo de exposición inadvertida de las credenciales raíz y el consiguiente peligro que esto supone para el entorno de la nube.

Resultado deseado: proteger al usuario raíz ayuda a reducir la posibilidad de que se produzcan daños accidentales o intencionados por el mal uso de las credenciales del usuario raíz. Establecer controles de detección también puede servir para alertar al personal adecuado cuando se llevan a cabo acciones con el usuario raíz.

Patrones comunes de uso no recomendados:

- Utilizar el usuario raíz para llevar a cabo tareas que no se encuentran entre las pocas que requieren credenciales de usuario raíz.
- Dejar de comprobar periódicamente los planes de contingencia para verificar el funcionamiento de las infraestructuras críticas, los procesos y el personal durante una emergencia.
- Considerar únicamente el flujo de inicio de sesión típico de la cuenta y olvidarse de considerar o probar métodos alternativos de recuperación de la cuenta.
- No ocuparse de DNS, servidores de correo electrónico y proveedores de telefonía como parte del perímetro crítico de seguridad, ya que estos se utilizan en el flujo de recuperación de la cuenta.

Beneficios de establecer esta práctica recomendada: proteger el acceso al usuario raíz aumenta la confianza de que las acciones de la cuenta están controladas y auditadas.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

AWS dispone de muchas herramientas para proteger su cuenta. Sin embargo, dado que algunas de estas medidas no están activadas de forma predeterminada, deberá implementarlas directamente. Considere estas recomendaciones como pasos básicos para proteger la Cuenta de AWS. A medida que vaya implementando estos pasos, es importante que cree un proceso para evaluar y supervisar continuamente los controles de seguridad.

Cuando crea una Cuenta de AWS por primera vez, empieza con una sola identidad que tiene acceso completo a todos los servicios y recursos de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la Cuenta de AWS. Puede iniciar sesión como usuario raíz utilizando la dirección de correo electrónico y contraseña que usó al crear la cuenta. Debido al acceso elevado que se concede al usuario raíz de AWS, debe limitar el uso del usuario raíz de AWS únicamente a las tareas que lo requieran específicamente. Las credenciales de inicio de sesión del usuario raíz deben estar muy bien protegidas y siempre se debe utilizar la autenticación multifactor (MFA) para el usuario raíz de la Cuenta de AWS.

Además del flujo de autenticación normal para iniciar sesión con el usuario raíz mediante un nombre de usuario, una contraseña y un dispositivo de autenticación multifactor (MFA), existen flujos de recuperación de la cuenta para iniciar sesión con el usuario raíz de la Cuenta de AWS que tiene acceso a la dirección de correo electrónico y al número de teléfono asociados a la cuenta. Por lo tanto, también es muy importante proteger la cuenta de correo electrónico del usuario raíz a la que se envía el mensaje de recuperación y el número de teléfono asociado a la cuenta. Tenga en cuenta también las posibles dependencias circulares si la dirección de correo electrónico asociada al usuario raíz está alojada en servidores de correo electrónico o recursos del servicio de nombres de dominio (DNS) de la misma Cuenta de AWS.

Cuando se utiliza AWS Organizations, hay varias Cuentas de AWS y cada una de ellas tiene un usuario raíz. Se designa una cuenta como cuenta de administración y, a continuación, se pueden agregar varias capas de cuentas miembro por debajo de esa cuenta de administración. Priorice la seguridad del usuario raíz de su cuenta de administración y, luego, céntrese en los usuarios raíz de las cuentas miembros. La estrategia para proteger el usuario raíz de la cuenta de administración puede ser diferente de la de los usuarios raíz de las cuentas miembro, y puede colocar controles de seguridad preventivos en los usuarios raíz de las cuentas miembro.

Pasos para la implementación

Se recomienda seguir estos pasos de implementación para establecer controles para el usuario raíz. Cuando corresponda, las recomendaciones se cotejan con la versión 1.4.0 del punto de referencia de CIS AWS Foundations. Además de estos pasos, consulte las pautas de prácticas recomendadas de AWS para proteger los recursos y la Cuenta de AWS.

Controles preventivos

1. Configure información de contacto precisa para la cuenta.
    a. Esta información se utiliza para el flujo de recuperación de las contraseñas perdidas, el flujo de recuperación de cuentas de los dispositivos MFA perdidos y para comunicaciones críticas relacionadas con la seguridad con su equipo.
    b. Utilice una dirección de correo electrónico alojada en su dominio corporativo (preferiblemente una lista de distribución) como dirección de correo electrónico del usuario raíz. Al utilizar una lista de distribución en lugar de la cuenta de correo electrónico de una persona, se consigue redundancia y continuidad adicionales para acceder a la cuenta raíz durante largos periodos de tiempo.
    c. El número de teléfono que figure en la información de contacto debe ser un teléfono dedicado y seguro para este fin. El número de teléfono no debe figurar en ninguna parte ni compartirse con nadie.
2. No cree claves de acceso para el usuario raíz. Si existen claves de acceso, elimínelas (CIS 1.4).
    a. Elimine cualquier credencial programática de larga duración (claves de acceso y secretas) para el usuario raíz.
    b. Si ya existen claves de acceso del usuario raíz, debe hacer la transición de los procesos que utilizan esas claves para utilizar claves de acceso temporales de un rol de AWS Identity and Access Management (IAM) y, a continuación, eliminar las claves de acceso del usuario raíz.
3. Determine si necesita almacenar las credenciales del usuario raíz.
    a. Si utiliza AWS Organizations para crear nuevas cuentas miembro, la contraseña inicial del usuario raíz de esas nuevas cuentas miembro se establece en un valor aleatorio que no se le revela. Considere la posibilidad de utilizar el flujo de restablecimiento de contraseñas de la cuenta de administración de su organización de AWS para acceder a la cuenta de miembro si es necesario.
    b. Para Cuentas de AWS independientes o la cuenta de administración de AWS, considere la posibilidad de crear y almacenar de forma segura credenciales para el usuario raíz. Utilice MFA para el usuario raíz.

4. Use controles preventivos para los usuarios raíz de las cuentas miembro en entornos de varias cuentas de AWS.
   a. Considere la posibilidad de utilizar la barrera de protección preventiva No permitir la creación de claves de acceso raíz para el usuario raíz como barrera preventiva para las cuentas de los miembros.
   b. Considere la posibilidad de utilizar la barrera de protección preventiva No permitir la creación de claves de acceso raíz para el usuario raíz para las cuentas de los miembros.
5. Si necesita credenciales para el usuario raíz:
   a. Utilice una contraseña compleja.
   b. Active la autenticación multifactor (MFA) para el usuario raíz, especialmente para las cuentas de administración de AWS Organizations (pagador) (CIS 1.5).
   c. Considere la posibilidad de usar dispositivos MFA físicos para mejorar la resiliencia y la seguridad, ya que los dispositivos de un solo uso pueden reducir las posibilidades de que los dispositivos que contienen los códigos MFA puedan reutilizarse para otros fines. Verifique que los dispositivos MFA físicos que funcionan con baterías se sustituyan periódicamente (CIS 1.6).
      - Para configurar la MFA en el usuario raíz, siga las instrucciones a fin de crear un dispositivo MFA virtual o un dispositivo MFA físico.
   d. Considere la posibilidad de inscribir varios dispositivos MFA para hacer copias de seguridad. Se permiten hasta 8 dispositivos MFA por cuenta.
      - Tenga en cuenta que al inscribir más de un dispositivo MFA para el usuario raíz, se desactiva automáticamente el flujo de recuperación de la cuenta en caso de pérdida del dispositivo MFA.
   e. Guarde la contraseña con todas las medidas de seguridad y tenga en cuenta las dependencias circulares si la guarda electrónicamente. No guarde la contraseña de forma que sea necesario acceder a la misma Cuenta de AWS para obtenerla.
6. Opcional: considere la posibilidad de establecer un programa de rotación periódica de contraseñas para el usuario raíz.
   - Las prácticas recomendadas de administración de credenciales dependen de los requisitos de las normativas y políticas que tenga. Los usuarios raíz protegidos por MFA no dependen de una contraseña como único factor de autenticación.
   - Si se cambia la contraseña del usuario raíz de forma periódica, se reduce el riesgo de que una contraseña expuesta de forma inadvertida se utilice indebidamente.

Controles de detección

- Cree alarmas para detectar el uso de las credenciales del usuario raíz (CIS 1.7). Amazon GuardDuty puede supervisar y alertar sobre el uso de las credenciales de las API del usuario raíz mediante el resultado RootCredentialUsage.
- Evalúe e implemente los controles de detección incluidos en el paquete de conformidad del pilar de seguridad de AWS Well-Architected para AWS Config o, si utiliza AWS Control Tower, los controles más recomendados disponibles en Control Tower.

Guía operativa

- Determine qué persona de la organización debe tener acceso a las credenciales del usuario raíz.
  - Utilice la regla de dos personas para no haya una sola persona que tenga acceso a todas las credenciales y el dispositivo MFA necesarios para obtener acceso de usuario raíz.
  - Compruebe que sea la organización, y no una única persona, quien mantenga un control del número de teléfono y el alias de correo electrónico asociados a la cuenta (que se utilizan para el restablecimiento de la contraseña y el flujo de restablecimiento de MFA).
- Utilice el usuario raíz únicamente de forma excepcional (CIS 1.7).
  - El usuario raíz de AWS no debe utilizarse para las tareas diarias, ni siquiera para las tareas administrativas. Inicie sesión únicamente como usuario raíz para llevar a cabo las tareas de AWS que lo requieran. Todas las demás acciones deben hacerlas otros usuarios que asuman los roles apropiados.
- Compruebe periódicamente que el acceso al usuario raíz funcione con el fin de probar los procedimientos antes de que se produzca una situación de emergencia que requiera el uso de las credenciales del usuario raíz.
- Compruebe periódicamente que la dirección de correo electrónico asociada a la cuenta y las que aparecen en Contactos alternativos funcionen. Supervise las bandejas de entrada de estas direcciones de correo electrónico para comprobar si se reciben notificaciones de seguridad de `<abuse@amazon.com>`. Asegúrese también de que los números de teléfono asociados a la cuenta funcionen.
- Prepare procedimientos de respuesta a incidentes para responder al uso indebido de la cuenta raíz. Consulte AWS Security Incident Response Guide y las prácticas recomendadas en la sección Respuesta ante incidentes del documento técnico sobre el Pilar de seguridad para obtener más información sobre cómo crear una estrategia de respuesta a incidentes adecuada para su Cuenta de AWS.

Recursos

Prácticas recomendadas relacionadas:

- SEC01-BP01 Separación de cargas de trabajo con cuentas
- SEC02-BP01 Uso de mecanismos de inicio de sesión sólidos
- SEC03-BP02 Concesión de acceso con privilegios mínimos
- SEC03-BP03 Establecimiento de un proceso de acceso de emergencia
- SEC10-BP05 Aprovisionamiento previo del acceso

Documentos relacionados:

- AWS Control Tower
- AWS Directivas de auditoría de seguridad de
- Prácticas recomendadas de IAM
- Amazon GuardDuty – root credential usage alert
- Step-by-step guidance on monitoring for root credential use through CloudTrail
- Tokens de MFA aprobados para su uso con AWS
- Implementación del acceso de emergencia en AWS
- Top 10 security items to improve in your Cuenta de AWS
- What do I do if I notice unauthorized activity in my Cuenta de AWS?

Videos relacionados:

- Enable AWS adoption at scale with automation and governance
- Security Best Practices the Well-Architected Way
- Limiting use of AWS root credentials from AWS re:inforce 2022 – Security best practices with AWS IAM

Funcionamiento seguro de las cargas de trabajo

El funcionamiento seguro de las cargas de trabajo abarca todo su ciclo de vida: desde el diseño, la creación y la ejecución hasta las mejoras constantes. Una de las formas de mejorar la capacidad de trabajar de forma segura en la nube es mediante la adopción de un enfoque organizativo de la

gobernanza. La gobernanza es la forma en que las decisiones se guían de forma coherente sin tener que depender únicamente del buen juicio de las personas implicadas. El proceso y modelo de gobernanza son la forma con la que responde a la pregunta: "¿Cómo puedo saber si se logran los objetivos de control de una determinada carga de trabajo y si son los adecuados?" Contar con un enfoque coherente a la hora de tomar decisiones acelera la implementación de cargas de trabajo y ayuda a subir el nivel de la capacidad de seguridad de la organización.

Para gestionar su carga de trabajo de forma segura, debe aplicar las prácticas recomendadas generales en todas las áreas de seguridad. Tome los requisitos y procesos que ha definido en materia de excelencia operativa en los niveles organizativo y de carga de trabajo, y aplíquelos a todas las áreas. Mantenerse al día con las recomendaciones de AWS y del sector y con la inteligencia sobre amenazas lo ayuda a desarrollar el modelo de amenazas y los objetivos de control. La automatización de los procesos de seguridad, las pruebas y la validación le ayudan a escalar las operaciones de seguridad.

La automatización permite la coherencia y la repetibilidad de los procesos. La gente hace bien muchas cosas, pero hacer lo mismo de forma coherente y en repetidas ocasiones sin cometer errores no es una de ellas. Incluso con manuales de procedimientos bien redactados, se corre el riesgo de que la gente no lleve a cabo tareas repetitivas de forma sistemática. Esto es especialmente cierto cuando cada uno tiene distintas responsabilidades y debe responder a alertas con las que no está familiarizado. Sin embargo, la automatización responde de la misma forma en cada momento. La mejor forma de implementar aplicaciones es a través de la automatización. El código que ejecuta la implementación puede probarse y utilizarse para llevarla a cabo. Esto aumenta la confianza en el proceso de cambio y reduce el riesgo de que se produzca un error en algún cambio.

Para verificar que la configuración cumple con los objetivos de control, pruebe primero la automatización y la aplicación implementada en un entorno de prueba y entrenamiento. De esta forma, podrá probar la automatización para demostrar que hizo correctamente todos los pasos. También puede obtener retroalimentación temprana en el ciclo de desarrollo e implementación, lo que reduce la posibilidad de tener que volver a repetir los procesos. Para reducir la posibilidad de se produzcan errores de implementación, haga cambios en la configuración por código y no por persona. Si tiene que volver a implementar una aplicación, la automatización le facilitará esta tarea. A medida que va definiendo objetivos de control adicionales, podrá ir agregándolos fácilmente a la automatización para todas las cargas de trabajo.

En lugar de que los propietarios de cargas de trabajo individuales tengan que invertir en seguridad específica de dichas cargas, ahorre tiempo mediante el uso de capacidades comunes y componentes compartidos. Algunos de los ejemplos de servicios que varios equipos pueden

consumir incluyen: el proceso de creación de cuentas de AWS, la identidad centralizada de personas, la configuración de registros comunes y la creación de imágenes base de AMI y contenedores. Este enfoque puede ayudar a los creadores a mejorar los tiempos de ciclo de las cargas de trabajo y lograr de forma coherente los objetivos de control de seguridad. Si los equipos son más coherentes, podrá validar los objetivos de control e informar mejor de su nivel de control y postura ante los riesgos a las partes interesadas.

Prácticas recomendadas

- SEC01-BP03 Identificación y validación de los objetivos de control
- SEC01-BP04 Actualización constante de las amenazas y recomendaciones de seguridad
- SEC01-BP05 Reducción del alcance de la administración de la seguridad
- SEC01-BP06 Automatización de la implementación de controles de seguridad estándares
- SEC01-BP07 Identificación de amenazas y priorización de mitigaciones con un modelo de amenazas
- SEC01-BP08 Evaluación e implementación de nuevos servicios y características de seguridad de forma periódica

SEC01-BP03 Identificación y validación de los objetivos de control

En función de sus requisitos de cumplimiento y los riesgos identificados a partir de su modelo de amenazas, extraiga y valide los objetivos de control y los controles que tiene que aplicar a su carga de trabajo. La validación continua tanto de los objetivos de control como de los controles le ayuda a medir la efectividad de la mitigación de riesgos.

Resultado deseado: los objetivos de control de seguridad de su empresa están bien definidos y alineados con sus requisitos de conformidad. Se implementan y ponen en marcha controles mediante la automatización y las políticas, y se evalúan de forma continua con el fin de determinar su eficacia para lograr sus objetivos. Poner a disposición de los auditores demostraciones de eficacia, tanto en un momento determinado como durante un periodo de tiempo.

Patrones comunes de uso no recomendados:

- Incomprensión por parte de la empresa de los requisitos normativos, las expectativas del mercado y los estándares del sector en cuanto al control de la seguridad.
- Alineación incorrecta de los marcos de ciberseguridad y los objetivos de control con los requisitos de la empresa.

- Ausencia de una correspondencia estrecha y medible entre la implementación de los controles y los objetivos de control.
- Falta de uso de la automatización para informar sobre la eficacia de los controles.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Existen muchos marcos de ciberseguridad comunes que pueden constituir la base de sus objetivos de control de seguridad. Debe tener en cuenta los requisitos normativos, las expectativas del mercado y los estándares del sector para su empresa con el objetivo de determinar qué marcos se adaptan mejor a sus necesidades. Entre los ejemplos, se incluyen AICPA SOC 2, HITRUST, PCI-DSS, ISO 27001 y NIST SP 800-53.

Una vez identificados los objetivos de control, debe analizar cómo los servicios de AWS de los que hace uso le ayudan a conseguir dichos objetivos. Utilice AWS Artifact para buscar la documentación y los informes que se alineen con sus marcos objetivo que describan el alcance de la responsabilidad cubierta por AWS y una guía para el ámbito restante que caiga bajo su responsabilidad. Para obtener más orientación específica sobre los servicios que se ajusten a las diversas declaraciones de control del marco, consulte AWS Customer Compliance Guides.

A medida que defina unos controles que sirvan para lograr sus objetivos, reglamente su aplicación mediante controles preventivos y automatice las mitigaciones mediante controles de detección. Ayude a evitar configuraciones y acciones de recursos no conformes en todo su sistema de AWS Organizations mediante las políticas de control de servicios (SCP). Implemente reglas en AWS Config para supervisar los recursos que no cumplan con las normas e informar sobre ellos y, a continuación, cambie las reglas a un modelo de cumplimiento una vez que esté seguro de su comportamiento. Para implementar conjuntos de reglas predefinidas y administradas que se ajusten a sus marcos de ciberseguridad, evalúe el uso de estándares de AWS Security Hub CSPM como primera opción. El estándar Prácticas recomendadas de seguridad básicas (FSBP) de AWS y el CIS AWS Foundations Benchmark son buenos puntos de partida y contienen controles alineados con muchos de los objetivos comunes en varios marcos estándares. Cuando Security Hub CSPM no cuente intrínsecamente con las detecciones de control deseadas, puede complementarse con paquetes de conformidad de AWS Config.

Utilice los paquetes para socios de APN recomendados por el equipo de AWS Global Security and Compliance Acceleration (GSCA) para obtener asistencia de asesores de seguridad, agencias

consultoras, sistemas de recopilación de pruebas y presentación de informes, auditores y otros servicios complementarios cuando sea necesario.

Pasos para la implementación

1. Valore los marcos de ciberseguridad comunes y alinee sus objetivos de control con los marcos elegidos.
2. Obtenga la documentación pertinente sobre la orientación y las responsabilidades de su marco con AWS Artifact. Determine qué partes del cumplimiento corresponden a AWS según el modelo de responsabilidad compartida y qué partes son de su responsabilidad.
3. Utilice SCP, políticas de recursos, políticas de confianza de roles y otras barreras de protección para evitar configuraciones y acciones de recursos no conformes.
4. Evalúe la implementación de estándares de Security Hub CSPM y paquetes de conformidad de AWS Config que se alineen con sus objetivos de control.

Recursos

Prácticas recomendadas relacionadas:

- SEC03-BP01 Definición de los requisitos de acceso
- SEC04-BP01 Configuración del registro de servicios y aplicaciones
- SEC07-BP01 Comprensión del esquema de clasificación de datos
- OPS01-BP03 Evaluación de los requisitos de gobernanza
- OPS01-BP04 Evaluación de los requisitos de cumplimiento
- PERF01-BP05 Uso de políticas y arquitecturas de referencia
- COST02-BP01 Desarrollo de políticas basadas en los requisitos de su organización

Documentos relacionados:

- AWS Customer Compliance Guides

Herramientas relacionadas:

- AWS Artifact

SEC01-BP04 Actualización constante de las amenazas y recomendaciones de seguridad

Para mantenerse al día de las amenazas y mitigaciones más recientes, supervise las publicaciones de inteligencia sobre amenazas del sector y analice las fuentes de datos en busca de actualizaciones. Evalúe las ofertas de servicios administrados que se actualizan automáticamente en función de los datos de amenazas más recientes.

Resultado deseado: se mantiene al día a medida que las publicaciones del sector se actualizan con las amenazas y recomendaciones más recientes. Utiliza la automatización para detectar posibles vulnerabilidades y exposiciones a medida que se identifiquen nuevas amenazas. Toma medidas de mitigación para estas amenazas. Adopta servicios de AWS que se actualicen automáticamente con la información de amenazas más reciente.

Patrones comunes de uso no recomendados:

- No disponer de un mecanismo fiable y repetible para mantenerse al día de la información más reciente sobre amenazas.
- Mantener un inventario manual de su cartera de tecnología, cargas de trabajo y dependencias que requiera una revisión humana para detectar posibles vulnerabilidades y exposiciones.
- No disponer de mecanismos para actualizar sus cargas de trabajo y dependencias a las versiones más recientes disponibles que incluyan mitigaciones de amenazas conocidas.

Beneficios de establecer esta práctica recomendada: el uso de orígenes de inteligencia sobre amenazas para mantenerse al día reduce el riesgo de perderse cambios importantes en el panorama de amenazas que puedan afectar a su empresa. Utilizar la automatización para analizar, detectar y corregir posibles vulnerabilidades o exposiciones en sus cargas de trabajo y sus dependencias puede ayudarle a mitigar los riesgos de forma rápida y predecible, en comparación con las alternativas manuales. Esto ayuda a controlar el tiempo y los costos relacionados con la mitigación de vulnerabilidades.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Revise las publicaciones fiables de inteligencia sobre amenazas para mantenerse al día del panorama de amenazas. Consulte la base de conocimiento de MITRE ATT&CK para obtener

documentación sobre tácticas, técnicas y procedimientos (TTP) de confrontación conocidos. Consulte la lista de vulnerabilidades y exposiciones comunes (CVE) de MITRE para mantenerse al tanto de las vulnerabilidades conocidas de los productos que utiliza. Conozca los riesgos críticos de las aplicaciones web con el conocido proyecto OWASP Top 10 de Open Worldwide Application Security Project (OWASP).

Manténgase al día de los eventos de seguridad de AWS y las medidas de corrección recomendadas con los boletines de seguridad de AWS para las CVE.

Con el objetivo de reducir el esfuerzo general y los gastos que supone mantenerse al día, plantéese el uso de servicios de AWS que incorporen automáticamente nueva información sobre amenazas con el paso del tiempo. Por ejemplo, Amazon GuardDuty se mantiene al día con la inteligencia de amenazas del sector para detectar comportamientos anómalos y firmas de amenazas en las cuentas. Amazon Inspector mantiene actualizada automáticamente una base de datos de las CVE que utiliza para sus características de análisis continuo. Tanto AWS WAF como AWS Shield Advanced ofrecen grupos de reglas administrados que se actualizan automáticamente a medida que surgen nuevas amenazas.

Revise el pilar de excelencia operativa de Well-Architected para automatizar la administración de flotas y la aplicación de parches.

Pasos para la implementación

- Suscríbase a las actualizaciones de las publicaciones de inteligencia sobre amenazas que resulten pertinentes para su negocio y su sector. Suscríbase a los boletines de seguridad de AWS.
- Considere la posibilidad de adoptar servicios que incorporen automáticamente nuevos conocimientos sobre amenazas, como Amazon GuardDuty y Amazon Inspector.
- Implemente una estrategia de administración de flotas y aplicación de parches acorde con las prácticas recomendadas en el pilar de excelencia operativa de Well-Architected.

Recursos

Prácticas recomendadas relacionadas:

- SEC01-BP07 Identificación de amenazas y priorización de mitigaciones con un modelo de amenazas
- OPS01-BP05 Evaluación del panorama de amenazas
- OPS11-BP01 Implementación de un proceso de mejora continua

SEC01-BP05 Reducción del alcance de la administración de la seguridad

Determine si puede reducir su alcance de seguridad mediante el uso de servicios de AWS que transfieran la administración de ciertos controles a AWS (servicios administrados). Estos servicios pueden ayudar a reducir las tareas de mantenimiento de la seguridad, como el aprovisionamiento de infraestructuras, la configuración del software, la aplicación de parches o las copias de seguridad.

Resultado deseado: tenga en cuenta el alcance de la administración de la seguridad al seleccionar los servicios de AWS para su carga de trabajo. El costo de los gastos generales de administración y las tareas de mantenimiento (el costo total de propiedad o TCO) se compara con el costo de los servicios que seleccione, además de otras consideraciones relacionadas con el marco de Well-Architected. Incorpora la documentación de control y cumplimiento de AWS en sus procedimientos de evaluación y verificación del control.

Patrones comunes de uso no recomendados:

- Implementar cargas de trabajo sin comprender a fondo el modelo de responsabilidad compartida para los servicios que seleccione.
- Alojar bases de datos y otras tecnologías en máquinas virtuales sin haber evaluado un servicio administrado equivalente.
- No incluir las tareas de administración de la seguridad en el costo total de la propiedad de las tecnologías de host en máquinas virtuales en comparación con las opciones de servicios administrados.

Beneficios de establecer esta práctica recomendada: el uso de servicios administrados puede reducir la carga general que supone administrar los controles de seguridad operativos, lo que puede reducir los riesgos de seguridad y el costo total de la propiedad. El tiempo que de otro modo se dedicaría a determinadas tareas de seguridad puede reinvertirse en tareas que aporten más valor a la empresa. Los servicios administrados también pueden reducir el alcance de sus requisitos de cumplimiento al trasladar algunos requisitos de control a AWS.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Hay varias formas en las que puede integrar los componentes de la carga de trabajo en AWS. La instalación y ejecución de tecnologías en instancias de Amazon EC2 suele requerir que asuma la mayor parte de la responsabilidad general sobre la seguridad. Para ayudar a reducir la carga de

poner en práctica ciertos controles, identifique los servicios administrados de AWS que reduzcan su ámbito de responsabilidad en el modelo de responsabilidad compartida y piense en cómo puede utilizarlos en su arquitectura actual. Entre los ejemplos, se incluye el uso de Amazon Relational Database Service (Amazon RDS) para implementar bases de datos, Amazon Elastic Kubernetes Service (Amazon EKS) o Amazon Elastic Container Service (Amazon ECS) para orquestar contenedores, o el uso de opciones sin servidor. Al desarrollar nuevas aplicaciones, piense en qué servicios pueden ayudar a reducir el tiempo y el costo a la hora de implementar y administrar los controles de seguridad.

Los requisitos de cumplimiento también pueden ser un factor determinante a la hora de seleccionar los servicios. Los servicios administrados pueden trasladar la responsabilidad del cumplimiento de algunos requisitos a AWS. Hable con su equipo de cumplimiento sobre si se sentirían cómodos al auditar los aspectos de los servicios que opera y administra y al aceptar las declaraciones de control en los informes de auditoría de AWS pertinentes. Puede proporcionar los artefactos de auditoría que se encuentran en AWS Artifact a sus auditores o reguladores como prueba de los controles de seguridad de AWS. También puede utilizar la guía de responsabilidad que ofrecen algunos de los artefactos de auditoría de AWS para diseñar la arquitectura, junto con AWS Customer Compliance Guides. Esta guía ayuda a determinar los controles de seguridad adicionales que debe poner en práctica para permitir los casos de uso específicos de su sistema.

Cuando utilice servicios administrados, debe familiarizarse con el proceso de actualización de los recursos a versiones más recientes (por ejemplo, actualizar la versión de una base de datos administrada por Amazon RDS o el tiempo de ejecución de un lenguaje de programación para una función de AWS Lambda). Si bien el servicio administrado puede llevar a cabo esta operación automáticamente, sigue siendo su responsabilidad configurar el momento de la actualización y comprender el impacto en sus operaciones. Herramientas como AWS Health pueden ayudarle a hacer un seguimiento de estas actualizaciones y administrarlas en todos sus entornos.

Pasos para la implementación

1. Evalúe los componentes de la carga de trabajo que puedan sustituirse por un servicio administrado.
   a. Si está migrando una carga de trabajo a AWS, tenga en cuenta la simplificación de la administración (tiempo y gastos) y la reducción del riesgo al evaluar si debe volver a alojar, refactorizar, redefinir la plataforma, reconstruir o reemplazar la carga de trabajo. A veces, la inversión adicional al inicio de una migración puede generar ahorros significativos a largo plazo.
2. Considere la posibilidad de implementar servicios administrados, como Amazon RDS, en lugar de instalar y administrar implementaciones de su tecnología propia.

3. Utilice la guía de responsabilidades de AWS Artifact para determinar los controles de seguridad que debe poner en práctica para la carga de trabajo.
4. Mantenga un inventario de los recursos que se están utilizando y manténgase al día de los nuevos servicios y enfoques para identificar nuevas oportunidades y reducir el alcance.

Recursos

Prácticas recomendadas relacionadas:

- PERF02-BP01 Selección de las mejores opciones computacionales para su carga de trabajo
- PERF03-BP01 Uso de un almacén de datos personalizado que se adapte mejor a los requisitos de acceso y almacenamiento de datos
- SUS05-BP03 Uso de servicios administrados

Documentos relacionados:

- Planned lifecycle events for AWS Health

Herramientas relacionadas:

- AWS Health
- AWS Artifact
- AWS Customer Compliance Guides

Videos relacionados:

- How do I migrate to an Amazon RDS or Aurora MySQL DB instance using AWS DMS?
- AWS re:Invent 2023 - Manage resource lifecycle events at scale with AWS Health

SEC01-BP06 Automatización de la implementación de controles de seguridad estándares

Aplique prácticas modernas de DevOps a medida que desarrolle e implemente controles de seguridad estándar en todos sus entornos de AWS. Defina controles y configuraciones de seguridad estándar mediante plantillas de infraestructura como código (IaC), registre los cambios en un sistema

de control de versiones, pruebe los cambios como parte de una canalización de CI/CD y automatice la implementación de los cambios en sus entornos de AWS.

Resultado deseado: las plantillas de IaC capturan los controles de seguridad estandarizados y los envían a un sistema de control de versiones. Existen canalizaciones de CI/CD en lugares en los que se detectan cambios y se automatizan las pruebas y la implementación de sus entornos de AWS. Existen barreras de protección para detectar errores de configuración en las plantillas y alertar sobre ellos antes de proceder a la implementación. Se implementan cargas de trabajo en entornos donde existan controles estándar. Los equipos tienen acceso para implementar configuraciones de servicio aprobadas a través de un mecanismo de autoservicio. Existen estrategias de copia de seguridad y recuperación seguras para controlar las configuraciones, los scripts y los datos relacionados.

Patrones comunes de uso no recomendados:

- Hacer cambios en los controles de seguridad estándar de forma manual, mediante una consola web o una interfaz de línea de comandos.
- Confiar en los equipos de carga de trabajo individuales para implementar manualmente los controles que define un equipo central.
- Confiar en un equipo de seguridad central para implementar controles en el nivel de la carga de trabajo a petición de un equipo de carga de trabajo.
- Permitir que las mismas personas o equipos desarrollen, prueben e implementen scripts de automatización del control de seguridad sin una separación adecuada de funciones ni de controles y contrapesos.

Beneficios de establecer esta práctica recomendada: el uso de plantillas para definir los controles de seguridad estándar permite hacer un seguimiento y comparar los cambios a lo largo del tiempo mediante un sistema de control de versiones. El uso de la automatización para probar e implementar los cambios crea estandarización y previsibilidad, lo que aumenta las posibilidades de que la implementación se complete correctamente y reduce las tareas manuales repetitivas. Proporcionar un mecanismo de autoservicio para que los equipos de carga de trabajo implementen los servicios y configuraciones aprobados reduce el riesgo de errores de configuración y usos indebidos. Esto también les ayuda a incorporar controles en las primeras etapas del proceso de desarrollo.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Si sigue las prácticas descritas en SEC01-BP01 Separación de cargas de trabajo con cuentas, terminará teniendo varias Cuentas de AWS para diferentes entornos que administre mediante AWS Organizations. Si bien es posible que cada uno de estos entornos y cargas de trabajo necesite controles de seguridad diferentes, puede estandarizar algunos controles de seguridad en toda la organización. Entre algunos ejemplos de esto se incluyen la integración de proveedores de identidad centralizados, la definición de redes y firewalls y la configuración de ubicaciones estándar para almacenar y analizar los registros. Del mismo modo en que puede utilizar la infraestructura como código (IaC) para aplicar el mismo rigor en el desarrollo del código de aplicación al aprovisionamiento de infraestructuras, también puede utilizar la IaC para definir e implementar los controles de seguridad estándar.

Siempre que sea posible, defina los controles de seguridad de forma declarativa, como en AWS CloudFormation, y almacénelos en un sistema de control de código fuente. Utilice las prácticas de DevOps para automatizar la implementación de los controles para obtener versiones más predecibles, pruebas automatizadas con herramientas como AWS CloudFormation Guard y detectar desviaciones entre los controles implementados y la configuración deseada. Puede utilizar servicios como AWS CodePipeline, AWS CodeBuild y AWS CodeDeploy para crear una canalización de CI/CD. Tenga en cuenta las instrucciones de Organizing Your AWS Environment Using Multiple Accounts para configurar estos servicios en sus propias cuentas que sean independientes de otras canalizaciones de implementación.

También puede definir plantillas para estandarizar la definición y la implementación de Cuentas de AWS, servicios y configuraciones. Esta técnica permite que un equipo de seguridad central administre estas definiciones y se las proporcione a los equipos de la carga de trabajo mediante un enfoque de autoservicio. Una forma de lograrlo es mediante Service Catalog, donde puede publicar plantillas como productos que los equipos de la carga de trabajo pueden incorporar a las implementaciones de su propia canalización. Si utiliza AWS Control Tower, hay disponibles algunas plantillas y controles como punto de partida. Control Tower también ofrece la función Account Factory, lo que permite a los equipos de la carga de trabajo crear nuevas Cuentas de AWS con los estándares que defina. Esta función ayuda a eliminar las dependencias de un equipo central para aprobar y crear nuevas cuentas cuando los equipos de la carga de trabajo las identifiquen como necesarias. Es posible que necesite estas cuentas para aislar los diferentes componentes de la carga de trabajo en función de motivos como la función que cumplen, la confidencialidad de los datos que se procesan o su comportamiento.

Pasos para la implementación

1. Determine cómo va a almacenar y mantener las plantillas en un sistema de control de versiones.
2. Cree canalizaciones de CI/CD para probar e implementar las plantillas. Defina pruebas para comprobar si hay errores de configuración y si las plantillas se ajustan a los estándares de su empresa.
3. Cree un catálogo de plantillas estandarizadas para que los equipos de la carga de trabajo implementen Cuentas de AWS y servicios de acuerdo con sus requisitos.
4. Implemente estrategias de copia de seguridad y recuperación seguras para sus configuraciones de control, scripts y datos relacionados.

Recursos

Prácticas recomendadas relacionadas:

- OPS05-BP01 Uso del control de versiones
- OPS05-BP04 Uso de sistemas de administración de compilación e implementación
- REL08-BP05 Implementación de cambios con automatización
- SUS06-BP01 Adopción de métodos que permitan introducir mejoras en la sostenibilidad rápidamente

Documentos relacionados:

- Organización de su entorno de AWS con varias cuentas

Ejemplos relacionados:

- Automate account creation, and resource provisioning using Service Catalog, AWS Organizations, and AWS Lambda
- Strengthen the DevOps pipeline and protect data with AWS Secrets Manager, AWS KMS, and AWS Gestor de certificados

Herramientas relacionadas:

- AWS CloudFormation Guard

- Landing Zone Accelerator on AWS

SEC01-BP07 Identificación de amenazas y priorización de mitigaciones con un modelo de amenazas

Utilice el modelado de amenazas para identificar y mantener un registro actualizado de las amenazas potenciales y las mitigaciones asociadas para la carga de trabajo. Priorice sus amenazas y adapte sus mitigaciones de controles de seguridad para evitarlas, detectarlas y responder a ellas. Revisite y mantenga todo esto en el contexto de la carga de trabajo y de la evolución del panorama de seguridad.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Qué es el modelado de amenazas?

“El modelado de amenazas sirve para identificar, comunicar y comprender las amenazas y las mitigaciones en el contexto de la protección de algo de valor”. – Threat Modeling de Open Web Application Security Project (OWASP

Por qué debería crear un modelo de amenazas?

Los sistemas son complejos y, con el tiempo, se hacen más complejos y potentes aún, por lo que aportan más valor empresarial y aumentan la satisfacción y el compromiso de los clientes. Esto significa que, en las decisiones de diseño de TI, se deben tener en cuenta un número cada vez mayor de casos de uso. Debido a esta complejidad y al número de combinaciones de casos de uso, los enfoques no estructurados suelen resultar ineficaces para encontrar y mitigar las amenazas. En su lugar, se necesita un enfoque sistemático para encontrar las amenazas potenciales para el sistema, pero también para concebir mitigaciones y priorizarlas para asegurarse de que los limitados recursos de la organización tengan el máximo impacto en la mejora de la postura de seguridad general del sistema.

El modelado de amenazas está diseñado para proporcionar este enfoque sistemático, con el objetivo de encontrar y abordar los problemas en las primeras fases del proceso de diseño, cuando las mitigaciones tienen un costo y un esfuerzo relativamente bajos en comparación con las fases posteriores del ciclo de vida. Este enfoque se alinea con el principio del sector relativo al desplazamiento a la izquierda de la seguridad. En última instancia, el modelado de amenazas se

integra en el proceso de administración de riesgos de una organización y ayuda a tomar decisiones sobre qué controles aplicar mediante un enfoque basado en las amenazas.

Cuándo se debe llevar a cabo el modelado de amenazas?

Empiece a modelar las amenazas lo antes posible en el ciclo de vida de la carga de trabajo, ya que así tendrá más flexibilidad para actuar en relación con las amenazas que identifique. Al igual que ocurre con los errores de software, cuanto antes identifique las amenazas, más rentable le resultará abordarlas. Un modelo de amenazas es un documento vivo y debe evolucionar a medida que cambien las cargas de trabajo. Revisite los modelos de amenazas a lo largo del tiempo, especialmente cuando se produzca un cambio importante, un cambio en el panorama de las amenazas o cuando adopte una nueva característica o servicio.

Pasos para la implementación

Cómo podemos llevar a cabo el modelado de amenazas?

Hay muchas formas diferentes de llevar a cabo el modelado de amenazas. Al igual que ocurre con los lenguajes de programación, cada una tiene sus ventajas y sus inconvenientes, por lo que debe elegir la que mejor le convenga. Un enfoque consiste en empezar con Shostack's 4 Question Frame for Threat Modeling, que plantea preguntas abiertas para estructurar el ejercicio de modelado de amenazas:

1. En qué estamos trabajando?

   La finalidad de esta pregunta es ayudarle a comprender y acordar el sistema que está creando y los detalles de ese sistema que son pertinentes para la seguridad. Crear un modelo o diagrama es la forma más popular de responder a esta pregunta, ya que le ayuda a visualizar lo que está creando, por ejemplo, mediante un diagrama de flujo de datos. Anotar las suposiciones y los detalles importantes sobre el sistema también le ayuda a definir el alcance del trabajo. De esta manera, todas las personas que contribuyen al modelo de amenazas pueden centrarse en lo mismo, y evita dar largos rodeos hacia temas que están fuera del alcance (lo que incluye versiones desactualizadas del sistema). Por ejemplo, si crea una aplicación web, probablemente no merezca la pena que modele la secuencia de arranque de confianza del sistema operativo para los clientes del navegador, ya que no tiene capacidad para influir en esto con su diseño.
2. Qué puede salir mal?

   Aquí es donde se identifican las amenazas que afectan al sistema. Las amenazas son acciones o acontecimientos accidentales o intencionados que tienen repercusiones no deseadas y podrían

afectar a la seguridad del sistema. Si no tiene una idea clara de lo que podría salir mal, no podrá hacer nada al respecto.

No existe una lista formal de lo que puede salir mal. La creación de esta lista requiere una lluvia de ideas y la colaboración de todas las personas del equipo y las personas pertinentes involucradas en el ejercicio de modelado de amenazas. Para facilitar la reflexión, puede utilizar un modelo para identificar amenazas, como STRIDE, que sugiere distintas categorías para evaluarlas: suplantación de identidad, manipulación, repudio, divulgación de información, denegación de servicio y elevación de privilegios. Además, para contribuir a la lluvia de ideas, tal vez quiera consultar las listas existentes y buscar inspiración; por ejemplo, en OWASP Top 10, HiTrust Threat Catalog y el catálogo de amenazas propio de su organización.

3. Qué vamos a hacer al respecto?

   Igual que en la pregunta anterior, no existe una lista formal de todas las mitigaciones posibles. En este paso, tenemos las amenazas, los actores y las áreas de mejora identificados en el paso anterior.

   Los asuntos relacionados con la seguridad y la conformidad son una responsabilidad compartida entre el cliente y AWS. Es importante entender que, cuando se pregunta “¿Qué vamos a hacer al respecto?”, también se está preguntando “¿Quién es responsable de hacer algo al respecto?”. Comprender el reparto de responsabilidades entre el cliente y AWS le ayuda a delimitar el modelado de amenazas a las mitigaciones que están bajo su control, que suelen ser una combinación de opciones de configuración de los servicios de AWS y las mitigaciones específicas de su propio sistema.

   En cuanto a la parte de AWS de la responsabilidad compartida, descubrirá que los servicios de AWS forman parte del ámbito de aplicación de muchos programas de cumplimiento. Estos programas le ayudan a conocer los sólidos controles que hay en AWS para mantener la seguridad y la conformidad de la nube. Los informes de auditoría de estos programas están disponibles para que los clientes de AWS los descarguen de AWS Artifact.

   Independientemente de los servicios de AWS que utilice, el cliente siempre tiene una parte de la responsabilidad, y las mitigaciones que se corresponden con estas responsabilidades deben incluirse en el modelo de amenazas. En cuanto a las mitigaciones de los controles de seguridad de los propios servicios de AWS, debe considerar la posibilidad de implementar controles de seguridad en todos los dominios, como los de administración de identidades y accesos (autenticación y autorización), protección de datos (en reposo y en tránsito), seguridad de la infraestructura, registro y supervisión. La documentación de cada servicio de AWS incluye

un capítulo dedicado a la seguridad que proporciona orientación sobre los controles de seguridad que se deben considerar como medidas de mitigación. Y lo que es más importante, considere el código que está escribiendo y sus dependencias, y piense en los controles que podría establecer para hacer frente a esas amenazas. Estos controles pueden ser, por ejemplo, la validación de entradas, la gestión de sesiones y la gestión de límites. Muchas veces, la mayoría de las vulnerabilidades se introducen en el código personalizado, así que céntrese en esta área.

4. Hicimos un buen trabajo?

   El objetivo es que su equipo y su organización mejoren con el tiempo tanto la calidad de los modelos de amenazas como la velocidad a la que los llevan a cabo. Estas mejoras se deben a una combinación de práctica, aprendizaje, enseñanza y revisión. Para profundizar y ponerse manos a la obra, le recomendamos que usted y su equipo completen el curso de formación o el taller sobre modelado de amenazas para constructores. Además, si busca orientación sobre cómo integrar el modelado de amenazas en el ciclo de vida del desarrollo de aplicaciones de su organización, consulte la publicación How to approach threat modeling en el blog de seguridad de AWS.

Threat Composer

Como ayuda y orientación a la hora de modelar las amenazas, considere la posibilidad de utilizar la herramienta Threat Composer, cuyo objetivo es reducir el tiempo que se tarda en generar valor a la hora de crear modelos de amenazas. La herramienta le ayuda a hacer lo siguiente:

- Escribir instrucciones de amenazas útiles alineadas con la gramática de amenazas que funcionen en un flujo de trabajo natural y no lineal
- Generar un modelo de amenazas legible por humanos
- Generar un modelo de amenazas legible por máquina que le permita tratar los modelos de amenazas como código
- Ayudarle a identificar rápidamente las áreas de mejora de la calidad y la cobertura mediante el panel de información

Para obtener más información, visite Threat Composer y cambie al espacio de trabajo de ejemplo definido por el sistema.

Recursos

Prácticas recomendadas relacionadas:

- SEC01-BP03 Identificación y validación de los objetivos de control
- SEC01-BP04 Actualización constante de las amenazas y recomendaciones de seguridad
- SEC01-BP05 Reducción del alcance de la administración de la seguridad
- SEC01-BP08 Evaluación e implementación de nuevos servicios y características de seguridad de forma periódica

Documentos relacionados:

- How to approach threat modeling (blog de seguridad de AWS)
- NIST: Guide to Data-Centric System Threat modeling

Videos relacionados:

- AWS Summit ANZ 2021 - How to approach threat modelling
- AWS Summit ANZ 2022 - Scaling security – Optimise for fast and secure delivery

Formación relacionada:

- Threat modeling the right way for builders – AWS Skill Builder virtual self-paced training
- Threat modeling the right way for builders – AWS Workshop

Herramientas relacionadas:

- Threat Composer

SEC01-BP08 Evaluación e implementación de nuevos servicios y características de seguridad de forma periódica

Evalúe e implemente servicios y características de seguridad de AWS y socios de AWS que le ayuden a desarrollar la postura de seguridad de su carga de trabajo.

Resultado deseado: cuenta con una práctica estándar que le informa sobre las nuevas características y servicios lanzados por AWS y socios de AWS. Evalúe en qué medida estas nuevas capacidades influyen en el diseño de los controles actuales y nuevos para sus entornos y cargas de trabajo.

Patrones comunes de uso no recomendados:

- No se suscribe a blogs de AWS y fuentes RSS para enterarse rápidamente de las nuevas características y servicios pertinentes.
- Confía en las noticias y actualizaciones sobre los servicios y características de seguridad de fuentes de segunda mano
- No fomenta entre los usuarios de AWS de su organización a mantenerse al día de las últimas actualizaciones

Beneficios de establecer esta práctica recomendada: si está al tanto de los nuevos servicios y características de seguridad, puede tomar decisiones informadas sobre la implementación de controles en cargas de trabajo y entornos de nube. Estos orígenes ayudan a concienciar sobre la evolución del panorama de seguridad y sobre cómo se pueden utilizar los servicios de AWS para protegerse contra las amenazas nuevas y emergentes.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: bajo

Guía para la implementación

AWS informa a los clientes sobre los nuevos servicios y características de seguridad a través de varios canales:

- AWS Novedades de
- AWS Blog de noticias de
- AWS Blog de seguridad de
- AWS Boletines de seguridad de
- AWS Descripción general de la documentación de

Puede suscribirse a un tema de actualizaciones diarias de características de AWS mediante Amazon Simple Notification Service (Amazon SNS) para obtener un resumen diario completo de las actualizaciones. Algunos servicios de seguridad, como Amazon GuardDuty y AWS Security Hub CSPM, ofrecen sus propios temas de SNS para mantenerse al día sobre los nuevos estándares, resultados y otras actualizaciones de esos servicios en particular.

Los nuevos servicios y características también se anuncian y describen en detalle durante las conferencias, eventos y seminarios web que se llevan a cabo en todo el mundo cada año. Cabe destacar la conferencia anual de seguridad AWS re:Inforce y la conferencia de carácter más general,

AWS re:Invent. Los canales de noticias de AWS mencionados anteriormente comparten estos anuncios de conferencias sobre seguridad y otros servicios, y pueden verse las sesiones temáticas informativas en línea en el canal de eventos de AWS en YouTube.

También puede preguntar a su equipo de Cuenta de AWS sobre las últimas actualizaciones y recomendaciones de los servicios de seguridad. Puede contactar con su equipo a través del formulario de soporte de ventas si no dispone de su información de contacto directo. Del mismo modo, si se suscribió a AWS Enterprise Support, recibirá actualizaciones semanales de su administrador técnico de cuentas (TAM) y podrá programar una reunión de revisión periódica con dicho administrador.

Pasos para la implementación

1. Suscríbase a los distintos blogs y boletines con su lector de RSS favorito o al tema de SNS sobre actualizaciones de características diarias.
2. Evalúe a qué eventos de AWS asistir para conocer de primera mano las nuevas características y servicios.
3. Programe reuniones con su equipo de Cuenta de AWS para resolver cualquier duda sobre la actualización de los servicios y características de seguridad.
4. Plantéese la posibilidad de suscribirse a Enterprise Support para acceder a consultas periódicas con un gerente técnico de cuentas (TAM).

Recursos

Prácticas recomendadas relacionadas:

- PERF01-BP01 Descubrimiento y comprensión de los servicios y las características disponibles en la nube
- COST01-BP07 Seguimiento de la información sobre las nuevas versiones de los servicios

Identity and Access Management

Para utilizar los servicios de AWS, debe conceder acceso a los usuarios y las aplicaciones a los recursos de las cuentas de AWS. A medida que vaya ejecutando más cargas de trabajo en AWS, tendrá que establecer permisos y procesos de administración de identidades sólidos para garantizar que las personas adecuadas tengan acceso a los recursos correctos en las condiciones apropiadas. AWS ofrece una gran selección de funcionalidades para ayudarle a administrar las identidades humanas y de máquinas y sus permisos. Las prácticas recomendadas para estas funcionalidades se incluyen en dos áreas principales.

Temas

- Administración de identidades
- Administración de permisos

Administración de identidades

Hay dos tipos de identidades que debe administrar al abordar la operación de cargas de trabajo de AWS seguras.

- Identidades humanas: las identidades humanas que requieren acceso a sus entornos y aplicaciones de AWS se pueden clasificar en tres grupos: personal, terceros y usuarios.

  El grupo de personal incluye administradores, desarrolladores y operadores que forman parte de su organización. Necesitan acceso para administrar, crear y operar sus recursos de AWS.

  Los terceros son colaboradores externos, como contratistas, proveedores o socios. Interactúan con sus recursos de AWS como parte de su compromiso con su organización.

  Los usuarios son quienes utilizan sus aplicaciones. Acceden a los recursos de AWS a través de navegadores web, aplicaciones de cliente, aplicaciones móviles o herramientas de línea de comandos interactivas.
- Identidades de máquinas: las aplicaciones de carga de trabajo, las herramientas operativas y los componentes requieren una identidad para hacer solicitudes a los servicios de AWS, por ejemplo, para leer datos. Estas identidades incluyen máquinas que se ejecutan en su entorno de AWS, como instancias de Amazon EC2 o funciones de AWS Lambda. También se podrían administrar identidades de máquina para las partes externas a AWS que necesiten acceso a su entorno de AWS.

Prácticas recomendadas

- SEC02-BP01 Uso de mecanismos de inicio de sesión sólidos
- SEC02-BP02 Uso de credenciales temporales
- SEC02-BP03 Almacenamiento y uso seguros de secretos
- SEC02-BP04 Uso de un proveedor de identidades centralizado
- SEC02-BP05 Auditoría y rotación periódicas de las credenciales
- SEC02-BP06 Uso de grupos y atributos de usuarios

SEC02-BP01 Uso de mecanismos de inicio de sesión sólidos

Los inicios de sesión (autenticación mediante credenciales de inicio de sesión) pueden presentar riesgos si no se utilizan mecanismos como la autenticación multifactor (MFA), especialmente en situaciones en las que las credenciales de inicio de sesión se han revelado de forma inadvertida o son fáciles de adivinar. Utilice mecanismos de inicio de sesión sólidos para reducir estos riesgos. Para ello, exija que se cumplan políticas de contraseñas sólidas y se utilice MFA.

Resultado deseado: reduzca los riesgos de acceso no deseado a las credenciales en AWS mediante el uso de mecanismos de inicio de sesión sólidos para los usuarios de AWS Identity and Access Management (IAM), el usuario raíz de la Cuenta de AWS, AWS IAM Identity Center y los proveedores de identidades de terceros. Esto significa exigir que se use MFA, aplicar políticas de contraseñas sólidas y detectar comportamientos de inicio de sesión anómalos.

Patrones comunes de uso no recomendados:

- No aplicar una política de contraseñas segura para sus identidades que incluya contraseñas complejas y MFA.
- Compartir las mismas credenciales entre diferentes usuarios.
- No utilizar controles de detección de inicios de sesión sospechosos.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Existen muchas formas en que las identidades humanas puedan iniciar sesión en AWS. Una práctica recomendada de AWS es confiar en un proveedor de identidades centralizado que utilice la federación (federación directa SAML 2.0 entre AWS IAM y el IdP centralizado o usando AWS IAM

Identity Center) a la hora de autenticarse en AWS. En ese caso, deberá establecer un proceso de inicio de sesión seguro con su proveedor de identidades o Microsoft Active Directory.

Cuando abre una Cuenta de AWS por primera vez, comienza con un usuario raíz de la Cuenta de AWS. Solo debe usar el usuario raíz de la cuenta para configurar el acceso de los usuarios (y para las tareas que requieren el usuario raíz). Es importante activar la autenticación multifactor (MFA) para el usuario raíz de la cuenta inmediatamente después de abrir la Cuenta de AWS y proteger al usuario raíz según la guía de prácticas recomendadas de AWS.

AWS IAM Identity Center está diseñado para usuarios de la plantilla, y puede crear y administrar las identidades de los usuarios dentro del servicio y proteger el proceso de inicio de sesión con MFA. AWS Cognito, por otro lado, está diseñado para la gestión de la identidad y el acceso de los clientes (CIAM), que proporciona grupos de usuarios y proveedores de identidad para las identidades de los usuarios externos en sus aplicaciones.

Si crea usuarios en el AWS IAM Identity Center, proteja el proceso de inicio de sesión en ese servicio y active la MFA. Para las identidades de los usuarios externos en sus aplicaciones, puede utilizar grupos de usuarios de Amazon Cognito y proteger el proceso de inicio de sesión en ese servicio, o bien utilizar uno de los proveedores de identidades compatibles con los grupos de usuarios de Amazon Cognito.

Además, en el caso de los usuarios del Centro de Identidad de AWS IAM, se puede utilizar Acceso verificado de AWS para proporcionar un nivel de seguridad adicional mediante la verificación de la identidad del usuario y la posición del dispositivo antes de que se les conceda acceso a los recursos de AWS.

Si utiliza usuarios de AWS Identity and Access Management (IAM), debe proteger el proceso de inicio de sesión mediante IAM.

Puede utilizar tanto AWS IAM Identity Center y la federación de IAM directa de forma simultánea para gestionar el acceso a AWS. Puede utilizar la federación de IAM para administrar el acceso a la Consola de administración de AWS y a los servicios e IAM Identity Center para administrar el acceso a aplicaciones empresariales como Quick o Amazon Q Business.

Independientemente del método de inicio de sesión que se utilice, es fundamental aplicar una política de inicio de sesión sólida.

Pasos para la implementación

Estas son recomendaciones generales para un inicio de sesión sólido. Los ajustes reales que configure deben estar establecidos por la política de la empresa o utilizar un estándar como NIST 800-63.

- Require MFA (Requerir MFA): Es práctica recomendada de IAM exigir la MFA para las identidades humanas y las cargas de trabajo. Si se activa MFA, habrá una capa adicional de seguridad que exigirá que los usuarios proporcionen credenciales de inicio de sesión y una contraseña de un solo uso (OTP) o una cadena que se verifica criptográficamente y se genera desde un dispositivo físico.
- Imponga una longitud mínima para la contraseña. Esto es un factor fundamental para la seguridad de la contraseña.
- Imponga una complejidad de las contraseñas para que sean más difíciles de adivinar.
- Permita que los usuarios cambien sus contraseñas.
- Cree identidades individuales en lugar de credenciales compartidas. Si crea identidades individuales, puede dar a cada usuario un conjunto único de credenciales de seguridad. Tener usuarios individuales permite auditar la actividad de cada uno de ellos.

Recomendaciones de IAM Identity Center:

- IAM Identity Center proporciona una política de contraseñas predefinida cuando se utiliza el directorio predeterminado, que establece la longitud, la complejidad y los requisitos de reutilización de las contraseñas.
- Active la MFA y configure los ajustes contextuales o permanentes para la MFA cuando el origen de la identidad sea el directorio predeterminado, AWS Managed Microsoft AD, o AD Connector.
- Permita a los usuarios registrar sus propios dispositivos MFA.

Recomendaciones del directorio de grupos de usuarios de Amazon Cognito:

- Configurar los ajustes de Seguridad de la contraseña.
- Requiera MFA para los usuarios.
- Utilizar la configuración de seguridad avanzada de grupos de usuarios de Amazon Cognito para las características, como la autenticación adaptativa, que puede bloquear los inicios de sesión sospechosos.

Recomendaciones de usuarios de IAM:

- Lo ideal es que utilice IAM Identity Center o la federación directa. Sin embargo, es posible que necesite usuarios de IAM. En ese caso, establezca una política de contraseñas para los usuarios de IAM. Puede usar una política de contraseñas para definir requisitos, tales como la longitud mínima o si deben contener caracteres no alfanuméricos.
- Cree una política de IAM para imponer el inicio de sesión con MFA de modo que los usuarios puedan administrar sus propias contraseñas y dispositivos MFA.

Recursos

Prácticas recomendadas relacionadas:

- SEC02-BP03 Almacenamiento y uso seguros de secretos
- SEC02-BP04 Uso de un proveedor de identidades centralizado
- SEC03-BP08 Uso compartido de recursos de forma segura en su organización

Documentos relacionados:

- Política de contraseñas del AWS IAM Identity Center
- Política de contraseñas para usuarios de IAM
- Configuración de la contraseña del usuario raíz de la Cuenta de AWS
- Política de contraseñas de Amazon Cognito
- Credenciales de AWS
- Prácticas recomendadas de seguridad de IAM

Videos relacionados:

- Managing user permissions at scale with AWS IAM Identity Center
- Mastering identity at every layer of the cake

SEC02-BP02 Uso de credenciales temporales

Al llevar a cabo cualquier tipo de autenticación, es mejor utilizar credenciales temporales en lugar de credenciales de larga duración para reducir o eliminar riesgos. Por ejemplo, que las credenciales se divulguen, compartan o roben de forma inadvertida.

Resultado deseado: para reducir el riesgo de credenciales a largo plazo, utilice credenciales temporales siempre que sea posible para las identidades humanas y de máquinas. Las credenciales de larga duración entrañan muchos riesgos. Por ejemplo, podrían subirse a repositorios públicos y quedar expuestas. Al utilizar credenciales temporales, reducirá enormemente las posibilidades de que las credenciales se vean comprometidas.

Patrones comunes de uso no recomendados:

- Desarrolladores que utilizan claves de acceso de larga duración de usuarios de IAM en lugar de obtener credenciales temporales de la CLI mediante federación.
- Desarrolladores que incrustan claves de acceso de larga duración en su código y suben ese código a repositorios de Git públicos.
- Desarrolladores que incrustan claves de acceso de larga duración en aplicaciones móviles que luego se ponen a disposición de todo el mundo en las tiendas de aplicaciones.
- Usuarios que comparten claves de acceso de larga duración con otros usuarios, o empleados que abandonan la empresa con claves de acceso de larga duración aún en su poder.
- Utilizar claves de acceso de larga duración para identidades de máquinas cuando podrían utilizarse credenciales temporales.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Utilice credenciales de seguridad temporales en lugar de credenciales de larga duración para todas las solicitudes de la API y la AWS CLI. Las solicitudes de la API y la CLI a los servicios de AWS deben, en casi todos los casos, firmarse mediante claves de acceso de AWS. Estas solicitudes pueden firmarse con credenciales temporales o de larga duración. La única vez que debe utilizar credenciales de larga duración, también conocidas como claves de acceso a largo plazo, es si utiliza un usuario de IAM o un usuario raíz de la Cuenta de AWS. Al federarse en AWS o asumir un rol de IAM mediante otros métodos, se generan credenciales temporales. Incluso cuando accede a la Consola de administración de AWS mediante credenciales de inicio de sesión, se generan

credenciales temporales para que pueda hacer llamadas a los servicios de AWS. Hay pocas situaciones en las que necesite credenciales de larga duración, y casi todas las tareas se pueden llevar a cabo mediante credenciales temporales.

Evitar el uso de credenciales de larga duración en favor de credenciales temporales debería acompañarse de una estrategia de reducción del uso de usuarios de IAM a favor de la federación y los roles de IAM. Aunque en el pasado se han utilizado usuarios de IAM tanto para identidades humanas como de máquinas, ahora recomendamos no utilizarlos para evitar los riesgos que conlleva el uso de claves de acceso de larga duración.

Pasos para la implementación

Identidades humanas

Para identidades de la plantilla, como las de empleados, administradores, desarrolladores, operadores y clientes:

- Debería basarse en un proveedor de identidades centralizado y exigir que los usuarios humanos utilicen la federación con un proveedor de identidades para acceder a AWS con credenciales temporales. La federación de los usuarios se puede efectuar mediante la federación directa a cada Cuenta de AWS o con AWS IAM Identity Center y el proveedor de identidades que prefiera. La federación tiene una serie de ventajas con respecto a los usuarios de IAM, además de eliminar las credenciales de larga duración. Los usuarios también pueden solicitar credenciales temporales desde la línea de comandos para la federación directa o mediante IAM Identity Center. Esto significa que hay pocos casos de uso que requieran usuarios de IAM o credenciales de larga duración para los usuarios.

Para identidades de terceros:

- Al conceder a terceros, como a proveedores de software como servicio (SaaS), acceso a los recursos en su Cuenta de AWS, puede utilizar roles entre cuentas y políticas basadas en recursos. Además, puede utilizar el flujo de concesión de credenciales de cliente de Amazon Cognito OAuth 2.0 para clientes o socios de SaaS B2B.

Las identidades de usuario que acceden a los recursos de AWS a través de navegadores web, aplicaciones de cliente, aplicaciones móviles o herramientas de línea de comando interactivas:

- Si necesita conceder a las aplicaciones para consumidores o clientes acceso a los recursos de su AWS, puede utilizar grupos de identidades de Amazon Cognito o grupos de usuarios de Amazon

Cognito para proporcionar credenciales temporales. Los permisos de las credenciales se controlan mediante los roles de IAM que cree. También puede definir un rol de IAM independiente con permisos limitados para los usuarios invitados que no estén autenticados.

Identidades de máquina

En el caso de las identidades de máquina, puede que necesite utilizar credenciales de larga duración. En estos casos, puede exigir que las cargas de trabajo utilicen credenciales temporales con roles de IAM para acceder a AWS.

- Para Amazon Elastic Compute Cloud (Amazon EC2), puede utilizar roles para Amazon EC2.
- AWS Lambda permite configurar un rol de ejecución de Lambda para conceder al servicio permisos para llevar a cabo acciones de AWS mediante credenciales temporales. Existen muchos otros modelos similares para que los servicios de AWS concedan credenciales temporales con roles de IAM.
- En el caso de los dispositivos de IoT, puede utilizar el proveedor de credenciales de AWS IoT Core para solicitar credenciales temporales.
- Para los sistemas en las instalaciones o los que se ejecutan fuera de AWS que necesitan acceso a los recursos de AWS, puede utilizar IAM Roles Anywhere.

Hay escenarios en los que no se admiten credenciales temporales, pero requieren el uso de credenciales de larga duración. En estas situaciones, audite y rote las credenciales periódicamente y rote las claves de acceso periódicamente. En el caso de las claves de acceso de los usuarios de IAM muy restringidas, tenga en cuenta las siguientes medidas de seguridad adicionales:

- Otorgue permisos muy restringidos:
  - Cumpla con el principio de privilegio mínimo (sea específico en cuanto a las acciones, los recursos y las condiciones).
  - Plantéese la opción de conceder al usuario de IAM solo la operación AssumeRole para un rol específico. En función de la arquitectura local, este enfoque ayuda a aislar y proteger las credenciales de IAM a largo plazo.
- Limite las fuentes de red y las direcciones IP permitidas en la política de confianza de roles de IAM.
- Supervise el uso y configure alertas para detectar permisos no utilizados o mal uso (mediante alarmas y filtros de métricas de AWS CloudWatch Logs).

- Exija el cumplimiento de los límites de los permisos (las políticas de control de servicios [SCP]) y los límites de permisos se complementan entre sí: las SCP son muy generales, mientras que los límites de los permisos son más precisos).
- Implemente un proceso para aprovisionar y almacenar de forma segura (en un almacén local) las credenciales.

Entre las opciones para los escenarios que requieren credenciales a largo plazo también se incluyen:

- Crear su propia API de venta de tokens (mediante Amazon API Gateway).
- En situaciones en las que deba utilizar credenciales de larga duración o para credenciales distintas de las claves de acceso de AWS (como los inicios de sesión en bases de datos), puede utilizar un servicio diseñado para gestionar los secretos, como AWS Secrets Manager. Secrets Manager simplifica la administración, la rotación y el almacenamiento seguro de los secretos cifrados. Muchos servicios de AWS admiten la integración directa con Secrets Manager.
- Para las integraciones multinube, puede utilizar la federación de identidades en función de las credenciales del proveedor de servicios de credenciales (CSP) de origen (consulte AWS STS AssumeRoleWithWebIdentity).

Para obtener más información sobre cómo cambiar las credenciales de larga duración, consulte cómo rotar las claves de acceso.

Recursos

Prácticas recomendadas relacionadas:

- SEC02-BP03 Almacenamiento y uso seguros de secretos
- SEC02-BP04 Uso de un proveedor de identidades centralizado
- SEC03-BP08 Uso compartido de recursos de forma segura en su organización

Documentos relacionados:

- Credenciales de seguridad temporales
- Credenciales de AWS
- Prácticas recomendadas de seguridad de IAM
- Roles de IAM

- IAM Identity Center
- Federación y proveedores de identidades
- Rotación de las claves de acceso
- Soluciones de socios de seguridad: acceso y control de acceso
- El usuario raíz de la cuenta de AWS
- Access AWS using a Google Cloud Platform native workload identity
- How to access AWS resources from Microsoft Entra ID tenants using AWS Security Token Service

Videos relacionados:

- Managing user permissions at scale with AWS IAM Identity Center
- Mastering identity at every layer of the cake

SEC02-BP03 Almacenamiento y uso seguros de secretos

Una carga de trabajo necesita una capacidad automatizada para demostrar su identidad a bases de datos, recursos y servicios de terceros. Para ello, se utilizan credenciales de acceso secretas, como claves de acceso a API, contraseñas y tokens OAuth. El uso de un servicio creado específicamente para almacenar, administrar y rotar estas credenciales ayuda a reducir la probabilidad de que dichas credenciales se vean comprometidas.

Resultado deseado: implementación de un mecanismo de administración segura de las credenciales de las aplicaciones que logre los siguientes objetivos:

- Identificar qué secretos son necesarios para la carga de trabajo.
- Reducir el número de credenciales de larga duración necesarias y sustituirlas por credenciales de corta duración cuando sea posible.
- Establecer un almacenamiento seguro y una rotación automatizada de las credenciales restantes de larga duración.
- Auditar el acceso a los secretos que existen en la carga de trabajo.
- Supervisar de forma continua para verificar que no se incruste ningún secreto en el código fuente durante el proceso de desarrollo.
- Reduzca la probabilidad de que las credenciales se divulguen por accidente.

Patrones comunes de uso no recomendados:

- No rotar las credenciales.
- Almacenar credenciales a largo plazo en el código fuente o en archivos de configuración.
- Almacenar credenciales en reposo sin cifrar.

Beneficios de establecer esta práctica recomendada:

- Los secretos se almacenan cifrados en reposo y en tránsito.
- El acceso a las credenciales se controla a través de una API (considérela como una máquina expendedora de credenciales).
- El acceso a una credencial (tanto de lectura como de escritura) se audita y registra.
- Separación de preocupaciones: la rotación de credenciales la hace un componente independiente, que puede separarse del resto de la arquitectura.
- Los secretos se distribuyen automáticamente bajo demanda a los componentes de software, y la rotación se produce en una ubicación central.
- El acceso a las credenciales puede controlarse de forma detallada.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

En el pasado, las credenciales que se utilizaban para autenticarse en bases de datos, API de terceros, tokens y otros secretos podían estar incrustadas en el código fuente o en archivos del entorno. AWS proporciona varios mecanismos para almacenar estas credenciales de forma segura, rotarlas automáticamente y auditar su uso.

La mejor manera de abordar la administración de secretos es seguir la norma de eliminar, sustituir y rotar. La credencial más segura es aquella que no se tiene que almacenar, administrar ni manejar. Es posible que haya credenciales que ya no sean necesarias para el funcionamiento de la carga de trabajo y que, por tanto, puedan eliminarse de forma segura.

En el caso de las credenciales que siguen siendo necesarias para el correcto funcionamiento de la carga de trabajo, podría existir la oportunidad de sustituir una credencial de larga duración por una credencial temporal o de corta duración. Por ejemplo, en lugar de codificar rígidamente una clave de acceso secreta de AWS, considere la posibilidad de sustituir esa credencial de larga duración por una credencial temporal a través de roles de IAM.

Es posible que algunos secretos de larga duración no puedan eliminarse ni sustituirse. Estos secretos se pueden almacenar en un servicio, como AWS Secrets Manager, donde se pueden almacenar, administrar y rotar de forma centralizada periódicamente.

Una auditoría del código fuente y de los archivos de configuración de la carga de trabajo puede revelar muchos tipos de credenciales. La siguiente tabla resume las estrategias para manejar los tipos comunes de credenciales:

Tipo de credenciales	Descripción	Estrategia sugerida
claves de acceso de IAM	Claves de acceso y secretas de AWS IAM que se utilizan para asumir roles de IAM dentro de una carga de trabajo	Reemplazo: utilice los roles de IAM asignados a las instancias de cómputo (como Amazon EC2 o AWS Lambda) en su lugar. Para garantizar la interoperabilidad con terceros que tengan que acceder a los recursos en la Cuenta de AWS, pregunte si admiten el acceso entre cuentas de AWS. En el caso de aplicaciones móviles, considere la posibilidad de usar credenciales temporales a través de grupos de identidades de Amazon Cognito (identidades federadas). Para las cargas de trabajo que se ejecutan fuera de AWS, considere IAM Roles Anywhere o Activaciones híbridas de AWS Systems Manager. Para los contenedores, consulte el rol de IAM de la tarea de Amazon ECS o el rol de IAM del nodo de Amazon EKS.

Tipo de credenciales	Descripción	Estrategia sugerida
Claves de SSH	Las claves privadas de Secure Shell se utilizan para iniciar sesión en las instancias de EC2 de Linux, de forma manual o como parte de un proceso automatizado	Reemplazo: utilice AWS Systems Manager o EC2 Instance Connect para proporcionar acceso mediante programación y humano a las instancias de EC2 mediante roles de IAM.
Credenciales de aplicaciones y bases de datos	Contraseñas: cadena de texto sin formato	Rotación: almacene las credenciales en AWS Secrets Manager y establezca una rotación automatizada si es posible.
Credenciales de Amazon RDS y Aurora Admin Database	Contraseñas: cadena de texto sin formato	Reemplazo: utilice la integración de Secrets Manager en Amazon RDS o Amazon Aurora. Además, algunos tipos de bases de datos de RDS pueden utilizar roles de IAM en lugar de contraseñas en algunos casos de uso (para obtener más información, consulte Autenticación de bases de datos de IAM).
Tokens OAuth	Tokens secretos: cadena de texto sin formato	Rotación: almacene los tokens en AWS Secrets Manager y configure la rotación automatizada.
Tokens y claves de API	Tokens secretos: cadena de texto sin formato	Rotación: almacénelas en AWS Secrets Manager y establezca una rotación automatizada si es posible.

Un patrón común de uso no recomendado es incrustar claves de acceso de IAM dentro del código fuente, los archivos de configuración o las aplicaciones móviles. Cuando se necesite una clave de acceso de IAM para comunicarse con un servicio de AWS, utilice credenciales de seguridad temporales (a corto plazo). Estas credenciales a corto plazo se pueden proporcionar mediante roles de IAM para instancias de EC2, roles de ejecución para funciones de Lambda, roles de IAM de Cognito para el acceso de usuarios móviles y políticas de IoT Core para dispositivos de IoT. Al interactuar con terceros, dé prioridad a delegar el acceso a un rol de IAM con el acceso necesario a los recursos de su cuenta en lugar de configurar un usuario de IAM y enviar al tercero la clave de acceso secreta de ese usuario.

Hay muchos casos en los que la carga de trabajo requiere el almacenamiento de los secretos necesarios para interoperar con otros servicios y recursos. AWS Secrets Manager está diseñado específicamente para administrar estas credenciales de forma segura, así como para el almacenamiento, el uso y la rotación de los tokens de API, las contraseñas y otras credenciales.

AWS Secrets Manager proporciona cinco funciones clave para garantizar el almacenamiento y la administración seguros de las credenciales confidenciales: cifrado en reposo, cifrado en tránsito, auditoría exhaustiva, control de acceso detallado y rotación de credenciales ampliable. También son aceptables otros servicios de administración de secretos de socios de AWS o soluciones desarrolladas localmente que proporcionen capacidades y garantías similares.

Cuando recupera un secreto, puede utilizar el componente de almacenamiento en caché del cliente de Secrets Manager para utilizarlo más adelante. Recuperar un secreto almacenado en la memoria caché es más rápido que recuperarlo desde Secrets Manager. Asimismo, dado que la llamada a las API de Secrets Manager conlleva un coste, el uso de una caché puede reducirlo. Para conocer todas las formas en las que puede recuperar secretos, consulte Obtener secretos.

> **Note**
>
> Algunos lenguajes pueden pedirle que implemente su propio cifrado en memoria para el almacenamiento en caché del cliente.

Pasos para la implementación

1. Identifique las rutas de código que contienen credenciales con codificación rígida mediante herramientas automatizadas, como Amazon CodeGuru.

   a. Utilice Amazon CodeGuru para analizar los repositorios de código. Una vez finalizada la revisión, filtre por Type=Secrets en CodeGuru para encontrar líneas de código que presentan problemas.
2. Identifique las credenciales que pueden eliminarse o sustituirse.
   a. Identifique las credenciales que ya no sean necesarias y márquelas para eliminarlas.
   b. En el caso de las claves secretas de AWS que estén incrustadas en el código fuente, sustitúyalas por roles de IAM asociados a los recursos necesarios. Si parte de la carga de trabajo se encuentra fuera de AWS, pero requiere credenciales de IAM para acceder a los recursos de AWS, considere la posibilidad de usar IAM Roles Anywhere o Activaciones híbridas de AWS Systems Manager.
3. Para otros secretos de terceros de larga duración que requieran el uso de la estrategia de rotación, integre Secrets Manager en el código para recuperar secretos de terceros en tiempo de ejecución.
   a. La consola de CodeGuru puede crear automáticamente un secreto en Secrets Manager con las credenciales detectadas.
   b. Integre la recuperación de secretos desde Secrets Manager en el código de la aplicación.
      i. Las funciones de Lambda sin servidor pueden utilizar una extensión de Lambda independiente del lenguaje.
      ii. Para las instancias o contenedores de EC2, AWS proporciona un ejemplo de código del lado del cliente para recuperar secretos de Secrets Manager en varios lenguajes de programación populares.
4. Revise periódicamente la base de código y vuelva a analizarla para verificar que no se hayan agregado nuevos secretos al código.
   a. Considere la posibilidad de utilizar una herramienta, como git-secrets, para evitar confirmar nuevos secretos en el repositorio del código fuente.
5. Supervisión de la actividad de Secrets Manager para detectar indicios de uso inesperado, acceso inapropiado a secretos o intentos de eliminar secretos.
6. Reduzca la exposición humana a las credenciales. Restrinja el acceso para leer, escribir y modificar credenciales a un rol de IAM dedicado a este fin, y solo proporcione acceso para asumir el rol a un pequeño subconjunto de usuarios operativos.

Recursos

Prácticas recomendadas relacionadas:

- SEC02-BP02 Uso de credenciales temporales
- SEC02-BP05 Auditoría y rotación periódicas de las credenciales

Documentos relacionados:

- Introducción a AWS Secrets Manager
- Federación y proveedores de identidades
- Amazon CodeGuru presenta el detector de secretos
- Cómo AWS Secrets Manager utiliza AWS Key Management Service
- Cifrado y descifrado de secretos en Secrets Manager
- Entradas del blog de Secrets Manager
- Amazon RDS presenta la integración con AWS Secrets Manager

Videos relacionados:

- Best Practices for Managing, Retrieving, and Rotating Secrets at Scale
- Find Hard-Coded Secrets Using Amazon CodeGuru Secrets Detector
- Securing Secrets for Hybrid Workloads Using AWS Secrets Manager

Talleres relacionados:

- Store, retrieve, and manage sensitive credentials in AWS Secrets Manager
- Activaciones híbridas de AWS Systems Manager

SEC02-BP04 Uso de un proveedor de identidades centralizado

Para las identidades de la plantilla (empleados y contratistas), recurra a un proveedor de identidades que le permita administrar las identidades desde un lugar centralizado. De este modo se facilita la administración del acceso en varias aplicaciones y sistemas, pues crea, asigna, administra, revoca y audita el acceso desde un único lugar.

Resultado deseado: tiene un proveedor de identidades centralizado en el que administra de forma centralizada los usuarios de la plantilla, las políticas de autenticación (como la exigencia de la autenticación multifactor [MFA]) y la autorización de los sistemas y las aplicaciones (como la asignación del acceso en función de la pertenencia o los atributos del grupo del usuario). Los

usuarios de la plantilla inician sesión en el proveedor de identidades central y se federan (inicio de sesión único) en aplicaciones internas y externas, lo que elimina la necesidad de que los usuarios recuerden varias credenciales. El proveedor de identidades está integrado en sus sistemas de recursos humanos (RR. HH.) para que los cambios de personal se sincronicen automáticamente con su proveedor de identidades. Por ejemplo, si alguien abandona la organización, puede revocar automáticamente el acceso a las aplicaciones y sistemas federados (incluido AWS). Ha habilitado el registro de auditoría detallado en su proveedor de identidades y supervisa estos registros para detectar comportamientos inusuales de los usuarios.

Patrones comunes de uso no recomendados:

- No utiliza la federación ni el inicio de sesión único. Los usuarios de la plantilla crean cuentas de usuario y credenciales independientes en diversas aplicaciones y sistemas.
- No ha automatizado el ciclo de vida de las identidades de los usuarios de la plantilla, por ejemplo, no ha integrado su proveedor de identidades en sus sistemas de recursos humanos. Cuando un usuario abandona la organización o cambia de rol, se sigue un proceso manual para eliminar o actualizar sus registros en varias aplicaciones y sistemas.

Beneficios de establecer esta práctica recomendada: al usar un proveedor de identidades centralizado, hay un único lugar en el que se administran las identidades y políticas de los usuarios en plantilla, la capacidad de asignar acceso a aplicaciones a los usuarios y grupos y la capacidad de supervisar la actividad de inicio de sesión de los usuarios. Al integrarse en sus sistemas de recursos humanos (RR. HH.), cuando un usuario cambia de rol, estos cambios se sincronizan con el proveedor de identidades, y las aplicaciones y permisos asignados se actualizan automáticamente. Cuando un usuario abandona la organización, su identidad se inhabilita automáticamente en el proveedor de identidades, lo que revoca su acceso a las aplicaciones y sistemas federados.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Orientaciones para los usuarios de la plantilla que acceden a AWS Es posible que los usuarios de la plantilla, como empleados y contratistas de su organización, tengan que acceder a AWS mediante la Consola de administración de AWS o la AWS Command Line Interface (AWS CLI) para trabajar. Para conceder acceso a AWS, puede federar a los usuarios en plantilla desde su proveedor de identidades centralizado en AWS en dos niveles: federación directa a cada Cuenta de AWS o federación de varias cuentas en su organización de AWS.

Para federar a los usuarios en plantilla directamente con cada Cuenta de AWS, puede utilizar un proveedor de identidades centralizado para federar a AWS Identity and Access Management en esa cuenta. La flexibilidad de IAM le permite habilitar un proveedor de identidades SAML 2.0 u Open ID Connect (OIDC) por separado para cada Cuenta de AWS y utilizar atributos de usuario federado para el control de acceso. Para iniciar sesión en el proveedor de identidades, los usuarios en plantilla utilizarán su navegador web y proporcionarán sus credenciales (como contraseñas y códigos de token de MFA). El proveedor de identidades envía una aserción SAML a su navegador que se envía a la URL de inicio de sesión de la Consola de administración de AWS para permitir que el usuario haga un inicio de sesión único en la Consola de administración de AWS al asumir un rol de IAM. Los usuarios también pueden obtener credenciales temporales de la API de AWS para usarlas en la AWS CLI o los SDK de AWS desde AWS STS si asumen el rol de IAM mediante una aserción de SAML del proveedor de identidades.

Para federar a los usuarios en plantilla con varias cuentas en su organización de AWS, puede utilizar IAM Identity Center de AWS para administrar de forma centralizada el acceso de los usuarios en plantilla a las Cuentas de AWS y a las aplicaciones. Puede habilitar Identity Center para su organización y configurar el origen de las identidades. IAM Identity Center proporciona un directorio predeterminado de orígenes de identidad que puede utilizar para administrar usuarios y grupos. Como alternativa, puede elegir un origen de identidades externo mediante la conexión con el proveedor de identidades externo con SAML 2.0 y el aprovisionamiento automático de usuarios y grupos con SCIM, o mediante la conexión con el directorio de Microsoft AD a través de Directory Service. Una vez configurado un origen de identidades, puede asignar acceso a Cuentas de AWS a usuarios y grupos al definir políticas de privilegios mínimos en los conjuntos de permisos. Los usuarios en plantilla pueden autenticarse a través de su proveedor de identidades central para iniciar sesión en el portal de acceso de AWS e iniciar sesión de forma única en Cuentas de AWS y en las aplicaciones en la nube que tengan asignadas. Los usuarios pueden configurar la AWS CLI v2 para autenticarse en IAM Identity Center y obtener credenciales para ejecutar comandos de la AWS CLI. Identity Center también permite el acceso mediante inicio de sesión único a aplicaciones de AWS, como Amazon SageMaker AI Studio y portales de AWS IoT Sitewise Monitor.

Tras seguir las instrucciones anteriores, los usuarios en plantilla ya no tendrán que usar grupos y usuarios de IAM para las operaciones normales al administrar las cargas de trabajo en AWS. En cambio, los usuarios y grupos se administran fuera de AWS, y los usuarios pueden acceder a los recursos de AWS como una identidad federada. Las identidades federadas utilizan los grupos definidos por el proveedor de identidades centralizado. Debe identificar y eliminar los grupos de IAM, los usuarios de IAM y las credenciales de usuario de larga duración (contraseñas y claves de acceso) que ya no sean necesarios en sus Cuentas de AWS. Puede encontrar las credenciales sin

usar mediante los informes de credenciales de IAM, eliminar los usuarios de IAM correspondientes y eliminar los grupos de IAM. En su organización, puede aplicar una política de control de servicio (SCP) que ayude a evitar la creación de nuevos usuarios y grupos de IAM, y exigir que el acceso a AWS se haga mediante identidades federadas.

> **Note**
>
> Es su responsabilidad gestionar la rotación de los tokens de acceso de SCIM, tal como se describe en la documentación de Aprovisionamiento automático. Además, es responsable de rotar los certificados que respaldan su federación de identidades.

Orientaciones para los usuarios de sus aplicaciones Puede administrar las identidades de los usuarios de sus aplicaciones, como una aplicación móvil, mediante Amazon Cognito como proveedor de identidades centralizado. Amazon Cognito permite la autenticación, autorización y administración de usuarios para sus aplicaciones móviles y web. Amazon Cognito proporciona un almacén de identidades que se escala a millones de usuarios, admite la federación de identidades sociales y empresariales, y ofrece características de seguridad avanzadas para ayudar a proteger a sus usuarios y a su empresa. Puede integrar su aplicación web o móvil personalizada en Amazon Cognito para agregar autenticación de usuarios y control de acceso a sus aplicaciones en cuestión de minutos. Basado en estándares de identidad abiertos, como SAML y Open ID Connect (OIDC), Amazon Cognito es compatible con varias normativas de cumplimiento y se integra en los recursos de desarrollo de frontend y backend.

Pasos para la implementación

Pasos para los usuarios em plantilla que acceden a AWS

- Federe a los usuarios en plantilla en AWS mediante un proveedor de identidades centralizado con uno de los siguientes enfoques:
  - Utilice IAM Identity Center para habilitar el inicio de sesión único en varias Cuentas de AWS de su organización de AWS mediante la federación con su proveedor de identidades.
  - Utilice IAM para conectar su proveedor de identidades directamente a cada Cuenta de AWS, lo que permite un acceso federado y detallado.
- Identifique y elimine los grupos y usuarios de IAM que se sustituyan por identidades federadas.

Pasos para los usuarios de sus aplicaciones

- Utilice Amazon Cognito como proveedor de identidades centralizado para sus aplicaciones.
- Integre sus aplicaciones personalizadas en Amazon Cognito mediante OpenID Connect y OAuth. Puede desarrollar sus aplicaciones personalizadas mediante las bibliotecas de Amplify, que proporcionan interfaces sencillas para integrarse con una variedad de servicios de AWS, como Amazon Cognito, para la autenticación.

Recursos

Prácticas recomendadas relacionadas:

- SEC02-BP06 Uso de grupos y atributos de usuarios
- SEC03-BP02 Concesión de acceso con privilegios mínimos
- SEC03-BP06 Administración del acceso en función del ciclo de vida

Documentos relacionados:

- Federación de identidades en AWS
- Security best practices in IAM (Prácticas recomendadas de seguridad en IAM)
- Prácticas recomendadas de AWS Identity and Access Management
- Getting started with IAM Identity Center delegated administration
- How to use customer managed policies in IAM Identity Center for advanced use cases
- AWS CLI v2: proveedor de credenciales de IAM Identity Center

Videos relacionados:

- AWS re:Inforce 2022 - AWS Identity and Access Management (IAM) deep dive
- AWS re:Invent 2022 - Simplify your existing workforce access with IAM Identity Center
- AWS re:Invent 2018: Mastering Identity at Every Layer of the Cake

Ejemplos relacionados:

- Workshop: Using AWS IAM Identity Center to achieve strong identity management

Herramientas relacionadas:

- Socios con competencia en seguridad de AWS: Identity and Access Management
- saml2aws

SEC02-BP05 Auditoría y rotación periódicas de las credenciales

Audite y rote las credenciales periódicamente para limitar el tiempo que pueden utilizarse para acceder a los recursos. Las credenciales de larga duración entrañan muchos riesgos, pero estos riesgos pueden reducirse con una rotación frecuente.

Resultado deseado: implemente la rotación de credenciales para ayudar a reducir los riesgos asociados al uso de credenciales a largo plazo. Audita regularmente y corrige la no conformidad con las políticas de rotación de credenciales.

Patrones comunes de uso no recomendados:

- No auditar el uso de credenciales.
- Utilizar credenciales de larga duración de forma innecesaria.
- Utilizar credenciales de larga duración y no rotarlas regularmente.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Cuando no pueda confiar en credenciales temporales y necesite credenciales de larga duración, audítelas para verificar que los controles definidos, por ejemplo, la autenticación multifactor (MFA), se aplican, se rotan periódicamente y tienen el nivel de acceso adecuado.

Es necesario llevar a cabo una validación periódica, preferiblemente mediante una herramienta automatizada, para verificar que se están aplicando los controles correctos. En el caso de las identidades humanas, debe exigir a los usuarios que cambien sus contraseñas periódicamente y retirar las claves de acceso para sustituirlas por credenciales temporales. Al pasar de usuarios de AWS Identity and Access Management (IAM) a identidades centralizadas, puede generar un informe de credenciales para auditar a los usuarios.

También recomendamos que aplique y supervise una configuración de MFA en su proveedor de identidades. Puede configurar Reglas de AWS Config o utilizar estándares de seguridad de AWS Security Hub CSPM para supervisar si los usuarios han configurado la MFA. Si lo considera oportuno, puede utilizar IAM Roles Anywhere para proporcionar credenciales temporales

para identidades de máquinas. En situaciones en las que no sea posible utilizar roles de IAM y credenciales temporales, es necesario llevar a cabo auditorías frecuentes y rotar las claves de acceso.

Pasos para la implementación

- Auditoría periódica de las credenciales: auditar las identidades que están configuradas en el proveedor de identidades e IAM le permite asegurarse de que las únicas identidades que pueden acceder a su carga de trabajo son aquellas que estén autorizadas. Dichas identidades pueden incluir, entre otras, usuarios de IAM, usuarios de AWS IAM Identity Center, usuarios de Active Directory o usuarios de un proveedor de identidades ascendente diferente. Por ejemplo, elimine las personas que abandonen la organización y los roles entre cuentas que ya no sean necesarios. Implante un proceso para auditar periódicamente los permisos a los servicios a los que accede una entidad de IAM. Esto le ayudará a identificar las políticas que debe modificar para eliminar los permisos que no se utilizan. Utilice los informes de credenciales e AWS Identity and Access Management Access Analyzer para auditar las credenciales y los permisos de IAM. Puede usar Amazon CloudWatch para configurar alarmas para llamadas específicas a las API dentro de su entorno de AWS. Además, Amazon GuardDuty puede avisarle de una actividad inesperada, que podría indicar un acceso demasiado permisivo o no intencionado a las credenciales de IAM.
- Rotación periódica de las credenciales: si no puede utilizar credenciales temporales, rote periódicamente las claves de acceso a IAM de larga duración (como máximo cada 90 días). Si se revela una clave de acceso de forma involuntaria sin su conocimiento, esto limita el tiempo durante el que se pueden utilizar las credenciales para acceder a los recursos. Si desea obtener información sobre la rotación de las claves de acceso de los usuarios de IAM, consulte Rotación de las claves de acceso.
- Revisión de los permisos de IAM: para mejorar la seguridad de su Cuenta de AWS, debe revisar y supervisar periódicamente cada una de sus políticas de IAM. Verifique que las políticas sigan el principio del privilegio mínimo.
- Si lo estima oportuno, puede automatizar la creación y las actualizaciones de los recursos de IAM: IAM Identity Center automatiza muchas tareas de IAM, como la administración de roles y políticas. Como alternativa, se puede utilizar AWS CloudFormation para automatizar la implementación de los recursos de IAM, incluidos los roles y las políticas, para reducir la posibilidad de que se produzcan errores humanos, ya que las plantillas se pueden verificar y controlar por versiones.
- Uso de IAM Roles Anywhere para sustituir los usuarios de IAM por identidades de máquinas: IAM Roles Anywhere le permite utilizar roles en áreas que antes no podía utilizar, como en servidores locales. IAM Roles Anywhere utiliza un certificado X.509 de confianza para autenticarse en AWS y

recibir credenciales temporales. El uso de IAM Roles Anywhere evita la necesidad de rotar estas credenciales, ya que las credenciales de larga duración ya no se almacenan en el entorno en las instalaciones. Tenga en cuenta que deberá supervisar y rotar el certificado X.509 a medida que se acerque su fecha de vencimiento.

Recursos

Prácticas recomendadas relacionadas:

- SEC02-BP02 Uso de credenciales temporales
- SEC02-BP03 Almacenamiento y uso seguros de secretos

Documentos relacionados:

- Introducción a AWS Secrets Manager
- Prácticas recomendadas de IAM
- Federación y proveedores de identidades
- Soluciones de socios de seguridad: acceso y control de acceso
- Credenciales de seguridad temporales
- Generación de informes de credenciales para su Cuenta de AWS

Videos relacionados:

- Best Practices for Managing, Retrieving, and Rotating Secrets at Scale
- Managing user permissions at scale with AWS IAM Identity Center
- Mastering identity at every layer of the cake

SEC02-BP06 Uso de grupos y atributos de usuarios

Definir los permisos según los grupos y los atributos de usuarios ayuda a reducir la cantidad y la complejidad de las políticas, lo que facilita la aplicación del principio de privilegio mínimo. Puede emplear los grupos de usuarios para administrar los permisos de muchas personas en un solo lugar según la función que desempeñen en su organización. Los atributos, como el departamento, el proyecto o la ubicación, pueden proporcionar un nivel adicional en el ámbito de los permisos si hay personas que hacen una función similar, pero para diferentes subconjuntos de recursos.

Resultado deseado: puede aplicar cambios en los permisos según la función a todos los usuarios que desempeñen esa función. La pertenencia a grupos y los atributos determinan los permisos de los usuarios, lo que reduce la necesidad de administrar los permisos para cada usuario individual. Los grupos y atributos que defina en su proveedor de identidades (IdP) se propagan automáticamente a sus entornos de AWS.

Patrones comunes de uso no recomendados:

- Administrar los permisos de usuarios individuales y duplicarlos para muchos usuarios.
- Definir grupos en un nivel demasiado alto y conceder permisos demasiado amplios.
- Definir grupos en un nivel demasiado detallado, lo que crea duplicación y confusión en torno a la pertenencia a dichos grupos.
- Usar grupos con permisos duplicados en diversos subconjuntos de recursos cuando, en su lugar, se pueden usar atributos.
- No administrar grupos, atributos y pertenencias a grupos con un proveedor de identidades estandarizado integrado con sus entornos de AWS.
- Usar encadenamiento de roles al utilizar las sesiones del AWS IAM Identity Center.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Los permisos de AWS se definen en documentos denominados políticas que están asociados a una entidad principal, como un usuario, grupo, rol o recurso. Puede escalar la gestión de permisos organizando las asignaciones de permisos (grupo, permisos o cuenta) dependiendo de la función del trabajo, la carga de trabajo y el entorno de SDLC. En el caso de su plantilla, esto le permite definir grupos según la función que desempeñen los usuarios en su organización, en lugar de en virtud de los recursos a los que se accede. Por ejemplo, un grupo de desarrolladores de aplicaciones web puede tener una política adjunta para configurar servicios como Amazon CloudFront dentro de una cuenta de desarrollo. Es posible que un grupo de `AutomationDeveloper` tenga algunos permisos que coincidan con los del grupo de `WebAppDeveloper`. Estos permisos pueden recopilarse en una política independiente y asociarse a ambos grupos, en lugar de permitir que los usuarios de ambas funciones pertenezcan a un grupo de `CloudFrontAccess`.

Además de los grupos, puede utilizar atributos para ampliar el acceso al ámbito. Por ejemplo, puede tener un atributo Proyecto para los usuarios del grupo de `WebAppDeveloper` para limitar el acceso a los recursos específicos de su proyecto. El uso de esta técnica elimina la necesidad de tener

diferentes grupos para los desarrolladores de aplicaciones que trabajen en diferentes proyectos si, por lo demás, sus permisos son los mismos. La forma de hacer referencia a los atributos en las políticas de permisos se basa en su origen, ya sea que estén definidos como parte de su protocolo de federación (como SAML, OIDC o SCIM), como aserciones SAML personalizadas o que se hayan configurado en IAM Identity Center.

Pasos para la implementación

1. Establezca dónde definirá los grupos y los atributos:
   a. Al seguir las instrucciones que se indican en SEC02-BP04 Uso de un proveedor de identidades centralizado, puede determinar si tiene que definir grupos y atributos en el proveedor de identidades, en IAM Identity Center o usar grupos de usuarios de IAM en una cuenta específica.
2. Defina grupos:
   a. Determine los grupos según la función y el ámbito del acceso requerido. Puede utilizar una estructura jerárquica o convenciones de nomenclatura para organizar los grupos de forma eficaz.
   b. Si especifica la definición en IAM Identity Center, cree grupos y asocie el nivel de acceso deseado mediante conjuntos de permisos.
   c. Si especifica la definición con un proveedor de identidades externo, determine si el proveedor admite el protocolo SCIM y plantéese la posibilidad de habilitar el aprovisionamiento automático en IAM Identity Center. Esta capacidad sincroniza la creación, la pertenencia y la eliminación de grupos entre su proveedor e IAM Identity Center.
3. Defina los atributos:
   a. Si utiliza un proveedor de identidades externo, los protocolos SCIM y SAML 2.0 proporcionan ciertos atributos de forma predeterminada. Los atributos adicionales se pueden definir y transferir mediante aserciones de SAML que utilizan el nombre del atributo `https://aws.amazon.com/SAML/Attributes/PrincipalTag`. Consulte la documentación de su proveedor de identidades a fin de conocer las instrucciones necesarias para definir y configurar atributos personalizados.
   b. Si define roles en IAM Identity Center, active la característica de control de acceso basado en atributos (ABAC) y defina los atributos como desee. Debería usar atributos que vayan en consonancia con la estructura o la estrategia de etiquetado de recursos de su organización.

Si necesita encadenar los roles de IAM a partir de los roles de IAM asumidos a través del centro de identidad de IAM, los valores como `source-identity` y `principal-tags` no se propagarán.

Para obtener información más detallada, consulte Habilitación y configuración de atributos para el control de acceso.

1. Los permisos de ámbito se basan en grupos y atributos:
    a. Plantéese la posibilidad de incluir condiciones en las políticas de permisos que comparen los atributos de su entidad principal con los atributos de los recursos a los que se accede. Por ejemplo, puede definir una condición para permitir el acceso a un recurso solo si el valor de una clave de condición `PrincipalTag` coincide con el valor de una clave `ResourceTag` del mismo nombre.
    b. Al definir las políticas de la ABAC, siga las instrucciones de las prácticas recomendadas y ejemplos de autorización de la ABAC.
    c. Revise y actualice periódicamente su estructura de grupos y atributos a medida que evolucionen las necesidades de su organización para garantizar una gestión óptima de los permisos.

Recursos

Prácticas recomendadas relacionadas:

- SEC02-BP04 Uso de un proveedor de identidades centralizado
- SEC03-BP02 Concesión de acceso con privilegios mínimos
- COST02-BP04 Implementación de grupos y roles

Documentos relacionados:

- Prácticas recomendadas de IAM
- Manage Identities in IAM Identity Center
- What Is ABAC for AWS?
- ABAC In IAM Identity Center
- Ejemplos de políticas ABAC

Videos relacionados:

- Managing user permissions at scale with AWS IAM Identity Center
- Mastering identity at every layer of the cake

Administración de permisos

Administre permisos para controlar el acceso a identidades humanas y de máquinas que requieran acceso a AWS y sus cargas de trabajo. Los permisos le permiten controlar a qué puede acceder cada usuario y en qué condiciones. Al establecer permisos para identidades específicas humanas y de máquinas, concede acceso a acciones de servicio específicas en determinados recursos. Asimismo, puede especificar condiciones que deben cumplirse para que se conceda el acceso.

Existen diversas formas de conceder acceso a distintos tipos de recursos. Una forma es mediante el uso de distintos tipos de políticas.

Las políticas basadas en la identidad de IAM se administran o se insertan y se adjuntan a las identidades de IAM, incluidos los usuarios, los grupos o los roles. Estas políticas le permiten especificar lo que esa identidad puede hacer (sus permisos). Las políticas basadas en la identidad también pueden clasificarse de la siguiente manera.

Políticas administradas – Políticas independientes basadas en la identidad que puede adjuntar a varios usuarios, grupos y funciones en su cuenta de AWS. Existen dos tipos de políticas administradas:

- Políticas administradas de AWS: políticas administradas creadas y administradas por AWS.
- Políticas administradas por el cliente: políticas administradas que crea y administra en su cuenta de AWS. Las políticas administradas por el cliente ofrecen un control más preciso de las políticas que las políticas administradas de AWS.

Las políticas administradas son el método preferido para aplicar permisos. Sin embargo, también puede usar políticas insertadas que agrega directamente a un usuario único, grupo o rol. Las políticas insertadas mantienen una relación estricta de uno a uno entre una política y una identidad. Las políticas insertadas se eliminan cuando elimine la identidad.

En la mayoría de los casos, debe crear sus propias políticas administradas por el cliente según el principio de privilegio mínimo.

Las políticas basadas en recursos se asocian a un recurso. Por ejemplo, una política de bucket de S3 es una política basada en recursos. Estas políticas conceden permiso a una entidad principal que puede estar en la misma cuenta que el recurso o en otra cuenta. Para obtener una lista de los servicios compatibles con los permisos basados en recursos, consulte Servicios de AWS que funcionan con IAM.

Los límites de permisos son una política administrada para establecer los permisos máximos que un administrador puede establecer. Esto le permite delegar la capacidad de crear y administrar permisos a los desarrolladores, como, por ejemplo, la creación de un rol de IAM, pero también limitar los permisos que pueden conceder para que no puedan escalar su permiso con la opción que han creado.

El control de acceso basado en atributos (ABAC) en AWS le permite conceder permisos basados en atributos, denominados etiquetas. Estas etiquetas pueden asociarse a entidades principales de IAM (usuarios o roles) y a recursos de AWS. Los administradores pueden crear políticas de IAM reutilizables que aplican permisos en función de los atributos de la entidad principal de IAM. Por ejemplo, un administrador puede usar una única política de IAM que conceda a los desarrolladores de la organización acceso a los recursos de AWS que coincidan con las etiquetas de su proyecto. A medida que el equipo de desarrolladores vaya agregando recursos a los proyectos, los permisos se irán aplicando automáticamente en función de los atributos y ya no será necesario actualizar las políticas de cada recurso.

Las políticas de control de servicio (SCP) de Organizations definen los permisos máximos para los miembros de las cuentas de una organización o unidad organizativa (OU). Las SCP limitan los permisos que las políticas basadas en la identidad o en recursos conceden a las entidades (usuarios o roles) dentro de la cuenta, pero no conceden permisos.

Las políticas de sesión asumen un rol o un usuario federado. Apruebe políticas de sesión al utilizar las políticas de la AWS CLI o API de AWS para limitar los permisos que las políticas basadas en la identidad del rol o el usuario conceden a la sesión. Estas políticas limitan los permisos para una sesión creada, pero no conceden permisos. Para obtener más información, consulte Políticas de sesión.

Prácticas recomendadas

- SEC03-BP01 Definición de los requisitos de acceso
- SEC03-BP02 Concesión de acceso con privilegios mínimos
- SEC03-BP03 Establecimiento de un proceso de acceso de emergencia
- SEC03-BP04 Reducción continua de los permisos
- SEC03-BP05 Definición de las barreras de protección de los permisos para una organización
- SEC03-BP06 Administración del acceso en función del ciclo de vida
- SEC03-BP07 Análisis del acceso público y entre cuentas
- SEC03-BP08 Uso compartido de recursos de forma segura en su organización

- SEC03-BP09 Uso compartido seguro de recursos con terceros

SEC03-BP01 Definición de los requisitos de acceso

Los administradores, los usuarios finales u otros componentes deben acceder a cada componente o recurso de la carga de trabajo. Establezca una definición clara de quién o qué debe tener acceso a cada componente y elija el tipo de identidad y el método de autenticación y autorización adecuados.

Patrones comunes de uso no recomendados:

- Codificar de forma rígida o almacenar secretos en la aplicación.
- Conceder permisos personalizados para cada usuario.
- Utilizar credenciales de larga duración.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Los administradores, los usuarios finales u otros componentes deben acceder a cada componente o recurso de la carga de trabajo. Establezca una definición clara de quién o qué debe tener acceso a cada componente y elija el tipo de identidad y el método de autenticación y autorización adecuados.

El acceso periódico a las Cuentas de AWS dentro de una organización debe proporcionarse mediante acceso federado o un proveedor de identidades centralizado. También debe centralizar la administración de identidades y asegurarse de que existe una práctica establecida para integrar el acceso de AWS al ciclo de vida de los empleados. Por ejemplo, cuando un empleado cambia a un cargo con un nivel de acceso distinto, su pertenencia al grupo también debe cambiar para reflejar los nuevos requisitos de acceso.

Al definir los requisitos de acceso para las identidades que no son humanas, determine qué aplicaciones y componentes necesitan acceso y cómo se conceden los permisos. El enfoque recomendado es utilizar roles de IAM creados con el modelo de acceso de privilegio mínimo. AWS Las políticas administradas proporcionan políticas de IAM predefinidas que cubren los casos de uso más comunes.

Los servicios de AWS, como AWS Secrets Manager y el Almacén de parámetros de AWS Systems Manager, pueden ayudar a desvincular los secretos de la aplicación o la carga de trabajo de forma segura. En Secrets Manager, puede establecer una rotación automática de las credenciales. Puede utilizar Systems Manager para hacer referencia a los parámetros en los scripts, comandos,

documentos SSM, configuración y flujos de trabajo de automatización con el nombre único que especificó al crear el parámetro.

Puede utilizar AWS IAM Roles Anywhere para obtener credenciales de seguridad temporales en IAM para cargas de trabajo que se ejecutan fuera de AWS. Las cargas de trabajo pueden usar las mismas políticas de IAM y roles de IAM que utiliza con las aplicaciones de AWS para acceder a los recursos de AWS.

Siempre que sea posible, se deben preferir las credenciales temporales a corto plazo en lugar de las credenciales estáticas a largo plazo. En aquellas situaciones en las que necesite usuarios con acceso programático y credenciales de larga duración, utilice la información de la última clave de acceso utilizada para rotar y eliminar las claves de acceso.

Los usuarios necesitan acceso programático si desean interactuar con AWS fuera de la Consola de administración de AWS. La forma de conceder el acceso programático depende del tipo de usuario que acceda a AWS.

Para conceder acceso programático a los usuarios, seleccione una de las siguientes opciones.

¿Qué usuario necesita acceso programático?	Para	Mediante
IAM	(Recomendado) Use credenciales de consola como credenciales temporales para firmar las solicitudes programáticas a la AWS CLI, los AWS SDK y las API de AWS.	Siga las instrucciones de la interfaz que desea utilizar: • Para la AWS CLI, consulte Iniciar sesión para el desarrollo local de AWS en la Guía del usuario de AWS Command Line Interface. • Para los AWS SDK, consulte Iniciar sesión para el desarrollo local de AWS en la Guía de referencia de AWS SDK y herramientas.
Identidad del personal	Utiliza credenciales temporales para firmar las solicitudes programáticas a la AWS CLI,	Siga las instrucciones de la interfaz que desea utilizar:

¿Qué usuario necesita acceso programático?	Para	Mediante
(Usuarios administrados en el IAM Identity Center)	los AWS SDK y las API de AWS.	• Para utilizar la AWS CLI, consulte Configuring the AWS CLI to usa AWS IAM Identity Center en la Guía del usuario de AWS Command Line Interface. • Para usar AWS SDK, las herramientas y las API de AWS, consulta IAM Identity Center authentication en la Guía de referencia del SDK y las herramientas de AWS.
IAM	Utiliza credenciales temporales para firmar las solicitudes programáticas a la AWS CLI, los AWS SDK y las API de AWS.	Siguiendo las instrucciones de Uso de credenciales temporales con recursos de AWS de la Guía del usuario de IAM.

¿Qué usuario necesita acceso programático?	Para	Mediante
IAM	(No recomendado) Utilizar credenciales a largo plazo para firmar las solicitud es programáticas a la AWS CLI, los AWS SDK o las API de AWS.	Siga las instrucciones de la interfaz que desea utilizar: • Para la AWS CLI, consulte Autenticación mediante credenciales de usuario de IAM en la Guía del usuario de AWS Command Line Interface. • Para ver los AWS SDK y las herramientas, consulte Autenticar mediante credenciales a largo plazo en la Guía de referencia de AWS SDK y herramientas. • Para las API de AWS, consulta Administración de claves de acceso para usuarios de IAM en la Guía del usuario de IAM.

Recursos

Documentos relacionados:

- Control de acceso basado en atributos (ABAC)
- AWS IAM Identity Center
- IAM Roles Anywhere
- AWS Managed policies for IAM Identity Center
- AWS IAM policy conditions
- IAM use cases
- Revisar y eliminar periódicamente usuarios, roles, permisos, políticas y credenciales no utilizados

- Uso de políticas de
- How to control access to AWS resources based on Cuenta de AWS, OU, or organization
- Identify, arrange, and manage secrets easily using enhanced search in AWS Secrets Manager

Videos relacionados:

- Become an IAM Policy Master in 60 Minutes or Less
- Separation of Duties, Least Privilege, Delegation, and CI/CD
- Streamlining identity and access management for innovation

SEC03-BP02 Concesión de acceso con privilegios mínimos

Conceda exclusivamente el acceso que las identidades necesitan para efectuar acciones concretas en recursos específicos en determinadas condiciones. Utilice atributos de grupo y de identidad para configurar dinámicamente los permisos en función de las necesidades en lugar de configurarlos para cada usuario. Por ejemplo, puede conceder acceso a un grupo de desarrolladores para que solamente puedan administrar recursos de su proyecto. De este modo, si un desarrollador abandona el proyecto, su acceso se revoca automáticamente sin cambiar las políticas de acceso subyacentes.

Resultado deseado: los usuarios solo tienen los permisos mínimos necesarios para el trabajo específico que desempeñan. Utiliza Cuentas de AWS independientes para aislar a los desarrolladores de los entornos de producción. Cuando los desarrolladores necesitan acceder a los entornos de producción para realizar tareas específicas, solo se les concede un acceso limitado y controlado durante el tiempo que se necesita para esas tareas. Su acceso a la producción se revoca inmediatamente después de completar el trabajo necesario. Realiza revisiones periódicas de los permisos y los revoca de inmediato cuando ya no son necesarios; por ejemplo, cuando un usuario cambia de rol o deja la organización. Restringe los privilegios de administrador a un grupo pequeño y de confianza para reducir la exposición al riesgo. Concede a las cuentas de máquinas o sistemas los permisos mínimos necesarios para realizar las tareas previstas.

Patrones comunes de uso no recomendados:

- Concede permisos de administrador a los usuarios de forma predeterminada.
- Utiliza la cuenta de usuario raíz para tareas cotidianas.
- Crea políticas demasiado permisivas sin un alcance adecuado.
- Revisa sus permisos con poca frecuencia, lo que provoca un aumento excesivo de los permisos.

- Aísla el entorno o gestiona los permisos basándose exclusivamente en un control de acceso basado en atributos.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

El principio del privilegio mínimo establece que a las identidades solo se les debe permitir llevar a cabo el conjunto más reducido de acciones necesarias para efectuar una tarea específica. De este modo, se equilibra la facilidad de uso, la eficiencia y la seguridad. Operar según este principio contribuye a limitar el acceso involuntario y a hacer el seguimiento de quién tiene acceso a determinados recursos. Los usuarios y los roles de IAM no tienen permisos de forma predeterminada. De forma predeterminada, el usuario raíz tiene acceso total y debe controlarse y supervisarse rigurosamente, y utilizarse únicamente para las tareas que requieren acceso raíz.

Las políticas de IAM se usan para conceder permisos a roles de IAM o recursos específicos. Por ejemplo, las políticas basadas en la identidad se pueden adjuntar a grupos de IAM, mientras que los buckets de S3 se pueden controlar mediante políticas basadas en recursos.

Al crear una política de IAM, puede especificar las acciones de servicio, los recursos y las condiciones que se deben cumplir para que AWS permita o deniegue el acceso. AWS es compatible con una amplia variedad de condiciones que lo ayudarán a acotar el acceso. Por ejemplo, al usar la clave de condición PrincipalOrgID, puede denegar acciones si el solicitante no forma parte de su organización de AWS.

También puede controlar las solicitudes que hagan los servicios de AWS en su nombre, como que AWS CloudFormation cree una función de AWS Lambda, mediante la clave de condición CalledVia. Puede estratificar los diferentes tipos de políticas para establecer una defensa en profundidad y limitar los permisos generales de sus usuarios. También puede restringir qué permisos se pueden conceder y en qué condiciones. Por ejemplo, puede permitir que sus equipos de carga de trabajo creen sus propias políticas de IAM para los sistemas que creen, pero solo si aplican también un límite de permisos para determinar el número máximo de permisos que el sistema puede recibir.

Pasos para la implementación

- Implementación de políticas de privilegio mínimo: asigne políticas de acceso con privilegio mínimo a los grupos y roles de IAM para reflejar el rol o la función del usuario que haya definido.

- Aísle los entornos de desarrollo y de producción separando las Cuentas de AWS: utilice Cuentas de AWS distintas para los entornos de desarrollo y los de producción y controle el acceso entre ellos mediante políticas de control de servicios, políticas de recursos y políticas de identidad.
- Uso de las API como base de las políticas: una forma de determinar los permisos necesarios consiste en revisar los registros de AWS CloudTrail. Esta revisión le permite crear permisos adaptados a las acciones que el usuario lleva a cabo en AWS. El Analizador de acceso de IAM puede generar automáticamente una política de IAM basada en la actividad de acceso. Puede utilizar el asesor de acceso de IAM en la organización o en la cuenta para hacer un seguimiento de la información a la que se accedió por última vez en relación con una política concreta.
- Puede usar políticas administradas por AWS para funciones de trabajo: cuando empiece a crear políticas de permisos detalladas, puede ser útil usar políticas administradas por AWS para funciones de trabajo comunes, como facturación, administradores de bases de datos y científicos de datos. Estas políticas pueden servir para limitar el acceso que tienen los usuarios al mismo tiempo que se determina cómo implementar las políticas de privilegio mínimo.
- Elimine los permisos innecesarios: detecte y elimine las entidades, credenciales y permisos de IAM no utilizados para cumplir con el principio de privilegios mínimos. Puede utilizar Analizador de acceso de IAM para identificar el acceso externo y el no utilizado, y la generación de políticas de Analizador de acceso de IAM puede ayudar a afinar las políticas de permisos.
- Garantía de que los usuarios tengan un acceso limitado a los entornos de producción: los usuarios solo deben tener acceso a los entornos de producción con un caso de uso válido. Después de que el usuario lleve a cabo las tareas específicas que requieren el acceso a producción, se debe revocar el acceso. La limitación del acceso a los entornos de producción previene los eventos involuntarios que afectan a la producción y reduce el ámbito de las consecuencias del acceso involuntario.
- Plantéese utilizar límites de permisos: un límite de permisos es una característica avanzada que permite utilizar una política administrada para establecer los permisos máximos que una política basada en identidades puede conceder a una entidad de IAM. Un límite de permisos para una entidad le posibilita realizar las acciones que le permitan tanto sus políticas basadas en identidad como sus límites de permisos.
- Limite el acceso mediante el control de acceso basado en atributos y las etiquetas de recursos: el control de acceso basado en atributos (ABAC) que utiliza etiquetas de recursos se puede utilizar para refinar los permisos cuando es compatible. Puede utilizar un modelo ABAC que compare las etiquetas principales con las etiquetas de recursos para refinar el acceso en función de las dimensiones personalizadas que defina. Este método puede simplificar y reducir la cantidad de políticas de permisos en su organización.

    - Se recomienda utilizar ABAC únicamente para el control de accesos cuando tanto las entidades principales como los recursos sean propiedad de su organización de AWS. Las partes externas pueden usar los mismos nombres y valores de etiqueta que su organización para sus propias entidades principales y recursos. Si concede acceso a las entidades principales o los recursos de terceros basándose únicamente en estos pares de nombre-valor, podría conceder permisos que no desea conceder.
- Utilizar políticas de control de servicios para AWS Organizations: las políticas de control de servicios controlan de forma centralizada el máximo de permisos disponibles para las cuentas de los miembros de su organización. Es importante destacar que puede utilizar las políticas de control de servicios para restringir los permisos del usuario raíz en las cuentas de los miembros. Considere también la posibilidad de utilizar AWS Control Tower, que proporciona controles prescriptivos administrados que enriquecen AWS Organizations. También puede definir sus propios controles en Control Tower.
- Establecimiento de una política de ciclo de vida de los usuarios para su organización: las políticas de ciclo de vida de los usuarios definen las tareas que deben llevarse a cabo cuando los usuarios se incorporan a AWS, cuando cambian de rol o ámbito de trabajo, o cuando ya no necesitan acceder a AWS. Realice revisiones de permisos en cada paso del ciclo de vida de un usuario para verificar si son restrictivos de forma correcta y para evitar la acumulación de permisos.
- Establecimiento de una programación periódica para revisar los permisos y eliminar los que no sean necesarios: debe revisar periódicamente el acceso de los usuarios para comprobar que no tengan un acceso demasiado permisivo. AWS Config y el Analizador de acceso de IAM pueden ayudarlo durante las auditorías de permisos.
- Establecimiento de una matriz de roles de trabajo: una matriz de roles de trabajo permite visualizar las distintas funciones y niveles de acceso necesarios en su entorno de AWS. Con una matriz de roles de trabajo, puede definir y separar los permisos según las responsabilidades de usuario en su organización. Utilice grupos en lugar de aplicar los permisos directamente a los usuarios o roles individuales.

Recursos

Documentos relacionados:

- Aplicar permisos de privilegios mínimos
- Límites de permisos para las entidades de IAM
- Techniques for writing least privilege IAM policies

- IAM Access Analyzer makes it easier to implement least privilege permissions by generating IAM policies based on access activity
- Delegate permission management to developers by using IAM permissions boundaries
- Perfeccionar los permisos con la información sobre los últimos accesos
- Tipos de políticas de IAM y cuándo usarlas
- Probar las políticas de IAM con el simulador de política de IAM
- Guardrails in AWS Control Tower
- Zero Trust architectures: An AWS perspective
- How to implement the principle of least privilege with CloudFormation StackSets
- Control de acceso basado en atributos (ABAC)
- Reducción del ámbito de las políticas mediante la consulta de la actividad de los usuarios
- Visualización del acceso a los roles
- Utilizar el etiquetado para organizar el entorno e impulsar la responsabilidad
- AWS Tagging Strategies
- Etiquetado de recursos de AWS

Videos relacionados:

- Next-generation permissions management
- Zero Trust: An AWS perspective

SEC03-BP03 Establecimiento de un proceso de acceso de emergencia

Cree un proceso que permita el acceso de emergencia a sus cargas de trabajo en el caso improbable de que se produzca un problema con su proveedor de identidades centralizado.

Debe diseñar procesos para diferentes modos de error que puedan provocar un evento de emergencia. Por ejemplo, en circunstancias normales, los usuarios de la plantilla se federan en la nube mediante un proveedor de identidades centralizado (SEC02-BP04) para administrar sus cargas de trabajo. Sin embargo, si su proveedor de identidades centralizado no responde o se modifica la configuración de la federación en la nube, es posible que los usuarios de la plantilla no puedan federarse en esta. Un proceso de acceso de emergencia permite a los administradores autorizados acceder a los recursos de la nube a través de medios alternativos (como una forma alternativa de

federación o acceso directo de los usuarios) para solucionar problemas con la configuración de la federación o las cargas de trabajo. El proceso de acceso de emergencia se utiliza hasta que se restablezca el mecanismo de federación normal.

Resultado deseado:

- Ha definido y documentado los modos de error que se consideran una emergencia: tenga en cuenta sus circunstancias normales y los sistemas de los que dependen los usuarios para administrar sus cargas de trabajo. Considere cómo cada una de estas dependencias puede no funcionar y provocar una situación de emergencia. Es posible que las preguntas y las prácticas recomendadas del pilar de fiabilidad resulten útiles para identificar los modos de error y diseñar sistemas más resilientes para minimizar la probabilidad de errores.
- Ha documentado los pasos que se deben seguir para confirmar que el error se trata de un caso de emergencia. Por ejemplo, puede solicitar a sus administradores de identidades que comprueben el estado de sus proveedores de identidades principales y en espera y, si ninguno estuviera disponible, declarar un evento de emergencia por error en el proveedor de identidades.
- Ha definido un proceso de acceso de emergencia concreto para cada tipo de modo de emergencia o error. La especificidad puede reducir la tentación de los usuarios de abusar de un proceso general para todo tipo de emergencias. Los procesos de acceso de emergencia describen las circunstancias en las que se debe utilizar cada proceso y, por otra parte, las situaciones en las que no se debe utilizar el proceso y señala los procesos alternativos que podrían aplicarse.
- Sus procesos están bien documentados con instrucciones detalladas y manuales de estrategias que se pueden seguir de forma rápida y eficiente. Recuerde que un evento de emergencia puede resultar estresante para sus usuarios, ya que pueden estar sometidos a una fuerte presión de plazos, por lo que debe diseñar su proceso de la manera más sencilla posible.

Patrones comunes de uso no recomendados:

- No tiene procesos de acceso de emergencia bien documentados y probados. Cuando los usuarios no están preparados para emergencias, siguen procesos improvisados cuando estas se producen.
- Tener procesos de acceso de emergencia que dependan de los mismos sistemas (como un proveedor de identidades centralizado) que sus mecanismos de acceso normales. Esto significa que el error de un sistema de este tipo podría afectar tanto a sus mecanismos de acceso normales como a los de emergencia y, por lo tanto, repercutir en la capacidad para recuperarse del error.
- Se utilizan los procesos de acceso de emergencia en situaciones que no son de emergencia. Por ejemplo, los usuarios suelen hacer un uso inapropiado de los procesos de acceso de

emergencia, ya que les resulta más fácil hacer cambios directamente que enviarlos a través de una canalización.

- Tener procesos de acceso de emergencia que no generan registros suficientes para auditar los procesos o no supervisar los registros para alertar de un posible uso indebido de los procesos.

Beneficios de establecer esta práctica recomendada:

- Contar con procesos de acceso de emergencia bien documentados y probados puede reducir el tiempo que tardan los usuarios en responder y resolver un evento de emergencia. Esto puede reducir el tiempo de inactividad y aumentar la disponibilidad de los servicios que presta a sus clientes.
- Puede hacer un seguimiento de cada solicitud de acceso de emergencia y detectar intentos no autorizados de uso indebido de los procesos para eventos que no sean de emergencia y alertar sobre estos.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Esta sección proporciona guías para crear procesos de acceso de emergencia para varios modos de error relacionados con las cargas de trabajo implementadas en AWS, comenzando con una guía común que se aplica a todos los modos de error y siguiendo con una guía específica basada en el tipo de modo de error.

Guía común para todos los modos de error

Tenga en cuenta lo siguiente al diseñar un proceso de acceso de emergencia para un modo de error:

- Documente las condiciones previas y los supuestos del proceso, es decir, cuándo el proceso debe o no debe aplicarse. Esto ayuda a detallar el modo de error y a documentar los supuestos, como el estado de otros sistemas relacionados. Por ejemplo, el proceso del modo de error 2 da por sentado que el proveedor de identidades está disponible, pero que la configuración activada en AWS se ha modificado o ha caducado.
- Cree de antemano los recursos necesarios para el proceso de acceso de emergencia (SEC10-BP05). Por ejemplo, cree de antemano el acceso de emergencia a la Cuenta de AWS con roles y usuarios de IAM, y los roles de IAM entre cuentas en todas las cuentas de la carga de trabajo. Esto asegurará que estos recursos estén listos y disponibles cuando ocurra una emergencia. Al crear previamente los recursos, no dependerá de las API del plano de control de AWS (que se utilizan

para crear y modificar recursos de AWS) que pueden no estar disponibles en caso de emergencia. Además, al crear previamente los recursos de IAM, no es necesario tener en cuenta los posibles retrasos debidos a una posible coherencia.

- Incluya los procesos de acceso de emergencia como parte de sus planes de administración de incidentes (SEC10-BP02). Documente cómo se hace el seguimiento de los eventos de emergencia y cómo se comunican a otros miembros de su organización, como los equipos de compañeros o la dirección y, cuando corresponda, externamente a sus clientes y socios comerciales.
- Defina el proceso de solicitud de acceso de emergencia en su sistema de flujo de trabajo de solicitudes de servicio existente, si dispone de uno. Por lo general, estos sistemas de flujo de trabajo le permiten crear formularios de entrada para recopilar información sobre la solicitud, hacer un seguimiento de la solicitud en cada etapa del flujo de trabajo y agregar pasos de aprobación automatizados y manuales. Relacione cada solicitud con el correspondiente evento de emergencia registrado en su sistema de administración de incidentes. Disponer de un sistema uniforme para los accesos de emergencia le permite hacer un seguimiento de esas solicitudes en un solo sistema, analizar las tendencias de uso y mejorar sus procesos.
- Compruebe que solo los usuarios autorizados puedan iniciar los procesos de acceso de emergencia y que estos procesos requieran la aprobación de los compañeros del usuario o de la dirección, según corresponda. El proceso de aprobación debe funcionar de manera eficaz, tanto dentro como fuera del horario laboral. Defina cómo admiten las solicitudes de aprobación aprobadores secundarios si los principales no están disponibles y cómo se escalan en la cadena de administración hasta la aprobación.
- Implemente mecanismos sólidos de registro, monitoreo y alerta para el proceso y los mecanismos de acceso de emergencia. Genere registros y eventos de auditoría detallados para los intentos correctos e infructuosos de obtener acceso de emergencia. Correlacione la actividad con los eventos de emergencia en curso de su sistema de administración de incidentes e inicie alertas cuando se produzcan acciones fuera de los periodos de tiempo esperados o cuando se use la cuenta de acceso de emergencia durante las operaciones normales. Solo se debe acceder a la cuenta de acceso de emergencia durante las emergencias, ya que los procedimientos acceso excepcional pueden considerarse una puerta trasera. Intégrela con su herramienta de gestión de eventos e información de seguridad (SIEM) o AWS Security Hub CSPM para informar y auditar todas las actividades durante el periodo de acceso de emergencia. Al volver al funcionamiento normal, cambie automáticamente las credenciales de acceso de emergencia y avise a los equipos pertinentes.
- Pruebe los procesos de acceso de emergencia de manera periódica para verificar que los pasos estén claros y garantizar el nivel de acceso correcto de manera rápida y eficiente. Sus procesos de

acceso de emergencia deben probarse como parte de las simulaciones de respuesta a incidentes (SEC10-BP07) y las pruebas de recuperación de desastres (REL13-BP03).

Modo de error 1: el proveedor de identidades utilizado para federarse en AWS no está disponible

Tal como se describe en SEC02-BP04 Uso de un proveedor de identidades centralizado, recomendamos confiar en un proveedor de identidades centralizado para federar a los usuarios de su plantilla y concederles acceso a las Cuentas de AWS. La federación se puede configurar a varias Cuentas de AWS de su organización de AWS con IAM Identity Center, o bien puede configurar la federación a Cuentas de AWS individuales mediante IAM. En ambos casos, los usuarios de la plantilla se autentican con su proveedor de identidades centralizado antes de que se les redirija a un punto de conexión de inicio de sesión de AWS para el inicio de sesión único.

En el caso poco probable de que su proveedor de identidades centralizado no esté disponible, los usuarios de la plantilla no podrán federarse en las Cuentas de AWS ni administrar sus cargas de trabajo. En este caso de emergencia, puede proporcionar un proceso de acceso de emergencia para que un pequeño grupo de administradores acceda a las Cuentas de AWS con el fin de llevar a cabo tareas cruciales que no puedan esperar a que sus proveedores de identidades centralizados vuelvan a estar disponibles. Por ejemplo, su proveedor de identidades no estará disponible durante 4 horas y, durante ese periodo, necesita modificar los límites superiores de un grupo de Amazon EC2 Auto Scaling en una cuenta de producción para gestionar un aumento inesperado en el tráfico de clientes. Los administradores de emergencias deben seguir el proceso de acceso de emergencia para acceder a la Cuenta de AWS de producción específica y hacer los cambios necesarios.

El proceso de acceso de emergencia se basa en una Cuenta de AWS de acceso de emergencia creada de antemano que se utiliza únicamente para el acceso de emergencia y dispone de recursos de AWS (como los usuarios y roles de IAM) para respaldar el proceso de acceso de emergencia. Durante las operaciones normales, nadie debe acceder a la cuenta de acceso de emergencia y usted debe supervisar y alertar sobre el uso indebido de esta cuenta (para obtener más información, consulte la sección anterior de guía común).

La cuenta de acceso de emergencia tiene roles de IAM de acceso de emergencia con permisos para asumir roles entre cuentas en las Cuentas de AWS que requieran acceso de emergencia. Estos roles de IAM se crean de antemano y se configuran con políticas de confianza que confían en los roles de IAM de la cuenta de emergencia.

El proceso de acceso de emergencia puede utilizar uno de los siguientes enfoques:

- Puede crear previamente un conjunto de usuarios de IAM para sus administradores de emergencia en la cuenta de acceso de emergencia con contraseñas seguras y tokens de MFA asociados. Estos usuarios de IAM tienen permisos para asumir los roles de IAM que, entonces, permiten el acceso entre cuentas a la Cuenta de AWS donde se requiere el acceso de emergencia. Recomendamos crear el menor número posible de usuarios y asignar cada usuario a un único administrador de emergencias. Durante una emergencia, un usuario administrador de emergencias inicia sesión en la cuenta de acceso de emergencia con su contraseña y el código de token de MFA, cambia el rol de IAM de acceso de emergencia en la cuenta de emergencia y, finalmente, cambia el rol de IAM de acceso de emergencia en la cuenta de carga de trabajo para llevar a cabo la acción de cambio de emergencia. La ventaja de este enfoque es que cada usuario de IAM se asigna a un administrador de emergencias y usted puede saber qué usuario inició sesión al revisar los eventos de CloudTrail. La desventaja es que hay que mantener varios usuarios de IAM con sus contraseñas de larga duración y tokens de MFA asociados.
- Puede usar el usuario raíz de Cuenta de AWS de acceso de emergencia para iniciar sesión en la cuenta de acceso de emergencia, asumir el rol de IAM de acceso de emergencia y asumir el rol entre cuentas en la cuenta de carga de trabajo. Recomendamos configurar una contraseña segura y varios tokens de MFA para el usuario raíz. También recomendamos almacenar la contraseña y los tokens de MFA en un almacén de credenciales empresarial seguro que aplique una autenticación y una autorización sólidas. Debe proteger los factores de restablecimiento de la contraseña y el token de MFA. Para ello, establezca la dirección de correo electrónico de la cuenta en una lista de distribución de correo electrónico supervisada por los administradores de seguridad en la nube y el número de teléfono de la cuenta en un número de teléfono compartido también supervisado por los administradores de seguridad. La ventaja de este enfoque es que solo hay que administrar un conjunto de credenciales de usuario raíz. La desventaja es que, dado que se trata de un usuario compartido, es posible que varios administradores inicien sesión como usuario raíz. Debe auditar los eventos de registro del almacén empresarial para identificar qué administrador extrajo la contraseña del usuario raíz.

Modo de error 2: la configuración del proveedor de identidades en AWS se ha modificado o ha caducado

Para permitir que los usuarios de la plantilla se federen en Cuentas de AWS, puede configurar IAM Identity Center con un proveedor de identidades externo o crear un proveedor de identidades de IAM (SEC02-BP04). Por lo general, estos se configuran al importar un documento XML de metadatos de SAML que proporciona el proveedor de identidades. El documento XML de metadatos incluye un

certificado X.509 que corresponde a una clave privada que el proveedor de identidades utiliza para firmar sus aserciones SAML.

Un administrador podría modificar o eliminar estas configuraciones de AWS de forma accidental. En otro escenario, el certificado X.509 importado a AWS podría caducar cuando aún no se ha importado a AWS un nuevo XML de metadatos con un certificado nuevo. Ambas situaciones pueden desbaratar la federación a AWS de los usuarios de la plantilla y provocar una emergencia.

En un caso de emergencia de este tipo, puede proporcionar a sus administradores de identidades acceso a AWS para solucionar los problemas de federación. Por ejemplo, el administrador de identidades utiliza el proceso de acceso de emergencia para iniciar sesión en la Cuenta de AWS de acceso de emergencia, cambia a un rol en la cuenta de administrador del centro de identidades y actualiza la configuración del proveedor de identidades externo al importar el último documento XML de metadatos SAML de su proveedor de identidades para volver a habilitar la federación. Una vez que se corrija la federación, los usuarios de la plantilla seguirán utilizando el proceso operativo normal para federarse en sus cuentas de carga de trabajo.

Puede seguir los enfoques detallados en el modo de error 1 anterior para crear un proceso de acceso de emergencia. Puede conceder permisos con privilegios mínimos a sus administradores de identidades para que accedan únicamente a la cuenta de administrador del centro de identidades y lleven a cabo acciones en el centro de identidades en esa cuenta.

Modo de error 3: interrupción del centro de identidades

En el caso poco probable de que se produzca una interrupción en IAM Identity Center o en una Región de AWS, le recomendamos que establezca una configuración que pueda utilizar para proporcionar acceso temporal a la Consola de administración de AWS.

El proceso de acceso de emergencia utiliza la federación directa desde su proveedor de identidades a IAM en una cuenta de emergencia. Para obtener información detallada sobre el proceso y las consideraciones de diseño, consulte Set up emergency access to the Consola de administración de AWS.

Pasos para la implementación

Pasos comunes para todos los modos de error

- Cree una Cuenta de AWS dedicada a los procesos de acceso de emergencia. Cree de antemano los recursos de IAM necesarios en la cuenta, como roles de IAM o usuarios de IAM, y opcionalmente, proveedores de identidades de IAM. Además, cree de antemano roles de IAM entre cuentas en las Cuentas de AWS de la carga de trabajo con relaciones de confianza

con los roles de IAM correspondientes en la cuenta de acceso de emergencia. Puede usar CloudFormation StackSets con AWS Organizations para crear dichos recursos en las cuentas de los miembros de su organización.

- Cree políticas de control de servicio (SCP) de AWS Organizations para denegar la eliminación y modificación de los roles de IAM entre cuentas en las Cuentas de AWS de miembros.
- Habilite CloudTrail para la Cuenta de AWS de acceso de emergencia y envíe los eventos de ruta a un bucket de S3 central en su Cuenta de AWS de recopilación de registros. Si utiliza AWS Control Tower para configurar y gobernar su entorno multicuenta de AWS, cada cuenta que cree con AWS Control Tower o inscriba en AWS Control Tower tendrá CloudTrail habilitado de forma predeterminada y se enviará a un bucket de S3 en una Cuenta de AWS de archivo de registro dedicada.
- Supervise la actividad de la cuenta de acceso de emergencia mediante la creación de reglas de EventBridge que concuerden con el inicio de sesión de la consola y la actividad de la API por parte de los roles de IAM de emergencia. Envíe notificaciones a su centro de operaciones de seguridad cuando se produzca actividad fuera de un evento de emergencia continuo registrado en su sistema de administración de incidentes.

Pasos adicionales para el modo de error 1: el proveedor de identidades utilizado para federarse en AWS no está disponible y el modo de error 2: la configuración del proveedor de identidades en AWS se ha modificado o ha caducado

- Cree de antemano los recursos en función del mecanismo que elija para el acceso de emergencia:
  - Uso de usuarios de IAM: cree de antemano los usuarios de IAM con contraseñas seguras y los dispositivos MFA asociados.
  - Uso del usuario raíz de la cuenta de emergencia: configure el usuario raíz con una contraseña segura y almacene la contraseña en el almacén de credenciales de su empresa. Asocie varios dispositivos MFA físicos al usuario raíz y almacene los dispositivos en lugares a los que puedan acceder rápidamente los miembros de su equipo de administradores de emergencias.

Pasos adicionales para el modo de error 3: interrupción del centro de identidades

- Tal como se describe en Set up emergency access to the Consola de administración de AWS, en la Cuenta de AWS de acceso de emergencia, cree un proveedor de identidades de IAM para habilitar la federación SAML directa desde su proveedor de identidades.

- Cree grupos de operaciones de emergencia en su IdP sin miembros.
- Cree los roles de IAM correspondientes a los grupos de operaciones de emergencia en la cuenta de acceso de emergencia.

Recursos

Prácticas recomendadas de Well-Architected relacionadas:

- SEC02-BP04 Uso de un proveedor de identidades centralizado
- SEC03-BP02 Concesión de acceso con privilegios mínimos
- SEC10-BP02 Desarrollo de planes de administración de incidentes
- SEC10-BP07 Ejecución de simulaciones

Documentos relacionados:

- Set up emergency access to the Consola de administración de AWS
- Concesión de acceso a la a los usuarios federados SAML Consola de administración de AWS
- Break glass access

Videos relacionados:

- AWS re:Invent 2022 - Simplify your existing workforce access with IAM Identity Center
- AWS re:Inforce 2022 - AWS Identity and Access Management (IAM) deep dive

Ejemplos relacionados:

- AWS Break Glass Role
- AWS customer playbook framework
- AWS incident response playbook samples

SEC03-BP04 Reducción continua de los permisos

A medida que los equipos determinen qué acceso es necesario, elimine los permisos innecesarios y establezca procesos de revisión para conseguir permisos con privilegios mínimos. Supervise

y elimine continuamente las identidades y los permisos que no se utilicen, tanto para el acceso humano como para el de las máquinas.

Resultado deseado: las políticas de permisos deben cumplir con el principio de privilegio mínimo. A medida que se definan mejor las responsabilidades y los roles del trabajo, debe revisar sus políticas de permisos para eliminar los permisos innecesarios. Este enfoque reduce el alcance del impacto en caso de que las credenciales se expongan de forma inadvertida o se acceda a ellas sin autorización.

Patrones comunes de uso no recomendados:

- Conceder permisos de administrador a los usuarios de forma predeterminada.
- Crear políticas excesivamente permisivas, pero sin todos los privilegios de administrador.
- Mantener políticas de permisos después de que ya no son necesarias.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Cuando los equipos y los proyectos están dando sus primeros pasos, utilizar unas políticas de permisos permisivas sirve para fomentar la innovación y la agilidad. Por ejemplo, en un entorno de desarrollo o de pruebas, se puede dar acceso a los desarrolladores a un amplio conjunto de servicios de AWS. Recomendamos que evalúe el acceso continuamente y lo restrinja únicamente a aquellos servicios y acciones de servicio que sean necesarios para llevar a cabo el trabajo actual. Recomendamos llevar a cabo esta evaluación tanto para las identidades humanas como para las de máquina. Las identidades de máquina, que a veces se denominan cuentas del sistema o del servicio, son identidades que dan acceso a AWS a aplicaciones o servidores. Este acceso es especialmente importante en un entorno de producción, donde unos permisos demasiado permisivos pueden tener un impacto enorme y el potencial de exponer los datos de los clientes.

AWS tiene numerosos métodos para ayudar a identificar a los usuarios, roles, permisos y credenciales no utilizados. AWS también puede ayudar a analizar la actividad de acceso de los usuarios y roles de IAM, incluidas las claves de acceso asociadas, y el acceso a recursos de AWS, como los objetos de los buckets de Amazon S3. La generación de políticas de AWS Identity and Access Management Access Analyzer puede ayudarle a crear políticas de permisos restrictivas basadas en los servicios y acciones reales con los que interactúa una entidad principal. El control de acceso basado en atributos (ABAC) puede ayudar a simplificar la administración de permisos, ya que permite proporcionar permisos a los usuarios mediante sus atributos en lugar de asociar las políticas de permisos directamente a cada usuario.

Pasos para la implementación

- Uso de AWS Identity and Access Management Access Analyzer: el Analizador de acceso de IAM le ayuda a identificar los recursos de su organización y sus cuentas, como los buckets de Amazon Simple Storage Service (Amazon S3) o los roles de IAM, que se comparten con una entidad externa.
- Uso de la generación de políticas del Analizador de acceso de IAM: la generación de políticas del Analizador de acceso de IAM le ayuda a crear políticas de permisos detalladas basadas en la actividad de acceso de un usuario o rol de IAM.
- Pruebe los permisos en los entornos inferiores antes de la producción: comience por utilizar los entornos de pruebas y de desarrollo menos críticos a fin de probar los permisos necesarios para diversas funciones de trabajo con IAM Access Analyzer. A continuación, ajuste y valide progresivamente estos permisos en los entornos de pruebas, control de calidad y ensayo antes de aplicarlos a la producción. Los entornos más bajos pueden tener permisos más flexibles al principio, ya que las políticas de control de servicios (SCP) imponen barreras de protección al limitar el número máximo de permisos concedidos.
- Determinación de un marco temporal y una política de uso aceptables para los usuarios y roles de IAM: use la marca de tiempo del último acceso para identificar los usuarios y roles no utilizados y eliminarlos. Revise la información del último acceso a servicios y acciones para identificar y establecer el alcance de los permisos para usuarios y roles específicos. Por ejemplo, puede utilizar la información sobre el último acceso para identificar las acciones específicas de Amazon S3 necesarias para el rol de su aplicación y restringir el acceso únicamente a dichas acciones. Estas características de información sobre el último acceso están disponibles en la Consola de administración de AWS y permiten de manera programática incorporarlas en sus flujos de trabajo de infraestructura y sus herramientas automatizadas.
- Consideración de la posibilidad de registrar eventos de datos en AWS CloudTrail: de manera predeterminada, CloudTrail no registra los eventos de datos, como la actividad de nivel de objeto de Amazon S3 (por ejemplo, `GetObject` y `DeleteObject`) o las actividades de las tablas de Amazon DynamoDB (por ejemplo `PutItem` y `DeleteItem`). Considere la posibilidad de habilitar el registro de estos eventos para determinar qué usuarios y roles necesitan acceder a objetos de Amazon S3 o elementos de tabla de DynamoDB específicos.

Recursos

Documentos relacionados:

- Aplicar permisos de privilegios mínimos
- Revisar y eliminar periódicamente usuarios, roles, permisos, políticas y credenciales no utilizados
- What is AWS CloudTrail?
- Uso de políticas de
- Registro y supervisión en DynamoDB
- Habilitación del registro de eventos de CloudTrail para buckets y objetos de Amazon S
- Generación de informes de credenciales para su Cuenta de AWS

Videos relacionados:

- Become an IAM Policy Master in 60 Minutes or Less
- Separation of Duties, Least Privilege, Delegation, and CI/CD
- AWS re:Inforce 2022 - AWS Identity and Access Management (IAM) deep dive

SEC03-BP05 Definición de las barreras de protección de los permisos para una organización

Utilice las barreras de protección de permisos para reducir el ámbito de los permisos disponibles que se pueden conceder a las entidades principales. La cadena de evaluación de la política de permisos incluye sus barreras de protección para determinar los permisos efectivos de una entidad principal al tomar decisiones de autorización. Puede definir barreras de protección mediante un enfoque basado en capas. Aplique algunas barreras de protección de manera generalizada en toda la organización y aplique otras de forma específica a las sesiones de acceso temporal.

Resultado deseado: cuenta con un aislamiento claro de los entornos mediante el uso de Cuentas de AWS separadas. Las políticas de control de servicios (SCP) se utilizan para definir las barreras de protección de permisos en toda la organización. Las barreras de protección más amplias se establecen en los niveles jerárquicos más cercanos a la raíz de la organización, y las más estrictas se establecen más cerca del nivel de las cuentas individuales.

En los casos en los que se pueden utilizar, las políticas de recursos definen las condiciones que debe cumplir una entidad principal para tener acceso a un recurso. Las políticas de recursos también acotan el conjunto de acciones permitidas cuando corresponde. Los límites de permisos se aplican a entidades principales que administran permisos de las cargas de trabajo y delegan la administración de permisos a los propietarios individuales de las cargas de trabajo.

Patrones comunes de uso no recomendados:

- Crear Cuentas de AWS de miembros dentro de una organización de AWS, pero no usar SCP para restringir el uso y los permisos disponibles para sus credenciales raíz.
- Asignar permisos según el principio de privilegio mínimo, pero sin aplicar barreras de protección al conjunto máximo de permisos que se pueden conceder.
- Confiar en el principio de denegación implícita de AWS IAM para restringir los permisos y esperar que las políticas no concedan un permiso explícito no deseado.
- Ejecutar varios entornos de carga de trabajo en la misma Cuenta de AWS y, a continuación, recurrir a mecanismos como las VPC, las etiquetas o las políticas de recursos para hacer cumplir los límites de los permisos.

Beneficios de establecer esta práctica recomendada: las barreras de protección de permisos ayudan a generar confianza en que no se van a conceder permisos no deseados, incluso cuando una política de permisos intente hacerlo. Esto puede simplificar la definición y la administración de los permisos al reducir el ámbito máximo de los permisos que deben tenerse en cuenta.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Le recomendamos que utilice un enfoque basado en capas para definir las barreras de protección de permisos para su organización. Este enfoque reduce sistemáticamente el conjunto máximo de permisos posibles a medida que se aplican capas adicionales. Esto le ayuda a conceder acceso según el principio de privilegios mínimos, lo que reduce el riesgo de accesos no deseados debidos a una configuración errónea de las políticas.

El primer paso para establecer barreras de protección de permisos es aislar las cargas de trabajo y los entornos en Cuentas de AWS separadas. Las entidades principales de una cuenta no pueden acceder a los recursos de otra cuenta sin un permiso explícito para hacerlo, incluso aunque ambas cuentas se encuentren en la misma organización de AWS o en la misma unidad organizativa (OU). Puede usar las unidades organizativas para agrupar las cuentas que prefiera administrar como una sola unidad.

El siguiente paso consiste en reducir el conjunto máximo de permisos que puede conceder a las entidades principales dentro de las cuentas de los miembros de su organización. Para ello, puede usar las políticas de control de servicios (SCP), que puede aplicar a una unidad organizativa o a

una cuenta. Las SCP pueden aplicar controles de acceso comunes, como restringir el acceso a determinadas Regiones de AWS, ayudar a evitar que se eliminen recursos o deshabilitar acciones de servicio potencialmente arriesgadas. Las SCP que se apliquen a la raíz de su organización solo afectan a las cuentas de los miembros, no a la cuenta de administración. Las SCP solo controlan las entidades principales de su organización. Las SCP no controlan las entidades principales externas a su organización que accedan a sus recursos.

Si está utilizando AWS Control Tower, puede aprovechar sus controles y zonas de aterrizaje como base para sus barreras de protección de permisos y su entorno de múltiples cuentas. Las zonas de aterrizaje proporcionan un entorno básico seguro y preconfigurado con cuentas independientes para diferentes cargas de trabajo y aplicaciones. Las barreras de protección imponen controles obligatorios en materia de seguridad, operaciones y cumplimiento mediante una combinación de políticas de control de servicios (SCP), reglas de AWS Config y otras configuraciones. Sin embargo, cuando se utilizan las barreras de protección y las zonas de aterrizaje de Control Tower junto con los SCP personalizados de las organizaciones, es fundamental seguir las prácticas recomendadas descritas en la documentación de AWS para evitar conflictos y garantizar un gobierno adecuado. Consulte la guía de AWS Control Tower para AWS Organizations a fin de obtener recomendaciones detalladas sobre la administración de los SCP, las cuentas y las unidades organizativas (OU) en un entorno de Control Tower.

Si sigue estas directrices, podrá aprovechar de forma eficaz las barreras de protección, las zonas de aterrizaje y los SCP personalizados de Control Tower, a la vez que mitigará los posibles conflictos y garantizará el gobierno y el control adecuados de su entorno de múltiples cuentas de AWS.

Otro paso consiste en usar políticas de recursos de IAM para determinar el ámbito de las acciones disponibles que se pueden llevar a cabo con respecto a los recursos que controlan, junto con cualquier condición que deba cumplir la entidad principal activa. El ámbito puede ser tan amplio como para permitir todas las acciones siempre que la entidad principal forme parte de su organización (mediante la clave de condición PrincipalOrgID), o tan detallado como para permitir solo acciones específicas para un rol de IAM específico. Puede adoptar un enfoque similar con las condiciones de las políticas de confianza para un rol de IAM. Si una política de confianza de recursos o roles nombra explícitamente una entidad principal en la misma cuenta que el rol o el recurso que controla, esa entidad principal no necesita una política de IAM asociada que otorgue los mismos permisos. Si la entidad principal está en una cuenta diferente a la del recurso, esa entidad principal necesita una política de IAM asociada que otorgue esos permisos.

A menudo, un equipo de carga de trabajo querrá administrar los permisos que requiere su carga de trabajo. Esto podría exigirles la creación de nuevos roles de IAM y políticas de permisos.

Puede definir el alcance máximo de los permisos que el equipo puede conceder dentro en un límite de permisos de IAM y asociar este documento a un rol de IAM que el equipo pueda utilizar posteriormente para gestionar sus permisos y roles de IAM. Este método puede proporcionarles la capacidad de completar su trabajo y, al mismo tiempo, mitigar los riesgos de disponer de acceso administrativo a IAM.

Un paso más detallado consiste en implementar técnicas de administración de acceso privilegiado (PAM) y administración de acceso elevado temporal (TEAM). Un ejemplo de PAM consiste en exigir a las entidades principales que lleven a cabo una autenticación multifactor antes de tomar medidas privilegiadas. Para obtener más información, consulte Configuring MFA-protected API access. TEAM requiere una solución que administre la aprobación y el plazo en el que se permite que una entidad principal tenga acceso de alto nivel. Un enfoque consiste en agregar temporalmente la entidad principal a la política de confianza del rol para un rol de IAM que tenga un acceso de alto nivel. Otro enfoque consiste, en condiciones normales, en reducir los permisos que un rol de IAM concede a una entidad principal mediante una política de sesión y, a continuación, eliminar temporalmente esta restricción durante el periodo de tiempo aprobado. Para obtener más información sobre las soluciones que AWS y determinados socios han validado, consulte Temporary elevated access.

Pasos para la implementación

1. Aísle las cargas de trabajo y los entornos en Cuentas de AWS separadas.
2. Use las SCP para reducir el conjunto máximo de permisos que se pueden conceder a las entidades principales dentro de las cuentas de los miembros de su organización.
   a. Al definir las SCP para reducir el conjunto máximo de permisos que se pueden conceder a las entidades principales dentro de las cuentas de los miembros de su organización, puede elegir entre una estrategia de lista de permitidos o de lista de denegaciones. La estrategia de listas de permisos especifica de forma explícita el acceso permitido y bloquea de forma implícita todos los demás accesos. La estrategia de listas de permisos especifica de forma explícita el acceso permitido y permite de forma predeterminada todos los demás accesos. Ambas estrategias tienen sus ventajas y desventajas, y la elección adecuada depende de los requisitos específicos y del modelo de riesgo de su organización. Para obtener más información, consulte Strategy for using SCPs.
   b. Además, revise los ejemplos de políticas de control de servicios para comprender cómo construir los SCP de manera eficaz.
3. Utilice las políticas de recursos de IAM para acotar y especificar las condiciones para las acciones permitidas en los recursos. Use las condiciones de las políticas de confianza en roles de IAM para crear restricciones a la hora de asumir roles.

4. Asigne límites de permisos de IAM a los roles de IAM que los equipos de carga de trabajo puedan usar para administrar sus propios roles y permisos de IAM en las cargas de trabajo.
5. Evalúe las soluciones de PAM y TEAM en función de sus necesidades.

Recursos

Documentos relacionados:

- Data perimeters on AWS
- Establecimiento de barreras de protección de permisos mediante perímetros de datos
- Lógica de evaluación de políticas

Ejemplos relacionados:

- Service control policy examples

Herramientas relacionadas:

- AWS Solution: Temporary Elevated Access Management
- Validated security partner solutions for TEAM

SEC03-BP06 Administración del acceso en función del ciclo de vida

Supervise y ajuste los permisos otorgados a sus entidades principales (usuarios, cargos y grupos) a lo largo de su ciclo de vida dentro de su organización. Ajuste la pertenencia a grupos a medida que los usuarios cambien de cargo y elimine el acceso cuando un usuario abandone la organización.

Resultado deseado: supervisa y ajusta los permisos a lo largo del ciclo de vida de los directores de la organización, lo que reduce el riesgo de privilegios innecesarios. Concede el acceso pertinente al crear un usuario. Modifica el acceso a medida que cambien las responsabilidades del usuario y elimina el acceso cuando el usuario ya no está activo o ha abandonado la organización. Administra de forma centralizada los cambios en los usuarios, los cargos y los grupos. Utiliza la automatización para propagar los cambios en sus entornos de AWS.

Patrones comunes de uso no recomendados:

- Concede privilegios de acceso excesivos o amplios a las identidades por adelantado, más allá de lo que se requiere inicialmente.
- No revisa ni ajusta los privilegios de acceso, a medida que los cargos y las responsabilidades cambian con el tiempo.
- Deja identidades inactivas o terminadas con privilegios de acceso activos. Esto aumenta el riesgo de acceso no autorizado.
- No aprovecha la automatización para gestionar el ciclo de vida de las identidades.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Administre y ajuste cuidadosamente los privilegios de acceso que otorga a las identidades (como usuarios, cargos y grupos) a lo largo de su ciclo de vida. Este ciclo de vida incluye la fase de incorporación inicial, los cambios continuos en los cargos y las responsabilidades y, en última instancia, la baja o el despido. Gestione el acceso de forma proactiva en función de la etapa del ciclo de vida para mantener el nivel de acceso adecuado. Respete el principio de privilegio mínimo para reducir el riesgo de privilegios de acceso excesivos o innecesarios.

Puede administrar el ciclo de vida de los usuarios de IAM directamente dentro de la Cuenta de AWS, o mediante la federación del proveedor de identidades de su personal con AWS IAM Identity Center. Para los usuarios de IAM, puede crear, modificar y eliminar usuarios y sus permisos asociados dentro de la Cuenta de AWS. En el caso de los usuarios federados, puede utilizar IAM Identity Center para administrar su ciclo de vida mediante la sincronización de la información de usuarios y grupos del proveedor de identidades de su organización mediante el protocolo del sistema de administración de identidades entre dominios (System for Cross-domain Identity Management o SCIM).

El SCIM es un protocolo estándar abierto para el aprovisionamiento y desaprovisionamiento automatizados de identidades de usuario en diferentes sistemas. Al integrar su proveedor de identidades con IAM Identity Center mediante SCIM, puede sincronizar automáticamente la información de los usuarios y los grupos, lo que ayuda a validar que los privilegios de acceso se concedan, modifiquen o revoquen en función de los cambios en la fuente de identidad autorizada de su organización.

A medida que cambien los cargos y responsabilidades de los empleados dentro de su organización, ajuste sus privilegios de acceso en consecuencia. Puede usar los conjuntos de permisos de IAM Identity Center para definir diferentes cargos o responsabilidades laborales y asociarlos a las

políticas y los permisos de IAM correspondientes. Cuando cambia el cargo de un empleado, puede actualizar su conjunto de permisos asignado para que refleje sus nuevas responsabilidades. Verifique que tenga el acceso necesario y, al mismo tiempo, cumpla el principio de privilegio mínimo.

Pasos para la implementación

1. Defina y documente un proceso del ciclo de vida de la administración de accesos, incluidos los procedimientos para conceder el acceso inicial, las revisiones periódicas y la baja.
2. Implemente límites de roles, grupos y permisos de IAM para administrar el acceso de manera colectiva y aplicar los niveles de acceso máximos permitidos.
3. Integre con un proveedor de identidades federado (como Microsoft Active Directory, Okta o Ping Identity) como fuente autorizada de la información de usuarios y grupos mediante IAM Identity Center.
4. Utilice el protocolo SCIM para sincronizar la información de usuarios y grupos del proveedor de identidades con el Almacén de identidades de IAM Identity Center.
5. Cree conjuntos de permisos en IAM Identity Center que representen diferentes cargos o responsabilidades laborales dentro de su organización. Defina las políticas y los permisos de IAM adecuados para cada conjunto de permisos.
6. Implemente revisiones del acceso periódicas, medidas de revocación rápida del acceso y mejora continua del proceso del ciclo de vida de la administración accesos.
7. Proporcione formación y concienciación a los empleados sobre las prácticas recomendadas de administración de accesos.

Recursos

Prácticas recomendadas relacionadas:

- SEC02-BP04 Uso de un proveedor de identidades centralizado

Documentos relacionados:

- Manage your identity source
- Manage identities in IAM Identity Center
- Uso de AWS Identity and Access Management Access Analyzer
- Generación de políticas del Analizador de acceso de IAM

Videos relacionados:

- AWS re:Inforce 2023 - Manage temporary elevated access with AWS IAM Identity Center
- AWS re:Invent 2022 - Simplify your existing workforce access with IAM Identity Center
- AWS re:Invent 2022 - Harness power of IAM policies & rein in permissions w/Access Analyzer

SEC03-BP07 Análisis del acceso público y entre cuentas

Supervise continuamente los resultados que pongan en relieve el acceso público y entre cuentas. Reduzca el acceso público y el acceso entre cuentas solo a los recursos que requieran este tipo de acceso.

Resultado deseado: sepa cuáles de los recursos de AWS se comparten y con quién. Supervise y audite continuamente sus recursos compartidos para verificar que solo se compartan con las entidades principales autorizadas.

Patrones comunes de uso no recomendados:

- No mantener un inventario de los recursos compartidos.
- No seguir un proceso para aprobar el acceso público o entre cuentas a los recursos.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: bajo

Guía para la implementación

Si su cuenta pertenece a AWS Organizations, puede conceder acceso a los recursos a toda la organización, a unidades organizativas específicas o a cuentas individuales. Si su cuenta no es miembro de una organización, puede compartir recursos con cuentas individuales. Puede conceder acceso entre cuentas mediante políticas basadas en recursos (por ejemplo, las políticas de buckets de Amazon Simple Storage Service (Amazon S3), o si permite que la entidad principal de otra cuenta asuma un rol de IAM en su cuenta. Cuando utilice políticas de recursos, compruebe que solo se concede acceso a las entidades principales autorizadas. Defina un proceso para aprobar todos los recursos que deban estar disponibles públicamente.

AWS Identity and Access Management Access Analyzer usa la seguridad comprobable para identificar todas las rutas de acceso a un recurso desde fuera de su cuenta. Revisa continuamente las políticas de recursos e informa de los resultados del acceso público y entre cuentas para facilitarle el análisis de un acceso potencialmente amplio. Considere la posibilidad de configurar el

Analizador de acceso de IAM con AWS Organizations para verificar que tiene visibilidad en todas sus cuentas. El Analizador de acceso de IAM también permite obtener una vista previa de los resultados antes de implementar los permisos de recursos. Esto le permite validar que sus cambios de política conceden solo el acceso público y entre cuentas previsto a sus recursos. Al diseñar el acceso a varias cuentas, puede utilizar políticas de confianza para controlar en qué casos se puede asumir un rol. Por ejemplo, puede usar la clave de condición `PrincipalOrgId` para denegar un intento de asumir un rol desde fuera de AWS Organizations.

AWS Config puede informar de los recursos que están mal configurados y, mediante comprobaciones de políticas de AWS Config, puede detectar los recursos que tienen configurado el acceso público. Los servicios como AWS Control Tower y AWS Security Hub CSPM simplifican la implementación de controles y barreras de protección en AWS Organizations para identificar y corregir los recursos expuestos públicamente. Por ejemplo, AWS Control Tower tiene una barrera de protección administrada que puede detectar si Cuentas de AWS puede restaurar alguna instantánea de Amazon EBS.

Pasos para la implementación

- Planteamiento de uso de AWS Config para AWS Organizations: AWS Config permite agregar los resultados de varias cuentas de una AWS Organizations cuenta de administrador delegado. Esto proporciona una visión completa y le permite implementar Reglas de AWS Config en todas las cuentas para detectar los recursos de acceso público.
- Configuración de AWS Identity and Access Management Access Analyzer: el Analizador de acceso de IAM lo ayuda a identificar los recursos y cuentas de su organización, como los buckets de Amazon S3 o los roles de IAM que se comparten con una entidad externa.
- Uso de la corrección automática de AWS Config para responder a los cambios en la configuración de acceso público de los buckets de Amazon S3: puede activar automáticamente la configuración de bloqueo de acceso público para los buckets de Amazon S3.
- Implementación de la supervisión y las alertas para identificar si los buckets de Amazon S3 se han convertido en públicos: debe disponer de supervisión y alertas para identificar cuándo está desactivado el bloqueo de acceso público de Amazon S3 y si los buckets de Amazon S3 pasan a ser públicos. Además, si utiliza AWS Organizations, puede crear una política de control de servicios que impida cambios en las políticas de acceso público de Amazon S3. AWS Trusted Advisor comprueba los buckets de Amazon S3 que tienen permisos de acceso abierto. Los permisos del bucket que otorgan, suben o eliminan el acceso para todo el mundo crean posibles vulnerabilidades de seguridad, ya que permiten que cualquiera agregue, modifique o elimine elementos en un bucket. La comprobación de Trusted Advisor examina los permisos explícitos

del bucket y las políticas asociadas que podrían anular los permisos del bucket. También puede utilizar AWS Config para supervisar si sus buckets de Amazon S3 tienen acceso público. Para obtener más información, consulte el blog How to Use AWS Config to Monitor for and Respond to Amazon S3 Buckets Allowing Public Access.

Al revisar los controles de acceso de los buckets de Amazon S3, es importante tener en cuenta la naturaleza de los datos almacenados en ellos. Amazon Macie es un servicio diseñado para ayudarlo a descubrir y proteger datos confidenciales, como la información de identificación personal (PII), la información de salud protegida (PHI) y las credenciales, como las claves privadas o las claves de acceso de AWS.

Recursos

Documentos relacionados:

- Uso de AWS Identity and Access Management Access Analyzer
- AWS Control Tower controls library
- AWS Foundational Security Best Practices standard
- AWS Config Reglas de administradas
- AWS Trusted Advisor check reference
- Monitoring AWS Trusted Advisor check results with Amazon EventBridge
- Managing AWS Config Rules Across All Accounts in Your Organization
- AWS Config y AWS Organizations
- Publicación de la AMI para utilizarla en Amazon EC2

Videos relacionados:

- Best Practices for securing your multi-account environment
- Dive Deep into IAM Access Analyzer

SEC03-BP08 Uso compartido de recursos de forma segura en su organización

A medida que el número de cargas de trabajo va aumentando, es posible que necesite compartir el acceso a los recursos de esas cargas de trabajo o aprovisionar los recursos varias veces entre varias

cuentas. Es posible que disponga de constructos para compartimentar el entorno, como, por ejemplo, entornos de desarrollo, pruebas y producción. Sin embargo, disponer de constructos de separación no le impide compartir de forma segura. Al compartir componentes que se solapan, puede reducir la sobrecarga operativa y conseguir una experiencia uniforme sin tener que adivinar qué podría haber pasado por alto al crear el mismo recurso varias veces.

Resultado deseado: minimice el acceso no deseado mediante el uso de métodos seguros para compartir los recursos dentro de su organización y ayudar con su iniciativa de prevención de la pérdida de datos. Reduzca la sobrecarga operativa en comparación con la administración de componentes individuales, reduzca los errores derivados de la creación manual del mismo componente varias veces y aumentar la escalabilidad de las cargas de trabajo. Puede disminuir el tiempo de resolución en situaciones con varios puntos de fallo y aumentar su confianza a la hora de determinar cuándo un componente ya no es necesario. Para obtener una guía prescriptiva sobre el análisis de los recursos compartidos externamente, consulte SEC03-BP07 Análisis del acceso público y entre cuentas.

Patrones comunes de uso no recomendados:

- Falta de un proceso para supervisar continuamente y alertar automáticamente sobre un uso compartido externo inesperado.
- Falta de una referencia sobre lo que se debe compartir y lo que no.
- Adoptar de manera predeterminada una política muy abierta en lugar de compartir explícitamente cuando es necesario.
- Crear manualmente recursos fundamentales que se solapan cuando es necesario.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Diseñe sus controles y patrones de acceso para que rijan el consumo de recursos compartidos de forma segura y solo con entidades de confianza. Supervise los recursos compartidos y revise el acceso a ellos de forma continua; además, reciba alertas sobre un uso compartido inapropiado o inesperado. Revise Analizar el acceso público y entre cuentas para que le sirva de ayuda para establecer una gobernanza que reduzca el acceso externo únicamente a los recursos que lo requieran, y para establecer un proceso de monitoreo continuo y alertas automáticas.

Servicios de AWS como, por ejemplo, AWS Security Hub CSPM, Amazon GuardDuty y AWS Backup, permiten el uso compartido entre cuentas en AWS Organizations. Estos servicios permiten

compartir datos con una cuenta central, acceder a ellos desde una cuenta central o administrar recursos y datos desde una cuenta central. Por ejemplo, AWS Security Hub CSPM puede transferir resultados desde cuentas individuales a una cuenta central en la que podrá verlos todos. AWS Backup puede hacer una copia de seguridad de un recurso y compartirlo entre varias cuentas. Puede usar AWS Resource Access Manager (AWS RAM) para compartir otros recursos comunes, como subredes de VPC y conexiones de puerta de enlace de tránsito, AWS Network Firewall o canalizaciones de Amazon SageMaker AI.

Para restringir su cuenta y compartir solo los recursos de su organización, utilice las políticas de control de servicios (SCP) para impedir el acceso a entidades principales externas. Al compartir recursos, combine los controles basados en la identidad y los controles de red para crear un perímetro de datos para su organización que ofrezca protección frente al acceso no deseado. Un perímetro de datos es un conjunto de barreras de protección preventivas para ayudar a verificar que solo sus identidades de confianza accedan a los recursos de confianza desde las redes previstas. Estos controles ponen límites apropiados a los recursos que se pueden compartir y evitan que se compartan o expongan recursos que no deberían permitirse. Por ejemplo, como parte de su perímetro de datos, puede utilizar las políticas de punto de conexión de VPC y la condición de `AWS:PrincipalOrgId` para garantizar que las identidades que acceden a sus buckets de Amazon S3 pertenezcan a su organización. Es importante tener en cuenta que los SCP no se aplican a los roles o entidades principales de AWS vinculados al servicio.

Cuando utilice Amazon S3, desactive las ACL de su bucket de Amazon S3 y utilice las políticas de IAM para definir el control de acceso. Para restringir el acceso a un origen de Amazon S3 desde Amazon CloudFront, migre desde la identidad de acceso de origen (OAI) al control de acceso de origen (OAC), que admite características adicionales como el cifrado del servidor con AWS Key Management Service.

En algunos casos, es posible que desee permitir compartir recursos fuera de su organización o conceder a un tercero acceso a sus recursos. Para obtener una guía prescriptiva sobre la administración de permisos para compartir recursos de forma externa, consulte Administración de permisos.

Pasos para la implementación

1. Utilice AWS Organizations: AWS Organizations es un servicio de administración de cuentas que le permite unificar varias Cuentas de AWS en una organización que crea y administra de forma centralizada. Puede agrupar sus cuentas en unidades organizativas (OU) y asociar diferentes políticas a cada OU para ayudarle a satisfacer sus necesidades presupuestarias, de seguridad y de conformidad. También puede controlar cómo los servicios de inteligencia artificial (IA) y

machine learning (ML) de AWS pueden recopilar y almacenar datos, y utilizar la administración de varias cuentas de los servicios de AWS integrada con las organizaciones.

2. Integre AWS Organizations con los servicios de AWS: cuando utiliza un servicio de AWS para efectuar tareas en su nombre en las cuentas de los miembros de su organización, AWS Organizations crea un rol vinculado al servicio (SLR) de IAM para ese servicio en cada cuenta miembro. Debe administrar el acceso de confianza mediante la Consola de administración de AWS, las API de AWS o la AWS CLI. Para obtener instrucciones prescriptivas sobre cómo activar el acceso de confianza, consulte Uso de AWS Organizations con otros servicios de AWS y Servicios de AWS que puede usar con las organizaciones.
3. Establezca un perímetro de datos: un perímetro de datos proporciona un límite claro de confianza y propiedad. En AWS, se suele representar como su organización de AWS administrada por AWS Organizations, junto con cualquier red o sistema local que acceda a sus recursos de AWS. El objetivo del perímetro de datos es verificar que se permite el acceso si la identidad es de confianza, el recurso es de confianza y la red es la que se espera. Sin embargo, establecer un perímetro de datos no es una estrategia universal. Evalúe y adopte los objetivos de control descritos en el documento técnico Construir un perímetro en AWS a partir de sus requisitos y modelos de riesgo de seguridad específicos. Debe plantearse detenidamente su postura de riesgo única e implementar los controles perimetrales que se ajusten a sus necesidades de seguridad.
4. Use los recursos compartidos de los servicios de AWS y aplique las restricciones pertinentes: muchos servicios de AWS le permiten compartir recursos con otra cuenta o dirigirse a un recurso de otra cuenta, como Imágenes de máquina de Amazon (AMI) y AWS Resource Access Manager (AWS RAM). Restrinja la API de `ModifyImageAttribute` para especificar las cuentas de confianza con las que compartir la AMI. Especifique la condición `ram:RequestedAllowsExternalPrincipals` cuando se utilice AWS RAM para restringir el uso compartido únicamente a su organización y, de este modo, evitar el acceso desde identidades que no sean de confianza. Para obtener consideraciones e instrucciones prescriptivas, consulte Uso compartido de recursos y objetivos externos.
5. Utilice AWS RAM para compartir de forma segura en una cuenta o con otras Cuentas de AWS: AWS RAM lo ayuda a compartir de forma segura los recursos que ha creado con roles y usuarios de su cuenta y con otras Cuentas de AWS. En un entorno de varias cuentas, AWS RAM le permite crear un recurso una vez y compartirlo con otras cuentas. Este enfoque ayuda a reducir su sobrecarga operativa a la vez que proporciona coherencia, visibilidad y auditabilidad en integraciones con Amazon CloudWatch y AWS CloudTrail, algo que no tiene cuando utiliza el acceso entre cuentas.

Si tiene recursos que ha compartido anteriormente mediante una política basada en recursos, puede usar la API de `PromoteResourceShareCreatedFromPolicy` o una equivalente para convertir el uso compartido de recursos en un uso compartido de recursos de AWS RAM completo.

En algunos casos, puede que tenga que dar pasos adicionales para compartir recursos. Por ejemplo, para compartir una instantánea cifrada, debe compartir una clave de AWS KMS.

Recursos

Prácticas recomendadas relacionadas:

- SEC03-BP07 Análisis del acceso público y entre cuentas
- SEC03-BP09 Uso compartido seguro de recursos con terceros
- SEC05-BP01 Creación de capas de red

Documentos relacionados:

- Propietario de bucket que concede permisos entre cuentas para objetos que no le pertenecen
- How to use Trust Policies with IAM
- Building Data Perimeter on AWS
- Cómo utilizar un ID externo al conceder a un tercero el acceso a sus recursos de AWS
- AWS services you can use with AWS Organizations
- Establishing a data perimeter on AWS: Allow only trusted identities to access company data

Videos relacionados:

- Granular Access with AWS Resource Access Manager
- Securing your data perimeter with VPC endpoints
- Establishing a data perimeter on AWS

Herramientas relacionadas:

- Data Perimeter Policy Examples

SEC03-BP09 Uso compartido seguro de recursos con terceros

La seguridad de su entorno en la nube no se limita a su organización. Su organización puede recurrir a terceros para administrar una parte de sus datos. La administración de permisos para el sistema administrado por terceros debe seguir la práctica del acceso justo a tiempo mediante el principio del privilegio mínimo con credenciales temporales. Si colabora estrechamente con un tercero, podrán reducir juntos el alcance del impacto y el riesgo de un acceso no intencionado.

Resultado deseado: evita el uso de credenciales a largo plazo de AWS Identity and Access Management (IAM), como claves de acceso y claves secretas, ya que representan un riesgo para la seguridad si se utilizan indebidamente. En su lugar, utiliza los roles de IAM y las credenciales temporales para mejorar su posición de seguridad y minimizar la sobrecarga operativa que implica la administración de credenciales a largo plazo. Al conceder acceso a terceros, utiliza un identificador único universal (UUID) como ID externo en la política de confianza de IAM y mantiene bajo su control las políticas de IAM asociadas al rol para garantizar acceso con privilegios mínimos. Para obtener orientaciones prescriptivas sobre el análisis de recursos compartidos externamente, consulte SEC03-BP07 Análisis del acceso público y entre cuentas.

Patrones comunes de uso no recomendados:

- Utilizar la política de confianza de IAM predeterminada sin ninguna condición.
- Utilizar claves de acceso y credenciales de IAM a largo plazo.
- Reutilizar ID externos.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Es posible que desee permitir que se compartan recursos fuera de AWS Organizations o conceder a un tercero acceso a su cuenta. Por ejemplo, es posible que un tercero le proporcione una solución de supervisión que necesite acceder a los recursos de su cuenta. En esos casos, cree un rol entre cuentas de IAM con solo los privilegios que necesite el tercero. Defina, además, una política de confianza mediante la condición de ID externo. Cuando utilice un ID externo, usted o el tercero podrán generar un ID único para cada cliente, tercero o tenencia. El ID único no debe controlarlo nadie más que usted después de crearlo. El tercero debe implementar un proceso para relacionar el ID externo con el cliente de una forma segura, auditable y reproducible.

También puede utilizar IAM Roles Anywhere para administrar los roles de IAM para aplicaciones externas a AWS que usan las API de AWS.

Si el tercero ya no necesita acceder a su entorno, elimine el rol. Procure no proporcionar credenciales a largo plazo a terceros. Conozca otros servicios de AWS que permiten el uso compartido, como AWS Well-Architected Tool, que permite compartir una carga de trabajo con otras Cuentas de AWS, y AWS Resource Access Manager, que lo ayuda a compartir de forma segura un recurso de AWS de su propiedad con otras cuentas.

Pasos para la implementación

1. Utilice roles entre cuentas para permitir el acceso a cuentas externas. Los roles entre cuentas reducen la cantidad de información confidencial que almacenan las cuentas externas y los terceros para atender a sus clientes. Los roles entre cuentas le permiten conceder acceso a los recursos de AWS de su cuenta de forma segura a terceros, como Socios de AWS u otras cuentas de su organización, al tiempo que mantiene la capacidad de administrar y auditar dicho acceso. El tercero podría estar prestando servicio desde una infraestructura híbrida o extrayendo datos a una ubicación externa. IAM Roles Anywhere lo ayuda a permitir que las cargas de trabajo de terceros interactúen de forma segura con sus cargas de trabajo de AWS y a reducir aún más la necesidad de credenciales a largo plazo.

   No debe utilizar credenciales a largo plazo ni claves de acceso asociadas a usuarios para proporcionar acceso a cuentas externas. En su lugar, utilice roles entre cuentas para proporcionar el acceso entre cuentas.
2. Actúe con la diligencia debida y garantice el acceso seguro para los proveedores de SaaS de terceros. Al compartir recursos con proveedores de SaaS externos, actúe estrictamente con la diligencia debida para garantizar que ofrezca una estrategia segura y responsable de acceso a sus recursos de AWS. Evalúe su modelo de responsabilidad compartida para comprender qué medidas de seguridad ofrecen y cuáles son de su responsabilidad. Asegúrese de que el proveedor de SaaS cuente con un proceso seguro y auditable de acceder a sus recursos, incluido el uso de identificadores externos y los principios de acceso con privilegios mínimos. El uso de ID externos ayuda a resolver el problema de la sustitución confusa.

   Implemente controles de seguridad para garantizar un acceso seguro y el cumplimiento del principio de privilegios mínimos al conceder acceso a proveedores de SaaS externos. Esto puede incluir el uso de identificadores externos, identificadores únicos universales (UUID) y políticas de confianza de IAM que limitan el acceso únicamente a lo estrictamente necesario. Trabaje en estrecha colaboración con el proveedor de SaaS para establecer mecanismos de acceso seguro,

revise periódicamente su acceso a sus recursos de AWS y lleve a cabo auditorías para garantizar el cumplimiento de sus requisitos de seguridad.

3. Declare obsoletas las credenciales a largo plazo proporcionadas por el cliente. Declare obsoleto el uso de credenciales a largo plazo y utilice roles de cuentas cruzadas o IAM Roles Anywhere. Si debe utilizar credenciales a largo plazo, establezca un plan para migrar al acceso basado en roles. Para obtener más información sobre la administración de claves, consulte Administración de identidades. Reúnase también con su equipo de Cuenta de AWS y el tercero para establecer un manual de procedimientos de mitigación de riesgos. Para obtener orientación normativa sobre cómo responder y mitigar el impacto potencial de un incidente de seguridad, consulte Respuesta ante incidentes.
4. Compruebe que la configuración cuente con una guía prescriptiva o que esté automatizada. El ID externo no debe tratarse como un secreto, pero no debe ser un valor fácil de adivinar, como un número de teléfono, un nombre o un ID de cuenta. Convierta el ID externo en un campo de solo lectura para que no pueda modificarse con el fin de suplantar la configuración.

   El ID externo puede generarlo usted o el tercero. Defina un proceso para determinar quién es el responsable de generar el ID. Independientemente de la entidad que cree el ID externo, el tercero aplica la unicidad y los formatos de manera uniforme en todos los clientes.

   La política que se cree para el acceso entre cuentas en sus cuentas debe seguir el principio del privilegio mínimo. El tercero debe proporcionarle un documento de políticas de roles o un mecanismo de configuración automatizado que utilice una plantilla de AWS CloudFormation o algo equivalente. Esto reduce la posibilidad de que se produzcan errores asociados a la creación manual de políticas y ofrece un registro de seguimiento auditable. Para obtener más información sobre el uso de una plantilla de AWS CloudFormation para crear roles entre cuentas, consulte Cross-Account Roles.

   El tercero debe proporcionar un mecanismo de configuración automatizado y auditable. Sin embargo, debería automatizar la configuración del rol mediante el documento de la política de roles que describe el acceso necesario. Con una plantilla de AWS CloudFormation o un elemento equivalente, debe supervisar los cambios y utilizar la detección de desviaciones como parte de la práctica de auditoría.
5. Tenga en cuenta los cambios. La estructura de su cuenta, su necesidad de utilizar al tercero o la oferta de servicios que este presta pueden cambiar. Debe anticiparse a los cambios y a los fallos, y planificar en consecuencia las personas, los procesos y la tecnología adecuados. Audite de forma periódica el nivel de acceso que proporciona e implemente métodos de detección que lo alerten de cambios inesperados. Monitoree y audite el uso del rol y el almacén de datos de los

ID externos. Debe tenerlo todo preparado para revocar el acceso del tercero, de forma temporal o permanente, a causa de cambios o patrones de acceso inesperados. Asimismo, mida el impacto en su operación de revocación, incluido el tiempo que lleva hacerla, las personas implicadas, el costo y el impacto en otros recursos.

Para obtener una guía prescriptiva sobre los métodos de detección, consulte las prácticas recomendadas de detección.

Recursos

Prácticas recomendadas relacionadas:

- SEC02-BP02 Uso de credenciales temporales
- SEC03-BP05 Definición de las barreras de protección de los permisos para una organización
- SEC03-BP06 Administración del acceso en función del ciclo de vida
- SEC03-BP07 Análisis del acceso público y entre cuentas
- SEC04 Detección

Documentos relacionados:

- Propietario de bucket que concede permisos entre cuentas para objetos que no le pertenecen
- How to use trust policies with IAM roles
- Delegación del acceso entre Cuentas de AWS mediante roles de IAM
- ¿Cómo accedo a los recursos de otra Cuenta de AWS mediante IAM?
- Security best practices in IAM (Prácticas recomendadas de seguridad en IAM)
- Lógica de evaluación de políticas entre cuentas
- Cómo utilizar un ID externo al otorgar acceso a los recursos de AWS a terceros
- Collecting Information from AWS CloudFormation Resources Created in External Accounts with Custom Resources
- Securely Using External ID for Accessing AWS Accounts Owned by Others
- Extend IAM roles to workloads outside of IAM with IAM Roles Anywhere

Videos relacionados:

- How do I allow users or roles in a separate Cuenta de AWS access to my Cuenta de AWS?
- AWS re:Invent 2018: Become an IAM Policy Master in 60 Minutes or Less
- AWS Knowledge Center Live: IAM Best Practices and Design Decisions

Ejemplos relacionados:

- Configurar el acceso entre cuentas a Amazon DynamoDB
- AWS STS Network Query Tool

Detección

La detección consta de dos partes: la detección de cambios de configuración inesperados o no deseados y la detección de comportamientos inesperados. La primera puede tener lugar en varios lugares del ciclo de vida de entrega de una aplicación. Al utilizar la infraestructura como código (por ejemplo, una plantilla de CloudFormation), puede comprobar si hay configuraciones no deseadas antes de implementar una carga de trabajo mediante la aplicación de comprobaciones en las canalizaciones de CI/CD o en el control de origen. A continuación, a medida que implementa una carga de trabajo en entornos de producción y que no son de producción, puede comprobar la configuración mediante herramientas nativas de AWS, de código abierto o de socios de AWS. Estas comprobaciones pueden ser para una configuración que no cumpla con los principios de seguridad o las prácticas recomendadas, o para los cambios que se hicieron entre una configuración probada y una implementada. En el caso de una aplicación en ejecución, puede comprobar si la configuración se ha modificado de forma inesperada, incluso fuera de una implementación conocida o un evento de escalado automatizado.

Para la segunda parte de la detección (comportamiento inesperado), puede utilizar herramientas o emitir alertas cuando se produzca un aumento en un tipo concreto de llamada a la API. Con Amazon GuardDuty, puede recibir alertas cuando se produzcan actividades inesperadas, malintencionadas o potencialmente no autorizadas en sus cuentas de AWS. También debe supervisar de forma explícita las llamadas a la API mutantes que no esperaría que se utilizaran en su carga de trabajo y las llamadas a la API que cambien la posición de seguridad.

La detección le permite identificar un posible error de configuración de seguridad, una amenaza o un comportamiento inesperado. Es una parte fundamental del ciclo de vida de seguridad y se puede usar como complemento de procesos de calidad, para una obligación legal o de conformidad y para la identificación de amenazas y respuestas. Existen diferentes tipos de mecanismos de detección. Por ejemplo, los registros de su carga de trabajo se pueden analizar para detectar las vulnerabilidades que se estén utilizando. Debe revisar periódicamente los mecanismos de detección relacionados con su carga de trabajo para asegurarse de que cumpla con las políticas y los requisitos internos y externos. Las alertas y notificaciones automatizadas deben basarse en condiciones definidas para que sus equipos o herramientas puedan investigar la situación. Estos mecanismos son factores reactivos importantes que ayudan a su organización a identificar la actividad anómala y comprender sus repercusiones.

En AWS, hay varios métodos que puede utilizar para abordar los mecanismos de detección. En las siguientes secciones se describe cómo se usan estos métodos:

Prácticas recomendadas

- SEC04-BP01 Configuración del registro de servicios y aplicaciones
- SEC04-BP02 Recopilación de registros, resultados y métricas en ubicaciones estandarizadas
- SEC04-BP03 Correlación y enriquecimiento de las alertas de seguridad
- SEC04-BP04 Inicio de correcciones para recursos no conformes

SEC04-BP01 Configuración del registro de servicios y aplicaciones

Retenga los registros de eventos de seguridad de servicios y aplicaciones. Se trata de un principio fundamental de seguridad en casos de uso de auditoría, investigación y uso operativo, y un requisito de seguridad común basado en las normas, políticas y procedimientos de gobernanza, riesgo y cumplimiento (GRC).

Resultado deseado: una organización debe ser capaz de recuperar de manera fiable y uniforme los registros de eventos de seguridad de los servicios y aplicaciones de AWS en el momento oportuno cuando sea necesario llevar a cabo algún proceso o cumplir una obligación interna, como una respuesta a un incidente de seguridad. Considere la posibilidad de centralizar los registros para obtener mejores resultados operativos.

Patrones comunes de uso no recomendados:

- Almacenar los registros de forma indefinida o eliminarlos demasiado pronto.
- Todo el mundo puede acceder a los registros.
- Depender por completo de procesos manuales para la gobernanza y el uso de los registros.
- Almacenar todos y cada uno de los tipos de registros por si fueran necesarios.
- Comprobar la integridad de los registros solo cuando es necesario.

Beneficios de establecer esta práctica recomendada: implemente un mecanismo de análisis de la causa raíz (RCA) para los incidentes de seguridad y una fuente de pruebas para cumplir sus obligaciones de gobernanza, riesgo y conformidad.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Durante una investigación de seguridad u otros casos de uso basados en sus requisitos, necesita poder revisar los registros correspondientes para registrar y comprender todo el alcance y la

cronología del incidente. También necesita los registros para generar alertas que indican que se han producido determinadas acciones de interés. Es fundamental seleccionar, activar, almacenar y configurar mecanismos de consulta y recuperación, así como de alerta.

Pasos para la implementación

- Seleccione y utilice los orígenes de registros. Antes de una investigación de seguridad, necesita obtener los registros relevantes para reconstruir de forma retroactiva la actividad que se ha producido en una Cuenta de AWS. Seleccione las fuentes de registros relevantes para sus cargas de trabajo.

  Los criterios de selección de las fuentes de registros deben basarse en los casos de uso que requiera su negocio. Establezca un registro de seguimiento para cada Cuenta de AWS mediante AWS CloudTrail o un registro de seguimiento de AWS Organizations y, para ello, configure un bucket de Amazon S3.

  AWS CloudTrail es un servicio de registro que rastrea las llamadas a la API que se hacen en una Cuenta de AWS y captura la actividad de los servicios de AWS. Está activado de forma predeterminada con una retención de 90 días de los eventos de administración que se pueden recuperar a través del historial de eventos de CloudTrail mediante la Consola de administración de AWS, la AWS CLI o un SDK de AWS. Para prolongar la retención y la visibilidad de los eventos de datos, cree un registro de seguimiento de CloudTrail y asócielo a un bucket de Amazon S3 y, de forma opcional, a un grupo de registros de Amazon CloudWatch. Como alternativa, puede crear un CloudTrail Lake, que conserva los registros de CloudTrail durante un máximo de siete años y proporciona un servicio de consultas basado en SQL.

  AWS recomienda que los clientes que utilicen una VPC activen los registros de tráfico de red y DNS mediante los registros de flujo de VPC y los registros de consultas de Amazon Route 53 Resolver, respectivamente, y los transmitan a un bucket de Amazon S3 o a un grupo de registros de CloudWatch. Puede crear un registro de flujo de VPC para una VPC, una subred o una interfaz de red. En el caso de los registros de flujo de VPC, puede elegir cómo y dónde utilizar los registros de flujo para reducir costos.

  Los registros de AWS CloudTrail, los registros de flujo de VPC y los registros de consulta de Route 53 Resolver son los orígenes de registros básicos que facilitan las investigaciones de seguridad en AWS. También puede usar Amazon Security Lake para recopilar, normalizar y almacenar estos datos de registro en formato Apache Parquet y Open Cybersecurity Schema Framework (OCSF), que está listo para su consulta. Security Lake también admite otros registros de AWS y registros de orígenes de terceros.

Los servicios de AWS pueden generar registros que no capturan las fuentes de registros básicas, como los registros de Elastic Load Balancing, los registros de AWS WAF, los registros del registrador de AWS Config, los resultados de Amazon GuardDuty, los registros de auditoría de Amazon Elastic Kubernetes Service (Amazon EKS) y los registros del sistema operativo y las aplicaciones de las instancias de Amazon EC2. Para obtener una lista completa de las opciones de registro y supervisión, consulte el Apéndice A: Definiciones de las capacidades de la nube: registro y eventos de la Guía de respuesta ante incidentes de seguridad de AWS.

- Investigación de las capacidades de registro de cada servicio y aplicación de AWS: cada servicio y aplicación de AWS le ofrece opciones para el almacenamiento de registros, cada una de las cuales tiene sus propias capacidades de retención y ciclo de vida. Los dos servicios de almacenamiento de registros más comunes son Amazon Simple Storage Service (Amazon S3) y Amazon CloudWatch. Para periodos de retención largos, se recomienda utilizar Amazon S3 por su rentabilidad y la flexibilidad de sus ciclos de vida. Si la opción de registro principal es Registros de Amazon CloudWatch, quizá debería considerar la posibilidad de archivar los registros a los que se accede con menos frecuencia en Amazon S3.
- Selección del almacenamiento de registros: la elección del almacenamiento de registros suele estar relacionada con la herramienta de consulta que utilice, las capacidades de retención, la familiaridad y el costo. Las principales opciones para el almacenamiento de registros son un bucket de Amazon S3 o un grupo de registro de CloudWatch.

  Un bucket de Amazon S3 es un almacenamiento rentable y duradero que tiene una política de ciclo de vida opcional. Los registros almacenados en buckets de Amazon S3 pueden consultarse a través de servicios como Amazon Athena.

  Un grupo de registro de CloudWatch ofrece un almacenamiento duradero y una utilidad de consulta integrada a través de Información de registros de CloudWatch.
- Identificación de la retención de registros adecuada: cuando utilice un bucket de Amazon S3 o un grupo de registros de CloudWatch para almacenar registros, debe establecer ciclos de vida adecuados para cada fuente de registros a fin de optimizar los costos de almacenamiento y recuperación. Por lo general, los clientes tienen entre tres meses y un año de registros disponibles para su consulta, con un periodo de retención de hasta siete años. La elección de la disponibilidad y el periodo de retención debe ajustarse a sus requisitos de seguridad y a una combinación de requisitos legales, reglamentarios y empresariales.
- Uso del registro para cada servicio y aplicación de AWS con las políticas de retención y ciclo de vida adecuadas: para cada servicio o aplicación de AWS de su organización, busque la guía de configuración de registros específica:

  - Configuración de registros de seguimiento de AWS CloudTrail
  - Configuración de registros de flujo de VPC
  - Configuración de exportaciones de resultados de Amazon GuardDuty
  - Configuración de grabaciones de AWS Config
  - Configuración del tráfico de ACL web de AWS WAF
  - Configuración de registros del tráfico de red de AWS Network Firewall
  - Configuración de registros de acceso de Elastic Load Balancing
  - Configuración de registros de consultas de Amazon Route 53 Resolver
  - Configuración de registros de Amazon RDS
  - Configuración de registros de plano de control de Amazon EKS
  - Configuración del agente de Amazon CloudWatch para instancias de Amazon EC2 y servidores en las instalaciones
- Selección e implementación de mecanismos de consulta para los registros: para las consultas de registro, puede utilizar Información de registros de CloudWatch para los datos almacenados en los grupos de registros de CloudWatch, y Amazon Athena y Amazon OpenSearch Service para los datos almacenados en Amazon S3. También puede utilizar herramientas de consulta de terceros, como un servicio de administración de eventos e información de seguridad (SIEM).

  En el proceso de selección de una herramienta de consulta de registros, se deben tener en cuenta los aspectos relacionados con las personas, los procesos y la tecnología de sus operaciones de seguridad. Seleccione una herramienta que cumpla los requisitos operativos, empresariales y de seguridad, y que sea accesible y pueda mantenerse a largo plazo. Tenga en cuenta que las herramientas de consulta de registros funcionan de forma óptima cuando el número de registros a analizar se mantiene dentro de los límites de la herramienta. No es raro disponer de varias herramientas de consulta debido a limitaciones técnicas o de costos.

  Por ejemplo, podría utilizar una herramienta de administración de eventos e información de seguridad (SIEM) de terceros para hacer consultas en los últimos 90 días de datos, pero utilizar Athena para efectuar consultas anteriores a esos 90 días debido al costo de la ingestión de registros de un SIEM. Independientemente de cuál sea la implementación, compruebe que su enfoque permite reducir al mínimo el número de herramientas necesarias para maximizar la eficiencia operativa, especialmente durante la investigación de un evento de seguridad.
- Uso de registros para las alertas: AWS proporciona alertas a través de varios servicios de seguridad:

- AWS Config supervisa y registra las configuraciones de los recursos de AWS y permite automatizar la evaluación y la corrección con las configuraciones deseadas.
- Amazon GuardDuty es un servicio de detección de amenazas que supervisa continuamente cualquier actividad malintencionada y comportamiento no autorizado para proteger sus cargas de trabajo y sus Cuentas de AWS. GuardDuty ingiere, agrega y analiza la información de las fuentes, como los eventos de administración y datos de AWS CloudTrail, los registros de DNS, los registros de flujo de VPC y los registros de auditoría de Amazon EKS. GuardDuty extrae flujos de datos independientes directamente de CloudTrail, los registros de flujo de VPC, los registros de consultas de DNS y Amazon EKS. No es necesario que administre las políticas de los buckets de Amazon S3 ni que modifique la forma en que recopila y almacena los registros. Aun así, es recomendable que retenga estos registros para sus propios fines de investigación y conformidad.
- AWS Security Hub CSPM proporciona un único lugar en el que se agregan, organizan y priorizan las alertas de seguridad o los resultados de varios servicios de AWS y productos opcionales de terceros para ofrecerle una vista completa de las alertas de seguridad y los estados de conformidad.

También puede utilizar motores de generación de alertas personalizados para alertas de seguridad que no cubran estos servicios o para alertas específicas relevantes para su entorno. Para obtener información sobre cómo crear estas alertas y detecciones, consulte la sección Detección en la Guía de respuesta ante incidentes de seguridad de AWS.

Recursos

Prácticas recomendadas relacionadas:

- SEC04-BP02 Recopilación de registros, resultados y métricas en ubicaciones estandarizadas
- SEC07-BP04 Definición de la administración escalable del ciclo de vida de los datos
- SEC10-BP06 Implementación de las herramientas con anticipación

Documentos relacionados:

- AWS Security Incident Response Guide
- Cómo comenzar a utilizar Amazon Security Lake
- Getting started: Amazon CloudWatch Logs

Videos relacionados:

- AWS re:Invent 2022 - Introducing Amazon Security Lake

Ejemplos relacionados:

- Assisted Log Enabler for AWS
- AWS Security Hub CSPM Findings Historical Export

SEC04-BP02 Recopilación de registros, resultados y métricas en ubicaciones estandarizadas

Los equipos de seguridad se basan en los registros y los resultados para analizar aquellos eventos que podrían indicar una actividad no autorizada o cambios no intencionados. Para agilizar este análisis, recopile los registros de seguridad y los resultados en ubicaciones estandarizadas. Esto hace que los puntos de datos de interés estén disponibles para su correlación y puede simplificar la integración de herramientas.

Resultado deseado: cuenta con un enfoque estandarizado para recopilar, analizar y visualizar los datos de registro, los resultados y las métricas. Los equipos de seguridad pueden correlacionar, analizar y visualizar de manera eficiente los datos de seguridad en sistemas dispares para descubrir posibles eventos de seguridad e identificar anomalías. Dispone de sistemas de gestión de información y eventos de seguridad (SIEM) u otros mecanismos integrados para consultar y analizar los datos de registro con el fin de responder, rastrear y escalar los eventos de seguridad sin demora.

Patrones comunes de uso no recomendados:

- Los equipos tienen y administran de forma independiente registros y recopilaciones de métricas que no se ajustan a la estrategia de registro de la organización.
- Los equipos no tienen controles de acceso adecuados para restringir la visibilidad y la alteración de los datos recopilados.
- Los equipos no gestionan sus registros, resultados y métricas de seguridad como parte de su política de clasificación de datos.
- Los equipos no tienen en cuenta los requisitos de soberanía y localización de los datos al configurar las recopilaciones de datos.

Beneficios de establecer esta práctica recomendada: una solución de registro estandarizada para recopilar y consultar los datos y eventos de registro mejora los conocimientos obtenidos a partir de la información que contienen. La configuración de un ciclo de vida automatizado para los datos de registro recopilados puede reducir los costos derivados del almacenamiento de registros. Puede crear un control de acceso detallado para la información de registro recopilada de acuerdo con el nivel de confidencialidad de los datos y los patrones de acceso que necesiten sus equipos. Puede integrar herramientas para correlacionar, visualizar y obtener información a partir de los datos.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

El aumento del uso de AWS dentro de una organización se traduce en un número cada vez mayor de cargas de trabajo y entornos distribuidos. A medida que cada una de estas cargas de trabajo y entornos genera datos sobre la actividad que contienen, la captura y el almacenamiento de estos datos de forma local supone un desafío para las operaciones de seguridad. Los equipos de seguridad utilizan herramientas como los sistemas de gestión de información y eventos de seguridad (SIEM) para recopilar datos de fuentes distribuidas y llevar a cabo tareas de correlación, análisis y elaboración de flujos de trabajo de respuesta. Esto requiere administrar un conjunto complejo de permisos para acceder a los diversos orígenes de datos y una sobrecarga adicional para operar los procesos de extracción, transformación y carga (ETL).

Para superar estos desafíos, puede agregar todos los orígenes pertinentes de datos de registro de seguridad en una cuenta de archivo de registro, tal como se describe en Organizing Your AWS Environment Using Multiple Accounts. Esto incluye todos los datos relacionados con la seguridad de la carga de trabajo y los registros que generan los servicios de AWS, como AWS CloudTrail, AWS WAF, Elastic Load Balancing y Amazon Route 53. La recopilación de estos datos en ubicaciones estandarizadas de una Cuenta de AWS separada que cuente con los permisos multicuenta adecuados tiene varios beneficios. Esta práctica ayuda a evitar la manipulación de registros en cargas de trabajo y entornos comprometidos, proporciona un punto de integración único para herramientas adicionales y ofrece un modelo más simplificado para configurar el ciclo de vida y la retención de datos. Evalúe los impactos de la soberanía de los datos, los alcances de cumplimiento y otras normativas para determinar si se requieren varias ubicaciones de almacenamiento y periodos de retención de datos de seguridad.

Para facilitar la recopilación y estandarización de registros y resultados, valore la posibilidad de usar Amazon Security Lake en su cuenta de archivo de registro. Puede configurar Security Lake para que ingiera automáticamente datos de orígenes comunes como CloudTrail, Route

53, Amazon EKS y VPC Flow Logs. También puede configurar AWS Security Hub CSPM como origen de datos en Security Lake, lo que le permite correlacionar los resultados de otros servicios de AWS, como Amazon GuardDuty y Amazon Inspector, con sus datos de registro. Del mismo modo, puede usar integraciones de orígenes de datos de terceros o configurar orígenes de datos personalizados. Todas las integraciones estandarizan sus datos en el formato Open Cybersecurity Schema Framework (OCSF) y se almacenan en buckets de Amazon S3 como archivos Parquet, lo que elimina la necesidad de procesamiento de extracción, transformación y carga (ETL).

El almacenamiento de los datos de seguridad en ubicaciones estandarizadas proporciona capacidades de análisis avanzadas. AWS recomienda implementar herramientas de análisis de seguridad que estén activas en un entorno de AWS en una cuenta de Security Tooling independiente de su cuenta de archivo de registros. Este enfoque le permite implementar controles exhaustivos para proteger la integridad y la disponibilidad de los registros y el proceso de administración de registros diferentes de las herramientas que se emplean para acceder a ellos. Considere la posibilidad de usar servicios como Amazon Athena para ejecutar consultas bajo demanda que correlacionen varios orígenes de datos. También puede integrar herramientas de visualización como Quick. Cada vez hay más soluciones basadas en inteligencia artificial disponibles y pueden llevar a cabo funciones como traducir los resultados en resúmenes legibles por humanos o la interacción en lenguaje natural. Estas soluciones suelen integrarse más fácilmente al tener una ubicación de almacenamiento de datos estandarizada para efectuar consultas.

Pasos para la implementación

1. Cree las cuentas de archivo de registros y Security Tooling
    a. Mediante AWS Organizations, cree las cuentas de archivo de registros y Security Tooling en una unidad organizativa de seguridad. Si usa AWS Control Tower para administrar su organización, las cuentas de archivo de registros y Security Tooling se crean automáticamente. Configure los roles y permisos para acceder a estas cuentas y administrarlas según sea necesario.
2. Configure las ubicaciones de datos de seguridad estandarizadas
    a. Determine su estrategia para crear ubicaciones de datos de seguridad estandarizadas. Puede hacerlo mediante opciones como los enfoques de arquitectura de lagos de datos comunes, productos de datos de terceros o Amazon Security Lake. AWS recomienda recopilar los datos de seguridad de Regiones de AWS que haya elegido para sus cuentas, incluso aunque no estén en uso activamente.
3. Configure la publicación de orígenes de datos en sus ubicaciones estandarizadas

   a. Identifique los orígenes de sus datos de seguridad y configúrelos para que se publiquen en sus ubicaciones estandarizadas. Evalúe las opciones para exportar automáticamente los datos en el formato deseado, en lugar de aquellas que requieran desarrollar los procesos de ETL. Con Amazon Security Lake, podrá recopilar datos de orígenes compatibles con AWS y sistemas integrados de terceros.

4. Configure las herramientas para acceder a sus ubicaciones estandarizadas
   a. Configure herramientas como Amazon Athena, Quick o soluciones de terceros para disponer del acceso necesario a las ubicaciones estandarizadas. Configure estas herramientas para que funcionen desde la cuenta de Security Tooling con acceso de lectura multicuenta a la cuenta de Log Archive, cuando corresponda. Cree suscriptores en Amazon Security Lake para que estas herramientas puedan acceder a sus datos.

Recursos

Prácticas recomendadas relacionadas:

- SEC01-BP01 Separación de cargas de trabajo con cuentas
- SEC07-BP04 Definición de la administración escalable del ciclo de vida de los datos
- SEC08-BP04 Aplicación del control de acceso
- OPS08-BP02 Análisis de los registros de la carga de trabajo

Documentos relacionados:

- AWS Whitepapers: Organizing Your AWS Environment Using Multiple Accounts
- AWS Prescriptive Guidance: AWS Security Reference Architecture (AWS SRA)
- AWS Prescriptive Guidance: Logging and monitoring guide for application owners

Ejemplos relacionados:

- Agregación, búsqueda y visualización de datos de registro procedentes de fuentes distribuidas con Amazon Athena y Quick.
- Cómo visualizar los resultados de Amazon Security Lake con Quick
- Generate AI powered insights for Amazon Security Lake using Amazon SageMaker AI Studio and Amazon Bedrock

- Identify cybersecurity anomalies in your Amazon Security Lake data using Amazon SageMaker AI
- Ingest, transform, and deliver events published by Amazon Security Lake to Amazon OpenSearch Service
- Simplify AWS CloudTrail log analysis with natural language query generation in CloudTrail Lake

Herramientas relacionadas:

- Amazon Security Lake
- Integraciones de socios de Amazon Security Lake
- Open Cybersecurity Schema Framework (OCSF)
- Amazon Athena
- Quick
- Amazon Bedrock

SEC04-BP03 Correlación y enriquecimiento de las alertas de seguridad

La actividad inesperada puede generar múltiples alertas de seguridad de diferentes fuentes, lo que requiere una mayor correlación y enriquecimiento para comprender el contexto completo. Implemente la correlación y el enriquecimiento automatizados de las alertas de seguridad para ayudar a lograr una identificación y una respuesta a los incidentes más precisas.

Resultado deseado: los mecanismos automatizados correlacionan los datos y enriquecen dichos datos con información adicional a medida que la actividad genere diferentes alertas en sus cargas de trabajo y entornos. Este preprocesamiento ofrece una comprensión más detallada del evento, lo que ayuda a los investigadores a determinar la gravedad del evento y si constituye un incidente que requiere una respuesta formal. Este proceso reduce la carga para los equipos de supervisión e investigación.

Patrones comunes de uso no recomendados:

- Existen grupos de personas distintos que investigan los resultados y alertas generados por los diferentes sistemas, a menos que los requisitos de separación de funciones exijan lo contrario.

- Canalizar en la organización todos los datos de alertas y resultados de seguridad a ubicaciones estándar, pero con la necesidad de que los investigadores lleven a cabo una correlación y un enriquecimiento manuales.
- Confiar únicamente en la inteligencia de los sistemas de detección de amenazas para informar sobre los resultados y establecer el nivel de gravedad.

Beneficios de establecer esta práctica recomendada: la correlación y el enriquecimiento automatizados de las alertas ayudan a reducir la carga cognitiva general y la preparación manual de los datos que requieren los investigadores. Esta práctica puede reducir el tiempo necesario para determinar si el evento representa un incidente e iniciar una respuesta formal. El contexto adicional también ayuda a evaluar con precisión la verdadera gravedad de un evento, ya que puede ser mayor o menor de lo que sugiere una alerta.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: bajo

Guía para la implementación

Las alertas de seguridad pueden provenir de muchos orígenes diferentes en AWS, entre los que se encuentran:

- Servicios como Amazon GuardDuty, AWS Security Hub CSPM, Amazon Macie, Amazon Inspector, AWS Config, AWS Identity and Access Management Access Analyzer y Analizador de acceso a la red
- Alertas del análisis automatizado de los registros de aplicaciones, infraestructuras y servicios de AWS, como las de Security Analytics para Amazon OpenSearch Service.
- Alarmas que responden a cambios en su actividad de facturación procedentes de orígenes como Amazon CloudWatch, Amazon EventBridge o AWS Budgets.
- Orígenes de terceros, como orígenes de inteligencia sobre amenazas y Soluciones de socios de seguridad de la AWS Partner Network.
- Contactos de AWS Trust & Safety u otros orígenes, como clientes o empleados internos.
- Utilice el Catálogo de técnicas de amenazas (TTC) de AWS para ayudar a identificar y correlacionar el comportamiento de los actores de amenazas mediante la identificación del indicador de compromiso (IoC). El TTC es una extensión del marco MITRE ATT&CK, que clasifica todos los comportamientos y técnicas de los actores de amenazas conocidos y observados dirigidos a los recursos de AWS.

En su forma más básica, las alertas contienen información sobre quién (la entidad principal o la identidad) está haciendo qué (la acción efectuada) a qué (los recursos afectados). Para cada uno de estos orígenes, identifique si hay formas de crear asignaciones entre identificadores para estas identidades, acciones y recursos como base para llevar a cabo la correlación. Esto puede consistir en integrar las fuentes de las alertas con una herramienta de administración de eventos e información de seguridad (SIEM) para llevar a cabo una correlación automática en su nombre, crear sus propios procesos y canalizaciones de datos, o una combinación de ambas estrategias.

Un ejemplo de servicio que puede efectuar la correlación es Amazon Detective. Detective ingiere continuamente alertas de diversos orígenes de AWS y de terceros, y utiliza diferentes formas de inteligencia para crear un gráfico visual de sus relaciones con el fin de asistir en las investigaciones.

Si bien el nivel de gravedad inicial de una alerta ayuda a establecer prioridades, el contexto en el que se haya producido la alerta determina su verdadero nivel de gravedad. Por ejemplo, Amazon GuardDuty puede avisar de que una instancia de Amazon EC2 de su carga de trabajo está consultando un nombre de dominio inesperado. GuardDuty puede asignar una gravedad baja a esta alerta. Sin embargo, la correlación automatizada con otras actividades en el momento de la alerta podría revelar que varios cientos de instancias de EC2 se han implementado con la misma identidad, lo que aumenta los costos operativos generales. En este caso, este contexto de eventos correlacionados justificaría una nueva alerta de seguridad y el nivel de gravedad se ajustaría en alto, lo que aceleraría las acciones futuras.

Pasos para la implementación

1. Identifique los orígenes de la información de alertas de seguridad. Comprenda en qué medida las alertas de estos sistemas representan la identidad, la acción y los recursos para determinar dónde se puede establecer una correlación.
2. Establezca un mecanismo para capturar las alertas de diferentes orígenes. Para ello, considere la posibilidad de utilizar servicios como Security Hub CSPM, EventBridge y CloudWatch.
3. Identifique los orígenes para la correlación y el enriquecimiento de los datos. Entre las fuentes de ejemplo se incluyen AWS CloudTrail, los registros de flujo de VPC, los registros de Route 53 Resolver y los registros de infraestructura y aplicaciones. Algunos o todos estos registros pueden consumirse mediante una única integración con Amazon Security Lake.
4. Integre sus alertas con sus fuentes de correlación y enriquecimiento de datos para crear contextos de eventos de seguridad más detallados y establecer el nivel de gravedad.
    a. Amazon Detective, las herramientas de SIEM u otras soluciones de terceros pueden llevar a cabo un cierto nivel de ingesta, correlación y enriquecimiento automáticamente.

b. También puede usar los servicios de AWS para crear sus propias soluciones. Por ejemplo, puede invocar una función de AWS Lambda para ejecutar una consulta de Amazon Athena a AWS CloudTrail o Amazon Security Lake y publicar los resultados en EventBridge.

Recursos

Prácticas recomendadas relacionadas:

- SEC10-BP03 Preparación de las capacidades forenses
- OPS08-BP04 Creación de alertas procesables
- REL06-BP03 Envío de notificaciones (procesamiento y alarmas en tiempo real)

Documentos relacionados:

- AWS Security Incident Response Guide

Ejemplos relacionados:

- How to enrich AWS Security Hub CSPM findings with account metadata

Herramientas relacionadas:

- Amazon Detective
- Amazon EventBridge
- AWS Lambda
- Amazon Athena

SEC04-BP04 Inicio de correcciones para recursos no conformes

Sus controles de detección pueden alertarle sobre la presencia de recursos no conformes con sus requisitos de configuración. Puede iniciar soluciones definidas mediante programación, de forma manual o automática, para corregir estos recursos y ayudar a minimizar los posibles impactos. Al definir las correcciones mediante programación, puede tomar medidas rápidas y coherentes.

Si bien la automatización puede mejorar las operaciones de seguridad, debe implementarla y administrarla con cuidado. Establezca mecanismos de supervisión y control adecuados para verificar

que las respuestas automatizadas sean eficaces, precisas y estén alineadas con las políticas de la organización y la propensión al riesgo.

Resultado deseado: defina los estándares de configuración de los recursos junto con los pasos para corregir las situaciones en las que se detecte que los recursos no cumplen los requisitos. Cuando sea posible, defina las medidas de corrección mediante programación para que puedan iniciarse de forma manual o automática. Dispone de sistemas de detección para identificar los recursos disconformes y publica alertas en herramientas centralizadas y supervisadas por su personal de seguridad. Usa estas herramientas para ejecutar las correcciones programáticas, de forma manual o automática. Dispone de mecanismos de supervisión y control adecuados en las correcciones automáticas para regular su uso.

Patrones comunes de uso no recomendados:

- Implementar la automatización, pero no verificar ni validar minuciosamente las acciones de corrección. Esto puede tener consecuencias imprevistas, como obstaculizar las operaciones empresariales legítimas o provocar inestabilidad en el sistema.
- Mejorar los tiempos de respuesta y los procedimientos mediante la automatización, pero sin contar con la supervisión y los mecanismos adecuados que permitan la intervención y la decisión de un humano en los casos necesarios.
- Confiar únicamente en las correcciones, en lugar de incluirlas como parte de un programa más amplio de respuesta y recuperación ante incidentes.

Beneficios de establecer esta práctica recomendada: las correcciones automáticas pueden responder a los errores de configuración con mayor rapidez que los procesos manuales, lo que ayuda a minimizar los posibles impactos empresariales, así como a reducir las oportunidades de usos no previstos. Cuando define las correcciones mediante programación, se aplican de forma coherente, lo que reduce el riesgo de error humano. La automatización también puede gestionar un mayor volumen de alertas simultáneamente, lo que resulta particularmente importante en entornos que funcionan a gran escala.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Tal como se describe en SEC01-BP03 Identificación y validación de los objetivos de control, servicios como AWS Config y AWS Security Hub CSPM pueden ayudarlo a supervisar la configuración de los recursos de sus cuentas para garantizar el cumplimiento de sus requisitos. Cuando se detectan

recursos no conformes, servicios como AWS Security Hub CSPM pueden ayudar a enrutar las alertas de manera adecuada y a corregirlas. Estas soluciones proporcionan un punto central en el que los investigadores de seguridad puedan supervisar los problemas y tomar medidas correctivas.

Además de AWS Security Hub CSPM, AWS presentó Security Hub Advanced. Este servicio, anunciado en re:Invent 2025, transforma la forma en que las organizaciones priorizan sus problemas de seguridad más críticos y responden a gran escala para proteger sus entornos de nube. Security Hub mejorado ahora utiliza análisis avanzados para correlacionar, enriquecer y priorizar automáticamente las señales de seguridad en todo su entorno de nube. Security Hub se integra perfectamente con Amazon GuardDuty, Amazon Inspector, Amazon Macie y AWS Security Hub CSPM. Los resultados correlacionados en Security Hub pueden dar lugar a un resultado totalmente nuevo, denominado resultado de exposición, que incluye una ruta de ataque supuesta basada en las vulnerabilidades encontradas en cada recurso.

Si bien algunas situaciones de recursos disconformes son únicas y requieren de juicio humano para corregirlas, otras situaciones requieren una respuesta estándar que se puede definir mediante programación. Por ejemplo, una respuesta estándar ante un error de configuración de un grupo de seguridad de VPC podría consistir en eliminar las reglas no permitidas y notificárselo al propietario. Las respuestas se pueden definir en funciones de AWS Lambda, documentos de Automatización de AWS Systems Manager o mediante otros entornos de código que prefiera. Asegúrese de que el entorno pueda autenticarse en AWS con un rol de IAM que tenga la cantidad mínima de permisos necesaria para tomar medidas correctivas.

Una vez que haya definido la corrección deseada, podrá determinar el medio que prefiera para iniciarla. AWS Config puede iniciar las correcciones. Si utiliza Security Hub CSPM, puede hacerlo mediante acciones personalizadas, que publican la información de búsqueda en Amazon EventBridge. A continuación, una regla de EventBridge puede iniciar la corrección. Puede configurar las correcciones a través de Security Hub CSPM para que se ejecuten de forma automática o manual.

En el caso de corrección mediante programación, le recomendamos que disponga de registros y auditorías exhaustivos de las medidas adoptadas, así como de sus resultados. Revise y analice estos registros para evaluar la eficacia de los procesos automatizados e identificar las áreas de mejora. Capture los registros en Registros de Amazon CloudWatch y los resultados de las correcciones como notas de resultados en Security Hub CSPM.

Como punto de partida, considere la posibilidad de utilizar la Respuesta de seguridad automatizada en AWS, que cuenta con soluciones de corrección prediseñadas para resolver los errores de configuración de seguridad más comunes.

Pasos para la implementación

1. Analice y priorice las alertas.
    a. Unifique las alertas de seguridad de varios servicios de AWS en Security Hub CSPM para obtener visibilidad, priorización y corrección centralizadas.
2. Desarrolle medidas de corrección.
    a. Utilice servicios como Systems Manager y AWS Lambda para ejecutar correcciones programáticas.
3. Configure cómo se inician las correcciones.
    a. Con Systems Manager, defina acciones personalizadas para publicar los resultados en EventBridge. Configure estas acciones para que se inicien manual o automáticamente.
    b. También puede usar Amazon Simple Notification Service (SNS) para enviar notificaciones y alertas a las partes interesadas pertinentes (como el equipo de seguridad o los equipos de respuesta a incidentes) para que intervengan manualmente o escalen el problema si es necesario.
4. Revise y analice los registros de corrección para comprobar su eficacia y mejora.
    a. Envíe la salida del registro a Registros de CloudWatch. Capture los resultados como notas de resultados en Security Hub CSPM.

Recursos

Prácticas recomendadas relacionadas:

- SEC06-BP03 Reducción de la administración manual y el acceso interactivo

Documentos relacionados:

- AWS Security Incident Response Guide - Detection

Ejemplos relacionados:

- Respuesta de seguridad automatizada en AWS
- Monitor EC2 instance key pairs using AWS Config
- Create AWS Config custom rules by using AWS CloudFormation Guard policies
- Automatically remediate unencrypted Amazon RDS DB instances and clusters

Herramientas relacionadas:

- AWS Systems Manager Automation
- Respuesta de seguridad automatizada en AWS

Protección de la infraestructura

La protección de la infraestructura abarca las metodologías de control, como la defensa en profundidad, necesarias para ajustarse a las prácticas recomendadas y las obligaciones organizativas o normativas. Usar estas metodologías es fundamental para operaciones continuas correctas en la nube.

La protección de la infraestructura representa una parte clave de un programa de seguridad de la información. Garantiza que los sistemas y servicios de la carga de trabajo estén protegidos frente a accesos no intencionados ni autorizados y posibles vulnerabilidades. Por ejemplo, definirá los límites de confianza (como límites de red y cuenta), el mantenimiento y la configuración de seguridad del sistema (como la minimización, la protección y la implementación de revisiones), autorizaciones y autenticación del sistema operativo (como los usuarios, claves y niveles de acceso) y otros puntos adecuados del cumplimiento de la política (como los firewalls de aplicaciones web o puertas de enlace de API).

Regiones, zonas de disponibilidad, zonas locales de AWS y AWS Outposts

Asegúrese de estar familiarizado con las regiones, las zonas de disponibilidad, las zonas locales de AWS y AWS Outposts, que son componentes de la infraestructura global segura de AWS.

AWS tiene el concepto de región, que es una ubicación física en todo el mundo donde agrupamos los centros de datos. Cada grupo de centros de datos lógicos se denomina zona de disponibilidad (AZ). Cada región de AWS se compone de múltiples zonas de disponibilidad aisladas y separadas físicamente dentro de un área geográfica. Si tiene requisitos de residencia de datos, puede elegir la región de AWS que esté cerca de la ubicación que desee. Usted retiene el control y la propiedad absolutos de la región donde se encuentran físicamente sus datos, lo que puede ser útil para el cumplimiento de los requisitos regionales de conformidad y residencia de datos. Cada zona de disponibilidad tiene alimentación, refrigeración y seguridad física independientes. Si una aplicación se particiona entre zonas de disponibilidad, tendrá un mejor aislamiento y protección frente a incidencias relacionadas con cortes de energía, rayos, tornados, terremotos, etc. Las zonas de disponibilidad están físicamente separadas por una distancia considerable, a muchos kilómetros de cualquier otra zona de disponibilidad, aunque todas se encuentran a unos 100 km (60 millas) la una de la otra. Todas las AZ de una región de AWS están interconectadas con ancho de banda alto y redes de baja latencia y utilizan fibra metropolitana dedicada y totalmente redundante, lo que ofrece una conexión de red de baja latencia y alto rendimiento entre las zonas de disponibilidad. Todo el tráfico entre las zonas de disponibilidad está cifrado. Los clientes de AWS que se centran en la alta disponibilidad pueden diseñar sus aplicaciones para que se ejecuten en varias zonas de

disponibilidad a fin de lograr una tolerancia a los errores aún mayor. Las regiones de AWS cumplen con los niveles más altos de seguridad, cumplimiento y protección de datos.

Las Zonas locales de AWS acercan los servicios de computación, almacenamiento, base de datos y otros servicios de AWS exclusivos a los usuarios finales. Con las Zonas locales de AWS, puede ejecutar fácilmente aplicaciones muy exigentes que requieren latencias de milisegundos de un solo dígito para sus usuarios finales, como la creación de contenido multimedia y de entretenimiento, juegos en tiempo real, simulaciones de depósitos, automatización del diseño electrónico y machine learning. Cada ubicación de zona local de AWS es una extensión de una región de AWS en la que puede ejecutar sus aplicaciones sensibles a la latencia mediante servicios de AWS, como Amazon EC2, Amazon VPC, Amazon EBS, Amazon File Storage y Elastic Load Balancing, en proximidad geográfica con los usuarios finales. Las Zonas locales de AWS proporcionan una conexión segura y de gran ancho de banda entre las cargas de trabajo locales y las que se ejecutan en la región de AWS, lo que le permite conectarse sin interrupciones a la gama completa de servicios de la región a través de las mismas API y los mismos conjuntos de herramientas.

AWS Outposts brinda servicios de AWS nativos, infraestructura y modelos operativos a prácticamente cualquier centro de datos, espacio de coubicación o instalación en las instalaciones. Puede usar las mismas API de AWS, herramientas e infraestructura en las instalaciones y en la nube de AWS para ofrecer una experiencia híbrida verdaderamente coherente. AWS Outposts está diseñado para entornos conectados y se puede usar para admitir cargas de trabajo que deben permanecer en las instalaciones debido a la baja latencia o a las necesidades de procesamiento de datos locales.

En AWS, existen varios enfoques para la protección de la infraestructura. En las siguientes secciones se describe cómo se usan estos enfoques.

Temas

- Protección de redes
- Protección de la computación

Protección de redes

Los usuarios, tanto de sus empleados como de sus clientes, pueden estar ubicados en cualquier lugar. Debe dejar atrás los modelos tradicionales que confían en cualquier persona y en cualquier cosa que tenga acceso a la red. Cuando sigue el principio de aplicar la seguridad en todos los

niveles, emplea un enfoque de Confianza cero. La seguridad de Confianza cero es un modelo en el que los componentes de la aplicación o los microservicios se consideran independientes entre sí y ningún componente o microservicio confía en ningún otro.

La planificación y administración minuciosas del diseño y la topología de red forma la base del modo de aislar y limitar los recursos en su carga de trabajo. Dado que muchos recursos de su carga de trabajo funcionan en una VPC y heredan las propiedades de seguridad, es fundamental que el diseño esté respaldado por mecanismos de inspección y protección respaldados por la automatización. Del mismo modo, para las cargas de trabajo que funcionan fuera de una VPC, que utilizan únicamente servicios periféricos o sin servidor, las prácticas recomendadas se aplican con un enfoque más simplificado. Consulte el documento AWS Well-Architected Serverless Applications Lens para obtener orientación específica sobre la seguridad sin servidor.

Prácticas recomendadas

- SEC05-BP01 Creación de capas de red
- SEC05-BP02 Control del flujo de tráfico dentro de las capas de red
- SEC05-BP03 Implementación de una protección basada en la inspección
- SEC05-BP04 Automatización de la protección de la red

SEC05-BP01 Creación de capas de red

Segmente la topología de red en diferentes capas en función de las agrupaciones lógicas de los componentes de la carga de trabajo según sus requisitos de acceso y la confidencialidad de los datos. Distinga entre los componentes que requieren acceso entrante desde Internet, como los puntos de conexión web públicos, y aquellos que solo necesitan acceso interno, como las bases de datos.

Resultado deseado: incorporar las capas de su red en un enfoque de seguridad integral de defensa en profundidad que complemente la estrategia de autenticación y autorización de identidad de sus cargas de trabajo. Dispone de las capas de acuerdo con los requisitos de acceso y confidencialidad de los datos, con los mecanismos de control y flujo de tráfico adecuados.

Patrones comunes de uso no recomendados:

- Crea todos los recursos en una única VPC o subred.
- Desarrolla las capas de red sin tener en cuenta los requisitos de confidencialidad de los datos, el comportamiento de los componentes o la funcionalidad.

- Utiliza las VPC y las subredes de forma predeterminada para todas las consideraciones sobre las capas de red y no tener en cuenta la forma en que los servicios administrados de AWS influyen en la topología.

Beneficios de establecer esta práctica recomendada: establecer las capas de red es el primer paso para restringir las rutas innecesarias a través de la red, sobre todo las que conducen a sistemas y datos críticos. Esto dificulta que los actores no autorizados accedan a su red y a los recursos adicionales que contiene. Las capas de red diferenciadas reducen de forma ventajosa el alcance del análisis de los sistemas de inspección, como la detección de intrusos o la prevención del malware. Esto reduce la posibilidad de que se produzcan falsos positivos y disminuye la sobrecarga de procesamiento innecesaria.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Al diseñar una arquitectura de carga de trabajo, es habitual separar los componentes en diferentes capas en función de su responsabilidad. Por ejemplo, una aplicación web puede tener una capa de presentación, una capa de aplicación y una capa de datos. Es posible adoptar un enfoque similar al diseñar su topología de la red. Los controles de red subyacentes pueden ayudarle a hacer cumplir los requisitos de acceso a los datos de su carga de trabajo. Por ejemplo, en una arquitectura de aplicaciones web de tres niveles, puede almacenar los archivos de la capa de presentación estática en Amazon S3 y distribuirlos desde una red de entrega de contenido (CDN), como Amazon CloudFront. La capa de aplicaciones puede tener puntos de conexión públicos a los que presta servicio un equilibrador de carga de aplicación (ALB) en una subred pública de Amazon VPC (similar a una zona desmilitarizada o DMZ), con servicios de backend implementados en subredes privadas. La capa de datos, en la que se alojan recursos como bases de datos y sistemas de archivos compartidos, puede encontrarse en subredes privadas diferentes de aquellas en las que están los recursos de la capa de aplicación. Puede implementar controles dentro de cada uno de estos límites de capa (CDN, subred pública, subred privada) para que solo los atraviese el tráfico autorizado.

Debe tener también en cuenta el nivel de confidencialidad de los datos que se vayan a procesar, de forma similar a cuando se modelan las capas de red en función del propósito funcional de los componentes de la carga de trabajo. Según el ejemplo de la aplicación web, si bien todos los servicios de carga de trabajo podrían encontrarse en la capa de aplicación, los distintos servicios podrían procesar datos con niveles de confidencialidad diferentes. En este caso, puede ser conveniente dividir la capa de aplicación con varias subredes privadas, distintas VPC en la

misma Cuenta de AWS o incluso distintas VPC en Cuentas de AWS diferentes para cada nivel de confidencialidad de los datos, en función de los requisitos de control.

Otra cuestión que debe plantearse para las capas de red es la coherencia del comportamiento de los componentes de la carga de trabajo. En ese mismo ejemplo, es posible que en la capa de aplicación haya servicios que acepten entradas de usuarios finales o integraciones de sistemas externos que planteen intrínsecamente más riesgos que las entradas procedentes de otros servicios. Entre algunos ejemplos de esta situación podemos citar la carga de archivos, la ejecución de scripts de código, el análisis de correo electrónico, etc. Al ubicar estos servicios en su propia capa de red se contribuye a crear un límite de aislamiento más sólido en torno a ellos, y esto permite evitar que su comportamiento peculiar genere alertas por falsos positivos en los sistemas de inspección.

Como parte del diseño, tenga en cuenta cómo el uso de AWS Managed Services influye en la topología de la red. Descubra de qué manera servicios como Amazon VPC Lattice pueden ayudar a facilitar la interoperabilidad de los componentes de la carga de trabajo entre las capas de la red. Al usar AWS Lambda, implemente en sus subredes de VPC, a menos que existan motivos específicos para no hacerlo. Determine en qué casos pueden los puntos de conexión de VPC y AWS PrivateLink simplificar el cumplimiento de las políticas de seguridad que limitan el acceso a las puertas de enlace de Internet.

Pasos para la implementación

1. Revise la arquitectura de su carga de trabajo. Agrupe de forma lógica los componentes y servicios según las funciones que cumplen, la confidencialidad de los datos que procesan y su comportamiento.
2. Para aquellos componentes que respondan a solicitudes de Internet, plantéese la posibilidad de usar equilibradores de carga u otros proxies para proporcionar puntos de conexión públicos. Valore la posibilidad de cambiar los controles de seguridad mediante el uso de servicios administrados, como CloudFront, Amazon API Gateway, Elastic Load Balancing y AWS Amplify para alojar puntos de conexión públicos.
3. Para los componentes que se ejecutan en entornos de computación, como instancias de Amazon EC2, contenedores de AWS Fargate o funciones de Lambda, lleve a cabo la implementación en subredes privadas en función de sus grupos del primer paso.
4. Para los servicios de AWS totalmente administrados, como Amazon DynamoDB, Amazon Kinesis o Amazon SQS, considere la posibilidad de utilizar puntos de conexión de VPC como valores predeterminados para el acceso a través de direcciones IP privadas.

Recursos

Prácticas recomendadas relacionadas:

- REL02 Planificación de la topología de la red
- PERF04-BP01 Comprensión del efecto de las redes en el rendimiento

Videos relacionados:

- AWS re:Invent 2023 - AWS networking foundations

Ejemplos relacionados:

- Ejemplos de VPC
- Acceder a las aplicaciones en contenedores de forma privada en Amazon ECS mediante AWS Fargate, un AWS PrivateLink y un equilibrador de carga de red
- Serve static content in an Amazon S3 bucket through a VPC by using Amazon CloudFront

SEC05-BP02 Control del flujo de tráfico dentro de las capas de red

Dentro de las capas de su red, utilice una mayor segmentación para restringir el tráfico únicamente a los flujos necesarios para cada carga de trabajo. En primer lugar, céntrese en controlar el tráfico entre Internet u otros sistemas externos a una carga de trabajo y su entorno (tráfico norte-sur). A continuación, observe los flujos entre los diferentes componentes y sistemas (tráfico de este a oeste).

Resultado deseado: permite que solo los flujos de red necesarios para que los componentes de sus cargas de trabajo se comuniquen entre sí, con sus clientes y con cualquier otro servicio del que dependan. Tiene en cuenta en su diseño cuestiones como la entrada y salida públicas en comparación con las privadas, la clasificación de datos, las normativas regionales y los requisitos de protocolo. Siempre que sea posible, prefiere los flujos punto a punto en lugar de la interconexión de redes como parte del diseño con el principio de privilegios mínimos.

Patrones comunes de uso no recomendados:

- Adoptar un enfoque de seguridad de red basado en el perímetro y controlar solamente el flujo de tráfico dentro de los límites de las capas de red.
- Dar por sentado que todo el tráfico dentro de una capa de red está autenticado y autorizado.

- Aplicar controles para el tráfico de entrada o de salida, pero no para ambos.
- Confiar solo en los componentes de la carga de trabajo y los controles de red para autenticar y autorizar el tráfico.

Beneficios de establecer esta práctica recomendada: esta práctica ayuda a reducir el riesgo de movimientos no autorizados dentro de la red y agrega un nivel adicional de autorización a sus cargas de trabajo. Al controlar el flujo de tráfico, puede restringir el alcance del impacto de un incidente de seguridad y acelerar la detección y la respuesta.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Si bien las capas de red ayudan a establecer límites en torno a los componentes de la carga de trabajo similares en cuanto a función, nivel de confidencialidad de los datos y comportamiento, puede crear un nivel de control del tráfico mucho más detallado mediante el uso de técnicas para segmentar aún más los componentes de estas capas según el principio de privilegio mínimo. En AWS, las capas de red se definen principalmente mediante subredes según los rangos de direcciones IP dentro de una Amazon VPC. Las capas también se pueden definir mediante diferentes VPC, por ejemplo, para agrupar entornos de microservicios por dominio empresarial. Cuando use varias VPC, intervenga en el enrutamiento mediante una AWS Transit Gateway. Si bien esto permite controlar el tráfico en el nivel de capa 4 (direcciones IP e intervalos de puertos) mediante grupos de seguridad y tablas de enrutamiento, puede obtener un mayor control mediante servicios adicionales como AWS PrivateLink, Amazon Route 53 Resolver DNS Firewall, AWS Network Firewall y AWS WAF.

Determine y haga un inventario de los requisitos de flujo de datos y comunicación de sus cargas de trabajo que incluya las entidades que inician la conexión, los puertos, los protocolos y las capas de red. Evalúe los protocolos disponibles para establecer conexiones y transmitir datos con el objetivo de seleccionar los que cumplan sus requisitos de protección (por ejemplo, HTTPS en lugar de HTTP). Capture estos requisitos tanto en los límites de sus redes como dentro de cada capa. Una vez identificados estos requisitos, explore las opciones para permitir solamente el tráfico requerido en cada punto de conexión. Un buen punto de partida es utilizar grupos de seguridad dentro de la VPC, ya que se pueden asociar a recursos que utilizan una interfaz de red elástica (ENI), como las instancias de Amazon EC2, las tareas de Amazon ECS, los pods de Amazon EKS o las bases de datos de Amazon RDS. A diferencia de un firewall de capa 4, un grupo de seguridad puede tener una regla que permita el tráfico de otro grupo de seguridad mediante su identificador, lo que reduce al mínimo las actualizaciones a medida que los recursos del grupo cambian con el tiempo. También puede filtrar el tráfico con reglas entrantes y salientes mediante grupos de seguridad.

Cuando el tráfico fluye entre las VPC, es habitual utilizar el emparejamiento de VPC para el enrutamiento sencillo o AWS Transit Gateway para el enrutamiento complejo. Con estos enfoques, se facilitan los flujos de tráfico entre el rango de direcciones IP de las redes de origen y destino. Sin embargo, si su carga de trabajo solo requiere flujos de tráfico entre componentes específicos de diferentes VPC, considere la posibilidad de utilizar una conexión punto a punto mediante AWS PrivateLink. Para ello, identifique qué servicio debe actuar como productor y cuál debe actuar como consumidor. Implemente un equilibrador de carga compatible para el productor, active PrivateLink en consecuencia y, a continuación, acepte una solicitud de conexión del consumidor. A continuación, se asignará al servicio del productor una dirección IP privada de la VPC del consumidor que el consumidor podrá usar para efectuar solicitudes posteriores. Este enfoque reduce la necesidad de emparejar las redes. Incluya los costos del procesamiento de datos y el equilibrio de carga como parte de la evaluación de PrivateLink.

Si bien los grupos de seguridad y PrivateLink ayudan a controlar el flujo entre los componentes de sus cargas de trabajo, otro aspecto importante que debe tener en cuenta es cómo controlar los dominios de DNS a los que pueden acceder sus recursos (si los hay). En función de la configuración de DHCP de sus VPC, puede optar por dos servicios de AWS para este fin. La mayoría de los clientes utilizan el servicio de DNS predeterminado de Route 53 Resolver (también denominado servidor DNS de Amazon o AmazonProvideDDNS) disponible para las VPC en la dirección +2 de su rango de CIDR. Con este enfoque, puede crear reglas de firewall de DNS y asociarlas a su VPC para determinar qué acciones tomar para las listas de dominios que proporcione.

Si no usa el servicio Route 53 Resolver o si desea complementarlo con capacidades de inspección y control de flujo más profundas que vayan más allá del filtrado de dominios, considere la posibilidad de implementar un AWS Network Firewall. Este servicio inspecciona los paquetes individuales mediante reglas sin estado o con estado para determinar si se debe denegar o permitir el tráfico. Puede adoptar un enfoque similar para filtrar el tráfico web entrante a sus puntos de enlace públicos con AWS WAF. Para obtener más información sobre estos servicios, consulte SEC05-BP03 Implementación de una protección basada en la inspección.

Pasos para la implementación

1. Identifique los flujos de datos necesarios entre los componentes de sus cargas de trabajo.
2. Aplique múltiples controles con un enfoque de defensa en profundidad tanto para el tráfico entrante como para el saliente, incluido el uso de grupos de seguridad y tablas de enrutamiento.
3. Utilice firewalls para definir un control detallado del tráfico de red entrante, saliente y que pase por sus VPC, como el Firewall DNS de Route 53 Resolver, AWS Network Firewall y AWS WAF.

Considere la posibilidad de usar AWS Firewall Manager para configurar y administrar de forma centralizada las reglas de firewall en toda la organización.

Recursos

Prácticas recomendadas relacionadas:

- REL03-BP01 Elección de cómo segmentar su carga de trabajo
- SEC09-BP02 Aplicación del cifrado en tránsito

Documentos relacionados:

- Prácticas recomendadas de seguridad de la VPC
- AWS Network Optimization Tips
- Guidance for Network Security on AWS
- Secure your VPC's outbound network traffic in the Nube de AWS

Herramientas relacionadas:

- AWS Firewall Manager

Videos relacionados:

- AWS Transit Gateway reference architectures for many VPCs
- Application Acceleration and Protection with Amazon CloudFront, AWS WAF, and AWS Shield
- AWS re:Inforce 2023: Firewalls and where to put them

SEC05-BP03 Implementación de una protección basada en la inspección

Configure puntos de inspección del tráfico entre las capas de la red para asegurarse de que los datos en tránsito coincidan con las categorías y los patrones esperados. Analice los flujos de tráfico, los metadatos y los patrones para ayudar a identificar y detectar los eventos y responder a ellos de manera más eficaz.

Resultado deseado: se inspecciona y se autoriza el tráfico que atraviesa las capas de la red. Basa las decisiones de permiso o denegación en reglas explícitas, información sobre amenazas y

desviaciones de los comportamientos de referencia. Las protecciones son más estrictas a medida que el tráfico se acerca a los datos confidenciales.

Patrones comunes de uso no recomendados:

- Confiar únicamente en las reglas de firewall basadas en puertos y protocolos. No aprovechar los sistemas inteligentes.
- Crear reglas de firewall sobre la base de patrones de amenazas actuales específicos sujetos a cambios.
- Inspeccionar únicamente el tráfico cuando fluye de subredes privadas a públicas, o de subredes públicas a Internet.
- No tener una visión básica del tráfico de la red para comparar las anomalías de comportamiento.

Beneficios de establecer esta práctica recomendada: los sistemas de inspección permiten crear reglas inteligentes, como permitir o denegar el tráfico únicamente cuando existan ciertas condiciones en los datos del tráfico. Beneficiarse de los conjuntos de reglas administradas de AWS y nuestros socios, sobre la base de la inteligencia de amenazas más reciente, a medida que el panorama de amenazas cambia con el tiempo. Esto reduce los gastos administrativos que supone mantener las reglas e investigar los indicadores de situaciones de riesgo, lo que reduce la posibilidad de que se produzcan falsos positivos.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Controle minuciosamente el tráfico de red con y sin estado mediante AWS Network Firewall, otros firewalls y otros sistemas de prevención de intrusiones (IPS) en AWS Marketplace, que puede implementar detrás de un equilibrador de carga de puerta de enlace (GWLB). AWS Network Firewall es compatible con las especificaciones de IPS de código abierto compatibles con Suricata para proteger su carga de trabajo.

Tanto AWS Network Firewall como las soluciones de otros proveedores que utilizan un GWLB admiten diferentes modelos de implementación de inspecciones en línea. Por ejemplo, puede llevar a cabo la inspección en cada VPC, centralizarla en una VPC de inspección o implementarla en un modelo híbrido en el que el tráfico este-oeste fluya a través de una VPC de inspección y las entradas a Internet se inspeccionen en cada VPC. Otra consideración es si la solución admite desempaquetar la seguridad de la capa de transporte (TLS), lo que permite una inspección profunda de los paquetes en busca de flujos de tráfico iniciados en cualquier dirección. Para obtener más información y

detalles en profundidad sobre estas configuraciones, consulte la guía AWS Network Firewall Best Practice.

Si utiliza soluciones que inspeccionan fuera de banda, como el análisis pcap de datos de paquetes de las interfaces de red que funcionan en modo promiscuo, puede configurar el reflejo del tráfico de la VPC. El tráfico reflejado se incluye en el ancho de banda disponible de sus interfaces y está sujeto a los mismos cargos por transferencia de datos que el tráfico no reflejado. Puede comprobar si hay versiones virtuales de estos dispositivos disponibles en AWS Marketplace, que podrían admitir la implementación en línea detrás de un GWLB.

En el caso de los componentes que llevan a cabo transacciones con protocolos basados en HTTP, proteja su aplicación ante las amenazas comunes con un firewall de aplicaciones web (WAF). AWS WAF es un firewall de aplicaciones web que le permite supervisar y bloquear las solicitudes HTTP(S) que coincidan con sus reglas configurables antes de enviarlas a Amazon API Gateway, Amazon CloudFront, AWS AppSync o un equilibrador de carga de aplicación. Piense en la posibilidad de llevar a cabo una inspección de paquetes en profundidad cuando evalúe la implementación del firewall de su aplicación web, ya que algunos requieren que finalice la seguridad de la capa de transporte (TLS) antes de la inspección del tráfico. Para empezar con AWS WAF, puede usar Reglas administradas de AWS junto con sus propias integraciones de socios o utilizar las existentes.

Puede administrar de forma centralizada AWS WAF, AWS Shield Advanced, AWS Network Firewall y los grupos de seguridad de Amazon VPC en toda su organización de AWS con AWS Firewall Manager.

Pasos para la implementación

1. Determine si puede aplicar las reglas de inspección de manera amplia (por ejemplo, mediante una VPC de inspección) o si necesita un enfoque más detallado por cada VPC.
2. Para soluciones de inspección en línea:
   a. Si utiliza AWS Network Firewall, cree reglas, políticas de firewall y el propio firewall. Una vez configurado esto, puede redirigir el tráfico al punto de conexión del firewall para facilitar la inspección.
   b. Si utiliza un dispositivo de terceros con un equilibrador de carga de puerta de enlace (GWLB), implemente y configure su dispositivo en una o más zonas de disponibilidad. A continuación, cree su GWLB, el servicio de punto de conexión y el punto de conexión, y configure el enrutamiento para su tráfico.
3. Para soluciones de inspección fuera de banda:

1. Active el reflejo del tráfico de VPC en las interfaces en las que se deba reflejar el tráfico entrante y saliente. Puede usar reglas de Amazon EventBridge para invocar una función de AWS Lambda con el fin de activar el reflejo del tráfico en las interfaces cuando se creen nuevos recursos. Dirija las sesiones de reflejo del tráfico al equilibrador de carga de red situado frente al dispositivo que procese el tráfico.

4. Para soluciones de tráfico web entrante:

   a. Para configurar AWS WAF, comience por configurar una lista de control de acceso web (ACL web). La ACL web es una colección de reglas con una acción predeterminada procesada en serie (PERMITIR o DENEGAR) que define la forma en que gestiona el tráfico el WAF. Puede crear sus propias reglas y grupos o usar grupos de reglas administradas de AWS en su ACL web.

   b. Una vez configurada la ACL web, asocie la ACL web a un recurso de AWS (como un equilibrador de carga de aplicación, API Gateway, una API de REST o una distribución de CloudFront) para comenzar a proteger el tráfico web.

Recursos

Documentos relacionados:

- What is Traffic Mirroring?
- Implementing inline traffic inspection using third-party security appliances
- AWS Network Firewall example architectures with routing
- Centralized inspection architecture with AWS Gateway Load Balancer and AWS Transit Gateway

Ejemplos relacionados:

- Prácticas recomendadas para implementar el Equilibrador de carga de puerta de enlace
- TLS inspection configuration for encrypted egress traffic and AWS Network Firewall

Herramientas relacionadas:

- AWS Marketplace IDS/IPS

SEC05-BP04 Automatización de la protección de la red

Automatice la implementación de las protecciones de su red mediante prácticas de DevOps, como la infraestructura como código (IaC) y las canalizaciones de CI/CD. Estas prácticas pueden ayudarle a hacer un seguimiento de los cambios en las protecciones de la red a través de un sistema de control de versiones, a reducir el tiempo necesario para implementar los cambios y a detectar si las protecciones de la red se desvían de la configuración deseada.

Resultado deseado: defina las protecciones de red con plantillas y confirmarlas en un sistema de control de versiones. Las canalizaciones automatizadas se inician cuando se hacen nuevos cambios que sirvan para organizar sus pruebas e implementación. Dispone de comprobaciones de políticas y otras pruebas estáticas para validar los cambios antes de la implementación. Implementa los cambios en un entorno provisional para validar que los controles funcionen según lo esperado. También implementa en sus entornos de producción automáticamente una vez que se aprueben los controles.

Patrones comunes de uso no recomendados:

- Confiar en que los equipos de cada carga de trabajo definan individualmente toda su pila de red, sus protecciones y sus automatizaciones. No publicar los aspectos estándares de la pila de red y las protecciones de forma centralizada para que los consuman los equipos de carga de trabajo.
- Confiar en un equipo de red central para definir todos los aspectos de la red, las protecciones y las automatizaciones. No delegar los aspectos específicos de la carga de trabajo de la pila de red y las protecciones al equipo de esa carga de trabajo.
- Lograr el equilibrio adecuado entre la centralización y la delegación entre un equipo de red y los equipos de las cargas de trabajo, pero no aplicar estándares de prueba e implementación uniformes en todas las plantillas de IaC y las canalizaciones de CI/CD. No recoger las configuraciones requeridas en herramientas que comprueben si las plantillas se ajustan a dichas configuraciones.

Beneficios de establecer esta práctica recomendada: el uso de plantillas para definir las protecciones de la red le permite hacer un seguimiento y comparar los cambios a lo largo del tiempo con un sistema de control de versiones. El uso de la automatización para probar e implementar los cambios crea estandarización y previsibilidad, lo que aumenta las posibilidades de que la implementación tenga éxito y reduce las configuraciones manuales repetitivas.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Varios controles de protección de la red que se describen en SEC05-BP02 Control del flujo de tráfico dentro de las capas de red y SEC05-BP03 Implementación de una protección basada en la inspección incluyen sistemas de reglas administradas que pueden actualizarse automáticamente en función de la información sobre amenazas más reciente. Entre los ejemplos de protección de los puntos de enlace web se incluyen las reglas administradas de AWS WAF y la mitigación de DDoS automática en la capa de aplicaciones de AWS Shield Advanced. Utilice los grupos de reglas administradas de AWS Network Firewall para mantenerse al día de las listas de dominios de baja reputación y las firmas de amenazas.

Más allá de las reglas administradas, le recomendamos que utilice prácticas de DevOps para automatizar la implementación de los recursos de red, las protecciones y las reglas que especifique. Puede plasmar estas definiciones en AWS CloudFormation u otra herramienta de infraestructura como código (IaC) de su elección, confirmarlas en un sistema de control de versiones e implementarlas mediante canalizaciones de CI/CD. Utilice este enfoque para obtener los beneficios tradicionales de DevOps para administrar los controles de red, como versiones más predecibles, pruebas automatizadas con herramientas como AWS CloudFormation Guard y detección de desviaciones entre el entorno implementado y la configuración deseada.

En función de las decisiones que haya tomado como parte del proceso descrito en SEC05-BP01 Creación de capas de red, es posible que tenga un enfoque de administración centralizado para la creación de VPC dedicadas a los flujos de entrada, salida e inspección. Tal y como se describe en AWS Security Reference Architecture (AWS SRA), puede definir estas VPC en una cuenta de infraestructura de red dedicada. Puede utilizar técnicas similares para definir de forma centralizada las VPC que utilizan sus cargas de trabajo en otras cuentas, sus grupos de seguridad, las implementaciones de AWS Network Firewall, las reglas de Route 53 Resolver y las configuraciones de firewall DNS, además de otros recursos de red. Puede compartir estos recursos con sus demás cuentas mediante AWS Resource Access Manager. Con este enfoque, puede simplificar las pruebas automatizadas y la implementación de los controles de red en la cuenta de red, y solo tendrá un destino que administrar. Puede hacerlo en un modelo híbrido, en el que implementa y comparte ciertos controles de forma centralizada y delega otros controles a los equipos de carga de trabajo individuales y a sus respectivas cuentas.

Pasos para la implementación

1. Determine qué aspectos de la red y qué protecciones se definen de forma centralizada y cuáles pueden mantener sus equipos de carga de trabajo.

2. Cree entornos para probar e implementar cambios en su red y sus protecciones. Por ejemplo, utilice una cuenta de pruebas de red y una cuenta de producción de red.
3. Determine cómo va a almacenar y mantener las plantillas en un sistema de control de versiones. Almacene las plantillas centrales en un repositorio distinto de los repositorios de carga de trabajo; las plantillas de carga de trabajo se pueden almacenar en repositorios específicos para esa carga de trabajo.
4. Cree canalizaciones de CI/CD para probar e implementar plantillas. Defina pruebas para comprobar si hay errores de configuración y si las plantillas se ajustan a los estándares de su empresa.

Recursos

Prácticas recomendadas relacionadas:

- SEC01-BP06 Automatización de la implementación de controles de seguridad estándares

Documentos relacionados:

- AWS Security Reference Architecture - Network account

Ejemplos relacionados:

- AWS Deployment Pipeline Reference Architecture
- NetDevSecOps to modernize AWS networking deployments
- Integrating AWS CloudFormation security tests with AWS Security Hub CSPM and AWS CodeBuild reports

Herramientas relacionadas:

- AWS CloudFormation
- AWS CloudFormation Guard
- cfn_nag

Protección de la computación

Los recursos de computación incluyen instancias EC2, contenedores, funciones de AWS Lambda, servicios de bases de datos, dispositivos del IoT y más. Cada uno de estos tipos de recursos de computación requiere enfoques diferentes para protegerlos. Sin embargo, comparten estrategias comunes que hay que tener en cuenta: una defensa exhaustiva, la administración de las vulnerabilidades, la reducción de la superficie expuesta a ataques, la automatización de la configuración y el funcionamiento y la ejecución de acciones a distancia. En esta sección, encontrará una guía general para proteger sus recursos de computación de los servicios clave. Para cada servicio de AWS utilizado, es importante que consulte las recomendaciones de seguridad específicas que figuran en la documentación del servicio.

Prácticas recomendadas

- SEC06-BP01 Administración de las vulnerabilidades
- SEC06-BP02 Aprovisionamiento de computación a partir de imágenes reforzadas
- SEC06-BP03 Reducción de la administración manual y el acceso interactivo
- SEC06-BP04 Validación de la integridad del software
- SEC06-BP05 Automatización de la protección de computación

SEC06-BP01 Administración de las vulnerabilidades

Analice con frecuencia su código, sus dependencias y su infraestructura en busca de vulnerabilidades, y aplique parches para solucionarlas, para ayudarle a protegerse contra las nuevas amenazas.

Resultado deseado: tiene una solución que analiza continuamente su carga de trabajo en busca de vulnerabilidades de software, posibles defectos y exposición no intencionada a la red. Ha establecido procesos y procedimientos para identificar, priorizar y corregir estas vulnerabilidades en función de los criterios de evaluación de riesgos. Además, ha implementado la administración automática de parches para sus instancias de computación. Su programa de gestión de vulnerabilidades está integrado en su ciclo de vida de desarrollo de software, con soluciones para escanear el código fuente durante la canalización de CI/CD.

Patrones comunes de uso no recomendados:

- No disponer de un programa de administración de vulnerabilidades.

- Aplicar parches en el sistema sin tener en cuenta la gravedad o la forma de evitar riesgos.
- Utilizar software que haya superado la fecha de fin de vida útil (EOL) de su proveedor.
- Implementar código en producción antes de analizarlo en busca de problemas de seguridad.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

La gestión de vulnerabilidades es un aspecto clave para mantener un entorno de nube seguro y sólido. Conlleva un proceso integral que incluye escaneos de seguridad, identificación y priorización de problemas y operaciones de parches para resolver las vulnerabilidades identificadas. La automatización desempeña un papel fundamental en este proceso, ya que facilita el análisis continuo de las cargas de trabajo para detectar posibles problemas y una exposición no intencionada a la red, así como las iniciativas de corrección.

El modelo de responsabilidad compartida de AWS es un concepto fundamental que sustenta la gestión de vulnerabilidades. Según este modelo, AWS es responsable de proteger la infraestructura subyacente, incluido el equipo, el software, las redes y las instalaciones que ejecutan los servicios de AWS. Por el contrario, es su responsabilidad proteger sus datos, las configuraciones de seguridad y las tareas de administración asociadas a servicios como las instancias de Amazon EC2 y los objetos de Amazon S3.

AWS ofrece numerosos servicios para apoyar los programas de administración de vulnerabilidades. Amazon Inspector analiza continuamente las cargas de trabajo de AWS para detectar vulnerabilidades de software y accesos no deseados a la red, mientras que AWSSystems Manager Patch Manager ayuda a administrar los parches en todas las instancias de Amazon EC2. Estos servicios se pueden integrar con AWS Security Hub CSPM, un servicio de administración de la postura de seguridad en la nube que automatiza los controles de seguridad de AWS, centraliza las alertas de seguridad y proporciona una visión completa de la postura de seguridad de una organización. Además, Amazon CodeGuru Security utiliza el análisis estático del código para identificar posibles problemas en las aplicaciones Java y Python durante la fase de desarrollo.

Al incorporar prácticas de gestión de vulnerabilidades en el ciclo de vida del desarrollo del software, puede abordar las vulnerabilidades de forma proactiva antes de que se introduzcan en los entornos de producción, lo que reduce el riesgo de eventos de seguridad y minimiza el posible impacto de las vulnerabilidades.

Pasos para la implementación

1. Comprenda el modelo de responsabilidad compartida: revise el modelo de responsabilidad compartida de AWS para comprender sus responsabilidades a la hora de proteger sus cargas de trabajo y los datos en la nube. AWS es responsable de proteger la infraestructura en la nube subyacente, mientras que es su responsabilidad proteger las aplicaciones, los datos y los servicios que utiliza.
2. Implemente el análisis de vulnerabilidades: configure un servicio de análisis de vulnerabilidades, como Amazon Inspector, para que analice automáticamente sus instancias de computación (por ejemplo, máquinas virtuales, contenedores o funciones sin servidor) en busca de vulnerabilidades de software, posibles defectos y exposición no intencionada a la red.
3. Establezca procesos de gestión de vulnerabilidades: defina procesos y procedimientos para identificar, priorizar y corregir las vulnerabilidades. Aquí se puede incluir la configuración de programas periódicos de escaneo de vulnerabilidades, el establecimiento de criterios de evaluación de riesgos y la definición de plazos de corrección en función de la gravedad de la vulnerabilidad.
4. Configure la administración de parches: utilice un servicio de administración de parches para automatizar el proceso de aplicación de parches a sus instancias de computación, tanto para los sistemas operativos como para las aplicaciones. Puede configurar el servicio para que analice las instancias en busca de parches ausentes e instalarlos automáticamente de manera planificada. Si lo considera oportuno, puede usar AWS Systems Manager Patch Manager para proporcionar esta funcionalidad.
5. Configure la protección contra el malware: implemente mecanismos para detectar software malicioso en su entorno. Por ejemplo, puede usar herramientas como Amazon GuardDuty para analizar, detectar y alertar sobre el malware en los volúmenes de EC2 y EBS. GuardDuty también puede escanear los objetos recién cargados en Amazon S3 para detectar posibles virus o malware y tomar medidas para aislarlos antes de que se incorporen a los procesos posteriores.
6. Integre el análisis de vulnerabilidades en las canalizaciones de CI/CD: si utiliza una canalización de CI/CD para la implementación de sus aplicaciones, integre herramientas de análisis de vulnerabilidades en su canalización. Herramientas como Amazon CodeGuru Security y las opciones de código abierto pueden analizar el código fuente, las dependencias y los artefactos en busca de posibles problemas de seguridad.
7. Configure un servicio de monitoreo de seguridad: configure un servicio de monitoreo de seguridad, por ejemplo, AWS Security Hub CSPM, para obtener una perspectiva global del estado de su seguridad en varios servicios en la nube. El servicio debe recopilar los resultados de seguridad

de diversas fuentes y presentarlos en un formato estandarizado para facilitar la priorización y la corrección.

8. Implemente pruebas de penetración de aplicaciones web: si su aplicación es una aplicación web y su organización tiene personal capacitado o puede contratar asistencia externa, podría implementar pruebas de penetración de aplicaciones web para identificar posibles vulnerabilidades en su aplicación.
9. Automatice con la infraestructura como código: utilice herramientas de infraestructura como código (IaC), por ejemplo AWS CloudFormation, para automatizar la implementación y la configuración de sus recursos, incluidos los servicios de seguridad mencionados anteriormente. Esta práctica ayuda a crear una arquitectura de recursos más coherente y estandarizada en múltiples cuentas y entornos.
10. Supervise y mejore continuamente: supervise continuamente la eficacia de su programa de gestión de vulnerabilidades y realice las mejoras necesarias. Revise los resultados de seguridad, evalúe la eficacia de sus esfuerzos de corrección y ajuste sus procesos y herramientas en consecuencia.

Recursos

Documentos relacionados:

- AWS Systems Manager
- Security Overview of AWS Lambda
- Amazon CodeGuru
- Improved, Automated Vulnerability Management for Cloud Workloads with a New Amazon Inspector
- Automate vulnerability management and remediation in AWS using Amazon Inspector and AWS Systems Manager – Part 1

Videos relacionados:

- Securing Serverless and Container Services
- Security best practices for the Amazon EC2 instance metadata service

SEC06-BP02 Aprovisionamiento de computación a partir de imágenes reforzadas

Ofrezca menos oportunidades de acceso no deseado a sus entornos en tiempo de ejecución mediante la implementación desde imágenes reforzadas. Adquiera las dependencias de tiempo de ejecución (como imágenes de contenedores y bibliotecas de aplicaciones) únicamente de registros fiables y verifique sus firmas. Cree sus propios registros privados para almacenar imágenes y bibliotecas confiables para usarlas en sus procesos de desarrollo e implementación.

Resultado deseado: sus recursos informáticos se aprovisionan a partir de imágenes de referencia reforzadas. Recupera dependencias externas, como imágenes de contenedores y bibliotecas de aplicaciones, solamente de registros fiables y verifica sus firmas. Las almacena en registros privados para su consulta en los procesos de desarrollo e implementación. Escanea y actualiza las imágenes y las dependencias con regularidad para ayudar a protegerse contra cualquier vulnerabilidad recién descubierta.

Patrones comunes de uso no recomendados:

- Adquirir imágenes y bibliotecas de registros fiables, pero no verificar su firma ni analizar las vulnerabilidades antes de utilizarlas.
- Reforzar las imágenes, pero no probarlas con regularidad para detectar nuevas vulnerabilidades ni actualizarlas a la versión más reciente.
- Instalar o no eliminar paquetes de software que no sean necesarios durante el ciclo de vida esperado de la imagen.
- Confiar únicamente en los parches para mantener actualizados los recursos de computación de producción. El uso de parches por sí solo puede seguir haciendo que los recursos de computación diverjan del estándar reforzado con el paso del tiempo. También es posible que el uso de parches no elimine el malware que un actor de amenazas pueda haber instalado durante un evento de seguridad.

Beneficios de establecer esta práctica recomendada: el refuerzo de las imágenes ayuda a reducir la cantidad de rutas disponibles en el entorno de tiempo de ejecución que pueden permitir el acceso no deseado a usuarios o servicios no autorizados. También puede reducir el alcance del impacto en caso de que se produzca un acceso no deseado.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Para reforzar sus sistemas, comience con las versiones más recientes de los sistemas operativos, las imágenes de contenedores y las bibliotecas de aplicaciones. Aplique parches para solucionar los problemas conocidos. Reduzca al mínimo el sistema eliminando las aplicaciones, los servicios, los controladores de dispositivos, los usuarios predeterminados y otras credenciales que no sean necesarios. Lleve a cabo cualquier otra acción necesaria, como deshabilitar los puertos para crear un entorno que solo tenga los recursos y las capacidades que necesiten sus cargas de trabajo. A partir de ahí, puede instalar el software, los agentes u otros procesos que necesite para objetivos como la supervisión de la carga de trabajo o la administración de vulnerabilidades.

Puede reducir la carga que supone reforzar los sistemas utilizando la orientación que proporcionan orígenes fiables, como el Center for Internet Security (CIS) y las Security Technical Implementation Guides (STIG) de la Defense Information Systems Agency (DISA). Le recomendamos que comience con una imagen de máquina de Amazon (AMI) publicada por AWS o un socio de la APN y que utilice el Generador de imágenes de AWS EC2 para automatizar la configuración de acuerdo con una combinación adecuada de controles del CIS y las STIG.

Si bien existen imágenes reforzadas y recetas del Generador de imágenes de EC2 disponibles que aplican las recomendaciones del CIS o de las STIG de la DISA, es posible que su configuración impida que su software se ejecute correctamente. En esta situación, puede partir de una imagen de base no reforzada, instalar el software y, a continuación, aplicar los controles del CIS de forma gradual para comprobar su impacto. Para cualquier control del CIS que impida la ejecución del software, compruebe si puede implementar las recomendaciones de refuerzo más detalladas prescritas por la DISA. Lleve un registro de los diferentes controles del CIS y de las configuraciones especificadas en las STIG de la DISA que puede aplicar correctamente. Utilícelos para definir consecuentemente sus recetas de refuerzo de imágenes en el Generador de imágenes de EC2.

Para las cargas de trabajo en contenedores, hay imágenes reforzadas de Docker disponibles en el repositorio público de Amazon Elastic Container Registry (ECR). Puede usar el Generador de imágenes de EC2 para reforzar las imágenes de contenedor junto con las AMI.

Al igual que los sistemas operativos y las imágenes de contenedor, puede obtener paquetes de código (o bibliotecas) de repositorios públicos mediante herramientas como pip, npm, Maven y NuGet. Le recomendamos que administre los paquetes de código mediante la integración de repositorios privados, como los que hay en AWS CodeArtifact, con repositorios públicos de confianza. Esta integración puede ocuparse de la recuperación, el almacenamiento y la actualización de los paquetes. Durante los procesos de desarrollo de aplicaciones, se puede obtener y probar la versión más reciente de estos paquetes junto con la aplicación, mediante técnicas como el análisis

de composición de software (SCA), las pruebas de seguridad de aplicaciones estáticas (SAST) y las pruebas dinámicas de seguridad de aplicaciones (DAST).

Para las cargas de trabajo sin servidor que utilicen AWS Lambda, simplifique la administración de las dependencias de los paquetes mediante capas de Lambda. Use las capas de Lambda para configurar un conjunto de dependencias estándares que se compartan entre diferentes funciones en un archivo independiente. Puede crear y mantener capas según su propio proceso de creación, que proporciona un método centralizado de mantener al día sus funciones.

Pasos para la implementación

- Refuerce los sistemas operativos. Utilice imágenes de base de orígenes fiables para crear sus AMI reforzadas. Use el Generador de imágenes de EC2 para ayudar a personalizar el software instalado en las imágenes.
- Refuerce los recursos en contenedores. Configure los recursos en contenedores para cumplir con las prácticas recomendadas de seguridad. Cuando utilice contenedores, implemente el análisis de imágenes de ECR en su canalización de compilación y aplíquelo de forma frecuente a su repositorio de imágenes para buscar CVE en sus contenedores.
- Cuando utilice la implementación sin servidor con AWS Lambda, utilice capas de Lambda para dividir el código de función de la aplicación y las bibliotecas dependientes compartidas. Configure la firma de código para Lambda para asegurarse de que solo se ejecute código fiable en sus funciones de Lambda.

Recursos

Prácticas recomendadas relacionadas:

- OPS05-BP05 Administración de parches

Videos relacionados:

- Deep dive into AWS Lambda security

Ejemplos relacionados:

- Quickly build STIG-compliant AMI using EC2 Image Builder
- Building better container images

- Using Lambda layers to simplify your development process
- Develop & Deploy AWS Lambda Layers using Serverless Framework
- Building end-to-end AWS DevSecOps CI/CD pipeline with open source SCA, SAST and DAST tools

SEC06-BP03 Reducción de la administración manual y el acceso interactivo

Utilice la automatización para hacer tareas de implementación, configuración, mantenimiento e investigación siempre que sea posible. Plantéese el acceso manual a los recursos de computación en casos de procedimientos de emergencia o en entornos seguros (entornos de pruebas) cuando la automatización no esté disponible.

Resultado deseado: los scripts programáticos y los documentos de automatización (manuales de procedimientos) capturan las acciones autorizadas en sus recursos de computación. Estos manuales de procedimientos se inician de forma automática, mediante sistemas de detección de cambios, o manualmente, cuando se requiere una intervención humana. El acceso directo a los recursos de computación solo está disponible en situaciones de emergencia cuando la automatización no está disponible. Todas las actividades manuales se registran y se incorporan a un proceso de revisión para mejorar continuamente las capacidades de automatización.

Patrones comunes de uso no recomendados:

- Acceso interactivo a instancias de Amazon EC2 con protocolos como SSH o RDP.
- Mantener inicios de sesión de los usuarios individuales, como `/etc/passwd` o los usuarios locales de Windows.
- Compartir una contraseña o una clave privada para acceder a una instancia entre varios usuarios.
- Instalar el software y crear o actualizar los archivos de configuración manualmente.
- Actualizar o parchear el software manualmente.
- Iniciar sesión en una instancia para solucionar problemas.

Beneficios de establecer esta práctica recomendada: utilizar la automatización para llevar a cabo acciones le ayuda a reducir el riesgo operativo de los cambios no deseados y los errores de configuración. Eliminar el uso de Secure Shell (SSH) y Remote Desktop Protocol (RDP) para el acceso interactivo reduce el alcance del acceso a los recursos de computación. Todo esto elimina

una ruta que se utiliza habitualmente para llevar a cabo acciones no autorizadas. Al reflejar las tareas de administración de recursos de computación en documentos de automatización y scripts programáticos, se proporciona un mecanismo para definir y auditar todo el alcance de las actividades autorizadas con un alto nivel de detalle.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Iniciar sesión en una instancia es un enfoque clásico de la administración del sistema. Tras instalar el sistema operativo del servidor, los usuarios suelen iniciar sesión manualmente para configurar el sistema e instalar el software deseado. A lo largo de la vida útil del servidor, los usuarios pueden iniciar sesión para llevar a cabo actualizaciones de software, aplicar parches, cambiar configuraciones y solucionar problemas.

Sin embargo, el acceso manual plantea una serie de riesgos. Requiere un servidor que escuche las solicitudes, como un servicio SSH o RDP, que pueden proporcionar una ruta potencial para el acceso no autorizado. También aumenta el riesgo de errores humanos asociados con los pasos manuales. Todo esto puede provocar incidentes relacionados con la carga de trabajo, corrupción o destrucción de datos u otros problemas de seguridad. El acceso humano también requiere protecciones contra el uso compartido de credenciales, lo que genera una sobrecarga de administración adicional.

Para mitigar estos riesgos, puede implementar una solución de acceso remoto basada en agentes, como AWS Systems Manager. AWS Systems Manager El agente (SSM Agent) inicia un canal cifrado y, por lo tanto, no depende de la escucha de solicitudes iniciadas externamente. Tenga en cuenta la posibilidad de configurar el SSM Agent para establecer este canal en un punto de conexión de VPC.

Systems Manager le aporta un control detallado sobre cómo puede interactuar con las instancias administradas. Es el cliente quien define las automatizaciones que se ejecutarán, quién puede ejecutarlas y cuándo pueden ejecutarse. Systems Manager puede aplicar parches, instalar software y hacer cambios en la configuración sin acceso interactivo a la instancia. Systems Manager también puede proporcionar acceso a un intérprete de comandos remoto y registrar todos los comandos invocados y sus resultados durante la sesión en registros y en Amazon S3. AWS CloudTrail registra las invocaciones de las API de Systems Manager para su inspección.

Pasos para la implementación

1. Instale el AWS Systems Manager Agent (SSM Agent) en sus instancias de Amazon EC2. Compruebe si el SSM Agent está incluido y se ha iniciado automáticamente como parte de la configuración básica de la AMI.

2. Compruebe que los roles de IAM asociados a sus perfiles de instancia de EC2 incluyan la política de IAM administrada `AmazonSSMManagedInstanceCore`.
3. Inhabilite SSH, RDP y otros servicios de acceso remoto que se ejecuten en sus instancias. Para hacerlo, puede ejecutar scripts configurados en la sección de datos de usuario de sus plantillas de lanzamiento o crear AMI personalizadas con herramientas como el Generador de imágenes de EC2.
4. Compruebe que las reglas de ingreso de grupos de seguridad aplicables a sus instancias de EC2 no permitan el acceso al puerto 22/tcp (SSH) o al puerto 3389/tcp (RDP). Implemente la detección y las alertas en grupos de seguridad mal configurados mediante servicios como AWS Config.
5. Defina las automatizaciones, los manuales de procedimientos y los comandos de ejecución adecuados en Systems Manager. Utilice políticas de IAM para definir quién puede llevar a cabo estas acciones y las condiciones en las que están permitidas. Pruebe estas automatizaciones minuciosamente en un entorno que no sea de producción. Invoque estas automatizaciones cuando sea necesario, en lugar de acceder a la instancia de forma interactiva.
6. Use AWS Systems Manager Session Manager para proporcionar acceso interactivo a las instancias cuando sea necesario. Active el registro de actividad de la sesión para mantener un registro de auditoría en Registros de Amazon CloudWatch o Amazon S3.

Recursos

Prácticas recomendadas relacionadas:

- REL08-BP04 Implementación mediante una infraestructura inmutable

Ejemplos relacionados:

- Replacing SSH access to reduce management and security overhead with AWS Systems Manager

Herramientas relacionadas:

- AWS Systems Manager

Videos relacionados:

- Controlling User Session Access to Instances in AWS Systems Manager Session Manager

SEC06-BP04 Validación de la integridad del software

Utilice la verificación criptográfica para validar la integridad de los artefactos de software (incluidas las imágenes) que utiliza su carga de trabajo. Firme criptográficamente su software como protección contra los cambios no autorizados que se ejecuten en sus entornos de computación.

Resultado deseado: todos los artefactos se obtienen de orígenes confiables. Se validan los certificados del sitio web del proveedor. Los artefactos descargados se verifican criptográficamente mediante sus firmas. Sus entornos de computación firman y verifican criptográficamente su propio software.

Patrones comunes de uso no recomendados:

- Confiar en los sitios web de proveedores acreditados para obtener artefactos de software, pero ignorar los avisos de caducidad de los certificados. Continuar con las descargas sin confirmar que los certificados son válidos.
- Validar los certificados de los sitios web de los proveedores, pero no verificar criptográficamente los artefactos descargados de estos sitios web.
- Confiar únicamente en resúmenes o hashes para validar la integridad del software. Los hashes establecen que los artefactos no se han modificado con respecto a la versión original, pero no validan su fuente.
- No firmar su propio software, código o bibliotecas, aunque solo los utilice en sus propias implementaciones.

Beneficios de establecer esta práctica recomendada: la validación de la integridad de los artefactos de los que depende su carga de trabajo ayuda a evitar que el malware acceda a sus entornos de computación. La firma de su software ayuda a protegerse contra la ejecución no autorizada en sus entornos informáticos. Proteja su cadena de suministro de software mediante la firma y verificación del código.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Las imágenes del sistema operativo, las imágenes de contenedores y los artefactos de código suelen distribuirse con comprobaciones de integridad disponibles, por ejemplo, mediante un resumen o un hash. Esto permite a los clientes verificar la integridad calculando su propio hash de la carga útil y validando que sea el mismo que el publicado. Si bien estas comprobaciones ayudan a verificar que

la carga útil no se ha manipulado, no validan que provenga de la fuente original (su procedencia). La verificación de la procedencia requiere un certificado emitido por una autoridad de confianza para firmar digitalmente el artefacto.

Si utiliza un software o artefactos descargados en su carga de trabajo, compruebe si el proveedor proporciona una clave pública para la verificación de la firma digital. Estos son algunos ejemplos de cómo AWS proporciona una clave pública e instrucciones de verificación para el software que publicamos:

- EC2 Image Builder: Verify the signature of the AWSTOE installation download
- AWS Systems Manager: Verifying the signature of SSM Agent
- Amazon CloudWatch: Verifying the signature of the CloudWatch agent package

Incorpore la verificación de firmas digitales en los procesos que utilice para obtener y reforzar las imágenes, como se explica en SEC06-BP02 Aprovisionamiento de computación a partir de imágenes reforzadas.

Puede usar AWS Signer para administrar la verificación de firmas, así como su propio ciclo de vida de firma de código para su propio software y artefactos. Tanto AWS Lambda como Amazon Elastic Container Registry proporcionan integraciones con Signer para verificar las firmas de su código y sus imágenes. Con los ejemplos de la sección Recursos, puede incorporar Signer a sus procesos de integración y entrega continuas (CI/CD) para automatizar la verificación de las firmas y la firma de su propio código e imágenes.

Recursos

Documentos relacionados:

- Cryptographic Signing for Containers
- Best Practices to help secure your container image build pipeline by using AWS Signer
- Announcing Container Image Signing with AWS Signer and Amazon EKS
- Configuring code signing for AWS Lambda
- Best practices and advanced patterns for Lambda code signing
- Code signing using AWS Gestor de certificados Private CA and AWS Key Management Service asymmetric keys

Ejemplos relacionados:

- Automate Lambda code signing with Amazon CodeCatalyst and AWS Signer
- Signing and Validating OCI Artifacts with AWS Signer

Herramientas relacionadas:

- AWS Lambda
- AWS Signer
- AWS Gestor de certificados
- AWS Key Management Service
- AWS CodeArtifact

SEC06-BP05 Automatización de la protección de computación

Automatice las operaciones de protección de computación para reducir la necesidad de intervención humana. Utilice el análisis automatizado para detectar posibles problemas en sus recursos de computación y use respuestas programáticas automatizadas u operaciones de administración de flotas para solucionarlos. Incorpore la automatización en sus procesos de CI/CD para implementar cargas de trabajo fiables con dependencias actualizadas.

Resultado deseado: los sistemas automatizados llevan a cabo todos los escaneos y parches de los recursos de computación. Use la verificación automática para comprobar que las imágenes y dependencias del software provengan de orígenes fiables y que no se hayan manipulado. Las cargas de trabajo se comprueban automáticamente para determinar si las dependencias están actualizadas y se firman para establecer la fiabilidad en los entornos de computación de AWS. Las correcciones automatizadas se inician cuando se detectan recursos no conformes con los requisitos.

Patrones comunes de uso no recomendados:

- Seguir la práctica de una infraestructura inmutable sin contar con una solución para la instalación de parches de emergencia o la sustitución de sistemas de producción.
- Usar la automatización para corregir los recursos mal configurados sin contar con un mecanismo de anulación manual. Es posible que surjan situaciones en las que necesite ajustar los requisitos y tenga que suspender las automatizaciones hasta haber hecho estos cambios.

Beneficios de establecer esta práctica recomendada: la automatización puede reducir el riesgo de accesos y usos no autorizados de sus recursos de computación. Ayuda a evitar que lleguen

configuraciones incorrectas a los entornos de producción y a detectarla y corregirlas en caso de que se produzcan. La automatización también contribuye a detectar el acceso y el uso no autorizados de los recursos informáticos para reducir el tiempo de respuesta. Esto, a su vez, puede reducir el alcance general del impacto del problema.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Puede aplicar las automatizaciones descritas en las prácticas del pilar de seguridad para proteger sus recursos de computación. En SEC06-BP01 Administración de las vulnerabilidades se describe cómo puede utilizar Amazon Inspector tanto en sus canalizaciones de CI/CD como para analizar continuamente sus entornos en tiempo de ejecución en busca de vulnerabilidades y exposiciones comunes (CVE) conocidas. Puede usar AWS Systems Manager para aplicar parches o volver a implementar imágenes nuevas mediante manuales de procedimientos automatizados para mantener su flota de computación actualizada con el software y las bibliotecas más recientes. Utilice estas técnicas para reducir la necesidad de recurrir a procesos manuales y el acceso interactivo a sus recursos informáticos. Consulte SEC06-BP03 Reducción de la administración manual y el acceso interactivo para obtener más información.

La automatización también desempeña un papel en la implementación de cargas de trabajo confiables, tal como se describe en SEC06-BP02 Aprovisionamiento de computación a partir de imágenes reforzadas y SEC06-BP04 Validación de la integridad del software. Puede usar servicios como el Generador de imágenes de EC2, AWS Signer, AWS CodeArtifact y Amazon Elastic Container Registry (ECR) para descargar, verificar, construir y almacenar dependencias de código e imágenes reforzadas y aprobadas. Junto con Inspector, cada uno de estos elementos puede desempeñar un papel en su proceso de CI/CD, de modo que su carga de trabajo llegue al entorno de producción solo cuando se confirme que sus dependencias están actualizadas y provienen de orígenes fiables. La carga de trabajo también está firmada para que los entornos de computación de AWS, como AWS Lambda y Amazon Elastic Kubernetes Service (EKS), puedan verificar que no se ha manipulado antes de permitir su ejecución.

Además de estos controles preventivos, también puede utilizar la automatización en sus controles de detección para sus recursos de computación. Por ejemplo, AWS Security Hub CSPM ofrece el estándar NIST 800-53 Rev. 5, que incluye comprobaciones como esta: [EC2.8] las instancias de EC2 deben usar la versión 2 del servicio de metadatos de instancia (IMDSv2). El IMDSv2 utiliza técnicas de autenticación de sesión y bloquea las solicitudes que contienen un encabezado HTTP X-Forwarded-For y un TTL de red de 1 para detener el tráfico que se origina en fuentes externas para recuperar información sobre la instancia de EC2. Esta comprobación en Security Hub CSPM puede

detectar si las instancias de EC2 utilizan IMDSv1 e iniciar una corrección automatizada. Obtenga más información sobre la detección y las correcciones automatizadas en SEC04-BP04 Inicio de correcciones para recursos no conformes.

Pasos para la implementación

1. Automatice la creación de AMI seguras, compatibles y reforzadas con el Generador de imágenes de EC2. Puede producir imágenes que incorporen los controles de los estándares comparativos del Center for Internet Security (CIS) o de la Security Technical Implementation Guide (STIG) a partir de imágenes base de AWS e imágenes de socios de APN.
2. Automatice la administración de la configuración. Aplique y valide configuraciones seguras en sus recursos de computación de forma automática mediante el uso de un servicio o herramienta de gestión de configuraciones.
    a. Administración automatizada de la configuración con AWS Config
    b. Administración automatizada de la posición de seguridad y cumplimiento mediante AWS Security Hub CSPM
3. Automatice la aplicación de parches o el reemplazo de instancias de Amazon Elastic Compute Cloud (Amazon EC2). AWS Systems Manager Patch Manager automatiza el proceso de aplicación de parches a instancias administradas con actualizaciones de seguridad y de otro tipo. Puede utilizar Patch Manager para aplicar parches a los sistemas operativos y a las aplicaciones.
    a. AWS Systems Manager Patch Manager
4. Automatice el análisis de los recursos de computación en busca de vulnerabilidades y exposiciones comunes (CVE) e incorpore soluciones de análisis de seguridad en su proceso de desarrollo.
    a. Amazon Inspector
    b. ECR Image Scanning
5. Plantéese el uso de Amazon GuardDuty para detectar amenazas y malware de forma automática con el fin de proteger los recursos de computación. GuardDuty también puede identificar posibles problemas cuando se invoca una función de AWS Lambda en su entorno de AWS.
    a. Amazon GuardDuty
6. Tenga en cuenta las soluciones de socios de AWS. AWS Los socios ofrecen cientos de productos destacados que son equivalentes o idénticos a los controles que ya utiliza en sus entornos en las instalaciones o que pueden integrarse con ellos. Estos productos complementan a los servicios de AWS existentes y le permiten implementar una arquitectura de seguridad integral, así como disfrutar de una experiencia más fluida tanto en la nube como en los entornos en las instalaciones.

a. Seguridad de la infraestructura

Recursos

Prácticas recomendadas relacionadas:

- SEC01-BP06 Automatización de la implementación de controles de seguridad estándares

Documentos relacionados:

- Get the full benefits of IMDSv2 and disable IMDSv1 across your AWS infrastructure

Videos relacionados:

- Security best practices for the Amazon EC2 instance metadata service

Protección de los datos

Antes de diseñar una carga de trabajo, hay que adoptar prácticas que influyen en la seguridad. Por ejemplo, la clasificación de datos ofrece una manera de categorizar los datos según los niveles de confidencialidad, mientras que el cifrado protege los datos al hacerlos ininteligibles para el acceso no autorizado. Estos métodos son importantes porque respaldan los objetivos, como la prevención de pérdidas financieras o el cumplimiento con las obligaciones normativas.

En AWS, existen varios enfoques distintos que hay que tener en cuenta en relación con la protección de datos. En la siguiente sección se describe cómo se usan estos enfoques.

Temas

- Clasificación de datos
- Protección de los datos en reposo
- Protección de los datos en tránsito

Clasificación de datos

La clasificación de datos proporciona una forma de categorizar los datos de la organización en función del nivel de importancia y la confidencialidad, para ayudarle a determinar los controles de protección y de conservación adecuados.

Prácticas recomendadas

- SEC07-BP01 Comprensión del esquema de clasificación de datos
- SEC07-BP02 Aplicación de controles de protección de datos según la confidencialidad de los datos
- SEC07-BP03 Automatización de la identificación y la clasificación
- SEC07-BP04 Definición de la administración escalable del ciclo de vida de los datos

SEC07-BP01 Comprensión del esquema de clasificación de datos

Comprenda la clasificación de los datos que procesa su carga de trabajo, los requisitos de su tratamiento, los procesos empresariales asociados, dónde se almacenan los datos y quién es su propietario. Su esquema de clasificación y tratamiento de datos debe tener en cuenta los requisitos

legales y de cumplimiento aplicables a su carga de trabajo y los controles de datos necesarios. La comprensión de los datos es el primer paso en el proceso de clasificación de los datos.

Resultado deseado: se comprenden y se documentan adecuadamente los tipos de datos presentes en su carga de trabajo. Dispone de controles adecuados para proteger los datos confidenciales en función de su clasificación. Estos controles determinan cuestiones como quién puede acceder a los datos y con qué propósito, dónde se almacenan los datos, la política de cifrado de esos datos y la forma en que se administran las claves de cifrado, el ciclo de vida de los datos y sus requisitos de retención, los procesos de destrucción pertinentes, los procesos de copia de seguridad y recuperación existentes y la auditoría del acceso.

Patrones comunes de uso no recomendados:

- No contar con una política formal de clasificación de datos para definir los niveles de confidencialidad de los datos y sus requisitos de tratamiento
- No comprender bien los niveles de confidencialidad de los datos dentro de su carga de trabajo y no reflejar esta información en la documentación de la arquitectura y las operaciones
- No aplicar los controles adecuados en torno a sus datos en función de su confidencialidad y sus requisitos, tal como se describe en su política de clasificación y tratamiento de datos
- No proporcionar comentarios sobre los requisitos de clasificación y tratamiento de datos a los propietarios de las políticas.

Beneficios de establecer esta práctica recomendada: esta práctica elimina la ambigüedad en torno al tratamiento adecuado de los datos dentro de su carga de trabajo. La aplicación de una política formal que defina los niveles de confidencialidad de los datos en su organización y las protecciones que requieren puede ayudarle a cumplir la normativa legal y otras acreditaciones y certificaciones de ciberseguridad. Los propietarios de las cargas de trabajo tienen la confianza de saber dónde se almacenan los datos confidenciales y qué controles de protección existen. Plasmar esta información en la documentación ayuda a los nuevos miembros del equipo a comprenderla mejor y a atenerse a estos controles desde el principio de su incorporación. Estas prácticas también pueden contribuir a reducir los costos al dimensionar correctamente los controles para cada tipo de datos.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Al diseñar una carga de trabajo, es posible que se plantee diversas formas de proteger los datos confidenciales de manera intuitiva. Por ejemplo, en una aplicación con varios inquilinos, resulta

intuitivo pensar que los datos de cada inquilino son confidenciales y establecer protecciones para que un inquilino no pueda acceder a los datos de otro. Del mismo modo, puede diseñar controles de acceso de forma intuitiva para que únicamente los administradores puedan modificar los datos y que otros usuarios solo tengan acceso de nivel de lectura o no tengan ningún tipo de acceso.

Al definir y plasmar estos niveles de confidencialidad de los datos en la política, junto con sus requisitos de protección de datos, puede identificar formalmente qué datos residen en su carga de trabajo. A continuación, puede determinar si cuenta con los controles correctos, si los controles se pueden auditar y qué respuestas son apropiadas si se determina que se está produciendo un tratamiento de los datos incorrecto.

Para ayudar a identificar dónde se encuentran los datos confidenciales dentro de su carga de trabajo, puede utilizar un catálogo de datos. Un catálogo de datos es una base de datos que mapea los datos de su organización, su ubicación, nivel de confidencialidad y los controles establecidos para proteger los datos. Además, tiene la opción de utilizar etiquetas de recursos si están disponibles. Por ejemplo, puede aplicar una etiqueta que tenga una clave de etiqueta de `Classification` y un valor de etiqueta de `PHI` para la información de salud protegida (PHI), y otra etiqueta que tenga una clave de etiqueta de `Sensitivity` y un valor de etiqueta de `High`. Servicios como AWS Config se pueden usar a continuación para supervisar estos recursos en busca de cambios y alertar si se modifican de modo que dejen de cumplir los requisitos de protección (por ejemplo, al cambiar la configuración de cifrado). Puede capturar la definición estándar de las claves de sus etiquetas y los valores aceptables mediante políticas de etiquetas, una característica de AWS Organizations. No se recomienda que la clave o el valor de la etiqueta contengan datos privados o confidenciales.

Pasos para la implementación

1. Comprenda el esquema de clasificación de datos y los requisitos de protección de su organización.
2. Identifique los tipos de datos confidenciales que procesan sus cargas de trabajo.
3. Recopile los datos en un catálogo de datos que proporcione una vista única de dónde residen los datos en la organización y su nivel de confidencialidad.
4. Plantéese el uso del etiquetado de recursos y datos (si está disponible) para etiquetar los datos con su nivel de confidencialidad y otros metadatos operativos que puedan contribuir a la supervisión y la respuesta a los incidentes.
   a. Se pueden utilizar políticas de etiquetas de AWS Organizations para hacer cumplir los estándares de etiquetado.

Recursos

Prácticas recomendadas relacionadas:

- SUS04-BP01 Implementación de una política de clasificación de datos

Documentos relacionados:

- Data Classification whitepaper
- Best Practices for Tagging AWS Resources

Ejemplos relacionados:

- AWS Organizations Tag Policy Syntax and Examples

Herramientas relacionadas

- Editor de etiquetas de AWS

SEC07-BP02 Aplicación de controles de protección de datos según la confidencialidad de los datos

Aplique controles de protección de datos que proporcionen un nivel de control adecuado para cada clase de datos definida en su política de clasificación. Esta práctica puede permitirle proteger los datos confidenciales ante el acceso y el uso no autorizados y, al mismo tiempo, preservar la disponibilidad y el uso de los datos.

Resultado deseado: cuenta con una política de clasificación que defina los diferentes niveles de confidencialidad de los datos de su organización. Para cada uno de estos niveles de confidencialidad, haber publicado directrices claras para los servicios y ubicaciones de almacenamiento y gestión aprobados, así como su configuración requerida. Implementa los controles para cada nivel de acuerdo con el nivel de protección requerido y sus costos asociados. Dispone de medidas de supervisión y generación de alertas para detectar si hay datos en ubicaciones no autorizadas, si se están procesando en entornos no autorizados, si hay actores no autorizados que accedan a ellos o si la configuración de los servicios relacionados deja de ser conforme a las normas.

Patrones comunes de uso no recomendados:

- Aplicar el mismo nivel de controles de protección a todos los datos. Esto puede provocar un aprovisionamiento excesivo de controles de seguridad para datos con un bajo nivel de confidencialidad o una protección insuficiente de los datos altamente confidenciales.
- No implicar a las partes interesadas pertinentes de los equipos de seguridad, de cumplimiento y de empresa al definir los controles de protección de datos.
- Pasar por alto los gastos operativos y los costos asociados con la implementación y el mantenimiento de los controles de protección de datos.
- No llevar a cabo revisiones periódicas del control de protección de datos para mantener la alineación con las políticas de clasificación.
- No tener un inventario completo de dónde se encuentran los datos en reposo y en tránsito.

Beneficios de establecer esta práctica recomendada: al alinear los controles con el nivel de clasificación de los datos, la organización puede invertir en niveles de control más altos cuando sea necesario. Esto podría suponer un aumento de los recursos destinados a proteger, supervisar, medir, corregir y notificar. Cuando resulte pertinente tener menos controles, puede mejorar la accesibilidad y la integridad de los datos para sus empleados, clientes o miembros. Este enfoque ofrece a su organización la máxima flexibilidad en el uso de los datos y, al mismo tiempo, sigue cumpliendo los requisitos de protección de datos.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

La implementación de controles de protección de datos según los niveles de confidencialidad de los datos implica varios pasos clave. En primer lugar, identifique los diferentes niveles de confidencialidad de los datos dentro de su arquitectura de cargas de trabajo (por ejemplo: públicos, internos, confidenciales y restringidos) y valore dónde almacenar y procesar estos datos. A continuación, defina los límites de aislamiento en torno a los datos en función de su nivel de confidencialidad. Le recomendamos que separe los datos en diferentes Cuentas de AWS y utilice políticas de control de servicios (SCP) para restringir los servicios y las acciones permitidos para cada nivel de confidencialidad de los datos. De esta manera, puede crear límites de aislamiento bien definidos y hacer cumplir el principio de privilegios mínimos.

Después de definir los límites de aislamiento, implemente los controles de protección adecuados en función de los niveles de confidencialidad de los datos. Consulte las prácticas recomendadas

para proteger los datos en reposo y proteger los datos en tránsito para implementar los controles pertinentes, como el cifrado, los controles de acceso y la auditoría. Plantéese técnicas como la tokenización o la anonimización para reducir el nivel de confidencialidad de sus datos. Simplifique la aplicación de políticas de datos coherentes en toda su empresa con un sistema centralizado de tokenización y destokenización.

Supervise y pruebe continuamente la eficacia de los controles implementados. Revise y actualice periódicamente el esquema de clasificación de datos, las evaluaciones de riesgos y los controles de protección a medida que evolucionen el panorama de datos y las amenazas de su organización. Alinee los controles de protección de datos implementados con los reglamentos, estándares y requisitos legales pertinentes de su sector. Además, ofrezca recursos de concienciación y formación sobre seguridad para ayudar a los empleados a comprender el esquema de clasificación de datos y sus responsabilidades en cuanto al tratamiento y la protección de los datos confidenciales.

Pasos para la implementación

1. Identifique los niveles de clasificación y confidencialidad de los datos dentro de su carga de trabajo.
2. Defina límites de aislamiento para cada nivel y determine una estrategia de cumplimiento.
3. Evalúe los controles definidos para regular el acceso, el cifrado, la auditoría, la retención y el resto de requisitos que exija su política de clasificación de datos.
4. Evalúe las opciones para reducir el nivel de confidencialidad de los datos cuando corresponda, como el uso de la tokenización o la anonimización.
5. Verifique sus controles mediante pruebas y medidas de supervisión automatizadas de los recursos configurados.

Recursos

Prácticas recomendadas relacionadas:

- PERF03-BP01 Uso de un almacén de datos personalizado que se adapte mejor a los requisitos de acceso y almacenamiento de datos
- COST04-BP05 Aplicación de políticas de retención de datos

Documentos relacionados:

- Data Classification whitepaper

- Prácticas recomendadas para la seguridad, la identidad y el cumplimiento
- Prácticas recomendadas de AWS KMS
- Encryption best practices and features for AWS services

Ejemplos relacionados:

- Building a serverless tokenization solution to mask sensitive data
- How to use tokenization to improve data security and reduce audit scope

Herramientas relacionadas:

- AWS Key Management Service (AWS KMS)
- AWS CloudHSM
- AWS Organizations

SEC07-BP03 Automatización de la identificación y la clasificación

La automatización de la identificación y clasificación de datos puede ayudarle a implementar los controles correctos. El uso de la automatización para aumentar la determinación manual reduce el riesgo de errores humanos y exposiciones.

Resultado deseado: puede verificar si dispone de los controles adecuados en función de su política de clasificación y gestión. Las herramientas y los servicios automatizados le ayudan a identificar y clasificar el nivel de confidencialidad de sus datos. La automatización también le ayuda a supervisar continuamente sus entornos para detectar y alertar si los datos se almacenan o gestionen de manera no autorizada, de modo que se puedan tomar medidas correctivas rápidamente.

Patrones comunes de uso no recomendados:

- Confiar únicamente en procesos manuales para la identificación y clasificación de datos, que pueden ser propensos a errores y requerir mucho tiempo. Esto puede provocar una clasificación de datos ineficiente e incoherente, especialmente a medida que aumentan los volúmenes de datos.
- No disponer de mecanismos para rastrear y administrar los activos de datos en toda la organización.

- Pasar por alto la necesidad de supervisar y clasificar continuamente los datos a medida que circulan y evolucionan dentro de la organización.

Beneficios de establecer esta práctica recomendada: la automatización de la identificación y la clasificación de datos puede provocar una aplicación más coherente y precisa de los controles de protección de datos, lo que reduce el riesgo de errores humanos. La automatización también puede proporcionar visibilidad sobre el acceso y la circulación de datos confidenciales, lo que le ayuda a detectar las manipulaciones no autorizadas y a tomar medidas correctivas.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Si bien es habitual recurrir a las decisiones humanas para clasificar los datos durante las fases iniciales del diseño de una carga de trabajo, plantéese la posibilidad de contar con sistemas que automaticen la identificación y la clasificación de los datos de prueba como control preventivo. Por ejemplo, a los desarrolladores se les puede proporcionar una herramienta o un servicio para analizar datos representativos y determinar su confidencialidad. En AWS, puede cargar conjuntos de datos en Amazon S3 y analizarlos con Amazon Macie, Amazon Comprehend o Amazon Comprehend Medical. Del mismo modo, piense en la posibilidad de incluir el análisis de datos como parte de las pruebas unitarias y de integración para detectar en qué puntos no se espera que haya datos confidenciales. Las alertas sobre la presencia de datos confidenciales en esta etapa pueden poner de manifiesto las brechas en las protecciones antes de la implementación en producción. Otras funciones, como la detección de datos confidenciales en AWS Glue, Amazon SNS y Amazon CloudWatch, también se pueden utilizar para detectar datos personales identificables y tomar medidas de mitigación. En el caso de las herramientas o servicios automatizados, comprenda cómo definen los datos confidenciales y compleméntelos con otras soluciones humanas o automatizadas para cubrir las carencias existentes, según sea necesario.

Como control de detección, utilice la supervisión continua de sus entornos para detectar si se están almacenando datos confidenciales de manera no conforme a las normas. Esto puede ayudar a detectar situaciones como la introducción de datos confidenciales en archivos de registro o la copia de este tipo de información en un entorno de análisis de datos sin la debida anonimización o edición. Los datos que se almacenan en Amazon S3 se pueden supervisar continuamente con Amazon Macie para detectar la presencia de datos confidenciales.

Pasos para la implementación

1. Revise el esquema de clasificación de datos de su organización que se describe en SEC07-BP01.

   a. Si comprende el esquema de clasificación de datos de su organización, podrá establecer procesos precisos para la identificación y clasificación automatizadas que se ajusten a las políticas de la empresa.

2. Analice sus entornos inicialmente para llevar a cabo una identificación y una clasificación automatizadas.

   a. El análisis completo inicial de sus datos puede contribuir a obtener un conocimiento detallado de dónde se encuentran los datos confidenciales en sus entornos. Si inicialmente no se requiere un análisis completo o no se puede completar por adelantado debido al costo, evalúe si las técnicas de muestreo de datos son adecuadas para lograr sus resultados. Por ejemplo, se puede configurar Amazon Macie para llevar a cabo una operación amplia y automatizada de detección de datos confidenciales en los buckets de S3. Esta capacidad utiliza técnicas de muestreo para llevar a cabo un análisis preliminar de dónde se encuentran los datos confidenciales de forma asequible. A continuación, se puede hacer un análisis en mayor profundidad de los buckets de S3 mediante un trabajo de detección de datos confidenciales. También se pueden exportar otros almacenes de datos a S3 para escanearlos con Macie.

   b. Establezca el control de acceso que se define en SEC07-BP02 para los recursos de almacenamiento de datos identificados en el análisis.

3. Configure análisis continuos de sus entornos.

   a. La capacidad automatizada de detección de datos confidenciales de Macie se puede utilizar para llevar a cabo análisis continuos de sus entornos. Los buckets de S3 conocidos autorizados para almacenar datos confidenciales se pueden excluir mediante el uso de una lista de permitidos en Macie.

4. Incorpore la identificación y la clasificación en sus procesos de desarrollo y prueba.

   a. Identifique las herramientas que los desarrolladores pueden usar para analizar los datos en busca de información confidencial mientras se están desarrollando las cargas de trabajo. Utilice estas herramientas como parte de las pruebas de integración para recibir alertas cuando la presencia de datos confidenciales sea inesperada y evitar así continuar con la implementación.

5. Implemente un sistema o manual de procedimientos para tomar medidas cuando se encuentren datos confidenciales en ubicaciones no autorizadas.

   a. Restrinja el acceso a los datos mediante la corrección automática. Por ejemplo, puede mover estos datos a un bucket de S3 con acceso restringido o etiquetar el objeto si utiliza el control de acceso basado en atributos (ABAC). Además, considere la posibilidad de enmascarar los datos cuando se detecten.

b. Avise a sus equipos de protección de datos y respuesta a incidentes para que investiguen la causa raíz del incidente. Cualquier aprendizaje que identifique puede ayudar a prevenir futuros incidentes.

Recursos

Documentos relacionados:

- AWS Glue: Detect and process sensitive data
- Using managed data identifiers in Amazon SNS
- Amazon CloudWatch Logs: Help protect sensitive log data with masking

Ejemplos relacionados:

- Enabling data classification for Amazon RDS database with Macie
- Detecting sensitive data in DynamoDB with Macie

Herramientas relacionadas:

- Amazon Macie
- Amazon Comprehend
- Amazon Comprehend Medical
- AWS Glue

SEC07-BP04 Definición de la administración escalable del ciclo de vida de los datos

Comprenda los requisitos del ciclo de vida de sus datos en relación con sus diferentes niveles de clasificación y gestión de datos. Entre ellos pueden estar la forma de gestionar los datos cuando entran por primera vez en su entorno, la manera de transformarlos y las reglas para su destrucción. Tenga en cuenta factores como los periodos de retención, el acceso, la auditoría y el seguimiento de la procedencia.

Resultado deseado: clasifica los datos lo más cerca posible del punto y la hora de la ingestión. Cuando la clasificación de datos requiera el enmascaramiento, la tokenización u otros procesos que

reduzcan el nivel de confidencialidad, llevar a cabo estas acciones lo más cerca posible del punto y el momento de su ingesta.

Elimina los datos de acuerdo con su política cuando ya no resulte apropiado conservarlos en función de su clasificación.

Patrones comunes de uso no recomendados:

- Implementar un enfoque único para la administración del ciclo de vida de los datos, sin tener en cuenta los diferentes niveles de confidencialidad y los requisitos de acceso.
- Plantearse la administración del ciclo de vida únicamente desde la perspectiva de los datos utilizables o de los datos para los que existan copias de seguridad, pero no desde ambas perspectivas.
- Dar por sentado que los datos que han llegado a la carga de trabajo son válidos, sin determinar su valor o procedencia.
- Confiar en la durabilidad de los datos como alternativa a hacer copias de seguridad y protegerlos.
- Retener los datos más allá de su plazo de utilidad y del periodo de retención requerido.

Beneficios de establecer esta práctica recomendada: una estrategia de administración del ciclo de vida de los datos bien definida y escalable ayuda a mantener el cumplimiento normativo, mejora la seguridad de los datos, optimiza los costos de almacenamiento y mejora la eficiencia en el acceso a los datos y el intercambio de estos, mientras se mantienen los controles pertinentes.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Los datos de una carga de trabajo suelen ser dinámicos. La forma que adoptan al entrar en el entorno de una carga de trabajo puede ser diferente a la que adoptan cuando se almacenan o se usan en la lógica empresarial, los informes, el análisis o el machine learning. Además, su valor puede cambiar con el tiempo. Algunos datos son de naturaleza temporal y pierden valor con el paso del tiempo. Tenga en cuenta cómo afectan estos cambios de los datos a la evaluación planteada según su esquema de clasificación de datos y los controles asociados. Siempre que sea posible, utilice un mecanismo de ciclo de vida automatizado, como las políticas de ciclo de vida de Amazon S3 y Amazon Data Lifecycle Manager, para configurar los procesos de retención, archivado y caducidad de datos. Para los datos almacenados en DynamoDB, puede utilizar la característica Tiempo de vida (TTL) para definir una marca de tiempo de caducidad por artículo.

Distinga entre los datos que están disponibles para su uso y aquellos almacenados en copias de seguridad. Plantéese la posibilidad de utilizar AWS Backup para automatizar la copia de seguridad de los datos en todos los servicios de AWS. Las instantáneas de Amazon EBS ofrecen una forma de copiar un volumen de EBS y almacenarlo mediante las funciones de S3, como el ciclo de vida, la protección de datos y el acceso a los mecanismos de protección. Dos de estos mecanismos son Bloqueo de objetos de S3 y Bloqueo de almacenes de AWS Backup, que pueden proporcionarle medidas de seguridad y control adicionales sobre sus copias de seguridad. Administre una separación clara de las funciones y el acceso a las copias de seguridad. Aísle las copias de seguridad de cuenta para mantener la separación del entorno afectado durante un evento.

Otro aspecto de la administración del ciclo de vida consiste en registrar el historial de los datos a medida que avanzan en la carga de trabajo, lo que se denomina seguimiento de la procedencia de los datos. Esto puede ofrecerle la confianza de saber de dónde provienen los datos, qué transformaciones se han hecho, qué propietario o proceso ha hecho esos cambios y cuándo los ha hecho. Disponer de este historial ayuda a solucionar problemas y a llevar a cabo investigaciones durante posibles eventos de seguridad. Por ejemplo, puede registrar los metadatos sobre las transformaciones en una tabla de Amazon DynamoDB. Dentro de un lago de datos, puede guardar copias de los datos transformados en diferentes buckets de S3 para cada etapa de la canalización de datos. Almacene la información del esquema y la marca de tiempo en un AWS Glue Data Catalog. Independientemente de cuál sea su solución, tenga en cuenta los requisitos de los usuarios finales a la hora de determinar las herramientas adecuadas que necesita para informar sobre la procedencia de sus datos. Esto le ayudará a determinar la mejor manera de rastrear su procedencia.

Pasos para la implementación

1. Analice los tipos de datos, los niveles de confidencialidad y los requisitos de acceso de la carga de trabajo para clasificar los datos y definir las estrategias de administración del ciclo de vida adecuadas.
2. Diseñe e implemente políticas de retención de datos y procesos de destrucción automatizados que se ajusten a los requisitos legales, normativos y organizativos.
3. Establezca procesos y medidas de automatización para la supervisión, la auditoría y el ajuste continuos de las estrategias, los controles y las políticas de administración del ciclo de vida de los datos a medida que evolucionen los requisitos y las normativas de la carga de trabajo.
    a. Detecte los recursos que no tienen activada la administración automatizada del ciclo de vida con AWS Config.

Recursos

Prácticas recomendadas relacionadas:

- COST04-BP05 Aplicación de políticas de retención de datos
- SUS04-BP03 Uso de políticas para administrar el ciclo de vida de los conjuntos de datos

Documentos relacionados:

- Data Classification Whitepaper
- AWS Blueprint for Ransomware Defense
- DevOps Guidance: Improve traceability with data provenance tracking

Ejemplos relacionados:

- How to protect sensitive data for its entire lifecycle in AWS
- Build data lineage for data lakes using AWS Glue, Amazon Neptune, and Spline

Herramientas relacionadas:

- AWS Backup
- Administrador de vida útil de datos de Amazon
- AWS Identity and Access Management Access Analyzer

Protección de los datos en reposo

Los datos en reposo representan cualquier dato que se almacene en un almacenamiento no volátil durante cualquier periodo de tiempo de su carga de trabajo. Esto incluye el almacenamiento en bloque, el almacenamiento de objetos, las bases de datos, los archivos, los dispositivos de IoT y todo tipo de forma de almacenamiento en la que se conserven los datos. La protección de los datos en reposo reduce el riesgo de acceso no autorizado si se implementan el cifrado y los controles de acceso adecuados.

El cifrado y la tokenización son dos esquemas de protección de datos importantes, pero distintos.

La tokenización es un proceso que le permite definir un token para representar un dato de carácter confidencial (por ejemplo, un token para representar el número de la tarjeta de crédito de un cliente). Un token debe carecer de sentido por sí solo y no debe derivarse de los datos que está tokenizando; por lo tanto, un resumen criptográfico no se puede utilizar como token. Al planificar minuciosamente el enfoque de tokenización, puede proporcionar protección adicional al contenido y puede asegurarse de que satisface los requisitos de conformidad. Por ejemplo, puede reducir el ámbito de complimiento de un sistema de procesamiento de tarjetas de crédito si aprovecha un token en lugar de un número de tarjeta de crédito.

El cifrado es un método de transformación de contenido que impide que este se pueda leer sin una clave secreta necesaria para descifrarlo y convertirlo en texto sin formato. La tokenización y el cifrado se pueden usar para asegurar y proteger la información cuando corresponda. Además, el enmascaramiento es una técnica que permite redactar parte de un dato hasta el punto de que el resto de los datos no se considere confidencial. Por ejemplo, PCI-DSS permite retener los últimos cuatro dígitos del número de una tarjeta fuera del límite de cumplimiento para su indexación.

Auditoría del uso de claves de cifrado: asegúrese de comprender y auditar el uso de las claves de cifrado para comprobar que los mecanismos de control de acceso de las claves se implementen de forma adecuada. Por ejemplo, cualquier servicio de AWS que utilice una clave de AWS KMS registra cada uso en AWS CloudTrail. A continuación, puede hacer consultas a AWS CloudTrail mediante una herramienta como Información de registros de Amazon CloudWatch para asegurarse de que todos los usos de sus claves sean válidos.

Prácticas recomendadas

- SEC08-BP01 Implementación de una administración de claves segura
- SEC08-BP02 Aplicación del cifrado en reposo
- SEC08-BP03 Automatización de la protección de los datos en reposo
- SEC08-BP04 Aplicación del control de acceso

SEC08-BP01 Implementación de una administración de claves segura

La administración segura de claves incluye el almacenamiento, la rotación, el control de acceso y la supervisión del material de claves necesario para proteger los datos en reposo para su carga de trabajo.

Resultado deseado: tiene un mecanismo de administración de claves escalable, repetible y automatizado. El mecanismo hace cumplir el acceso con privilegios mínimos al material de claves

y proporciona el equilibrio correcto entre la disponibilidad, la confidencialidad y la integridad de las claves. Supervisa el acceso a las claves y, si es necesario rotar el material de claves, las rota mediante un proceso automatizado. No permite que los operadores humanos accedan al material de claves.

Patrones comunes de uso no recomendados:

- Acceso humano a material de claves no cifrado.
- Crear algoritmos criptográficos personalizados.
- Permisos demasiado amplios para acceder a material de claves.

Beneficios de establecer esta práctica recomendada: al establecer un mecanismo de administración de claves seguro para su carga de trabajo, puede ayudar a proteger su contenido contra el acceso no autorizado. Además, es posible que esté sujeto a requisitos reglamentarios de cifrado de datos. Una solución de administración de claves eficaz puede proporcionar mecanismos técnicos alineados con esas regulaciones para proteger el material de claves.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

El cifrado de los datos en reposo es un control de seguridad fundamental. Para implementar este control, su carga de trabajo necesita un mecanismo que almacene y administre de forma segura el material de claves utilizado para cifrar los datos en reposo.

AWS ofrece AWS Key Management Service (AWS KMS) para proporcionar un almacenamiento duradero, seguro y redundante para las claves de AWS KMS. Muchos servicios de AWS se integran con AWS KMS para respaldar el cifrado de sus datos. AWS KMS utiliza módulos de seguridad de hardware validados por la norma FIPS 140-3 de nivel 3 para proteger sus claves. No hay ningún mecanismo para exportar claves de AWS KMS en texto sin formato.

Si se implementan cargas de trabajo mediante una estrategia de cuentas múltiples, se considera una debe mantener las claves de AWS KMS en la misma cuenta que la carga de trabajo que las utiliza. En este modelo distribuido, la responsabilidad de administrar las claves de AWS KMS recae sobre su equipo. En otros casos de uso, su organización puede optar por almacenar las claves de AWS KMS en una cuenta centralizada. Esta estructura centralizada requiere políticas adicionales para habilitar el acceso entre cuentas necesario para que la cuenta de carga de trabajo acceda a las claves almacenadas en la cuenta centralizada, pero puede ser más aplicable en casos de uso en los que una sola clave se comparte entre varias Cuentas de AWS.

Independientemente de dónde se almacene el material de claves, el acceso a la clave debe controlarse estrictamente mediante el uso de políticas de claves y políticas de IAM. Las políticas de claves son la forma principal de controlar el acceso a una clave de AWS KMS. Además, las concesiones de claves de AWS KMS pueden proporcionar acceso a servicios de AWS para cifrar y descifrar datos en su nombre. Revise las orientaciones de control de acceso a sus claves de AWS KMS.

Debería supervisar el uso de claves de cifrado para detectar patrones de acceso inusuales. Las operaciones hechas con claves administradas por AWS y claves administradas por el cliente almacenadas en AWS KMS pueden registrarse en AWS CloudTrail y deben revisarse periódicamente. Preste especial atención al monitoreo de los eventos de destrucción de claves. Para mitigar la destrucción accidental o malintencionada de material de claves, los eventos de destrucción de claves no eliminan el material de claves inmediatamente. Los intentos de eliminar claves de AWS KMS están sujetos a un periodo de espera predeterminado de 30 días y un mínimo de 7 días, lo que da tiempo a los administradores para revisar estas acciones y anular la solicitud si es necesario.

La mayoría de los servicios de AWS utilizan AWS KMS de forma transparente; su único requisito es decidir si desea utilizar una clave administrada por AWS o por el cliente. Si la carga de trabajo requiere el uso directo de AWS KMS para cifrar o descifrar datos, se recomienda utilizar cifrado de sobre para proteger los datos. La SDK de cifrado de AWS puede proporcionar a sus aplicaciones elementos básicos de cifrado del cliente para implementar el cifrado de sobre e integrarse con AWS KMS.

Pasos para la implementación

1. Determine las opciones de administración de claves apropiadas (administradas por AWS o administradas por el cliente) para la clave.
   a. Para facilitar el uso, AWS ofrece claves propias de AWS y administradas por AWS para la mayoría de los servicios, que proporcionan la capacidad de cifrado en reposo sin la necesidad de administrar el material de claves o las políticas de claves.
   b. Si utiliza claves administradas por el cliente, considere el almacén de claves predeterminado para ofrecer el mejor equilibrio entre agilidad, seguridad, soberanía de datos y disponibilidad. Otros casos de uso podrían exigir el uso de almacenes de claves personalizados con AWS CloudHSM o el almacén de clave externo.
2. Revise la lista de servicios que utiliza para su carga de trabajo para comprender cómo AWS KMS se integra con el servicio. Por ejemplo, las instancias de EC2 pueden usar volúmenes de EBS cifrados, que verifican que las instantáneas de Amazon EBS creadas a partir de esos volúmenes

también estén cifradas mediante una clave administrada por el cliente y mitigan la divulgación accidental de datos de instantáneas no cifrados.

   a. How AWS services use AWS KMS

   b. Para obtener información detallada sobre las opciones de cifrado que ofrece un servicio de AWS, consulte el tema de cifrado en reposo en la guía del usuario o en la guía para desarrolladores del servicio.

3. Implemente AWS KMS: AWS KMS le permite crear y administrar fácilmente las claves y controlar el uso del cifrado en una gran variedad de servicios de AWS y en sus aplicaciones.

   a. Introducción: AWS Key Management Service (AWS KMS)

   b. Revise las prácticas recomendadas de control de acceso a sus claves de AWS KMS.

4. Puede usar el SDK de cifrado de AWS: utilice el SDK de cifrado de AWS con la integración de AWS KMS cuando la aplicación necesite cifrar datos del cliente.

   a. SDK de cifrado de AWS

5. Habilite el Analizador de acceso de IAM para revisar y notificar automáticamente si hay políticas de claves de AWS KMS demasiado amplias.

   a. Plantéese utilizar comprobaciones de políticas personalizadas para comprobar que una actualización de la política de recursos no concede acceso público a las claves de KMS.

6. Habilite Security Hub CSPM para recibir notificaciones si hay políticas de claves mal configuradas, claves programadas para su eliminación o claves sin la rotación automática habilitada.

7. Determine el nivel de registro adecuado para sus claves de AWS KMS. Como las llamadas a AWS KMS, incluidos los eventos de solo lectura, se registran, los registros de CloudTrail asociados con AWS KMS pueden resultar voluminosos.

   a. Algunas organizaciones prefieren dividir la actividad de registro de AWS KMS en una ruta distinta. Para obtener más detalles, consulte la sección de registro de llamadas a la API de AWS KMS con CloudTrail de la guía para desarrolladores de AWS KMS.

Recursos

Documentos relacionados:

- AWS Key Management Service
- AWS cryptographic services and tools
- Protecting Amazon S3 Data Using Encryption
- Cifrado de sobre

- Digital sovereignty pledge
- Demystifying AWS KMS key operations, bring your own key, custom key store, and ciphertext portability
- AWS Key Management Service cryptographic details

Videos relacionados:

- How Encryption Works in AWS
- Securing Your Block Storage on AWS
- AWS data protection: Using locks, keys, signatures, and certificates

Ejemplos relacionados:

- Implement advanced access control mechanisms using AWS KMS

SEC08-BP02 Aplicación del cifrado en reposo

Cifre los datos privados en reposo para mantener la confidencialidad y proporcionar una capa adicional de protección contra la divulgación o exfiltración de datos no deseada. El cifrado protege los datos para que no sea posible leerlos ni acceder a ellos sin antes descifrarlos. Haga un inventario y lleve un control de los datos no cifrados para mitigar los riesgos asociados a la exposición de los datos.

Resultado deseado: tiene mecanismos que cifran los datos privados de forma predeterminada cuando estén en reposo. Estos mecanismos ayudan a mantener la confidencialidad de los datos y proporcionan una capa adicional de protección contra la divulgación o exfiltración involuntaria de datos. Mantiene un inventario de datos no cifrados y comprende los controles que existen para protegerlos.

Patrones comunes de uso no recomendados:

- No utilizar configuraciones para que el cifrado se haga de forma predeterminada.
- Proporcionar un acceso demasiado permisivo a las claves de descifrado.
- No supervisar el uso de las claves de cifrado y descifrado.
- Almacenar datos sin cifrar.

- Utilizar la misma clave de cifrado para todos los datos, independientemente de su uso, tipos y clasificación.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Asigne claves de cifrado a clasificaciones de datos en sus cargas de trabajo. Este enfoque ayuda a proteger contra un acceso excesivamente permisivo si utiliza una única clave de cifrado, o muy pocas, para sus datos (consulte SEC07-BP01 Comprensión del esquema de clasificación de datos).

AWS Key Management Service (AWS KMS) se integra con muchos servicios de AWS para facilitar el cifrado de sus datos en reposo. Por ejemplo, en Amazon Elastic Compute Cloud (Amazon EC2) puede establecer el cifrado predeterminado en cuentas para que todos los volúmenes nuevos de EBS se cifren automáticamente. Cuando utilice AWS KMS, tenga en cuenta hasta qué punto es necesario restringir los datos. Las claves de AWS KMS predeterminadas y controladas por el servicio son administradas y utilizadas por AWS en su nombre. En el caso de los datos confidenciales que requieren un acceso detallado a la clave de cifrado subyacente, considere la posibilidad de usar claves administradas por el cliente (CMK). Tiene el control total sobre las CMK, incluida la rotación y la administración del acceso mediante el uso de políticas de claves.

Además, servicios como Amazon Simple Storage Service (Amazon S3) ahora cifran todos los objetos nuevos de forma predeterminada. Esta implementación proporciona una seguridad mejorada sin afectar al rendimiento.

Otros servicios, como Amazon Elastic Compute Cloud (Amazon EC2) o Amazon Elastic File System (Amazon EFS) admiten ajustes para el cifrado predeterminado. También puede utilizar Reglas de AWS Config para comprobar automáticamente que está utilizando cifrado para volúmenes de Amazon Elastic Block Store (Amazon EBS), instancias de Amazon Relational Database Service (Amazon RDS), buckets de Amazon S3 y otros servicios de su organización.

AWS también proporciona opciones para el cifrado del cliente, lo que le permite cifrar los datos antes de subirlos a la nube. El AWS Encryption SDK proporciona una forma de cifrar sus datos mediante el cifrado de sobre. Proporciona la clave de encapsulado y AWS Encryption SDK genera una clave de datos única para cada objeto de datos que cifra. Considere la posibilidad de utilizar AWS CloudHSM si necesita un módulo de seguridad de hardware (HSM) administrado de un solo inquilino. AWS CloudHSM le permite generar, importar y administrar claves criptográficas en un HSM validado por FIPS 140-2 nivel 3. Entre los casos de uso de AWS CloudHSM, se incluye la protección de claves privadas para la emisión de una autoridad de certificación (CA) y la habilitación del cifrado

de datos transparente (TDE) para bases de datos Oracle. El SDK de cliente de AWS CloudHSM proporciona software que le permite cifrar datos del cliente mediante claves almacenadas dentro de AWS CloudHSM antes de subir sus datos a AWS. El Cliente de encriptación de Amazon DynamoDB también le permite cifrar y firmar elementos antes de subirlos a una tabla de DynamoDB.

Pasos para la implementación

- Configuración del cifrado predeterminado para los nuevos volúmenes de Amazon EBS: especifique que desea que todos los volúmenes de Amazon EBS recién creados se creen de forma cifrada, con la opción de utilizar la clave predeterminada que proporciona AWS o una clave que cree.
- Configuración de imágenes de máquina de Amazon (AMI) cifradas: al copiar una AMI existente con cifrado habilitado, se cifran automáticamente las instantáneas y los volúmenes raíz.
- Configuración del cifrado de Amazon RDS: configure el cifrado para sus clústeres de base de datos e instantáneas en reposo de Amazon RDS mediante la opción de cifrado.
- Creación y configuración de claves de AWS KMS con políticas que limiten el acceso a las entidades principales adecuadas para cada clasificación de datos: por ejemplo, cree una clave de AWS KMS para cifrar los datos de producción y otra distinta para cifrar los datos de desarrollo o de prueba. También puede proporcionar acceso a la clave a otras Cuentas de AWS. Considere la posibilidad de tener cuentas diferentes para sus entornos de desarrollo y de producción. Si en su entorno de producción es necesario descifrar artefactos en la cuenta de desarrollo, puede editar la política de CMK que se utiliza para cifrar los artefactos de desarrollo para otorgar a la cuenta de producción la capacidad de descifrar dichos artefactos. Después, el entorno de producción puede ingerir los datos descifrados para usarlos en producción.
- Configuración del cifrado en servicios de AWS adicionales: para otros servicios de AWS que utilice, revise la documentación de seguridad de ese servicio para determinar las opciones de cifrado del servicio.

Recursos

Documentos relacionados:

- AWS Crypto Tools
- AWS Encryption SDK
- AWS KMS Cryptographic Details Whitepaper
- AWS Key Management Service
- AWS cryptographic services and tools

- Amazon EBS Encryption
- Default encryption for Amazon EBS volumes
- Encrypting Amazon RDS Resources
- ¿Cómo puedo habilitar el cifrado predeterminado para un bucket de Amazon S3?
- Protecting Amazon S3 Data Using Encryption

Videos relacionados:

- How Encryption Works in AWS
- Securing Your Block Storage on AWS

SEC08-BP03 Automatización de la protección de los datos en reposo

Utilice la automatización para validar y aplicar los controles de datos en reposo. Utilice el análisis automatizado para detectar errores de configuración de sus soluciones de almacenamiento de datos y, en la medida de lo posible, aplique las correcciones mediante una respuesta programática automatizada. Incorpore la automatización en sus procesos de CI/CD para detectar errores de configuración del almacenamiento de datos antes de que se implementen en producción.

Resultado deseado: los sistemas automatizados analizan y supervisan las ubicaciones de almacenamiento de datos para detectar los errores de configuración de los controles, el acceso no autorizado y el uso inesperado. La detección de ubicaciones de almacenamiento mal configuradas inicia las correcciones automatizadas. Los procesos automatizados crean copias de seguridad de los datos y almacenan copias inmutables fuera del entorno original.

Patrones comunes de uso no recomendados:

- No tener en cuenta las opciones de habilitar el cifrado de forma predeterminada, cuando sea posible.
- No tener en cuenta los eventos de seguridad, además de los eventos operativos, al formular una estrategia automatizada de copias de seguridad y recuperación.
- No aplicar la configuración de acceso público a los servicios de almacenamiento.
- No supervisar ni auditar los controles para proteger los datos en reposo.

Beneficios de establecer esta práctica recomendada: la automatización ayuda a prevenir el riesgo de configurar erróneamente las ubicaciones de almacenamiento de datos. También ayuda a evitar

que los errores de configuración lleguen a los entornos de producción. Esta práctica recomendada también ayuda a detectar y corregir errores de configuración si se producen.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

La automatización es una noción común a todas las prácticas de protección de los datos en reposo. SEC01-BP06 Automatización de la implementación de controles de seguridad estándares describe cómo puede plasmar la configuración de sus recursos en plantillas de infraestructura como código (IaC), por ejemplo, conAWS CloudFormation. Estas plantillas están confirmadas con un sistema de control de versiones y se utilizan para implementar recursos en AWS a través de una canalización de CI/CD. Estas técnicas también se aplican a la automatización de la configuración de sus soluciones de almacenamiento de datos, como la configuración de cifrado en los buckets de Amazon S3.

Puede comprobar la configuración que defina en sus plantillas de IaC para determinar si hay errores de configuración en sus canalizaciones de CI/CD mediante las reglas en AWS CloudFormation Guard. Puede supervisar los ajustes que aún no estén disponibles en CloudFormation u otras herramientas de IaC para detectar errores de configuración con AWS Config. Las alertas que Config genera por errores de configuración se pueden corregir automáticamente, tal como se describe en SEC04-BP04 Inicio de correcciones para recursos no conformes.

El uso de la automatización como parte de su estrategia de administración de permisos también es un componente integral de las protecciones de datos automatizadas. SEC03-BP02 Concesión de acceso con privilegios mínimos y SEC03-BP04 Reducción continua de los permisos describen la configuración de políticas de acceso con privilegios mínimos bajo la supervisión continua del AWS Identity and Access Management Access Analyzer para generar resultados cuando puedan reducirse los permisos. Además de la automatización de los permisos de supervisión, puede configurar Amazon GuardDuty para detectar comportamientos anómalos en el acceso a los datos de sus volúmenes de EBS (a través de una instancia de EC2), buckets de S3 y bases de datos de Amazon Relational Database Service compatibles.

La automatización también desempeña un papel a la hora de detectar cuándo se almacenan datos confidenciales en ubicaciones no autorizadas. SEC07-BP03 Automatización de la identificación y la clasificación describe cómo Amazon Macie puede supervisar sus buckets de S3 para detectar datos confidenciales inesperados y generar alertas que puedan iniciar una respuesta automática.

Siga las prácticas de REL09 Copia de seguridad de los datos para desarrollar una estrategia automatizada de copia de seguridad y recuperación de datos. La copia de seguridad y la

recuperación de datos son tan importantes para la recuperación de los eventos de seguridad como para los eventos operativos.

Pasos para la implementación

1. Capture la configuración de almacenamiento de datos en plantillas de IaC. Utilice comprobaciones automatizadas en sus canalizaciones de CI/CD para detectar errores de configuración.
   a. Para CloudFormation puede usar sus plantillas de IaC, y CloudFormation Guard para comprobar si hay errores de configuración en las plantillas.
   b. Utilice AWS Config para ejecutar reglas en un modo de evaluación proactiva. Use esta configuración para comprobar la conformidad de un recurso como uno de los pasos del proceso de CI/CD antes de crearlo.
2. Supervise los recursos en busca de errores de configuración de almacenamiento de datos.
   a. Configure AWS Config para supervisar los recursos de almacenamiento de datos con el fin de detectar cambios en las configuraciones de control y para generar alertas que invoquen acciones correctivas cuando se detecte un error de configuración.
   b. Consulte SEC04-BP04 Inicio de correcciones para recursos no conformes para obtener más información sobre las correcciones automatizadas.
3. Supervise y reduzca los permisos de acceso a los datos de forma continua mediante la automatización.
   a. El Analizador de acceso de IAM puede ejecutarse de forma continua para generar alertas cuando los permisos puedan reducirse.
4. Supervise los comportamientos anómalos de acceso a los datos y emita alertas si detecta alguno.
   a. GuardDuty vigila tanto las firmas de amenazas conocidas como las desviaciones de los comportamientos de acceso básicos para los recursos de almacenamiento de datos, como los volúmenes de EBS, los buckets de S3 y las bases de datos de RDS.
5. Supervise los datos confidenciales que se almacenan en ubicaciones inesperadas y emita alertas si detecta algún caso.
   a. Use Amazon Macie para analizar continuamente sus buckets de S3 en busca de datos confidenciales.
6. Automatice las copias de seguridad seguras y cifradas de sus datos.
   a. AWS Backup es un servicio administrado que crea copias de seguridad de diferentes orígenes de datos en AWS. La Recuperación de desastres elástica le permite copiar cargas de trabajo completas del servidor y mantener una protección de datos continua con un objetivo de punto

de recuperación (RPO) medido en segundos. Puede configurar ambos servicios para que funcionen en conjunto con el fin de automatizar la creación de copias de seguridad de datos y su almacenamiento en ubicaciones de conmutación por error. Esto puede ayudar a mantener sus datos disponibles cuando se vean afectados por eventos operativos o de seguridad.

Recursos

Prácticas recomendadas relacionadas:

- SEC01-BP06 Automatización de la implementación de controles de seguridad estándares
- SEC03-BP02 Concesión de acceso con privilegios mínimos
- SEC03-BP04 Reducción continua de los permisos
- SEC04-BP04 Inicio de correcciones para recursos no conformes
- SEC07-BP03 Automatización de la identificación y la clasificación
- REL09-BP02 Protección y cifrado de copias de seguridad
- REL09-BP03 Copias de seguridad automáticas de los datos

Documentos relacionados:

- AWS Prescriptive Guidance: Automatically encrypt existing and new Amazon EBS volumes
- Ransomware Risk Management on AWS Using the NIST Cyber Security Framework (CSF)

Ejemplos relacionados:

- How to use AWS Config proactive rules and AWS CloudFormation Hooks to prevent creation of noncompliant cloud resources
- Automate and centrally manage data protection for Amazon S3 with AWS Backup
- AWS re:Invent 2023 - Implement proactive data protection using Amazon EBS snapshots
- AWS re:Invent 2022 - Build and automate for resilience with modern data protection

Herramientas relacionadas:

- AWS CloudFormation Guard
- AWS CloudFormation Guard Rules Registry

- IAM Access Analyzer
- Amazon Macie
- AWS Backup
- Recuperación de desastres elástica

SEC08-BP04 Aplicación del control de acceso

Para ayudarlo a proteger sus datos en reposo, aplique el control de acceso mediante mecanismos como el aislamiento y el control de versiones. Aplique controles de acceso condicional y de privilegios mínimos. Impida que se conceda acceso público a sus datos.

Resultado deseado: verifica que solo los usuarios autorizados puedan acceder a los datos en función de su necesidad de utilizarlos. Protege sus datos con copias de seguridad periódicas y el control de versiones para evitar que se modifiquen o eliminen de forma intencionada o involuntaria. Aísla los datos críticos de otros datos para proteger la confidencialidad y la integridad.

Patrones comunes de uso no recomendados:

- Almacenar juntos datos con diferentes requisitos de confidencialidad o clasificación.
- Utilizar permisos demasiado permisivos en las claves de descifrado.
- Clasificar incorrectamente los datos.
- No conservar copias de seguridad detalladas de los datos importantes.
- Proporcionar acceso persistente a los datos de producción.
- No auditar el acceso a los datos ni revisar periódicamente los permisos.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

La protección de los datos en reposo es importante para mantener la integridad, la confidencialidad y el cumplimiento de los requisitos normativos. Puede implementar varios controles para lograrlo, como el control de acceso, el aislamiento, el acceso condicional y el control de versiones.

Puede aplicar el control de acceso con el principio de privilegios mínimos, que proporciona a los usuarios y los servicios únicamente los permisos necesarios para realizar sus tareas. Esto incluye el acceso a las claves de cifrado. Revise sus políticas de AWS Key Management Service (AWS KMS)

para comprobar que el nivel de acceso que concede es el adecuado y que se aplican las condiciones pertinentes.

Puede separar los datos en función de diferentes niveles de clasificación utilizando distintas Cuentas de AWS para cada nivel y administrar estas cuentas utilizando AWS Organizations. Este aislamiento puede ayudar a evitar el acceso no autorizado y minimizar el riesgo de exposición de los datos.

Revise con regularidad el nivel de acceso concedido en las políticas de buckets de Amazon S3. Evite el uso de buckets de lectura o escritura pública a menos que sea absolutamente necesario. Plantéese utilizar AWS Config para detectar buckets disponibles para el público y Amazon CloudFront para ofrecer contenido de Amazon S3. Verifique que los buckets que no deben permitir el acceso público estén configurados correctamente para impedirlo.

Implemente mecanismos de control de versiones y bloqueo de objetos para los datos críticos almacenados en Amazon S3. El control de versiones de Amazon S3 conserva las versiones anteriores de los objetos para recuperar los datos en caso de que se eliminen o sobrescriban accidentalmente. Bloqueo de objetos de Amazon S3 proporciona un control de acceso obligatorio para los objetos, lo que impide que se eliminen o sobrescriban, incluso por parte del usuario raíz, hasta que caduque el bloqueo. Además, Amazon Glacier Vault Lock ofrece una característica similar para los archivos almacenados en Amazon Glacier.

Pasos para la implementación

1. Aplique el control de acceso con el principio del privilegio mínimo:
   - Revise los permisos de acceso concedidos a los usuarios y servicios y compruebe que solo tienen los permisos necesarios para realizar sus tareas.
   - Revise el acceso a las claves de cifrado consultando las políticas de AWS Key Management Service (AWS KMS).
2. Separe los datos en función de los diferentes niveles de clasificación:
   - Utilice distintas Cuentas de AWS para cada nivel de clasificación de datos.
   - Administre estas cuentas mediante AWS Organizations.
3. Revise los permisos de buckets y objetos de Amazon S3:
   - Revise con regularidad el nivel de acceso concedido en las políticas de buckets de Amazon S3.
   - Evite el uso de buckets de lectura o escritura pública a menos que sea absolutamente necesario.
   - Valore la posibilidad de utilizar AWS Config para detectar buckets con disponibilidad pública.
   - Use Amazon CloudFront para ofrecer contenido de Amazon S3.

- Verifique que los buckets que no deben permitir el acceso público estén configurados correctamente para impedirlo.
- Puede aplicar el mismo proceso de revisión a las bases de datos y a cualquier otro origen de datos que utilice la autenticación de IAM, como SQS o almacenes de datos de terceros.

4. Use AWS IAM Access Analyzer:
   - Puede configurar Analizador de acceso de IAM de AWS para analizar buckets de Amazon S3 y generar resultados cuando una política de S3 concede acceso a una entidad externa.
5. Implemente mecanismos de control de versiones y bloqueo de objetos:
   - Utilice el control de versiones de Amazon S3 para conservar las versiones anteriores de los objetos, lo que permite recuperarlos en caso de eliminaciones o sobrescrituras accidentales.
   - Utilice Bloqueo de objetos de Amazon S3 para añadir un control de acceso obligatorio para los objetos, con lo que ni siquiera el usuario raíz podrá eliminarlos o sobrescribirlos hasta que caduque el bloqueo.
   - Utilice Amazon Glacier Vault Lock para los archivos almacenados en Amazon Glacier.
6. Utilice el inventario de Amazon S:
   - Puede usar el inventario de Amazon S3 para auditar e informar sobre el estado de replicación y cifrado de sus objetos de S3.
7. Revise los permisos de uso compartido de Amazon EBS y AMI:
   - Revise los permisos de uso compartido de Amazon EBS y Uso compartido de AMI para comprobar que las imágenes y los volúmenes se compartan con Cuentas de AWS externas a su carga de trabajo.
8. Revise periódicamente los recursos compartidos de AWS Resource Access Manager:
   - Puede utilizar AWS Resource Access Manager para compartir recursos, como las políticas de AWS Network Firewall, las reglas de Amazon Route 53 Resolver y las subredes, dentro de sus Amazon VPC.
   - Audite periódicamente los recursos compartidos y deje de compartir los recursos que ya no sea necesario compartir.

Recursos

Prácticas recomendadas relacionadas:

- SEC03-BP01 Definición de los requisitos de acceso
- SEC03-BP02 Concesión de acceso con privilegios mínimos

Documentos relacionados:

- AWS KMS Cryptographic Details Whitepaper
- Introducción a la administración de permisos de acceso para los recursos de Amazon S
- Overview of managing access to your AWS KMS resources
- Reglas de AWS Config
- Amazon S3 + Amazon CloudFront: A Match Made in the Cloud
- Usar el control de versiones en buckets de S
- Usar Bloqueo de objetos de Amazon S
- Sharing an Amazon EBS Snapshot
- AMI compartidas
- Hosting a single-page application on Amazon S3
- AWS Claves de condición globales de
- Building a Data Perimeter on AWS

Videos relacionados:

- Securing Your Block Storage on AWS

Protección de los datos en tránsito

Los datos en tránsito son todos aquellos que se transmiten de un sistema a otro. Incluye la comunicación entre recursos de la carga de trabajo, así como entre otros servicios y los usuarios finales. Con el nivel de protección adecuado para los datos en tránsito, protege la confidencialidad y la integridad de los datos de la carga de trabajo.

Protección de los datos entre ubicaciones de VPC o en las instalaciones: puede utilizar AWS PrivateLinkpara crear una conexión de red segura y privada entre Amazon Virtual Private Cloud (Amazon VPC) o la conectividad en las instalaciones con los servicios alojados en AWS. Puede acceder a servicios de AWS, servicios de terceros y servicios de otras Cuentas de AWS como si estuvieran en su red privada. Con AWS PrivateLink, puede acceder a los servicios de todas las cuentas con CIDR de IP superpuestas sin necesidad de puertas de enlace de Internet o NAT. Tampoco es necesario configurar las reglas de firewall, las definiciones de rutas ni las tablas de enrutamiento. El tráfico permanece en la red troncal de Amazon y no atraviesa Internet, por lo que sus datos están protegidos. Puede mantener el cumplimiento de las normas de cumplimiento

específicas del sector, como la HIPAA y el Privacy Shield de la UE/EE. UU. AWS PrivateLink funciona sin problemas con soluciones de terceros para crear una red global simplificada, lo que le permite acelerar su migración a la nube y aprovechar los servicios de AWS disponibles.

Prácticas recomendadas

- SEC09-BP01 Implementación de la administración segura de claves y certificados
- SEC09-BP02 Aplicación del cifrado en tránsito
- SEC09-BP03 Autenticación de las comunicaciones de red

SEC09-BP01 Implementación de la administración segura de claves y certificados

Los certificados de seguridad de la capa de transporte (TLS) se utilizan para proteger las comunicaciones de red y establecer la identidad de los sitios web, los recursos y las cargas de trabajo a través de Internet, así como de las redes privadas.

Resultado deseado: un sistema de administración de certificados seguro que puede aprovisionar, implementar, almacenar y renovar certificados en una infraestructura de clave pública (PKI). Un mecanismo seguro de administración de claves y certificados evita que se divulgue el material de claves privadas del certificado y renueva automáticamente el certificado de forma periódica. También se integra con otros servicios para proporcionar comunicaciones de red e identidad seguras para los recursos de la máquina dentro de su carga de trabajo. Las identidades humanas nunca deben tener acceso al material de claves.

Patrones comunes de uso no recomendados:

- Seguir pasos manuales durante los procesos de implementación o renovación del certificado.
- No prestar suficiente atención a la jerarquía de la autoridad de certificación (CA) al diseñar una CA privada.
- Usar certificados autofirmados para recursos públicos.

Beneficios de establecer esta práctica recomendada:

- Simplificar la administración de certificados mediante la implementación y la renovación automatizadas
- Fomentar el cifrado de los datos en tránsito mediante certificados TLS

- Aumentar la seguridad y auditabilidad de las medidas de certificación adoptadas por la autoridad de certificación
- Organizar las tareas de administración en los diferentes capas de la jerarquía de CA

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Las cargas de trabajo modernas hacen un uso extensivo de las comunicaciones de red cifradas mediante protocolos PKI como TLS. La administración de certificados de PKI puede ser compleja, pero el aprovisionamiento, la implementación y la renovación automatizados de los certificados pueden reducir la fricción asociada con la administración de certificados.

AWS proporciona dos servicios para administrar los certificados de PKI de uso general: AWS Gestor de certificados y AWS Autoridad de certificación privada (AWS Privada CA). ACM es el servicio principal que los clientes utilizan para aprovisionar, administrar e implementar certificados para su uso tanto en cargas de trabajo de AWS tanto públicas como privadas. ACM emite certificados privados mediante AWS Privada CA y se integra con muchos otros servicios administrados de AWS para proporcionar certificados TLS seguros para las cargas de trabajo. ACM también puede emitir certificados de confianza pública de los servicios de confianza de Amazon. Los certificados públicos de ACM se pueden usar en cargas de trabajo públicas, ya que los navegadores y sistemas operativos modernos confían en estos certificados de forma predeterminada.

AWS Privada CA le permite establecer su propia autoridad de certificación raíz o subordinada y emitir certificados TLS a través de una API. Puede usar este tipo de certificados en situaciones en las que controla y administra la cadena de confianza en el lado del cliente de la conexión TLS. Además de los casos de uso de TLS, AWS Privada CA se puede utilizar para emitir certificados para pods de Kubernetes, atestaciones de productos de dispositivos Matter, firma de código y otros casos de uso con una plantilla personalizada. También puede utilizar IAM Roles Anywhere para proporcionar credenciales temporales de IAM a las cargas de trabajo en las instalaciones a las que se les hayan emitido certificados X.509 firmados por su CA privada.

Además de ACM y AWS Privada CA, AWS IoT Core proporciona soporte especializado para el aprovisionamiento, la administración y la implementación de certificados de PKI en dispositivos de IoT. AWS IoT Core proporciona mecanismos especializados para incorporar dispositivos de IoT en su infraestructura de clave pública a escala.

Algunos servicios de AWS, como Amazon API Gateway y Elastic Load Balancing, ofrecen sus propias capacidades de uso de certificados para proteger las conexiones de las aplicaciones. Por

ejemplo, tanto API Gateway como Application Load Balancer (ALB) admiten el TLS mutuo (mTLS) mediante certificados de cliente que se crean y exportan mediante la Consola de administración de AWS, CLI o las API.

Consideraciones para establecer una jerarquía de CA privada

Si tiene que establecer una CA privada, es importante prestar especial atención para diseñar correctamente la jerarquía de CA desde el principio. Se recomienda implementar cada nivel de jerarquía de CA en Cuentas de AWS independientes al crear una jerarquía de CA privada. Este paso deliberado reduce el área de superficie de cada nivel de la jerarquía de CA, lo que facilita la detección de anomalías en los datos de registro de CloudTrail y reduce el alcance del acceso o el impacto si se produce un acceso no autorizado a una de las cuentas. La CA raíz debe residir en su propia cuenta independiente y solo debe usarse para emitir uno o más certificados de CA intermedios.

A continuación, cree una o más CA intermedias en cuentas independientes de la cuenta de la CA raíz para emitir certificados para los usuarios finales, los dispositivos u otras cargas de trabajo. Por último, emita certificados desde su CA raíz a las CA intermedias, que a su vez emitirán certificados para sus usuarios finales o dispositivos. Para obtener más información sobre la planificación de la implementación de la CA y el diseño de la jerarquía de las CA, incluida la planificación de la resiliencia, la replicación entre regiones, el uso compartido de las CA en toda la organización y mucho más, consulte Planificación de la implementación de AWS Privada CA.

Pasos para la implementación

1. Determine los servicios de AWS pertinentes que necesita para su caso de uso:
    - Muchos casos de uso pueden utilizar la infraestructura de clave pública existente de AWS mediante AWS Gestor de certificados. ACM se puede usar para implementar certificados TLS para servidores web, equilibradores de carga u otros usos para certificados de confianza pública.
    - Considere AWS Privada CA cuando necesite establecer su propia jerarquía de autoridades de certificación privadas o necesite acceder a certificados exportables. ACM se puede utilizar entonces para emitir muchos tipos de certificados de entidad final mediante la AWS Privada CA.
    - Para los casos de uso en los que los certificados se deben aprovisionar a escala para dispositivos de Internet de las cosas (IoT) integrados, considere AWS IoT Core.
    - Puede utilizar la funcionalidad mTLS nativa en servicios como Amazon API Gateway o Application Load Balancer.
2. Implemente la renovación automática de certificados siempre que sea posible:

- Utilice la renovación administrada de ACM para los certificados emitidos por ACM junto con los servicios administrados de AWS integrados.

3. Establezca registros y registros de auditoría:
   - Habilite los registros de CloudTrail para hacer un seguimiento del acceso a las cuentas que tienen autoridades de certificación. Considere configurar la validación de integridad del archivo de registro en CloudTrail para verificar la autenticidad de los datos de registro.
   - Genere y revise periódicamente informes de auditoría que enumeren los certificados que su CA privada ha emitido o revocado. Estos informes se pueden exportar a un bucket de S3.
   - Al implementar una CA privada, también tendrá que establecer un bucket de S3 para almacenar la lista de revocación de certificados (CRL). Para obtener instrucciones sobre cómo configurar este bucket de S3 en función de los requisitos de su carga de trabajo, consulte Planificación de una lista de revocación de certificados (CRL).

Recursos

Prácticas recomendadas relacionadas:

- SEC02-BP02 Uso de credenciales temporales
- SEC08-BP01 Implementación de una administración de claves segura
- SEC09-BP03 Autenticación de las comunicaciones de red

Documentos relacionados:

- How to host and manage an entire private certificate infrastructure in AWS
- How to secure an enterprise scale ACM Private CA hierarchy for automotive and manufacturing
- Private CA best practices
- How to use AWS RAM to share your ACM Private CA cross-account

Videos relacionados:

- Activating AWS Gestor de certificados Private CA (workshop)

Ejemplos relacionados:

- Private CA workshop

- IOT Device Management Workshop (incluido el aprovisionamiento de dispositivos)

Herramientas relacionadas:

- Plugin to Kubernetes cert-manager to use AWS Privada CA

SEC09-BP02 Aplicación del cifrado en tránsito

Aplique los requisitos de cifrado definidos en función de las políticas, las obligaciones reglamentarias y las normas de su organización para ayudarle a cumplir los requisitos organizativos, legales y de cumplimiento. Utilice únicamente protocolos con cifrado cuando transmita datos confidenciales fuera de su nube privada virtual (VPC). El cifrado ayuda a mantener la confidencialidad de los datos incluso cuando transitan por redes que no son de confianza.

Resultado deseado: el tráfico de red entre sus recursos e Internet debe cifrarse para mitigar el acceso no autorizado a los datos. Cifra el tráfico de red en su entorno de AWS interno de acuerdo con sus requisitos de seguridad. Cifra todos los datos en tránsito mediante protocolos TLS seguros y conjuntos de cifrado.

Patrones comunes de uso no recomendados:

- Utilizar versiones de SSL, TLS y componentes del conjunto de cifrado obsoletos (por ejemplo, SSL v3.0, claves RSA de 1024 bits y cifrado RC4).
- Permitir tráfico no cifrado (HTTP) hacia o desde recursos destinados al público.
- No supervisar y sustituir los certificados X.509 antes de que caduquen.
- Utilizar certificados X.509 autofirmados para TLS.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Los servicios de AWS facilitan puntos de conexión HTTPS con TLS para la comunicación, lo que proporciona cifrado en tránsito al comunicarse con las API de AWS. Los protocolos no seguros, como HTTP, se pueden auditar y bloquear en una nube privada virtual (VPC) mediante el uso de grupos de seguridad. Las solicitudes HTTP también se pueden redirigir automáticamente a HTTPS en Amazon CloudFront o en un Equilibrador de carga de aplicación. Puede utilizar una política de buckets de Amazon Simple Storage Service (Amazon S3) para restringir la capacidad de cargar

objetos a través de HTTP, lo que impone el uso de HTTPS para cargar objetos en sus buckets. Dispone de un control total sobre los recursos de computación para implementar el cifrado en tránsito en los servicios. También puede usar la conectividad de VPN en la VPC desde una red externa o AWS Direct Connect para facilitar el cifrado de tráfico. Compruebe que sus clientes hagan llamadas a las API de AWS mediante al menos TLS 1.2, ya que AWS va a dejar de utilizar versiones anteriores de TLS en febrero de 2024. Se recomienda utilizar TLS 1.3. Si tiene requisitos especiales para el cifrado en tránsito, puede encontrar soluciones de terceros disponibles en AWS Marketplace.

Pasos para la implementación

- Aplicación del cifrado en tránsito: los requisitos de cifrado definidos deben basarse en los últimos estándares y prácticas recomendadas, y solo permitir protocolos seguros. Por ejemplo, configure un grupo de seguridad para permitir solamente el protocolo HTTPS a una instancia del equilibrador de carga de aplicaciones o una instancia de Amazon EC2.
- Configuración de protocolos seguros en los servicios de periferia: configure HTTPS con Amazon CloudFront y utilice un perfil de seguridad apropiado para su posición de seguridad y su caso de uso.
- Uso de una VPN para la conectividad externa: considere la posibilidad de utilizar una VPN IPsec para proteger las conexiones de punto a punto o de red a red para ofrecer tanto privacidad como integridad de los datos.
- Configuración de protocolos seguros en los equilibradores de carga: seleccione una política de seguridad que proporcione los conjuntos de cifrado más seguros que admitan los clientes que se conectarán al oyente. Cree un oyente HTTPS para su equilibrador de carga de aplicación.
- Configuración de protocolos seguros en Amazon Redshift: configure su clúster para que requiera una conexión de capa de sockets seguros (SSL) o de seguridad de la capa de transporte (TLS).
- Configuración de protocolos seguros: revise la documentación del servicio de AWS para determinar las capacidades de cifrado en tránsito.
- Configuración del acceso seguro al cargar en los buckets de Amazon S3: utilice los controles de políticas de buckets de Amazon S3 para aplicar el acceso seguro a los datos.
- Consideración de uso de AWS Gestor de certificados: ACM le permite aprovisionar, administrar e implementar certificados TLS públicos para utilizarlos con los servicios de AWS.
- Consideración de uso de AWS Autoridad de certificación privada para las necesidades de PKI privadas: AWS Privada CA le permite crear jerarquías de autoridades de certificación (CA) privadas para emitir certificados X.509 de entidad final que pueden utilizarse para crear canales TLS cifrados.

Recursos

Documentos relacionados:

- Uso de HTTPS con CloudFront
- Conectar la VPC a redes remotas mediante AWS Virtual Private Network
- Create an HTTPS listener for your Application Load Balancer
- Tutorial: Configure SSL/TLS on Amazon Linux 2
- Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos
- Configuración de las opciones de seguridad para las conexiones

SEC09-BP03 Autenticación de las comunicaciones de red

Verifique la identidad de las comunicaciones mediante el uso de protocolos que admiten la autenticación, como la seguridad de la capa de transporte (TLS) o IPsec.

Diseñe su carga de trabajo para utilizar protocolos de red seguros y autenticados siempre que haya una comunicación entre servicios, aplicaciones o usuarios. El uso de protocolos de red que admiten autenticación y autorización proporciona un mayor control sobre los flujos de red y reduce la repercusión del acceso no autorizado.

Resultado deseado: una carga de trabajo con flujos de tráfico entre servicios bien definidos en el plano de datos y en el plano de control. Los flujos de tráfico utilizan protocolos de red autenticados y cifrados cuando es técnicamente posible.

Patrones comunes de uso no recomendados:

- Tener tráfico no cifrado o no autenticado en la carga de trabajo.
- Reutilizar credenciales de autenticación para varios usuarios o entidades.
- Confiar únicamente en los controles de red como mecanismo de control de acceso.
- Crear un mecanismo de autenticación personalizado en lugar de confiar en los mecanismos de autenticación estándar del sector.
- Tener un tráfico excesivamente permisivo entre los componentes del servicio u otros recursos de la VPC.

Beneficios de establecer esta práctica recomendada:

- Limita el alcance de la repercusión del acceso no autorizado a una parte de la carga de trabajo.
- Proporciona un nivel de garantía mayor de que las acciones solo las llevan a cabo entidades autenticadas.
- Mejora el desacoplamiento de los servicios al definir claramente las interfaces de transferencia de datos previstas y obligar a usarlas.
- Mejora la supervisión, el registro y la respuesta a los incidentes mediante la atribución de solicitudes y unas interfaces de comunicación bien definidas.
- Proporciona una defensa en profundidad para las cargas de trabajo al combinar los controles de red con los controles de autenticación y autorización.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: bajo

Guía para la implementación

Los patrones de tráfico de red de la carga de trabajo se pueden clasificar en dos categorías:

- El tráfico este-oeste representa los flujos de tráfico entre los servicios que constituyen una carga de trabajo.
- El tráfico norte-sur representa los flujos de tráfico entre su carga de trabajo y los consumidores.

Aunque es una práctica común cifrar el tráfico norte-sur, es menos común proteger el tráfico este-oeste mediante protocolos autenticados. Las prácticas de seguridad modernas recomiendan que el diseño de red por sí solo no garantice una relación de confianza entre dos entidades. Cuando dos servicios pueden residir dentro de un límite de red común, sigue siendo una buena práctica recomendada cifrar, autenticar y autorizar las comunicaciones entre esos servicios.

Por ejemplo, las API del servicio de AWS utilizan el protocolo de firma AWS Signature Version 4 (SigV4) para autenticar a la persona que llama, independientemente de la red en la que se origine la solicitud. Esta autenticación garantiza que las API de AWS puedan verificar la identidad que solicitó la acción y, a continuación, esa identidad se pueda combinar con políticas para tomar una decisión de autorización que determine si la acción debe permitirse o no.

Servicios como Amazon VPC Lattice y Amazon API Gateway le permiten usar el mismo protocolo de firma SigV4 para incorporar autenticación y autorización al tráfico este-oeste en sus propias cargas de trabajo. Si los recursos fuera de su entorno de AWS necesitan comunicarse con servicios que requieren autenticación y autorización basadas en Sigv4, puede usar AWS Identity and Access

Management (IAM) Roles Anywhere en el recurso que no es de AWS para adquirir credenciales de AWS temporales. Estas credenciales se pueden usar para firmar solicitudes de los servicios que utilizan SigV4 para autorizar el acceso.

Otro mecanismo común para autenticar el tráfico este-oeste es la autenticación mutua de TLS (mTLS). Muchas aplicaciones de internet de las cosas (IoT), aplicaciones de empresa a empresa y microservicios utilizan mTLS para validar la identidad de ambos lados de una comunicación TLS mediante el uso de certificados X.509 del lado del cliente y del lado del servidor. Estos certificados puede emitirlos AWS Autoridad de certificación privada (AWS Privada CA). Puede utilizar servicios como Amazon API Gateway para proporcionar autenticación mTLS para la comunicación entre cargas de trabajo o dentro de ellas. El Equilibrador de carga de aplicación también admite mTLS para cargas de trabajo internas o externas. Aunque mTLS proporciona información de autenticación para ambos lados de una comunicación TLS, no tiene un mecanismo de autorización.

Por último, OAuth 2.0 y OpenID Connect (OIDC) son dos protocolos que se suelen utilizar para controlar el acceso de los usuarios a los servicios, pero ahora también se están popularizando para el tráfico de servicio a servicio. API Gateway proporciona un autorizador de token web JSON (JWT) que permite a las cargas de trabajo restringir el acceso a las rutas de la API mediante JWT emitidas por proveedores de identidad OIDC u OAuth 2.0. Los ámbitos OAuth2 pueden utilizarse como fuente para tomar las decisiones de autorización básicas, pero las comprobaciones de autorizaciones siguen teniendo que implementarse en la capa de aplicación, y los ámbitos OAuth2 por sí solos no pueden satisfacer necesidades de autorización más complejas.

Pasos para la implementación

- Definición y documentación de los flujos de red de su carga de trabajo: el primer paso para implementar una estrategia de defensa en profundidad es definir los flujos de tráfico de la carga de trabajo.
  - Cree un diagrama de flujo de datos en el que se defina claramente cómo se transmiten los datos entre los diferentes servicios que componen su carga de trabajo. Este diagrama es el primer paso para imponer esos flujos a través de canales de red autentificados.
  - Instrumente su carga de trabajo en las fases de desarrollo y prueba para validar que el diagrama de flujo de datos refleje con precisión el comportamiento de la carga de trabajo en tiempo de ejecución.
  - Un diagrama de flujo de datos también puede ser útil cuando se lleva a cabo un ejercicio de modelado de amenazas, como se describe en SEC01-BP07 Identificación de amenazas y priorización de mitigaciones con un modelo de amenazas.

- Establecimiento de controles de red: considere la posibilidad de usar las capacidades de AWS para establecer controles de red que se ajusten a sus flujos de datos. Aunque los límites de la red no deberían ser el único control de seguridad, estos proporcionan una capa en la estrategia de defensa en profundidad para proteger su carga de trabajo.
  - Use grupos de seguridad para establecer, definir y restringir los flujos de datos entre los recursos.
  - Considere la posibilidad de usar AWS PrivateLink para comunicarse con servicios de AWS y de terceros compatibles con AWS PrivateLink. Los datos que se envían a través de un punto de conexión de la interfaz de AWS PrivateLink permanecen en la estructura de red de AWS y no atraviesan la Internet pública.
- Implementación de autenticación y autorización en todos los servicios de su carga de trabajo: elija el conjunto de servicios de AWS más adecuado para proporcionar flujos de tráfico autenticados y cifrados en su carga de trabajo.
  - Considere la posibilidad de usar Amazon VPC Lattice para proteger la comunicación de servicio a servicio. VPC Lattice puede usar la autenticación SigV4 combinada con políticas de autenticación para controlar el acceso de un servicio a otro.
  - Para la comunicación de servicio a servicio mediante mTLS, puede usar API Gateway o Equilibrador de carga de aplicación. AWS Privada CA se puede usar para establecer una jerarquía de CA privada capaz de emitir certificados para su uso con los mTLS.
  - Al hacer la integración con servicios que utilizan OAuth 2.0 u OIDC, considere la posibilidad de usar API Gateway con el autorizador JWT.
  - Para la comunicación entre la carga de trabajo y los dispositivos de IoT, considere la posibilidad de usar AWS IoT Core, que ofrece varias opciones para el cifrado y la autenticación del tráfico de red.
- Supervisión del acceso no autorizado: supervise continuamente los canales de comunicación no deseados, las entidades principales no autorizadas que intentan acceder a los recursos protegidos y otros patrones de acceso inadecuados.
  - Si utiliza VPC Lattice para administrar el acceso a sus servicios, piense en la posibilidad de habilitar y supervisar registros de acceso de VPC Lattice. Estos registros de acceso incluyen información sobre la entidad solicitante, información de red, incluida la VPC de origen y destino, y los metadatos de la solicitud.
  - Considere la posibilidad de habilitar registros de flujo de VPC para capturar los metadatos de los flujos de red y revisarlos periódicamente para detectar anomalías.

- Consulte la AWS Security Incident Response Guide y la sección Respuesta ante incidentes del pilar de seguridad del Marco de AWS Well-Architected para obtener más información sobre la planificación, la simulación y la respuesta a los incidentes de seguridad.

Recursos

Prácticas recomendadas relacionadas:

- SEC03-BP07 Análisis del acceso público y entre cuentas
- SEC02-BP02 Uso de credenciales temporales
- SEC01-BP07 Identificación de amenazas y priorización de mitigaciones con un modelo de amenazas

Documentos relacionados:

- Evaluating access control methods to secure Amazon API Gateway APIs
- Configuring mutual TLS authentication for a REST API
- How to secure API Gateway HTTP endpoints with JWT authorizer
- Authorizing direct calls to AWS services using AWS IoT Core credential provider
- AWS Security Incident Response Guide

Videos relacionados:

- AWS re:invent 2022: Introducing VPC Lattice
- AWS re:invent 2020: Serverless API authentication for HTTP APIs on AWS

Ejemplos relacionados:

- Amazon VPC Lattice Workshop
- Taller “Zero-Trust Episode 1 – The Phantom Service Perimeter”

Respuesta a incidentes

Incluso con controles eficaces de detección y prevención, la organización debería continuar implementando mecanismos para responder ante incidentes de seguridad y mitigar su posible impacto. Su preparación afecta considerablemente a la capacidad de los equipos de operar de forma eficaz durante un incidente, de aislar, contener y hacer una investigación forense de los problemas y de restaurar operaciones a un estado conocido correcto. La preparación de las herramientas y el acceso en previsión de un incidente de seguridad, así como la práctica periódica de la respuesta ante incidentes durante simulacros, lo ayudan a asegurarse de que podrá recuperarse con una interrupción mínima en el negocio.

Temas

- Aspectos de la respuesta ante incidentes de AWS
- Diseño de objetivos de respuesta en la nube
- Preparación
- Operaciones
- Actividad posterior al incidente

Aspectos de la respuesta ante incidentes de AWS

Todos los usuarios de AWS de una organización deben tener un conocimiento básico de los procesos de respuesta ante incidentes de seguridad; de igual manera, el personal de seguridad debe entender cómo responder a los problemas de seguridad. La educación, la capacitación y la experiencia son fundamentales para el éxito de un programa de respuesta ante incidentes en la nube y, en un escenario ideal, deben implementarse mucho antes de tener que gestionar un posible incidente de seguridad. La base de un programa de respuesta antes incidentes exitoso en la nube es la preparación, las operaciones y la actividad posterior al incidente.

A continuación se describe cada uno de estos aspectos para que los entienda mejor:

- Preparación: prepare a su equipo de respuesta ante incidentes para que detecte y responda a los incidentes internos de AWS mediante la habilitación de controles de detección y la comprobación de que tengan el acceso adecuado a las herramientas y los servicios en la nube necesarios. Asimismo, prepare las guías de estrategias necesarias, tanto manuales como automatizadas, para comprobar respuestas fiables y coherentes.

- Operaciones: opere en caso de eventos de seguridad y posibles incidentes según las fases de respuesta ante incidentes del NIST (detección, análisis, contención, erradicación y recuperación).
- Actividad posterior al incidente: repita el resultado de sus eventos y simulaciones de seguridad para mejorar la eficacia de su respuesta, aumentar el valor derivado de la respuesta y la investigación y reducir aún más el riesgo. Hay que aprender de los incidentes y ser plenamente responsable de las actividades de mejora.

En el siguiente diagrama se muestra el flujo de estos aspectos y se alinea con el ciclo de vida de respuesta ante incidentes del NIST mencionado anteriormente, pero con operaciones que abarcan detección y análisis con contención, erradicación y recuperación.

Aspectos de la respuesta ante incidentes de AWS

Diseño de objetivos de respuesta en la nube

Si bien los procesos y mecanismos generales de respuesta ante incidentes, como los definidos en NIST SP 800-61 Computer Security Incident Handling Guide, siguen siendo válidos, le recomendamos que evalúe estos objetivos de diseño específicos que son pertinentes para responder a los incidentes de seguridad en un entorno de nube:

- Establecimiento de objetivos de repuesta: trabaje con las partes interesadas, el consejo legal y el equipo directivo de la organización para determinar el objetivo de respuesta ante un incidente. Algunos objetivos habituales incluyen la contención y mitigación del problema, la recuperación de los recursos afectados, la conservación de los datos para el análisis forense, el retorno a las operaciones seguras conocidas y, en última instancia, el aprendizaje de los incidentes.

- Respuesta a través de la nube: implemente los patrones de respuesta en la nube, donde tiene lugar el evento y se generan los datos.
- Conocimientos sobre lo que tiene y lo que necesita: preserve los registros, los recursos, las instantáneas y otras pruebas. Cópielos y almacénelos en una cuenta en la nube centralizada dedicada a la respuesta. Utilice etiquetas, metadatos y mecanismos que cumplan las políticas de retención. Deberá comprender qué servicios utiliza y, a continuación, identificar los requisitos para la investigación de dichos servicios. También puede utilizar etiquetas para comprender su entorno mejor.
- Uso de mecanismos de repetición de la implementación: si se puede atribuir una anomalía de seguridad a una configuración errónea, la solución podría ser tan sencilla como eliminar la varianza mediante la repetición de la implementación de los recursos con la configuración adecuada. En caso de que se identificara un posible compromiso, compruebe que la repetición de la implementación incluya una mitigación correcta y verificada de las causas raíz.
- Automatización siempre que sea posible: a medida que surjan problemas o se repitan los incidentes, cree mecanismos para clasificar y responder a eventos habituales mediante programación. Utilice respuestas humanas para incidentes únicos, complejos o delicados en los que las automatizaciones sean insuficientes.
- Uso de soluciones escalables: esfuércese por igualar la escalabilidad del enfoque de su organización con respecto a la computación en la nube. Implemente mecanismos de detección y respuesta que se escalen en todos sus entornos para reducir eficazmente el tiempo entre la detección y la respuesta.
- Mejora y aprendizaje del proceso: sea proactivo a la hora de identificar las carencias en sus procesos, herramientas o personas e implemente un plan para solucionarlas. Las simulaciones son métodos seguros para detectar carencias y mejorar los procesos.

Estos objetivos de diseño son un recordatorio para revisar la implementación de su arquitectura y determinar la capacidad de llevar a cabo tanto la respuesta a los incidentes como la detección de amenazas. Cuando planifique sus implementaciones en la nube, piense en responder a un incidente y lo ideal es que sea con una metodología de respuesta sólida desde el punto de vista forense. En algunos casos, esto significa que podría tener varias organizaciones, cuentas y herramientas configuradas específicamente para estas tareas de respuesta. Estas herramientas y funciones deben ponerse a disposición del personal de respuesta ante incidentes mediante una canalización de implementación. No deben ser estáticas porque pueden causar un riesgo mayor.

Preparación

Prepararse para un incidente es fundamental para ofrecer una respuesta oportuna y eficaz ante el incidente. La preparación se hace en tres dominios:

- Personal: la preparación del personal para un incidente de seguridad implica identificar a las partes interesadas pertinentes para la respuesta a los incidentes y capacitarlas en materia de respuesta ante incidentes y tecnologías en la nube.
- Procesos: la preparación de los procesos para un incidente de seguridad implica documentar las arquitecturas, desarrollar planes exhaustivos de respuesta ante los incidentes y crear guías de estrategias para responder de manera coherente a los eventos de seguridad.
- Tecnología: la preparación de la tecnología para un incidente de seguridad implica configurar el acceso, agregar y supervisar los registros necesarios, implementar mecanismos de alerta eficaces y desarrollar capacidades de respuesta e investigación.

Cada uno de estos dominios es igualmente importante para conseguir una respuesta eficaz ante los incidentes. Ningún programa de respuesta ante incidentes es completo o eficaz sin estos tres dominios. Debe preparar al personal, los procesos y la tecnología con una integración estrecha con el fin de estar preparado ante un incidente.

Prácticas recomendadas

- SEC10-BP01 Identificación del personal clave y los recursos externos
- SEC10-BP02 Desarrollo de planes de administración de incidentes
- SEC10-BP03 Preparación de las capacidades forenses
- SEC10-BP04 Desarrollo y prueba de manuales de estrategias de respuesta a incidentes de seguridad
- SEC10-BP05 Aprovisionamiento previo del acceso
- SEC10-BP06 Implementación de las herramientas con anticipación
- SEC10-BP07 Ejecución de simulaciones

SEC10-BP01 Identificación del personal clave y los recursos externos

Identifique las obligaciones legales, el personal y los recursos internos y externos que puedan ayudar a su organización a responder ante un incidente.

Resultado deseado: cuenta con una lista del personal clave, su información de contacto y las funciones que desempeñan al responder a un evento de seguridad. Revisa esta información con regularidad y la actualiza para reflejar los cambios de personal desde la perspectiva de las herramientas internas y externas. Al documentar esta información, tener en cuenta a todos los vendedores y proveedores de servicios externos, incluidos los socios de seguridad, los proveedores de nube y las aplicaciones de software como servicio (SaaS). Durante un evento de seguridad, disponer de personal con el nivel adecuado de responsabilidad, contexto y acceso para poder responder y recuperarse.

Patrones comunes de uso no recomendados:

- No mantener una lista actualizada del personal clave con información de contacto, sus cargos y responsabilidades al responder a los eventos de seguridad.
- Dar por sentada una comprensión general de las personas, las dependencias, la infraestructura y las soluciones pertinentes a la hora de responder a un evento y recuperarse de él.
- No contar con un repositorio de documentos o conocimientos relacionados con la infraestructura clave o el diseño de aplicaciones.
- No disponer de procesos de incorporación adecuados para que los nuevos empleados contribuyan de manera eficaz a la respuesta a un evento de seguridad, como llevar a cabo simulacros de eventos.
- No disponer de una ruta de escalado para los casos en los que el personal clave no esté disponible temporalmente o no responda durante los eventos de seguridad.

Beneficios de establecer esta práctica recomendada: esta práctica reduce el tiempo de clasificación y respuesta que se dedica a identificar al personal adecuado y sus funciones durante un evento. También disminuye al mínimo la pérdida de tiempo durante un evento, ya que mantiene una lista actualizada del personal clave y sus cargos, de modo que pueda recurrir a las personas adecuadas para la clasificación y la recuperación de un evento.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Identificación del personal clave de la organización: mantenga una lista de contactos del personal de su organización al que necesitaría involucrar. Revise y actualice periódicamente esta información en caso de que se produzcan cambios de personal, como cambios organizativos, ascensos y cambios

en el equipo. Esto es especialmente importante para los puestos clave, como los administradores de incidentes, el personal de respuesta a incidentes y el líder de comunicaciones.

- Administrador de incidentes: los administradores de incidentes tienen la autoridad general durante la respuesta al evento.
- Personal de respuesta a incidentes: el personal de respuesta a incidentes es el responsable de las actividades de investigación y corrección. Estas personas pueden variar según el tipo de evento, pero suelen ser desarrolladores y miembros de los equipos de operaciones responsables de la aplicación afectada.
- Líder de comunicaciones: el líder de comunicaciones es responsable de las comunicaciones internas y externas, especialmente las destinadas a agencias públicas, organismos reguladores y clientes.
- Proceso de incorporación: forme e incorpore periódicamente a nuevos empleados a fin de que adquieran las habilidades y los conocimientos necesarios para contribuir de manera eficaz a los esfuerzos de respuesta a incidentes. Incorpore simulaciones y ejercicios prácticos como parte del proceso de incorporación para facilitar su preparación.
- Expertos en la materia (SME): en el caso de equipos distribuidos y autónomos, le recomendamos que identifique un SME para las cargas de trabajo críticas. Ofrecen información sobre el funcionamiento y la clasificación de datos de las cargas de trabajo críticas relacionadas con el evento.

Formato de tabla de ejemplo:

```
  | Role | Name | Contact Information | Responsibilities |
1 | ——- | ——- | ——- | ——- |
2 | Incident Manager | Jane Doe| jane.doe@example.com | Overall authority during
 response |
3 | Incident Responder | John Smith | john.smith@example.com | Investigation and
 remediation |
4 | Communications Lead | Emily Johnson | emily.johnson@example.com | Internal and
 external communications |
5 | Communications Lead | Michael Brown | michael.brown@example.com | Insights on
 critical workloads |
```

Plantéese el uso de la característica Administrador de incidentes de AWS Systems Manager para determinar los contactos clave, definir un plan de respuesta, automatizar horarios de guardia y crear planes de escalado. Automatice y rote a todo el personal según un horario de guardias, de modo

que la responsabilidad de la carga de trabajo se comparta entre los responsables de esta. Esto fomenta las prácticas recomendadas, como la creación de métricas y registros relevantes, y también la definición de los umbrales de alarma pertinentes para la carga de trabajo.

Identificación de los socios externos: las empresas utilizan herramientas creadas por proveedores de software independientes (ISV), socios y subcontratistas con el fin de desarrollar soluciones diferenciadoras para sus clientes. Implique al personal clave de estos colectivos que pueda ayudarle a responder y recuperarse de un incidente. Le recomendamos que se registre en el nivel adecuado de Soporte para poder acceder rápidamente a expertos en la materia de AWS a través de un caso de soporte. Plantéese la posibilidad de establecer acuerdos similares con todos los proveedores de soluciones críticas para las cargas de trabajo. Algunos eventos de seguridad requieren que las empresas que coticen en bolsa notifiquen el evento y sus impactos a los organismos públicos y entidades normativas pertinentes. Mantenga y actualice la información de contacto de los departamentos pertinentes y las personas responsables.

Pasos para la implementación

1. Configure una solución de administración de incidentes.
   a. Piense en implementar el Administrador de incidentes en su cuenta de Security Tooling.
2. Defina los contactos en su solución de administración de incidentes.
   a. Defina al menos dos tipos de canales de contacto para cada contacto (como SMS, teléfono o correo electrónico) para garantizar la accesibilidad durante un incidente.
3. Defina un plan de respuesta.
   a. Identifique los contactos más apropiados para interactuar durante un incidente. Defina planes de escalado alineados con los cargos del personal al que se va a recurrir, en lugar de con los contactos individuales. Considere la posibilidad de incluir contactos que puedan ser responsables de informar a entidades externas, incluso aunque no participen directamente en la resolución del incidente.

Recursos

Prácticas recomendadas relacionadas:

- OPS02-BP03 Actividades operativas con propietarios identificados responsables de su rendimiento

Documentos relacionados:

- AWS Security Incident Response Guide

Ejemplos relacionados:

- AWS customer playbook framework
- Prepare for and respond to security incidents in your AWS environment

Herramientas relacionadas:

- AWS Systems Manager Incident Manager

Videos relacionados:

- Amazon's approach to security during development

SEC10-BP02 Desarrollo de planes de administración de incidentes

El primer documento que se desarrolla para la respuesta a incidentes es el plan de respuesta a incidentes. El plan de respuesta a incidentes está diseñado para ser la base de su programa y estrategia de respuesta a incidentes.

Beneficios de establecer esta práctica recomendada: desarrollar procesos de respuesta a incidentes exhaustivos y claramente definidos es clave para que el programa de respuesta a incidentes sea satisfactorio y escalable. Cuando se produce un evento de seguridad, tener unos pasos y flujos de trabajo claros puede ayudarle a responder a tiempo. Es posible que ya tenga procesos de respuesta a incidentes. Independientemente de su estado actual, es importante actualizar, iterar y probar sus procesos de respuesta a incidentes con regularidad.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Un plan de administración de incidentes es fundamental para responder y mitigar el impacto potencial de los incidentes de seguridad, así como de cara a la recuperación. Un plan de administración de incidentes es un proceso estructurado para identificar y solucionar los incidentes de seguridad y responder a ellos en el momento oportuno.

La nube tiene muchos de los mismos roles y requisitos operativos que se encuentran en un entorno en las instalaciones. A la hora de crear un plan de administración de incidentes, es importante tener en cuenta las estrategias de respuesta y recuperación que mejor se ajusten al resultado empresarial y a los requisitos de conformidad. Por ejemplo, si trabaja con cargas de trabajo en AWS que cumplen con la normativa FedRAMP en Estados Unidos, siga las recomendaciones de la Guía de administración de seguridad informática NIST SP 800-61. Del mismo modo, cuando opere con cargas de trabajo que almacenan información de identificación personal (PII), plantéese cómo proteger y responder a los problemas relacionados con la residencia y el uso de datos.

Al crear un plan de administración de incidentes para sus cargas de trabajo en AWS, comience con el Modelo de responsabilidad compartida de AWS para crear un enfoque de defensa en profundidad para la respuesta a los incidentes. En este modelo, AWS administra la seguridad de la nube y el cliente es responsable de la seguridad en la nube. Esto significa que retiene el control y es responsable de los controles de seguridad que decida implementar. La Guía de respuesta ante incidentes de seguridad de AWS expone en detalle los conceptos clave y las orientaciones básicas para crear un plan de administración de incidentes centrado en la nube.

Un plan eficaz de administración de incidentes debe iterarse continuamente, lo que le permite mantenerse al día con su objetivo de operaciones en la nube. Considere la posibilidad de utilizar los planes de implementación que se detallan a continuación cuando cree y haga evolucionar su plan de administración de incidentes.

Pasos para la implementación

1. Defina las funciones y responsabilidades dentro de su organización para gestionar los eventos de seguridad. Aquí debería incluir a los representantes de varios departamentos, entre los que se incluyen:
   - Recursos humanos (RR. HH.)
   - Equipo ejecutivo
   - Departamento legal
   - Propietarios y desarrolladores de aplicaciones (expertos en la materia o SME)
2. Describa con claridad quién es responsable, encargado, consultado e informado (RACI) durante un incidente. Cree un diagrama RACI para facilitar una comunicación rápida y directa, y describa claramente el liderazgo en las diferentes etapas de un evento.
3. Incluya a los propietarios y desarrolladores de aplicaciones (SME) durante un incidente, ya que pueden proporcionar información y contexto que resultan valiosos para ayudar a medir el impacto.

Entable relación con estos SME y practique con ellos escenarios de respuesta a incidentes antes de que se produzca un incidente real.

4. Incluya a socios de confianza o expertos externos en el proceso de investigación o de respuesta, ya que pueden ofrecer una mayor experiencia y amplitud de miras.
5. Acompase sus planes y funciones de administración de incidentes a cualquier normativa o requisito de cumplimiento local por los que se rija su organización.
6. Practique y pruebe sus planes de respuesta a incidentes con regularidad e incluya a todos los roles y responsabilidades definidos. Esto ayuda a agilizar el proceso y a verificar que se cuenta con una respuesta coordinada y eficiente a los incidentes de seguridad.
7. Revise y actualice los roles, las responsabilidades y el diagrama RACI periódicamente o a medida que cambien la estructura organizativa o los requisitos.

Información sobre los equipos de asistencia y respuesta de AWS

- AWS Support
  - Soporte ofrece una serie de planes que proporcionan acceso a herramientas y conocimientos que contribuyen al éxito y la salud operativa de sus soluciones de AWS. Si necesita asistencia técnica y más recursos para planificar, implementar y optimizar su entorno de AWS, puede seleccionar el plan de asistencia que mejor se adapte a su caso de uso de AWS.
  - Piense en el Centro de soporte de Consola de administración de AWS (es necesario iniciar sesión) como punto de contacto central para obtener asistencia en caso de problemas que afecten a sus recursos de AWS. El acceso a Soporte está controlado por AWS Identity and Access Management. Para obtener más información sobre el acceso a las características de Soporte, consulte Introducción a Soporte.
- AWS Equipo de respuesta a incidentes de clientes (CIRT) de)
  - El equipo de respuesta a incidentes de clientes (CIRT) de AWS es un equipo global de AWS especializado que ofrece asistencia a los clientes las 24 horas del día y los 7 días de la semana durante eventos de seguridad activos en el lado del cliente del Modelo de responsabilidad compartida de AWS.
  - Cuando el CIRT de AWS le ofrece asistencia, le ayuda en la clasificación y la recuperación de un evento de seguridad activo en AWS. Puede ayudarle a analizar la causa raíz mediante el uso de registros de servicio de AWS y ofrecerle recomendaciones para la recuperación. También puede proporcionar recomendaciones de seguridad y prácticas recomendadas para ayudarle a evitar eventos de seguridad en el futuro.

    - Los clientes de AWS pueden interactuar con el CIRT de AWS a través de un caso de Soporte.
- Respuesta frente a incidencias de seguridad de AWS
    - Anunciado en re:Invent 2024, Respuesta frente a incidencias de seguridad de AWS es un servicio administrado de respuesta a incidentes de seguridad que utiliza tanto tecnología moderna de clasificación como intervención humana. El servicio recopila todos los resultados de GuardDuty y cualquier resultado de terceros enviado para su clasificación, con el fin de alertar al cliente solo sobre los resultados que requieren una investigación. El servicio también proporciona un portal para enviar casos reactivos en caso de que el cliente detecte un incidente de seguridad y recibir asistencia del equipo avanzado de respuesta a incidentes de AWS.
- Asistencia en respuestas a DDoS
    - AWS ofrece AWS Shield, que ofrece un servicio administrado de protección contra ataques de denegación de servicio distribuidos (DDoS) que protege las aplicaciones web que se ejecutan en AWS. Shield proporciona una mitigación en línea automática y detección siempre activa que puede minimizar el tiempo de inactividad y la latencia de la aplicación, por lo que no es necesario disponer de Soporte para beneficiarse de la protección DDoS. Hay dos capas de Shield: AWS Shield Standard y AWS Shield Advanced. Para conocer las diferencias entre estos dos niveles, consulte la documentación de características de Shield.
- AWS Managed Services (AMS)
    - AWS Managed Services (AMS) proporciona una administración continua de su infraestructura de AWS para que pueda centrarse en sus aplicaciones. Mediante la implementación de prácticas recomendadas para mantener su infraestructura, AMS le ayuda a reducir la carga y el riesgo operativos. AMS automatiza actividades comunes, como solicitudes de cambios, supervisión, administración de parches, seguridad y servicios de copia de seguridad, y ofrece servicios de ciclo de vida completo para aprovisionar, ejecutar y brindar soporte a su infraestructura.
    - AMS asume la responsabilidad de implementar un conjunto de controles de detección de seguridad y proporciona una primera línea de respuesta a las alertas las 24 horas del día y los 7 días de la semana. Cuando se inicia una alerta, AMS sigue un conjunto estándar de guías automáticas y manuales para verificar una respuesta coherente. Estas guías de estrategias se comparten con los clientes de AMS durante la incorporación para que puedan desarrollar y coordinar una respuesta con AMS.

Desarrollo del plan de respuesta a incidentes

El plan de respuesta a incidentes está diseñado para ser la base de su programa y estrategia de respuesta a incidentes. El plan de respuesta a incidentes debe figurar en un documento formal. Un plan de respuesta a incidentes suele incluir las siguientes secciones:

- Descripción general del equipo de respuesta a incidentes: describe los objetivos y las funciones del equipo de respuesta a incidentes.
- Funciones y responsabilidades: enumera las partes interesadas de la respuesta a los incidentes y detalla sus funciones cuando se produce un incidente.
- Un plan de comunicación: detalla la información de contacto y cómo se comunica durante un incidente.
- Métodos de comunicación auxiliares: se recomienda tener un método de comunicación auxiliar fuera de banda para informar de los incidentes. Un ejemplo de una aplicación que proporciona un canal de comunicaciones fuera de banda seguro es AWS Wickr.
- Fases de la respuesta a un incidente y medidas que tomar: se enumeran las fases de la respuesta a un incidente (por ejemplo, detección, análisis, erradicación, contención y recuperación), incluidas las medidas de alto nivel que se deben tomar en esas fases.
- Definiciones de gravedad y priorización del incidente: detalla cómo clasificar la gravedad de un incidente, cómo priorizar el incidente y, a continuación, cómo las definiciones de gravedad afectan a los procedimientos de escalamiento.

Aunque estas secciones son comunes en empresas de diferentes tamaños y de diferentes sectores, el plan de respuesta a incidentes de cada organización es único. Debe elaborar un plan de respuesta a incidentes que mejor se adapte a su organización.

Recursos

Prácticas recomendadas relacionadas:

- SEC04 Detección

Documentos relacionados:

- AWS Security Incident Response Guide
- NIST: guía de administración de incidentes de seguridad informática

SEC10-BP03 Preparación de las capacidades forenses

Antes de que se produzca un incidente de seguridad, considere la posibilidad de desarrollar capacidades forenses que lo ayuden a investigar los eventos de seguridad.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Los conceptos de la ciencia forense tradicional que se utiliza en el entorno en las instalaciones también son aplicables a AWS. Para obtener información sobre cómo comenzar a desarrollar capacidades forenses en la Nube de AWS, consulte Forensic investigation environment strategies in the Nube de AWS.

Una vez que haya configurado la estructura del entorno y la Cuenta de AWS para el análisis forense, defina las tecnologías necesarias para ejecutar de forma eficaz unas metodologías sólidas desde el punto de vista forense en las cuatro fases:

- Recopilación: recopile registros de AWS pertinentes, como los registros de AWS CloudTrail, AWS Config, de flujo de VPC y de nivel de host. Siempre que sea posible, recopile instantáneas, copias de seguridad y volcados de memoria de los recursos de AWS afectados.
- Examen: examine los datos recopilados mediante la extracción y la evaluación de la información importante.
- Análisis: analice los datos recopilados para comprender el incidente y sacar conclusiones.
- Informes: presente la información resultante de la fase de análisis.

Pasos para la implementación

Preparación del entorno forense

AWS Organizations le permite administrar y gestionar un entorno de AWS de forma centralizada a medida que aumentan y se escalan los recursos de AWS. Una organización de AWS se encarga de agrupar las cuentas de Cuentas de AWS para que pueda administrarlas como una sola unidad. Puede utilizar unidades organizativas para agrupar las cuentas que desee administrar como una sola unidad.

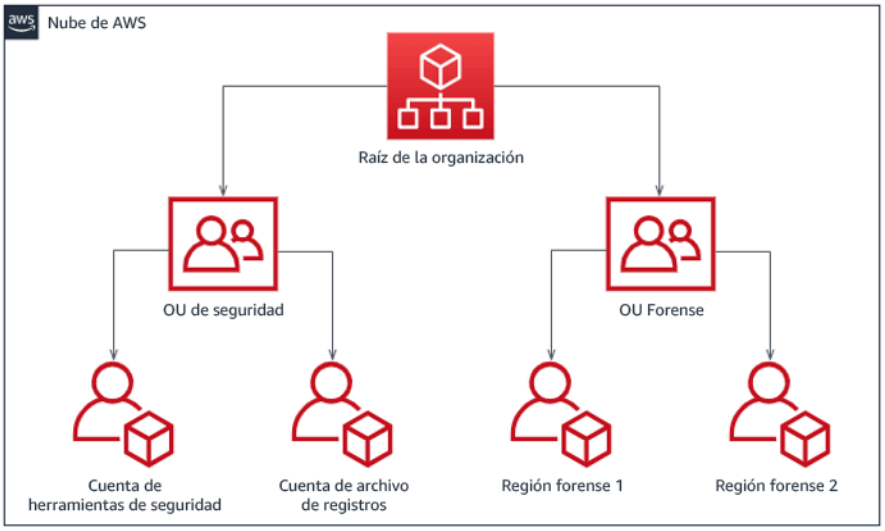
Para la respuesta a incidentes, es útil contar con una estructura de Cuenta de AWS que respalde las funciones de respuesta ante incidentes, lo que incluye una OU de seguridad y una OU forense. Dentro de la unidad organizativa de seguridad, debe tener cuentas para:

- Archivo de registros: agregue los registros en una Cuenta de AWS de archivo de registros con permisos limitados.
- Herramientas de seguridad: centralice los servicios de seguridad en una Cuenta de AWS de herramientas de seguridad. Esta cuenta funciona como un administrador delegado de los servicios de seguridad.

Dentro de la unidad organizativa forense, tiene la opción de implementar una o varias cuentas forenses diferentes para cada una de las regiones en las que opera, en función de lo que le venga mejor a su modelo empresarial y operativo. Si crea una cuenta forense para cada región, puede impedir que se creen recursos de AWS fuera de esa región y reducir el riesgo de que esos recursos se copien en una región no deseada. Por ejemplo, si solo opera en la región Este de EE. UU. (Norte de Virginia) (`us-east-1`) y Oeste de EE. UU. (Oregón) (`us-west-2`), tendría dos cuentas en la unidad organizativa forense: una para `us-east-1` y otra para `us-west-2`.

Puede crear una Cuenta de AWS forense para varias regiones. Debe tener cuidado al copiar los recursos de AWS en esa cuenta y asegurarse de que cumple los requisitos de soberanía de datos. Dado que aprovisionar nuevas cuentas lleva tiempo, es imperativo crear e instrumentar las cuentas forenses mucho antes de que se produzca un incidente para que los responsables puedan estar preparados y utilizarlas eficazmente en su respuesta.

En el siguiente diagrama, se muestra un ejemplo de una estructura de cuentas que incluye una unidad organizativa forense con cuentas forenses para cada región:



Estructura de cuentas por región para la respuesta a incidentes

Captura de copias de seguridad e instantáneas

Crear copias de seguridad de los principales sistemas y bases de datos es fundamental para poder recuperarse de un incidente de seguridad y para fines forenses. Con las copias de seguridad, puede restaurar los sistemas a su estado seguro anterior. En AWS, puede crear instantáneas de diversos recursos. Las instantáneas le proporcionan copias de seguridad puntuales de esos recursos. Hay muchos servicios de AWS que pueden ayudarle con la copia de seguridad y la recuperación. Para obtener más detalles sobre estos servicios y enfoques de copia de seguridad y recuperación, consulte la Backup and Recovery Prescriptive Guidance y Use backups to recover from security incidents.

Es esencial que las copias de seguridad estén bien protegidas, especialmente en ciertas situaciones, como el ransomware. Para obtener información sobre cómo proteger las copias de seguridad, consulte Top 10 security best practices for securing backups in AWS. Además de proteger las copias de seguridad, debe probar periódicamente los procesos de copia de seguridad y restauración para comprobar que la tecnología y los procesos que tiene implementados funcionan según lo previsto.

Automatización de los análisis forenses

Durante un evento de seguridad, es necesario que el equipo de respuesta a incidentes pueda recopilar y analizar las pruebas rápidamente y, al mismo tiempo, mantener la precisión durante todo el tiempo que rodee al evento (por ejemplo, capturar registros relacionados con un evento o recurso específico, o recopilar un volcado de memoria de una instancia de Amazon EC2). Para el equipo de respuesta a incidentes, resulta difícil y lleva mucho tiempo recopilar manualmente las pruebas pertinentes, especialmente en una gran cantidad de instancias y cuentas. Además, la recopilación manual puede ser más propensa a errores humanos. Por estas razones, debe desarrollar e implementar la automatización del análisis forense en la medida que sea posible.

AWS ofrece una serie de recursos de automatización para el análisis forense, que se enumeran en la sección de recursos. Estos recursos son ejemplos de patrones forenses que hemos desarrollado y que los clientes han implementado. Aunque pueden resultar útiles como arquitectura de referencia al empezar, valore la posibilidad de modificarlos o crear nuevos patrones de automatización forense en función del entorno, los requisitos, las herramientas y los procesos forenses.

Recursos

Documentos relacionados:

- AWS Security Incident Response Guide - Develop Forensics Capabilities
- AWS Security Incident Response Guide - Forensics Resources

- Forensic investigation environment strategies in the Nube de AWS
- How to automate forensic disk collection in AWS
- AWS Prescriptive Guidance - Automate incident response and forensics

Videos relacionados:

- Automating Incident Response and Forensics

Ejemplos relacionados:

- Automated Incident Response and Forensics Framework
- Automated Forensics Orchestrator for Amazon EC2

SEC10-BP04 Desarrollo y prueba de manuales de estrategias de respuesta a incidentes de seguridad

Una parte esencial de la preparación de los procesos de respuesta a incidentes consiste en desarrollar manuales de estrategias. Los manuales de estrategias de respuesta a incidentes ofrecen directrices y pasos prescriptivos que deben seguirse cuando se produce un evento de seguridad. Contar con una estructura y unos pasos claros simplifica la respuesta y reduce la probabilidad de que se produzcan errores humanos.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Deben crearse guías estratégicas para escenarios de incidentes, como, por ejemplo:

- Incidentes esperados: deben crearse manuales de estrategias para los incidentes que anticipe. Esto puede incluir amenazas como la denegación de servicio (DoS), el ransomware y las amenazas de las credenciales.
- Alertas o resultados de seguridad conocidos: deben crearse manuales de estrategias para abordar las alertas y los resultados de seguridad conocidos, como los resultados de Amazon GuardDuty. Cuando reciba un resultado de GuardDuty, el manual debería incluir medidas claras para evitar que la alerta se gestione mal o se ignore. Para obtener más información y orientación sobre las soluciones, consulte Corrección de problemas de seguridad detectados por GuardDuty.

Las guías estratégicas deben incluir los pasos técnicos que los analistas de seguridad deben completar para investigar y responder adecuadamente a un posible incidente de seguridad.

El equipo de respuesta a incidentes del cliente (CIRT) de AWS ha publicado un repositorio de GitHub que contiene manuales de estrategias de respuesta ante incidentes organizados por recurso, tipo y situación de amenaza. Estos manuales de estrategias se pueden adaptar para alinearlos con sus procedimientos de respuesta a incidentes existentes o servir como base para desarrollar otros nuevos.

Pasos para la implementación

Algunos de los elementos que deben incluirse en un manual de estrategias son los siguientes:

- Descripción general de la guía estratégica: ¿qué escenario de riesgo o incidente se aborda en este manual de estrategias? ¿Cuál es el objetivo del manual de estrategias?
- Requisitos previos: ¿qué registros, mecanismos de detección y herramientas automatizadas se necesitan en el escenario de este incidente? ¿Cuál es la notificación esperada?
- Información sobre la comunicación y la información de escalado: ¿quiénes participan y cuál es su información de contacto? ¿Cuáles son las responsabilidades de cada una de las partes interesadas?
- Medidas de respuesta: en las diferentes fases de respuesta a un incidente, ¿qué medidas tácticas se deben tomar? ¿Qué consultas deben ejecutar los analistas? ¿Qué código debe ejecutarse para lograr el resultado deseado?
  - Detección: ¿cómo se va a detectar el incidente?
  - Análisis: ¿cómo se va a determinar el alcance del impacto?
  - Contención: ¿cómo se va a aislar el incidente para limitar el alcance?
  - Erradicación: ¿cómo se va a eliminar la amenaza del entorno?
  - Recuperación: ¿cómo se va a conseguir que el sistema o recurso afectado vuelva a ser productivo?
- Resultados esperados: después de ejecutar las consultas y el código, ¿cuál es el resultado esperado de la guía estratégica?

Recursos

Prácticas recomendadas de Well-Architected relacionadas:

- SEC10-BP02 Desarrollo de planes de administración de incidentes

Documentos relacionados:

- Framework for Incident Response Playbooks
- Develop your own Incident Response Playbooks
- Incident Response Playbook Samples
- Building an AWS incident response runbook using Jupyter playbooks and CloudTrail Lake

SEC10-BP05 Aprovisionamiento previo del acceso

Verifique que haya aprovisionado previamente el acceso correcto a los equipos de intervención de incidentes en AWS para reducir el tiempo necesario de investigación hasta la recuperación.

Patrones comunes de uso no recomendados:

- Usar la cuenta raíz para la respuesta ante incidentes.
- Alterar las cuentas existentes.
- Manipular los permisos de IAM directamente al proporcionar un aumento puntual de los privilegios.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

AWS recomienda reducir o eliminar la dependencia de credenciales de larga duración siempre que sea posible, en favor de credenciales temporales y mecanismos de aumento puntual de los privilegios. Las credenciales de larga duración están expuestas a riesgos de seguridad y aumentan la carga operativa. Para la mayoría de las tareas de administración, así como para las tareas de respuesta ante incidentes, le recomendamos que implemente la federación de identidades junto con el escalado temporal para el acceso administrativo. En este modelo, un usuario solicita el aumento a un nivel superior de privilegios (como un rol de respuesta ante incidentes) y, siempre que el usuario reúna los requisitos para el aumento, se envía una solicitud a un aprobador. Si se aprueba la solicitud, el usuario recibe un conjunto de credenciales de AWS temporales que puede utilizar para completar sus tareas. Una vez que caducan estas credenciales, el usuario debe enviar una nueva solicitud de aumento.

Recomendamos el uso del escalado temporal de privilegios en la mayoría de las situaciones de respuesta ante incidentes. La forma correcta de hacerlo es utilizar AWS Security Token Service y las políticas de sesión para limitar el acceso.

Hay situaciones en las que las identidades federadas no están disponibles; por ejemplo:

- Interrupción relacionada con un proveedor de identidades (IdP) comprometido.
- Una configuración deficiente o un error humano provocan la ruptura del sistema de administración de acceso federado.
- Actividad maliciosa como un evento de denegación de servicio distribuido (DDoS) o un sistema no disponible.

En los casos anteriores, debe haber un acceso de emergencia break glass configurado para permitir la investigación y la reparación oportuna de los incidentes. Se recomienda utilizar un usuario, grupo o rol con los permisos adecuados para llevar a cabo tareas y acceder a los recursos de AWS. Utilice el usuario raíz únicamente para llevar a cabo tareas que requieran credenciales de usuario raíz. Para verificar que los equipos de intervención de incidentes disponen del nivel correcto de acceso a AWS y otros sistemas pertinentes, recomendamos el aprovisionamiento previo de cuentas exclusivas. Las cuentas requieren un acceso con privilegios y se deben controlar y supervisar de forma estricta. Las cuentas deben crearse con el menor número de privilegios requeridos para llevar a cabo las tareas necesarias y el nivel de acceso debe basarse en las guías de estrategias creadas como parte del plan de administración de incidentes.

La práctica recomendada es crear usuarios y roles personalizados y exclusivos. El hecho de escalar temporalmente el acceso de los usuarios o de los roles mediante la incorporación de políticas de IAM provoca que no esté claro qué acceso tenían los usuarios durante el incidente y se corre el riesgo de que los privilegios escalados no se revoquen.

Es importante eliminar tantas dependencias como sea posible para verificar que se puede acceder en el mayor número posible de escenarios de error. Como medida de apoyo, cree una guía de estrategias para verificar que los usuarios de respuesta ante incidentes se crean como usuarios en una cuenta de seguridad exclusiva y no se administran a través de una federación existente o una solución de inicio de sesión único (SSO). Cada miembro del equipo de intervención debe tener su propia cuenta con nombre. La configuración de la cuenta debe aplicar una política de contraseñas seguras y la autenticación multifactor (MFA). Si las guías de estrategias de respuesta ante incidentes solo requieren acceso a la Consola de administración de AWS, el usuario no debería tener configuradas las claves de acceso y se le debería prohibir explícitamente la creación de claves de acceso. Esto se puede configurar con políticas de IAM o políticas de control de servicios (SCP) como se menciona en las prácticas recomendadas de seguridad de AWS para SCP de AWS Organizations. Los usuarios solo deben tener el privilegio de poder asumir roles de respuesta ante incidentes en otras cuentas.

Durante un incidente, podría ser necesario conceder acceso a otras personas internas o externas para respaldar las actividades de investigación, reparación o recuperación. En este caso, utilice el mecanismo de guía de estrategias mencionado anteriormente. Debe haber un proceso para verificar que cualquier acceso adicional se revoque inmediatamente después de que finalice el incidente.

Para verificar que el uso de los roles de respuesta ante incidentes se puede supervisar y auditar de forma adecuada, es esencial que las cuentas de IAM creadas para este fin no se compartan con otras personas y que el Usuario raíz de la cuenta de AWS no se utilice a menos que se requiera para tareas específicas. Si el usuario raíz es necesario (por ejemplo, no está disponible el acceso de IAM a una cuenta específica), utilice un proceso aparte con una guía de estrategias disponible para verificar la disponibilidad de las credenciales de inicio de sesión y el token MFA del usuario raíz.

Para configurar las políticas de IAM para los roles de respuesta ante incidentes, considere la posibilidad de utilizar el Analizador de acceso de IAM para generar políticas basadas en los registros de AWS CloudTrail. Para ello, conceda acceso de administrador al rol de respuesta ante incidentes en una cuenta que no sea de producción y ejecute las guías de estrategias. Una vez completado, se puede crear una política que únicamente permita las acciones hechas. Esta política se puede aplicar a los roles de respuesta ante incidentes en todas las cuentas. Es recomendable crear una política de IAM independiente para cada manual de estrategias a fin de facilitar la administración y la auditoría. Entre los ejemplos de manuales de estrategias se podrían incluir planes de respuesta para ransomware, vulneraciones de datos, pérdida de acceso a la producción y otras situaciones.

Utilice las cuentas de respuesta ante incidentes para asumir los roles de IAM dedicados de respuesta ante incidentes en otras Cuentas de AWS. Estos roles se deben configurar para que solo puedan asumirlos los usuarios de la cuenta de seguridad. La relación de confianza debe requerir que la entidad principal de llamada se haya autenticado mediante MFA. Los roles deben utilizar políticas de IAM de ámbito estricto para controlar el acceso. Asegúrese de que todas las solicitudes de `AssumeRole` para estos roles estén registradas en CloudTrail y se haya alertado de ellas y que se registre cualquier acción hecha con estos roles.

Se recomienda que tanto las cuentas de IAM como los roles de IAM tengan nombres claros para poder encontrarlos fácilmente en los registros de CloudTrail. Un ejemplo sería asignar a las cuentas de IAM el nombre *<USER_ID>*`-BREAK-GLASS` y a los roles de IAM `BREAK-GLASS-ROLE`.

CloudTrail se utiliza para registrar la actividad de la API en sus cuentas de AWS y debe usarse para configurar alertas sobre el uso de las funciones de respuesta ante incidentes. Consulte la publicación del blog sobre la configuración de alertas cuando se utilizan claves de usuario raíz. Las instrucciones se pueden modificar para configurar la métrica de Amazon CloudWatch de filtro a filtro en los eventos de `AssumeRole` relacionados con el rol de IAM de respuesta ante incidentes:

```
{ $.eventName = "AssumeRole" && $.requestParameters.roleArn =
 "<INCIDENT_RESPONSE_ROLE_ARN>" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !
= "AwsServiceEvent" }
```

Como es probable que los roles de respuesta ante incidentes tengan un nivel de acceso alto, es importante que estas alertas lleguen a un grupo amplio y se actúe con rapidez.

Durante un incidente, es posible que un miembro del equipo de intervención necesite acceder a sistemas que no están directamente protegidos por IAM. Puede tratarse de instancias de Amazon Elastic Compute Cloud, bases de datos de Amazon Relational Database Service o plataformas de software como servicio (SaaS). Se recomienda encarecidamente que, en lugar de utilizar protocolos nativos como SSH o RDP, AWS Systems Manager Session Manager se utilice para todos los accesos administrativos a las instancias de Amazon EC2. Este acceso se puede controlar mediante IAM, que es seguro y está auditado. También es posible automatizar partes de sus guías de estrategias mediante documentos de ejecución de comandos de AWS Systems Manager, lo que puede reducir los errores de los usuarios y mejorar el tiempo de recuperación. Para el acceso a las bases de datos y a las herramientas de terceros, recomendamos almacenar las credenciales de acceso en AWS Secrets Manager y conceder el acceso a los roles de equipos de intervención ante incidentes.

Por último, la gestión de las cuentas de IAM de respuesta ante incidentes debe agregarse a sus procesos de incorporación, traslado y abandono, así como revisarse y probarse periódicamente para comprobar que solo se permite el acceso previsto.

Recursos

Documentos relacionados:

- Managing temporary elevated access to your AWS environment
- AWS Security Incident Response Guide
- AWS Elastic Disaster Recovery
- Administrador de incidentes de AWS Systems Manager
- Configuración de una política de contraseñas de la cuenta para usuarios de IAM
- Uso de autenticación multifactor (MFA) en AWS
- Configuring Cross-Account Access with MFA
- Using IAM Access Analyzer to generate IAM policies
- Best Practices for AWS Organizations Service Control Policies in a Multi-Account Environment

- How to Receive Notifications When Your AWS Account's Root Access Keys Are Used
- Create fine-grained session permissions using IAM managed policies
- Break glass access

Videos relacionados:

- Automating Incident Response and Forensics in AWS
- DIY guide to runbooks, incident reports, and incident response
- Prepare for and respond to security incidents in your AWS environment

SEC10-BP06 Implementación de las herramientas con anticipación

Asegúrese de que el personal de seguridad implementa las herramientas correctas con anticipación para reducir el plazo de investigación hasta conseguir la recuperación.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Para automatizar las funciones de operaciones y de respuesta de seguridad, puede utilizar un completo conjunto de API y herramientas de AWS. Puede automatizar totalmente las funcionalidades de administración de identidades, seguridad de red, protección de datos y supervisión, y hacer que estén disponibles a través de métodos de desarrollo de software populares que ya tenga establecidos. Al crear procesos de automatización de seguridad, el sistema podrá supervisar, revisar e iniciar una respuesta, y no necesitará empleados que supervisen el nivel de seguridad y reaccionen manualmente a los eventos.

Si los equipos de intervención de incidentes siguen respondiendo a alertas de la misma forma, corren el riesgo de fatigarse por el excesivo número de alertas. Con el paso del tiempo, el equipo puede llegar a no reaccionar ante las alertas e incluso cometer errores durante la gestión de situaciones habituales o pasar por alto alertas inusuales. La automatización ayuda a evitar este problema con funciones que procesan alertas repetitivas y habituales, dejando a las personas que gestionen los incidentes extraordinarios y delicados. La integración de sistemas de detección de anomalías, como Amazon GuardDuty, AWS CloudTrail Insights y Detección de anomalías de Amazon CloudWatch, puede reducir la carga de alertas comunes basadas en umbrales.

Puede mejorar los procesos manuales automatizando los pasos del proceso mediante programación. Después de definir el patrón de solución de un evento, puede descomponer dicho patrón en una

lógica procesable y escribir el código que ejecute dicha lógica. A continuación, los equipos de intervención pueden ejecutar ese código para solucionar el problema. Con el paso del tiempo, puede automatizar cada vez más pasos y, en última instancia, gestionar automáticamente todas las clases de incidentes comunes.

Durante una investigación de seguridad, necesitará poder revisar los registros correspondientes para registrar y comprender todo el alcance y la cronología del incidente. También necesita los registros para generar alertas que indican que se han producido determinadas acciones de interés. Es fundamental seleccionar, habilitar, almacenar y configurar mecanismos de consulta y recuperación, así como de alerta. Además, una forma eficaz de proporcionar herramientas para buscar datos de registro es usar Amazon Detective.

AWS tiene a su disposición más de 200 servicios en la nube y miles de características. Le recomendamos que revise los servicios que pueden respaldar y simplificar su estrategia de respuesta a incidentes.

Además de los registros, debe desarrollar e implementar una estrategia de etiquetado. El etiquetado puede ayudarle a proporcionar contexto en relación con el propósito de un recurso de AWS. El etiquetado también se puede utilizar en la automatización.

Pasos para la implementación

Selección y configuración de registros de análisis y alertas

Consulte la siguiente documentación sobre la configuración de registros para la respuesta a incidentes:

- Logging strategies for security incident response
- SEC04-BP01 Configuración del registro de servicios y aplicaciones

Activación de los servicios de seguridad para respaldar la detección y la respuesta

AWS ofrece funcionalidades de detección, prevención y respuesta, y se pueden utilizar otros servicios para diseñar soluciones de seguridad personalizadas. Para obtener una lista de los servicios más relevantes para la respuesta a incidentes de seguridad, consulte Definiciones de capacidades en la nube y la página de inicio de Respuesta a un incidente de seguridad.

Desarrollo e implementación de una estrategia de etiquetado

Puede resultar difícil obtener información contextual sobre el caso de uso empresarial y las partes interesadas internas pertinentes en relación con un recurso de AWS. Una forma de hacerlo es mediante etiquetas, que asignan metadatos a los recursos de AWS y se componen de una clave y un valor definidos por el usuario. Puede crear etiquetas para clasificar los recursos en función de su propósito, propietario, entorno, tipo de datos procesados y otros criterios de su elección.

Una estrategia de etiquetado coherente puede acelerar los tiempos de respuesta y minimizar el tiempo que se invierte en el contexto de la organización al permitirle identificar y discernir rápidamente la información contextual sobre un recurso de AWS. Las etiquetas también pueden servir como un mecanismo para iniciar automatizaciones de respuesta. Para obtener más información sobre qué etiquetar, consulte Tagging your AWS resources. Primero tendrá que definir las etiquetas que desea implementar en toda la organización. Después, implementará y hará cumplir la estrategia de etiquetado. Para obtener más información sobre la implementación y el cumplimiento, consulte Implement AWS resource tagging strategy using AWS Tag Policies and Service Control Policies (SCPs).

Recursos

Prácticas recomendadas de Well-Architected relacionadas:

- SEC04-BP01 Configuración del registro de servicios y aplicaciones
- SEC04-BP02 Recopilación de registros, resultados y métricas en ubicaciones estandarizadas

Documentos relacionados:

- Logging strategies for security incident response
- Definiciones de las capacidades de la nube de respuesta ante incidentes

Ejemplos relacionados:

- Threat Detection and Response with Amazon GuardDuty and Amazon Detective
- Security Hub Workshop
- Vulnerability Management with Amazon Inspector

SEC10-BP07 Ejecución de simulaciones

Las organizaciones crecen y evolucionan con el tiempo, pero también las amenazas, por lo que es importante que revise continuamente sus capacidades de respuesta a los incidentes. Ejecutar simulaciones (también conocidas como días de juego) es un buen método para llevar a cabo esta evaluación. En las simulaciones, se utilizan escenarios de eventos de seguridad reales diseñados para imitar las tácticas, técnicas y procedimientos (TTP) del actor de una amenaza y permiten a la organización probar y evaluar sus capacidades de respuesta a los incidentes respondiendo a estos simulacros de ataques cibernéticos tal y como podría ocurrir en la realidad.

Beneficios de establecer esta práctica recomendada: las simulaciones ofrecen una serie de beneficios:

- Comprobar si se está preparado para un ataque cibernético y mejorar la confianza de los equipos de respuesta a los incidentes.
- Probar la precisión y la eficiencia de las herramientas y los flujos de trabajo.
- Perfeccionar los métodos de comunicación y escalamiento en consonancia con su plan de respuesta a incidentes.
- Ofrecer la oportunidad de responder a vectores menos comunes.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Hay tres tipos principales de simulaciones:

- Ejercicios prácticos: el enfoque de los ejercicios prácticos consiste en llevar a cabo una sesión de debate en la que participen las diversas partes interesadas en la respuesta a los incidentes para practicar las funciones y responsabilidades y utilizar las herramientas de comunicación y los manuales de estrategia establecidos. Por lo general, este ejercicio se puede hacer durante un día completo en un lugar virtual o físico, o bien en una combinación de ambos. Como se trata de un debate, el ejercicio de simulación se centra en los procesos, las personas y la colaboración. La tecnología forma parte integral del debate, pero en este tipo de ejercicio no se hace un uso real de las herramientas o los guiones de respuesta a incidentes.
- Ejercicios del equipo morado: los ejercicios del equipo morado aumentan el nivel de colaboración entre las personas que se encargan de la respuesta a los incidentes (equipo azul) y los actores de las amenazas simuladas (equipo rojo). El equipo azul está compuesto por miembros del centro

de operaciones de seguridad (SOC), pero también puede incluir a otras partes interesadas que participarían durante un ataque cibernético real. El equipo rojo está compuesto por un equipo de pruebas de penetración o partes interesadas clave que cuentan con formación en seguridad ofensiva. El equipo rojo trabaja en colaboración con los facilitadores del ejercicio para diseñar un escenario que sea preciso y factible. Durante los ejercicios del equipo morado, la atención se centra en los mecanismos de detección, las herramientas y los procedimientos operativos estándar (SOP) que facilitan las iniciativas de respuesta a los incidentes.

- Ejercicios del equipo rojo: durante un ejercicio del equipo rojo, el atacante (equipo rojo) hace una simulación para lograr un determinado objetivo o conjunto de objetivos desde un ámbito predeterminado. Los defensores (equipo azul) no conocen necesariamente el ámbito y la duración del ejercicio; de esta manera, se consigue una evaluación más realista de cómo responderían ante un incidente real. Dado que los ejercicios de equipo rojo pueden ser pruebas invasivas, tenga cuidado e implemente controles para verificar que el ejercicio no produzca un daño real en su entorno.

Considere la posibilidad de llevar a cabo simulaciones de ataques cibernéticos con regularidad. Cada tipo de ejercicio puede aportar ventajas únicas para los participantes y la organización en su conjunto, por lo que puede optar por empezar con tipos de simulaciones menos complejos (como los ejercicios prácticos) y pasar luego a los más complejos (ejercicios de equipo rojo). El tipo de simulación se debe elegir en función de su nivel de madurez en seguridad, sus recursos y los resultados deseados. Es posible que algunos clientes opten por no llevar a cabo los ejercicios de equipo rojo por su complejidad y su costo.

Pasos para la implementación

Independientemente del tipo de simulación que elija, las simulaciones suelen tener estos pasos de implementación:

1. Definición de los elementos básicos del ejercicio: defina el escenario de simulación y los objetivos de la simulación. Ambos deben contar con la aceptación de los directivos.
2. Identificación de las principales partes interesadas: como mínimo, en un ejercicio debe haber facilitadores y participantes. En función del escenario, podrían participar otras partes interesadas, como los directivos del departamento legal, de comunicaciones o ejecutivo.
3. Creación y prueba del escenario: es posible que sea necesario redefinir el escenario a medida que se crea si algunos elementos específicos no son factibles. Se espera que, al final de esta etapa, haya un escenario definitivo.

4. Facilitación de la simulación: el tipo de simulación determina la forma de llevarla a cabo (un escenario en papel o un escenario simulado muy técnico). Los facilitadores deben adaptar sus tácticas de facilitación a los objetivos del ejercicio y, siempre que sea posible, involucrar a todos los participantes del ejercicio para obtener la mayor ventaja.
5. Desarrollo del informe posterior a la acción (AAR): identifique las áreas que funcionaron bien, las que pueden mejorar y las posibles carencias. El AAR debe medir la eficacia de la simulación, así como la respuesta del equipo al evento simulado, de modo que se pueda seguir su progreso a lo largo del tiempo con futuras simulaciones.

Recursos

Documentos relacionados:

- Guía de respuestas ante incidentes de AWS

Videos relacionados:

- AWS GameDay - Security Edition
- Running effective security incident response simulations

Operaciones

Las operaciones son el núcleo de la respuesta ante los incidentes. Aquí es donde se llevan a cabo las acciones de respuesta y reparación de los incidentes de seguridad. Las operaciones incluyen las cinco fases siguientes: detección, análisis, contención, erradicación y recuperación. Las descripciones de estas fases y los objetivos se encuentran en la siguiente tabla.

Fase	Objetivo
Detección	Identifique un posible evento de seguridad.
Análisis	Determine si el evento de seguridad es un incidente y evalúe el alcance de este.
Contención	Minimice y limite el alcance del evento de seguridad.

Fase	Objetivo
Erradicación	Elimine los recursos o artefactos no autorizados relacionados con el evento de seguridad. Implemente soluciones de mitigación para el incidente de seguridad.
Recuperación	Restaure los sistemas a un estado seguro conocido y supervise estos sistemas para comprobar que la amenaza no regrese.

Las fases deben servir de guía a la hora de responder y operar en los incidentes de seguridad con el fin de responder de manera eficaz y sólida. Las medidas reales que tome variarán según el incidente. Por ejemplo, un incidente relacionado con ransomware contará con un proceso de respuesta diferente al de un incidente que involucre a un bucket de Amazon S3 público. Además, no es necesario que estas fases se produzcan de forma secuencial. Tras la contención y la erradicación, es posible que tenga que volver al análisis para saber si sus acciones fueron eficaces.

La preparación minuciosa de su personal, sus procesos y su tecnología es clave para lograr la eficacia en las operaciones. Por lo tanto, siga las prácticas recomendadas de la sección Preparación para poder responder eficazmente a un evento de seguridad activo.

Para obtener más información, consulte la sección Operations de la Guía de respuesta ante incidentes de seguridad de AWS.

Actividad posterior al incidente

El panorama de amenazas cambia constantemente y es importante que su organización sea igual de dinámica a la hora de proteger sus entornos de manera eficaz. La clave de la mejora continua es la iteración de los resultados de sus incidentes y simulaciones con el fin de mejorar sus capacidades para detectar e investigar de forma eficaz los posibles incidentes de seguridad y responder a ellos con el objetivo de reducir las posibles vulnerabilidades, el tiempo de respuesta y el retorno a operaciones seguras. Los siguientes mecanismos pueden ayudarlo a comprobar que su organización está preparada con las capacidades y los conocimientos más recientes para responder de manera eficaz, sea cual sea la situación.

Prácticas recomendadas

- SEC10-BP08 Establecimiento de un marco de trabajo para aprender de los incidentes

SEC10-BP08 Establecimiento de un marco de trabajo para aprender de los incidentes

La implementación de un marco de trabajo sobre las lecciones aprendidas y una funcionalidad de análisis de la causa raíz no solo puede ayudar a mejorar las capacidades de respuesta a los incidentes, sino también a evitar que el incidente se repita. Al aprender de cada incidente, puede ayudar a evitar que se repitan los mismos errores, exposiciones o configuraciones incorrectas, lo que no solo mejorará el nivel de seguridad, sino también minimizará el tiempo que se pierde en situaciones evitables.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Es importante implementar un marco de trabajo sobre las lecciones aprendidas que establezca y logre, al más alto nivel, los puntos siguientes:

- ¿Cuándo se imparte una lección aprendida?
- ¿Qué implica el proceso de lecciones aprendidas?
- ¿Cómo se lleva a cabo una lección aprendida?
- ¿Quién participa en el proceso y cómo?
- ¿Cómo se van a identificar las áreas de mejora?
- ¿Cómo se va a garantizar que las mejoras se supervisan e implementan de manera efectiva?

El marco no debe centrarse en las personas ni en buscar culpables, sino en mejorar las herramientas y los procesos.

Pasos para la implementación

Además de los resultados generales enumerados anteriormente, es importante asegurarse de que se hacen las preguntas correctas para obtener el máximo valor del proceso (información que conduzca a mejoras viables). Considere la posibilidad de usar estas preguntas para fomentar el debate sobre las lecciones aprendidas:

- ¿Cuál fue el incidente?

- ¿Cuándo se identificó por primera vez el incidente?
- ¿Cómo se identificó?
- ¿Qué sistemas alertaron sobre la actividad?
- ¿Qué sistemas, servicios y datos estaban involucrados?
- ¿Qué ocurrió exactamente?
- ¿Qué funcionó correctamente?
- ¿Qué no funcionó correctamente?
- ¿Qué procesos o procedimientos fallaron o no se lograron escalar para responder al incidente?
- ¿Qué se puede mejorar en las siguientes áreas?:
  - People
    - ¿Las personas a las que había que contactar estaban realmente disponibles y la lista de contactos estaba actualizada?
    - ¿A las personas les faltaba formación o capacidades necesarias para responder e investigar el incidente de manera eficaz?
    - ¿Los recursos adecuados estaban listos y disponibles?
  - Proceso
    - ¿Se siguieron los procesos y los procedimientos?
    - ¿Los procesos y procedimientos para este (tipo de) incidente estaban documentados y disponibles?
    - ¿Faltaba algún proceso y procedimiento necesario?
    - ¿Los encargados de responder al incidente pudieron acceder oportunamente a la información necesaria para responder al problema?
  - Tecnología
    - ¿Los sistemas de alerta existentes identificaron la actividad y alertaron sobre ella eficazmente?
    - ¿Cómo podríamos haber reducido el tiempo de detección en un 50 %?
    - ¿Es necesario mejorar las alertas existentes o crear nuevas alertas para este (tipo de) incidente?
    - ¿Las herramientas existentes permitían investigar (buscar o analizar) el incidente de forma eficaz?
    - ¿Qué se puede hacer para poder identificar antes este (tipo de) incidente?
    - ¿Qué se puede hacer para ayudar a evitar que este (tipo de) incidente vuelva a ocurrir?

- ¿Quién es el responsable del plan de mejora y cómo comprobará que se ha implementado?
- ¿Qué plazos hay para implementar y probar otros procesos y controles preventivos o de supervisión?

Esta lista no incluye todas las posibilidades. Solo pretende servir como punto de partida para identificar cuáles son las necesidades de la organización y la empresa, y cómo se pueden analizar para aprender lo mejor posible de los incidentes y aumentar continuamente el nivel de seguridad. Lo más importante es empezar incorporando las lecciones aprendidas como un componente estándar del proceso de respuesta a incidentes, la documentación y las expectativas de las partes interesadas.

Recursos

Documentos relacionados:

- AWS Security Incident Response Guide - Establish a framework for learning from incidents
- NCSC CAF guidance - Lessons learned

Seguridad de las aplicaciones

La seguridad de las aplicaciones (AppSec) describe el proceso general de diseño, compilación y comprobación de las propiedades de seguridad de las cargas de trabajo que desarrolla. Debe contar con personal debidamente formado en su organización, comprender las propiedades de seguridad de su infraestructura de creación y lanzamiento, y utilizar la automatización para identificar problemas de seguridad.

La adopción de pruebas de seguridad de las aplicaciones como parte habitual del ciclo de vida de desarrollo del software (SDLC) y de los procesos posteriores al lanzamiento contribuye a garantizar que se dispone de un mecanismo estructurado para identificar, corregir y evitar que los problemas de seguridad de las aplicaciones entren en el entorno de producción.

La metodología de desarrollo de las aplicaciones debe incluir controles de seguridad a medida que diseña, compila, implementa y opera las cargas de trabajo. Al hacerlo, ajuste el proceso a fin de reducir continuamente los defectos y minimizar la deuda técnica. Por ejemplo, el uso de modelos de amenazas en la fase de diseño ayuda a detectar defectos de diseño en una fase temprana, lo que hace que sea más fácil y menos costoso solucionarlos, en lugar de esperar y mitigarlos más adelante.

El costo y la complejidad que supone resolver los defectos suelen ser menores cuanto antes se detecten en el SDLC. La forma más fácil de resolver los problemas es no tenerlos en primer lugar, por lo que empezar con un modelo de amenazas ayuda a centrarse en los resultados correctos desde la fase de diseño. A medida que su programa de AppSec madura, puede aumentar la cantidad de pruebas que se llevan a cabo mediante la automatización, mejorar la fidelidad de los comentarios para los creadores y reducir el tiempo necesario para las revisiones de seguridad. Todas estas medidas mejoran la calidad del software que crea y aumentan la velocidad de entrega de las características a la producción.

Estas directrices de implementación se centran en cuatro áreas: la organización y la cultura, la seguridad de la canalización, la seguridad en la canalización y la administración de las dependencias. Cada área proporciona un conjunto de principios que puede implementar y ofrece una visión integral de cómo diseñar, desarrollar, compilar, implementar y operar cargas de trabajo.

En AWS existen una serie de estrategias diferentes que puede utilizar a la hora de acometer su programa de seguridad de las aplicaciones. Algunas de ellas se basan en la tecnología, mientras que otras se centran en las personas y los aspectos organizativos de su programa de seguridad de las aplicaciones.

Prácticas recomendadas

- SEC11-BP01 Formación en seguridad de las aplicaciones
- SEC11-BP02 Automatización de las pruebas a lo largo del ciclo de vida de desarrollo y lanzamiento
- SEC11-BP03 Pruebas de penetración periódicas
- SEC11-BP04 Revisiones del código de conducta
- SEC11-BP05 Centralización de servicios para paquetes y dependencias
- SEC11-BP06 Implementación de software mediante programación
- SEC11-BP07 Evaluación periódica de las propiedades de seguridad de las canalizaciones
- SEC11-BP08 Creación de un programa que integre la propiedad de la seguridad en los equipos de la carga de trabajo

SEC11-BP01 Formación en seguridad de las aplicaciones

Forme a su equipo en prácticas de desarrollo y funcionamiento seguros, lo que los ayudará a crear software seguro y de alta calidad. Esta práctica ayuda a su equipo a prevenir, detectar y solucionar los problemas de seguridad en una fase temprana del ciclo de vida del desarrollo. Puede plantearse impartir formación sobre el modelado de amenazas, las prácticas de codificación segura y el uso de servicios para una configuración y funcionamiento seguros. Proporcione a su equipo acceso a la formación mediante recursos de autoservicio y recopile periódicamente sus comentarios para mejorar continuamente.

Resultado deseado: dota a su equipo de los conocimientos y las habilidades necesarios para diseñar y crear software teniendo en cuenta la seguridad desde el principio. Gracias a la formación sobre modelos de amenazas y prácticas de desarrollo seguro, su equipo tiene un profundo conocimiento de los posibles riesgos de seguridad y de cómo mitigarlos durante el ciclo de vida del desarrollo del software (SDLC). Este enfoque proactivo de la seguridad forma parte de la cultura de su equipo, por lo que podrá identificar y solucionar los posibles problemas de seguridad desde el principio. Como resultado, su equipo ofrece software y características seguras y de alta calidad de manera más eficiente, lo que acelera el plazo general de entrega. Su organización tiene una cultura de seguridad colaborativa e inclusiva, en la que todos los creadores comparten la propiedad de la seguridad.

Patrones comunes de uso no recomendados:

- Espera a una revisión de seguridad para estudiar las propiedades de seguridad de un sistema.
- Deja todas las decisiones de seguridad en manos del equipo de seguridad.

- No comunica claramente cómo se relacionan las decisiones tomadas en el SDLC con las expectativas o políticas generales de seguridad de la organización.
- Interviene demasiado tarde en el proceso de revisión de la seguridad.

Beneficios de establecer esta práctica recomendada:

- Entender mejor los requisitos de la organización en materia de seguridad en una fase temprana del ciclo de desarrollo.
- Poder identificar y corregir más rápidamente los posibles problemas de seguridad, lo que se traduce en una entrega más rápida de las características.
- Mejora de la calidad del software y los sistemas.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Para desarrollar software seguro y de calidad, forme a su equipo en prácticas habituales de desarrollo y funcionamiento seguros de las aplicaciones. Esta práctica puede ayudar a su equipo a prevenir, detectar y solucionar los problemas de seguridad en una fase temprana del ciclo de vida del desarrollo, lo que puede acelerar sus plazos de entrega.

Para que esta práctica dé resultado, considere la posibilidad de formar a su equipo en el modelado de amenazas mediante recursos de AWS, como el taller de modelado de amenazas. El modelado de amenazas puede ayudar a su equipo a comprender los posibles riesgos de seguridad y a diseñar sistemas teniendo en cuenta la seguridad desde el principio. Además, puede proporcionar acceso a formación de Formación de AWS and Certification, del sector o de los socios de AWS en prácticas de desarrollo seguras. Para obtener más información sobre un enfoque integral de diseño, desarrollo, protección y funcionamiento eficiente a escala, consulte la Guía de AWS DevOps.

Defina y comunique con claridad el proceso de revisión de la seguridad de su organización y describa las responsabilidades de su equipo, el equipo de seguridad y otras partes interesadas. Publique guías de autoservicio, ejemplos de código y plantillas con las que demuestre cómo cumplir sus requisitos de seguridad. Puede utilizar servicios de AWS como AWS CloudFormation, Constructos de Kit de desarrollo de la nube de AWS (AWS CDK) (AWS CDK) y Service Catalog para proporcionar configuraciones seguras y aprobadas previamente, y reducir la necesidad de configuraciones personalizadas.

Obtenga periódicamente comentarios de su equipo sobre su experiencia con el proceso de formación y revisión de la seguridad, y utilícelos para mejorar continuamente. Lleve a cabo días de juego o campañas de detección de errores para identificar y abordar los problemas de seguridad y, al mismo tiempo, mejorar las habilidades de su equipo.

Pasos para la implementación

1. Identifique las necesidades de formación: evalúe el nivel actual de habilidades y las brechas de conocimiento de su equipo en relación con las prácticas de desarrollo seguras mediante encuestas, revisiones de código o conversaciones con los miembros del equipo.
2. Planifique la formación: en función de las necesidades identificadas, cree un plan de formación que abarque temas relevantes, como el modelado de amenazas, las prácticas de codificación segura, las pruebas de seguridad y las prácticas de implementación segura. Emplee recursos como el taller de modelado de amenazas, Formación de AWS and Certification, y los programas de formación del sector o de los socios de AWS.
3. Programe e imparta formación: programe sesiones de formación o talleres periódicos para su equipo. Pueden ser impartidos por un instructor o a su propio ritmo, según las preferencias y la disponibilidad de su equipo. Haga hincapié en los ejercicios de aplicación de lo aprendido y en los ejemplos prácticos para reforzar el aprendizaje.
4. Defina un proceso de revisión de la seguridad: colabore con su equipo de seguridad y otras partes interesadas para definir claramente el proceso de revisión de la seguridad de las aplicaciones. Documente las responsabilidades de cada equipo o persona que participa en el proceso, incluidos el equipo de desarrollo, el equipo de seguridad y otras partes interesadas relevantes.
5. Cree recursos de autoservicio: elabore guías de autoservicio, ejemplos de código y plantillas que demuestren cómo cumplir los requisitos de seguridad de su organización. Puede usar servicios de AWS como CloudFormation, Constructos de AWS CDK y Service Catalog para proporcionar configuraciones seguras previamente aprobadas y reducir la necesidad de configuraciones personalizadas.
6. Comuníquese y socialice: comunique de manera eficaz a su equipo el proceso de revisión de la seguridad y los recursos de autoservicio disponibles. Lleve a cabo sesiones de formación o talleres para que se familiaricen con estos recursos y compruebe que entienden cómo usarlos.
7. Obtenga comentarios y mejore: obtenga periódicamente comentarios de su equipo sobre su experiencia con el proceso de formación y revisión de la seguridad. Utilice estos comentarios para identificar las áreas de mejora y perfeccionar continuamente los materiales de formación, los recursos de autoservicio y el proceso de revisión de la seguridad.

8. Realice ejercicios de seguridad: organice jornadas de juego o campañas de detección de errores para identificar y abordar los problemas de seguridad de las aplicaciones. Estos ejercicios no solo ayudan a descubrir posibles vulnerabilidades, sino que también sirven como oportunidades prácticas de aprendizaje para su equipo, ya que mejoran sus habilidades de desarrollo y funcionamiento seguros.
9. Siga aprendiendo y mejorando: anime a su equipo a mantenerse al día con las últimas prácticas, herramientas y técnicas de desarrollo seguro. Revise y actualice periódicamente los materiales y recursos de formación para reflejar la evolución del panorama de la seguridad y las prácticas recomendadas.

Recursos

Prácticas recomendadas relacionadas:

- SEC11-BP08 Creación de un programa que integre la propiedad de la seguridad en los equipos de la carga de trabajo

Documentos relacionados:

- Formación de AWS and Certification
- How to think about cloud security governance
- How to approach threat modeling
- Accelerating training – The AWS Skills Guild
- AWS Sagas de DevOps

Videos relacionados:

- Proactive security: Considerations and approaches

Ejemplos relacionados:

- Workshop on threat modeling
- Industry awareness for developers

Servicios relacionados:

- AWS CloudFormation
- Kit de desarrollo de la nube de AWS (AWS CDK) (AWS CDK) Constructs
- Service Catalog

SEC11-BP02 Automatización de las pruebas a lo largo del ciclo de vida de desarrollo y lanzamiento

Automatice las pruebas de las propiedades de seguridad a lo largo del ciclo de vida de desarrollo y lanzamiento. La automatización facilita la identificación coherente y repetible de posibles problemas en el software antes de su lanzamiento, lo que reduce el riesgo de problemas de seguridad en el software suministrado.

Resultado deseado: el objetivo de las pruebas automatizadas es proporcionar una forma programática de detectar posibles problemas de forma temprana y frecuente a lo largo del ciclo de vida del desarrollo. Al automatizar las pruebas de regresión, puede volver a ejecutar pruebas funcionales y no funcionales para verificar que el software probado previamente siga funcionando como se esperaba después de un cambio. Cuando se definen pruebas unitarias de seguridad para detectar errores de configuración habituales, como autenticación dañada o ausente, es posible identificar y solucionar estos problemas en una fase temprana del proceso de desarrollo.

La automatización de pruebas utiliza casos de prueba creados específicamente para la validación de aplicaciones, basados en los requisitos de la aplicación y la funcionalidad deseada. El resultado de las pruebas automatizadas se basa en la comparación de los resultados de las pruebas generados con los resultados esperados, lo que agiliza el ciclo de vida de las pruebas. Las metodologías de pruebas como las pruebas de regresión y los conjuntos de pruebas unitarias son las más adecuadas para la automatización. La automatización de las pruebas de las propiedades de seguridad permite a los creadores recibir información automatizada sin tener que esperar a una revisión de seguridad. Las pruebas automatizadas en forma de análisis de código estático o dinámico permiten aumentar la calidad del código y contribuyen a detectar posibles problemas de software en una fase temprana del ciclo de vida de desarrollo.

Patrones comunes de uso no recomendados:

- No comunicar los casos de prueba y los resultados de las pruebas automatizadas.
- Llevar a cabo las pruebas automatizadas solo justo antes del lanzamiento.
- Automatizar casos de prueba con requisitos que cambian con frecuencia.

- No proporcionar orientación sobre cómo abordar los resultados de las pruebas de seguridad.

Beneficios de establecer esta práctica recomendada:

- Se ha reducido la dependencia de las personas que evalúan las propiedades de seguridad de los sistemas.
- La obtención de resultados coherentes en numerosos flujos de trabajo mejora la coherencia general.
- Menos probabilidades de que se introduzcan problemas de seguridad en el software de producción.
- Reducción del intervalo de tiempo entre la detección y la corrección gracias a la detección temprana de los problemas de software.
- Mayor visibilidad del comportamiento sistémico o repetido en numerosos flujos de trabajo, que puede servir para impulsar mejoras en toda la organización.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

A medida que crea el software, adopte diversos mecanismos de prueba de software para asegurarse de probar tanto los requisitos funcionales, basados en la lógica empresarial, como los requisitos no funcionales, que se centran en la fiabilidad, el rendimiento y la seguridad de su aplicación.

Las pruebas de seguridad de aplicaciones estáticas (SAST) analizan el código fuente para revelar patrones de seguridad anómalos y proporcionan indicios de código propenso a errores. Las pruebas SAST se basan en datos estáticos, como la documentación (especificación de requisitos, documentación de diseño y especificaciones de diseño) y el código fuente de la aplicación, con objeto de encontrar una serie de problemas de seguridad conocidos. Los analizadores de código estático pueden ayudar a agilizar el análisis de grandes volúmenes de código. El NIST Quality Group ofrece una comparación de analizadores de seguridad del código fuente, que incluye herramientas de código abierto para analizadores de código de bytes y analizadores de código binario.

Complemente las pruebas estáticas con metodologías de pruebas de seguridad de análisis dinámico (DAST), que efectúan pruebas de la aplicación en ejecución a fin de identificar comportamiento potencialmente inesperado. Las pruebas dinámicas pueden utilizarse para detectar problemas potenciales que no son evidentes mediante el análisis estático. Las pruebas en las etapas de repositorio de código, compilación y canalización le permiten comprobar si existen diferentes tipos

de problemas potenciales que podrían introducirse en el código. Amazon Q Developer proporciona recomendaciones de código, incluido el análisis de seguridad, en el IDE del creador. Amazon CodeGuru Security puede identificar problemas cruciales, problemas de seguridad y errores difíciles de detectar durante el desarrollo de la aplicación, y proporciona recomendaciones para mejorar la calidad del código. La extracción de la lista de materiales del software (SBOM) también le permite extraer un registro formal que contiene los detalles y las relaciones de los distintos componentes utilizados en la creación del software. Esto le permite informar sobre la gestión de vulnerabilidades e identificar rápidamente las dependencias del software o los componentes y los riesgos de la cadena de suministro.

El taller Security for Developers usa herramientas para desarrolladores de AWS, como AWS CodeBuild, AWS CodeCommit y AWS CodePipeline, para la automatización de canalizaciones de lanzamiento que incluye las metodologías de prueba SAST y DAST.

A medida que avance en el SDLC, establezca un proceso iterativo que incorpore revisiones periódicas de las aplicaciones con su equipo de seguridad. Los comentarios recopilados en estas revisiones de seguridad deben abordarse y validarse como parte de la revisión de la preparación para el lanzamiento. Estas revisiones establecen una sólida postura de seguridad de la aplicación y proporcionan a los desarrolladores información práctica para afrontar posibles problemas.

Pasos para la implementación

- Implemente herramientas coherentes de IDE, revisión de código y CI/CD que incluyan pruebas de seguridad.
- Considere en qué momento del SDLC es apropiado bloquear las canalizaciones en lugar de limitarse a notificar a los creadores que es necesario solucionar los problemas.
- Automated Security Helper (ASH) es un ejemplo de herramienta de análisis de seguridad de código abierto.
- La ejecución de pruebas o el análisis de código mediante herramientas automatizadas, como Amazon Q Developer integrado con los IDE de los desarrolladores y el Amazon CodeGuru Security para escanear el código al confirmar, ayuda a los creadores a obtener información en el momento adecuado.
- Si usa AWS Lambda para la compilación, puede usar Amazon Inspector para analizar el código de la aplicación en sus funciones.
- Cuando se incluyen pruebas automatizadas en las canalizaciones de CI/CD, es preciso utilizar un sistema de tickets para hacer un seguimiento de la notificación y corrección de problemas de software.

- En el caso de las pruebas de seguridad que puedan generar resultados, la vinculación a orientaciones para la corrección ayuda a los creadores a mejorar la calidad del código.
- Analice periódicamente los resultados de las herramientas automatizadas para dar prioridad a la siguiente automatización, la formación de los creadores o la campaña de concienciación.
- Para extraer la SBOM como parte de las canalizaciones de CI/CD, utilice el generador de SBOM de Amazon Inspector para obtener SBOM de archivos, imágenes de contenedores, directorios, sistemas locales y binarios compilados de Go y Rust en el formato SBOM de CycloneDX.

Recursos

Prácticas recomendadas relacionadas:

- DevOps Guidance: DL.CR.3 Establish clear completion criteria for code tasks

Documentos relacionados:

- Entrega continua e implementación continua

- AWS Socios con competencias en DevOps de
- AWS Socios con competencia en seguridad de para la seguridad de aplicaciones
- Choosing a Well-Architected CI/CD approach
- Secrets detection in Amazon CodeGuru Security
- Amazon CodeGuru Security Detection Library
- Accelerate deployments on AWS with effective governance
- Automatización de implementaciones seguras y sin intervención de AWS
- How Amazon CodeGuru Security helps you effectively balance security and velocity

Videos relacionados:

- Hands-off: Automating continuous delivery pipelines at Amazon
- Automating cross-account CI/CD pipelines
- The Software Development Process at Amazon
- Testing software and systems at Amazon

Ejemplos relacionados:

- Industry awareness for developers
- Automated Security Helper (ASH)
- AWS CodePipeline Governance - Github

SEC11-BP03 Pruebas de penetración periódicas

Lleve a cabo pruebas de penetración periódicas de su software. Este mecanismo ayuda a identificar posibles problemas de software que no pueden detectarse mediante pruebas automatizadas o una revisión manual del código. También puede ayudarle a comprender la eficacia de sus controles de detección. Las pruebas de penetración deben tratar de determinar si se puede hacer que el software lleve a cabo operaciones inesperadas, como exponer datos que deberían estar protegidos o conceder permisos más amplios de lo esperado.

Resultado deseado: las pruebas de penetración se utilizan para detectar, corregir y validar las propiedades de seguridad de la aplicación. Las pruebas de penetración periódicas y programadas deben formar parte del ciclo de vida de desarrollo de software (SDLC). Los resultados de las pruebas de penetración deben resolverse antes del lanzamiento del software. Debe analizar los resultados de las pruebas de penetración para identificar si hay problemas que podrían detectarse mediante la automatización. El uso de un proceso de pruebas de penetración periódicas y repetibles que incluya un mecanismo de retroalimentación activo ayuda a orientar a los creadores y mejora la calidad del software.

Patrones comunes de uso no recomendados:

- Hacer pruebas de penetración solo para problemas de seguridad conocidos o frecuentes.
- Hacer pruebas de penetración de aplicaciones sin herramientas ni bibliotecas de terceros dependientes.
- Hacer pruebas de penetración solo para problemas de seguridad de paquete, sin evaluar la lógica empresarial implementada.

Beneficios de establecer esta práctica recomendada:

- Mayor confianza en las propiedades de seguridad del software antes de su lanzamiento.

- Oportunidad de identificar los patrones de aplicación preferidos, lo que conduce a una mayor calidad del software.
- Un ciclo de retroalimentación que identifica en una fase más temprana del ciclo de desarrollo dónde la automatización o la formación adicional podrían mejorar las propiedades de seguridad del software.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Las pruebas de penetración son un ejercicio estructurado de pruebas de seguridad en el que se ejecutan escenarios planificados de infracción de la seguridad para detectar, remediar y validar los controles de seguridad. Las pruebas de penetración comienzan con el reconocimiento, durante el cual se recopilan datos basados en el diseño actual de la aplicación y sus dependencias. Luego, se elabora y ejecuta una lista seleccionada de escenarios de pruebas de seguridad. El objetivo principal de estas pruebas es descubrir problemas de seguridad en la aplicación, que podrían aprovecharse para obtener acceso no deseado a su entorno o acceso no autorizado a los datos. Debe llevar a cabo pruebas de penetración cuando lance nuevas características, o siempre que la aplicación haya sufrido cambios importantes en su funcionamiento o implementación técnica.

Debe identificar la etapa más apropiada del ciclo de vida de desarrollo en el que llevar a cabo las pruebas de penetración. Estas pruebas deben hacerse lo bastante tarde como para que la funcionalidad del sistema se aproxime al estado de lanzamiento previsto, pero con tiempo suficiente para solucionar cualquier problema.

Pasos para la implementación

- Disponga de un proceso estructurado para determinar el alcance de las pruebas de penetración; basar este proceso en el modelo de amenazas es una buena forma de mantener el contexto.
- Identifique la etapa más apropiada del ciclo de desarrollo en el que llevar a cabo las pruebas de penetración. Debería ser cuando se espera un cambio mínimo en la aplicación, pero con tiempo suficiente para llevar a cabo la corrección.
- Forme a sus creadores sobre qué esperar de los resultados de las pruebas de penetración y cómo obtener información sobre la corrección.
- Utilice herramientas para acelerar el proceso de las pruebas de penetración mediante la automatización de pruebas habituales o repetibles.

- Analice los resultados de las pruebas de penetración con vistas a identificar problemas de seguridad sistémicos y utilice estos datos para efectuar pruebas automatizadas adicionales y para la formación continua de los creadores.

Recursos

Prácticas recomendadas relacionadas:

- SEC11-BP01 Formación en seguridad de las aplicaciones
- SEC11-BP02 Automatización de las pruebas a lo largo del ciclo de vida de desarrollo y lanzamiento

Documentos relacionados:

- Las pruebas de penetración de AWS proporcionan una guía detallada sobres las pruebas de penetración en AWS
- Accelerate deployments on AWS with effective governance
- AWS Socios con competencia en seguridad de
- Modernize your penetration testing architecture on AWS Fargate
- AWS Fault injection Simulator

Ejemplos relacionados:

- Automate API testing with AWS CodePipeline (GitHub)
- Automated security helper (GitHub)

SEC11-BP04 Revisiones del código de conducta

Implemente revisiones de código para ayudar a verificar la calidad y la seguridad del software que se está desarrollando. En las revisiones del código, otros miembros del equipo, además del autor del código original, revisan el código para detectar posibles problemas o vulnerabilidades y comprobar que cumpla con los estándares y las prácticas recomendadas de codificación. Este proceso ayuda a detectar errores, incoherencias y fallos de seguridad que el desarrollador original podría haber pasado por alto. Use herramientas automatizadas para que lo ayuden con las revisiones del código.

Resultado deseado: incluye revisiones de código durante el desarrollo para aumentar la calidad del software que se está escribiendo. Mejora las habilidades de los miembros del equipo con menos experiencia a través de lo aprendido durante la revisión del código. Identifica las oportunidades de automatización y apoya el proceso de revisión del código mediante herramientas y pruebas automatizadas.

Patrones comunes de uso no recomendados:

- No revisa el código antes de la implementación.
- El código lo escribe y lo revisa la misma persona.
- No utiliza la automatización como ayuda con las revisiones del código o para su organización.
- No forma a los creadores en seguridad de las aplicaciones antes de que revisen el código.

Beneficios de establecer esta práctica recomendada:

- Mayor calidad del código.
- Mayor coherencia en el desarrollo del código gracias a la reutilización de estrategias comunes.
- Reducción del número de problemas revelados durante las pruebas de penetración y etapas posteriores.
- Mejora de la transferencia de conocimientos dentro del equipo.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Las revisiones de código ayudan a verificar la calidad y la seguridad del software durante su desarrollo. En las revisiones del código, un miembro del equipo que no es el autor del código original revisa el código para detectar posibles problemas o vulnerabilidades y comprobar que cumpla con los estándares y las prácticas recomendadas de codificación. Este proceso ayuda a detectar errores, incoherencias y fallos de seguridad que el desarrollador original podría haber pasado por alto.

Puede usar Amazon CodeGuru Security como ayuda para realizar revisiones de código automatizadas. CodeGuru Security utiliza el machine learning y el razonamiento automatizado para analizar su código e identificar posibles vulnerabilidades de seguridad y problemas de codificación. Integre las revisiones automatizadas del código con los repositorios de código y las canalizaciones de implementación continua/implementación continua (CI/CD) existentes.

Pasos para la implementación

1. Establezca un proceso de revisión del código:
    - Defina cuándo deben realizarse las revisiones del código. Por ejemplo, antes de fusionar el código en la rama principal o antes de implementarlo en producción.
    - Determine quién debe participar en el proceso de revisión del código, como los miembros del equipo, los desarrolladores sénior y los expertos en seguridad.
    - Decida la metodología de revisión del código, incluidos el proceso y las herramientas que se utilizarán.
2. Configure las herramientas de revisión de código:
    - Evalúe y seleccione herramientas de revisión de código que se adapten a las necesidades de su equipo, como GitHub Pull Requests o CodeGuru Security.
    - Integre las herramientas elegidas con sus repositorios de código y canalizaciones de CI/CD existentes.
    - Configure las herramientas para aplicar los requisitos de revisión del código, como el número mínimo de revisores y las reglas de aprobación.
3. Defina una lista de verificación y directrices para la revisión del código:
    - Cree una lista de verificación o pautas para la revisión del código que describa lo que debe revisarse. Tenga en cuenta factores como la calidad del código, las vulnerabilidades de seguridad, el cumplimiento de los estándares de codificación y el rendimiento.
    - Comparta la lista de verificación o las directrices con el equipo de desarrollo y compruebe que todos entiendan lo que se espera.
4. Forme a los desarrolladores en las prácticas recomendadas de revisión de código:
    - Ofrezca a su equipo formación sobre cómo llevar a cabo revisiones de código eficaces.
    - Informe a su equipo sobre los principios de seguridad de las aplicaciones y las vulnerabilidades más comunes que deben tenerse en cuenta durante las revisiones.
    - Fomente el intercambio de conocimientos y combine las sesiones de programación para mejorar la competencia a los miembros del equipo con menos experiencia.
5. Implemente el proceso de revisión del código:
    - Integre el paso de revisión del código en su flujo de trabajo de desarrollo, como crear una solicitud de extracción y asignar revisores.
    - Exija que los cambios de código se sometan a revisión antes de fusionarlos o implementarlos.
    - Fomente una comunicación abierta y comentarios constructivos durante el proceso de revisión.

6. Supervise y mejore:
    - Revise periódicamente la eficacia del proceso de revisión del código y recopile los comentarios del equipo.
    - Identifique oportunidades de automatización o mejoras en las herramientas para agilizar el proceso de revisión del código.
    - Actualice y perfeccione continuamente la lista de verificación o las directrices de revisión del código en función de lo aprendido y las prácticas recomendadas del sector.
7. Fomente una cultura de revisión del código:
    - Haga hincapié en la importancia de las revisiones del código para mantener la calidad y la seguridad del código.
    - Celebre los éxitos y los aprendizajes del proceso de revisión del código.
    - Fomente un entorno colaborativo y de apoyo en el que los desarrolladores se sientan cómodos dando y recibiendo comentarios.

Recursos

Prácticas recomendadas relacionadas:

- SEC11-BP02 Automatización de las pruebas a lo largo del ciclo de vida de desarrollo y lanzamiento

Documentos relacionados:

- DevOps Guidance: DL.CR.2 Perform peer review for code changes
- About pull requests in GitHub

Ejemplos relacionados:

- Automate code reviews with Amazon CodeGuru Security
- Automating detection of security vulnerabilities and bugs in CI/CD pipelines using Amazon CodeGuru Security CLI

Videos relacionados:

- Continuous improvement of code quality with Amazon CodeGuru Security

SEC11-BP05 Centralización de servicios para paquetes y dependencias

Proporcione servicios centralizados para que sus equipos obtengan paquetes de software y otras dependencias. De este modo, se podrán validar los paquetes antes de incluirlos en el software que escriba y se dispondrá de un origen de datos para el análisis del software que se utiliza en su organización.

Resultado deseado: crea la carga de trabajo a partir de paquetes de software externos además del código que programe. Esto permite implementar más fácilmente funcionalidades de uso reiterado, como un analizador JSON o una biblioteca de cifrado. Centraliza los orígenes de estos paquetes y dependencias para que su equipo de seguridad los valide antes de utilizarlos. Utiliza este planteamiento junto con los flujos de pruebas manuales y automatizadas para aumentar la confianza en la calidad del software que desarrolla.

Patrones comunes de uso no recomendados:

- Obtiene paquetes de repositorios arbitrarios de Internet.
- No prueba los nuevos paquetes antes de ponerlos a disposición de los creadores.

Beneficios de establecer esta práctica recomendada:

- Mejor comprensión de los paquetes que se utilizan en el software que se crea.
- Poder notificar a los equipos de carga de trabajo cuándo es necesario actualizar un paquete en función de la comprensión de quién utiliza qué.
- Reducción del riesgo de que se incluya en el software un paquete con problemas.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: medio

Guía para la implementación

Proporcione servicios centralizados para paquetes y dependencias de una manera que resulte sencilla de consumir a los creadores. Los servicios centralizados pueden ser lógicamente centrales en lugar de implementarse como un sistema monolítico. Este método le permite proporcionar servicios de una manera que satisfaga las necesidades de los creadores. Debe implementar una forma eficaz de agregar paquetes al repositorio cuando se produzcan actualizaciones o surjan

nuevos requisitos. Los servicios de AWS como AWS CodeArtifact o las soluciones similares de socios de AWS son una forma de ofrecer esta capacidad.

Pasos para la implementación

- Implemente un servicio de repositorio lógicamente centralizado que esté disponible en todos los entornos en los que se desarrolla software.
- Incluya el acceso al repositorio como parte del proceso de aprovisionamiento de cuentas de Cuenta de AWS.
- Consolide la automatización para probar paquetes antes de que se publiquen en un repositorio.
- Mantenga métricas de los paquetes, lenguajes y equipos más utilizados y con mayor cantidad de cambios.
- Proporcione un mecanismo automatizado para que los equipos de creación soliciten nuevos paquetes y proporcionen comentarios.
- Analice periódicamente los paquetes del repositorio para identificar la posible repercusión de los problemas que se acaban de detectar.

Recursos

Prácticas recomendadas relacionadas:

- SEC11-BP02 Automatización de las pruebas a lo largo del ciclo de vida de desarrollo y lanzamiento

Documentos relacionados:

- DevOps Guidance: DL.CS.2 Sign code artifacts after each build
- Supply chain Levels for Software Artifacts (SLSA)

Ejemplos relacionados:

- Accelerate deployments on AWS with effective governance
- Tighten your package security with CodeArtifact Package Origin Control toolkit
- Multi Region Package Publishing Pipeline (GitHub)
- Publishing Node.js Modules on AWS CodeArtifact using AWS CodePipeline (GitHub)

- AWS CDK Java CodeArtifact Pipeline Sample (GitHub)
- Distribute private .NET NuGet packages with AWS CodeArtifact (GitHub)

Videos relacionados:

- Proactive security: Considerations and approaches
- The AWS Philosophy of Security (re:Invent 2017)
- When security, safety, and urgency all matter: Handling Log4Shell

SEC11-BP06 Implementación de software mediante programación

Siempre que sea posible, lleve a cabo las implementaciones de software mediante programación. Con este enfoque se reduce la probabilidad de que se produzca un error en la implementación o de que surja un problema inesperado debido a un error humano.

Resultado deseado: la versión de la carga de trabajo que se prueba es la versión que implementa, y la implementación se realiza de forma coherente en todo momento. Externaliza la configuración de su carga de trabajo, lo que ayuda a realizar la implementación en diferentes entornos sin cambios. Emplea la firma criptográfica de los paquetes de software para verificar que no ha cambiado nada entre entornos.

Patrones comunes de uso no recomendados:

- Implementar manualmente el software en producción.
- Hacer cambios manualmente en el software para adaptarlo a distintos entornos.

Beneficios de establecer esta práctica recomendada:

- Mayor confianza en el proceso de lanzamiento de software.
- Reducción del riesgo de que un cambio erróneo afecte a las funciones de la empresa.
- Aumento de la cadencia de lanzamiento debido al menor riesgo del cambio.
- Capacidad de reversión automática en caso de imprevistos durante la implementación.
- Capacidad para demostrar criptográficamente que el software probado es el software implementado.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Para mantener una infraestructura de aplicaciones sólida y fiable, aplique prácticas de implementación seguras y automatizadas. Esta práctica implica eliminar el acceso humano persistente de los entornos de producción, utilizar herramientas de CI/CD para las implementaciones y externalizar los datos de configuración específicos del entorno. Si utiliza esta estrategia, puede mejorar la seguridad, reducir el riesgo de errores humanos y agilizar el proceso de implementación.

Puede crear su estructura de Cuenta de AWS para eliminar el acceso humano persistente de los entornos de producción. Esta práctica minimiza el riesgo de cambios no autorizados o modificaciones accidentales, lo que mejora la integridad de los sistemas de producción. En lugar del acceso humano directo, puede utilizar herramientas de CI/CD como AWS CodeBuild y AWS CodePipeline para realizar implementaciones. Puede utilizar estos servicios para automatizar los procesos de creación, prueba e implementación, lo que reduce la intervención manual y aumenta la coherencia.

Para mejorar aún más la seguridad y la trazabilidad, puede firmar los paquetes de aplicaciones después de probarlos y validar estas firmas durante la implementación. Para ello, utilice herramientas criptográficas como AWS Signer o AWS Key Management Service (AWS KMS). Al firmar y verificar los paquetes, puede asegurarse de implementar solo código autorizado y validado en sus entornos.

Asimismo, su equipo puede diseñar la carga de trabajo para que los datos de configuración específicos del entorno se obtengan de una fuente externa, como el Almacén de parámetros de AWS Systems Manager. Esta práctica separa el código de la aplicación de los datos de configuración, lo que ayuda a administrar y actualizar las configuraciones de forma independiente sin modificar el código de la aplicación en sí.

Para agilizar el aprovisionamiento y la administración de la infraestructura, puede plantearse utilizar herramientas de infraestructura como código (IaC), por ejemplo, AWS CloudFormation o AWS CDK. Puede usar estas herramientas para definir su infraestructura como código, lo que mejora la coherencia y la repetibilidad de las implementaciones en diferentes entornos.

Plantéese usar las implementaciones canario para validar la implementación correcta de su software. Las implementaciones canario suponen implementar cambios en un subconjunto de instancias o usuarios antes de implementarlas en todo el entorno de producción. Luego, puede monitorear el impacto de los cambios y revertirlos si es necesario, lo que minimiza el riesgo de que los problemas se generalicen.

Siga las recomendaciones descritas en el documento técnico Organizing Your AWS Environment Using Multiple Accounts. Este documento técnico proporciona orientación sobre cómo separar los entornos (como los de desarrollo, ensayo y producción) en distintas Cuentas de AWS, lo que mejora aún más la seguridad y el aislamiento.

Pasos para la implementación

1. Configure la estructura de la Cuenta de AWS:
    - Siga las instrucciones del documento técnico Organizing Your AWS Environment Using Multiple Accounts para crear Cuentas de AWS separadas para diferentes entornos (por ejemplo, de desarrollo, ensayo y producción).
    - Configure los controles de acceso y los permisos adecuados para cada cuenta a fin de restringir el acceso humano directo a los entornos de producción.
2. Implemente un proceso de CI/CD:
    - Configure una canalización de CI/CD utilizando servicios como AWS CodeBuild y AWS CodePipeline.
    - Configure la canalización para compilar, probar e implementar automáticamente el código de la aplicación en los entornos respectivos.
    - Integre los repositorios de código con la canalización de CI/CD para el control de versiones y la administración del código.
3. Firme y verifique los paquetes de aplicaciones:
    - Utilice AWS Signer o AWS Key Management Service (AWS KMS) para firmar los paquetes de aplicaciones después de haberlos probado y validado.
    - Configure el proceso de implementación para verificar las firmas de los paquetes de aplicaciones antes de implementarlos en los entornos de destino.
4. Externalice los datos de configuración:
    - Guarde los datos de configuración específicos del entorno en el almacén de parámetros de AWS Systems Manager.
    - Modifique el código de la aplicación para recuperar los datos de configuración del almacén de parámetros durante la implementación o el tiempo de ejecución.
5. Implemente Infraestructura como código (IaC):
    - Utilice herramientas de IaC, como AWS CloudFormation o AWS CDK, para definir y administrar su infraestructura como código.

- Cree plantillas de CloudFormation o scripts de CDK para aprovisionar y configurar los recursos de AWS necesarios para su aplicación.
- Integre el IaC con la canalización de CI/CD para implementar automáticamente los cambios en la infraestructura junto con los cambios en el código de las aplicaciones.

6. Despliegue implementaciones canario:
   - Configure su proceso de implementación para que sea compatible con las implementaciones canario, en las que los cambios se implementan en un subconjunto de instancias o usuarios antes de implementarlos en todo el entorno de producción.
   - Utilice servicios como AWS CodeDeploy o AWSECS para gestionar las implementaciones canario y monitorear el impacto de los cambios.
   - Implemente mecanismos de reversión para volver a la versión estable anterior si se detectan problemas durante la implementación canario.
7. Monitoree y audite:
   - Configure mecanismos de supervisión y registro para llevar un seguimiento de las implementaciones, el rendimiento de las aplicaciones y los cambios en la infraestructura.
   - Utilice servicios como Amazon CloudWatch y AWS CloudTrail para recopilar y analizar registros y métricas.
   - Implemente comprobaciones de auditoría y conformidad para verificar el cumplimiento de las prácticas recomendadas de seguridad y los requisitos normativos.
8. Mejore continuamente:
   - Revise y actualice periódicamente las prácticas de implementación e incorpore los comentarios y las lecciones aprendidas de las implementaciones anteriores.
   - Automatice la mayor parte posible del proceso de implementación para reducir la intervención manual y los posibles errores humanos.
   - Colabore con equipos multifuncionales (por ejemplo, de operaciones o seguridad) para adaptar y mejorar continuamente las prácticas de implementación.

Si sigue estos pasos, puede desplegar prácticas de implementación seguras y automatizadas en su entorno de AWS, lo que mejora la seguridad, reduce el riesgo de errores humanos y agiliza el proceso de implementación.

Recursos

Prácticas recomendadas relacionadas:

- SEC11-BP02 Automatización de las pruebas a lo largo del ciclo de vida de desarrollo y lanzamiento
- DL.CI.2 Trigger builds automatically upon source code modifications

Documentos relacionados:

- Accelerate deployments on AWS with effective governance
- Automatización de implementaciones seguras y sin intervención
- Code signing using AWS Certificate Manager Private CA and AWS Key Management Service asymmetric keys
- Code Signing, a Trust and Integrity Control for AWS Lambda

Videos relacionados:

- Hands-off: Automating continuous delivery pipelines at Amazon

Ejemplos relacionados:

- Blue/Green deployments with AWS Fargate

SEC11-BP07 Evaluación periódica de las propiedades de seguridad de las canalizaciones

Aplique los principios del pilar de seguridad de Well-Architected a sus canalizaciones y preste especial atención a la separación de permisos. Evalúe periódicamente las propiedades de seguridad de su infraestructura de canalización. La administración eficaz de la seguridad de las canalizaciones le permite garantizar la seguridad del software que pasa por ellas.

Resultado deseado: las canalizaciones utilizadas para crear e implementar el software siguen las mismas prácticas recomendadas que cualquier otra carga de trabajo de su entorno. Los equipos que las utilizan no pueden editar las pruebas que implementa en las canalizaciones. Concede a las canalizaciones solo los permisos necesarios para las implementaciones que se están llevando a cabo mediante credenciales temporales. Implementa medidas de seguridad para evitar que las canalizaciones se desplieguen en los entornos incorrectos. Configura las canalizaciones en el estado de emisión para que se pueda validar la integridad de los entornos de compilación.

Patrones comunes de uso no recomendados:

- Pruebas de seguridad que los creadores pueden omitir.
- Permisos demasiado amplios para las canalizaciones de implementación.
- Canalizaciones no configuradas para validar entradas.
- No revisar periódicamente los permisos asociados a la infraestructura de CI/CD.
- Uso de credenciales a largo plazo o codificadas.

Beneficios de establecer esta práctica recomendada:

- Mayor confianza en la integridad del software que se crea e implementa a través de las canalizaciones.
- Capacidad para detener una implementación cuando hay actividades sospechosas.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: alto

Guía para la implementación

Las canalizaciones de implementación son un componente fundamental del ciclo de vida de desarrollo de software y deben seguir los mismos principios y prácticas de seguridad que cualquier otra carga de trabajo de su entorno. Esto incluye implementar controles de acceso adecuados, validar las entradas y revisar y auditar periódicamente los permisos asociados a la infraestructura de CI/CD.

Compruebe que los equipos responsables de crear e implementar las aplicaciones no tengan la capacidad de editar o eludir las pruebas y los controles de seguridad implementados en los procesos. Esta separación de preocupaciones ayuda a mantener la integridad de los procesos de creación e implementación.

Como punto de partida, si lo considera oportuno puede utilizar la arquitectura de referencia de canalizaciones de implementación de AWS. Esta arquitectura de referencia proporciona una base segura y escalable sobre la que construir las canalizaciones de CI/CD de AWS.

Además, puede utilizar servicios como AWS Identity and Access Management Access Analyzer para generar políticas de IAM con privilegios mínimos para los permisos de la canalización y como un paso más en la canalización para verificar los permisos de la carga de trabajo. Esto ayuda a comprobar que las canalizaciones y las cargas de trabajo solo tienen los permisos necesarios para

sus funciones específicas, lo que reduce el riesgo de que se produzcan accesos o acciones no autorizados.

Pasos para la implementación

- Comience con la arquitectura de referencia de canalizaciones de implementación de AWS.
- Considere la posibilidad de utilizar el Analizador de acceso de AWS IAM para generar mediante programación políticas de IAM con privilegio mínimo para las canalizaciones.
- Integre las canalizaciones con la supervisión y las alertas para recibir notificaciones de actividades inesperadas o anómalas. En el caso de los servicios administrados de AWS, Amazon EventBridge le permite dirigir los datos a destinos como AWS Lambda o Amazon Simple Notification Service (Amazon SNS).

Recursos

Documentos relacionados:

- AWS Deployment Pipelines Reference Architecture
- Supervisión de AWS CodePipeline
- Prácticas recomendadas de seguridad para AWS CodePipeline

Ejemplos relacionados:

- DevOps monitoring dashboard (GitHub)

SEC11-BP08 Creación de un programa que integre la propiedad de la seguridad en los equipos de la carga de trabajo

Elabore un programa o un mecanismo que permita a los equipos de creadores tomar decisiones de seguridad sobre el software que crean. Aun así, su equipo de seguridad debe validar estas decisiones durante una revisión, pero integrar la propiedad de la seguridad en los equipos de creadores permite crear cargas de trabajo más rápidas y seguras. Este mecanismo también fomenta una cultura de propiedad que repercute positivamente en el funcionamiento de los sistemas que se crean.

Resultado deseado: ha integrado la propiedad de la seguridad y la toma de decisiones en sus equipos. Ha formado a sus equipos sobre cómo pensar en la seguridad o los ha ampliado con personal de seguridad integrado o asociado. Como resultado, sus equipos toman decisiones de seguridad de mayor calidad en una fase más temprana del ciclo de desarrollo.

Patrones comunes de uso no recomendados:

- Dejar todas las decisiones del diseño de la seguridad en manos del equipo de seguridad.
- No hacer frente a los requisitos de seguridad con suficiente antelación en el proceso de desarrollo.
- No obtener comentarios de los creadores y del personal de seguridad sobre el funcionamiento del programa.

Beneficios de establecer esta práctica recomendada:

- Reducción del tiempo necesario para completar las revisiones de seguridad.
- Reducción de los problemas de seguridad que solo se detectan en la fase de revisión de la seguridad.
- Mejora de la calidad general del software que se programa.
- Oportunidad de identificar y comprender problemas sistémicos o áreas de mejora de alto valor.
- Reducción de la cantidad de tareas que es necesario repetir debido a los resultados de la revisión de seguridad.
- Mejora de la percepción de la función de seguridad.

Nivel de riesgo expuesto si no se establece esta práctica recomendada: bajo

Guía para la implementación

Comience con las directrices que se proporcionan en SEC11-BP01 Formación en seguridad de las aplicaciones. A continuación, identifique el modelo operativo para el programa que crea que puede funcionar mejor para su organización. Los dos modelos principales son formar a los desarrolladores o integrar al personal de seguridad en los equipos de creadores. Una vez que haya decidido el enfoque inicial, deberá llevar a cabo una prueba piloto con uno o un pequeño grupo de equipos de carga de trabajo para comprobar que el modelo funciona en su organización. El apoyo de los líderes de los departamentos de creación y seguridad de la organización contribuye a la implantación y al éxito del programa. A medida que cree este programa, es importante elegir métricas que sirvan para mostrar el valor del programa. Aprender de cómo AWS ha tratado este problema es una buena

experiencia de aprendizaje. Esta práctica recomendada se centra en gran medida en la cultura y el cambio organizativo. Las herramientas que emplee deben apoyar la colaboración entre las comunidades de creadores y de seguridad.

Pasos para la implementación

- Empiece por formar a los desarrolladores en la seguridad para las aplicaciones.
- Cree una comunidad y un programa de incorporación para educar a los desarrolladores.
- Elija un nombre para el programa. Los más utilizados son Guardians, Champions o Advocates.
- Identifique el modelo que se va a utilizar: formar a los desarrolladores, incorporar ingenieros de seguridad o tener roles de seguridad afines.
- Identifique a los patrocinadores del proyecto entre los encargados de la seguridad, los desarrolladores y, quizá, otros grupos pertinentes.
- Haga un seguimiento del número de personas que participan en el programa, el tiempo necesario para las revisiones y los comentarios de los desarrolladores y el personal de seguridad. Utilice estas métricas para hacer mejoras.

Recursos

Prácticas recomendadas relacionadas:

- SEC11-BP01 Formación en seguridad de las aplicaciones
- SEC11-BP02 Automatización de las pruebas a lo largo del ciclo de vida de desarrollo y lanzamiento

Documentos relacionados:

- How to approach threat modeling
- How to think about cloud security governance
- How AWS built the Security Guardians program, a mechanism to distribute security ownership
- How to build a Security Guardians program to distribute security ownership

Videos relacionados:

- Proactive security: Considerations and approaches

- AppSec tooling and culture tips from AWS and Toyota Motor North America

Conclusión

La seguridad es un esfuerzo constante. Cuando se produzca una incidencia, debe tratarse como una oportunidad de mejorar la seguridad de la arquitectura. Disponer de controles de identidad sólidos, automatizar las respuestas a eventos de seguridad, proteger la infraestructura a varios niveles y administrar datos bien clasificados con cifrado proporciona la defensa en profundidad deseada por todos los negocios. Este esfuerzo es más fácil gracias a las funciones de programación, las características y los servicios de AWS que se detallan en el presente documento.

La aspiración de AWS es ayudarle a compilar y operar arquitecturas que protejan la información, los sistemas y los activos mientras aumenta el valor de negocio.

Colaboradores

Las siguientes personas y organizaciones han colaborado en este documento:

- Jay Michael, Principal Security Lead Solutions Architect, Amazon Web Services
- Kiaan Sumeet, Principal Security Consultant, Amazon Web Services
- Michael Fischer, Principal Solutions Architect, Amazon Web Services
- Conor Colgan, Principal Solutions Architect, Amazon Web Services
- Dave Walker, Principal Solutions Architect, Security & Compliance, Amazon Web Services
- Patrick Palmer, Principal Solutions Architect, Security & Compliance, Amazon Web Services
- Monka Vu Minh, Security Consultant, Amazon Web Services
- Kurt Kumar, Security Consultant, Amazon Web Services
- Fahima Khan, Security Solutions Architect, Amazon Web Services
- Mutaz Hajeer, Senior Security Solutions Architect, Amazon Web Services
- Luis Pastor, Senior Security Solutions Architect, Amazon Web Services
- Colin Igbokwe, Senior Security Solutions Architect, Amazon Web Services
- Geoff Sweet, Senior Security Solutions Architect, Amazon Web Services
- Anthony Harvey, Senior Security Solutions Architect, Amazon Web Services
- Sowjanya Rajavaram, Senior Security Solutions Architect, Amazon Web Services
- Krishna Prasad, Senior Solutions Architect, Amazon Web Services
- Faisal Farooq, Senior Solutions Architect, Amazon Web Services
- Arun Krishnaswamy, Senior Solutions Architect, Amazon Web Services
- Dan Girard, Senior Solutions Architect, Amazon Web Services
- Marc Luescher, Senior Solutions Architect, Amazon Web Services
- Kyle Nicodemus, Senior Technical Account Manager, Amazon Web Services
- Irina Szabo, Senior Technical Account Manager, Amazon Web Services
- Arun Sivaraman, Solutions Architect, Amazon Web Services
- Stephen Novak, Technical Account Manager, Amazon Web Services
- Jonathan Risbrook, Technical Account Manager, Amazon Web Services
- Freddy Kasprzykowski, Practice Manager - Global Financial Services, Amazon Web Services
- Pat Gaw, Principal Security Consultant, Amazon Web Services

- Jason Garman, Principal Security Solutions Architect, Amazon Web Services
- Mark Keating, Principal Security Solutions Architect, Amazon Web Services
- Zach Miller, Principal Security Solutions Architect, Amazon Web Services
- Maitreya Ranganath, Principal Security Solutions Architect, Amazon Web Services
- Reef Dsouza, Principal Solutions Architect, Amazon Web Services
- Brad Burnett, Security Solutions Architect, Amazon Web Services
- Matt Saner, Senior Manager, Security Solutions Architecture, Amazon Web Services
- Priyank Ghedia, Senior Security Solutions Architect, Amazon Web Services
- Arthur Mnev, Senior Security Solutions Architect, Amazon Web Services
- Kyle Dickinson, Senior Security Solutions Architect, Amazon Web Services
- Kevin Boland, Senior Security Solutions Architect, Amazon Web Services
- Anna McAbee, Senior Security Solutions Architect, Amazon Web Services
- Recep Meric Degirmenci, Senior Security Solutions Architect, Amazon Web Services
- Daniel Salzedo, Senior Security Technical Product Manager, Amazon Web Services
- Jake Izumi, Senior Solutions Architect, Amazon Web Services
- Bert Bullough, Senior Solutions Architect, Amazon Web Services
- Robert McCall, Solutions Architect, Amazon Web Services
- Angela Chao, ESL TAM, AWS Enterprise Support, Amazon Web Services
- Pratima Singh, Senior ANZ Security Spec. Solutions Architect, Amazon Web Services
- Darran Boyd, jefe de la Oficina de CISO, AWS Security, Amazon Web Services
- Kevin Boland, arquitecto sénior de soluciones de seguridad, Amazon Web Services

Documentación adicional

Para obtener más ayuda, consulte estas fuentes:

- Documento técnico Marco de AWS Well-Architected
- Centro de arquitectura de AWS

Revisiones del documento

Para recibir notificaciones sobre las actualizaciones de este documento técnico, suscríbase a la fuente RSS.

Cambio	Descripción	Fecha
Actualización de las directrices de prácticas recomendadas	Las prácticas recomendadas se han actualizado con nuevas guías en las siguientes áreas: SEC 2, SEC 3, SEC 4, SEC 6, SEC 7, SEC 8, SEC 9, SEC 10 y SEC 11. La guía se ha actualizado y perfeccionado en todo el pilar.	6 de noviembre de 2024
Actualización de las directrices de prácticas recomendadas	Se han aplicado actualizaciones a gran escala de las prácticas recomendadas en todo el pilar. Se reordenaron y consolidaron varias prácticas recomendadas. Cambios significativos en SEC 1, 4, 5, 6, 7, 8 y 9.	27 de junio de 2024
Actualización de las directrices de prácticas recomendadas	Se actualizaron las prácticas recomendadas con nuevas directrices en las siguientes áreas: Funcionamiento seguro de las cargas de trabajo y Protección de los datos en tránsito.	6 de diciembre de 2023
Actualización de las directrices de prácticas recomendadas	Actualizaciones importantes de las guías y prácticas recomendadas para la	3 de octubre de 2023

	Respuesta frente a incidencias.	
	Se actualizaron numerosas prácticas recomendadas en Preparación. Se agregaron dos áreas nuevas a Respuesta frente a incidencias: Operaciones y Actividad posterior a las incidencias. Se agregó una práctica recomendada nueva a SEC10-BP08 Establecimiento de un marco de trabajo para aprender de los incidentes.	
Actualización de las directrices de prácticas recomendadas	Se actualizaron las prácticas recomendadas con nuevas guías en las siguientes áreas: Preparación y Simulación.	13 de julio de 2023
Actualizaciones del nuevo marco.	Se actualizaron las prácticas recomendadas con una guía prescriptiva y se agregaron nuevas prácticas recomendadas. Se agregó una nueva área de prácticas recomendadas de Seguridad de las aplicaciones (AppSec).	10 de abril de 2023
Documento técnico actualizado	Se actualizaron las prácticas recomendadas con una nueva guía de implementación.	15 de diciembre de 2022
Documento técnico actualizado	Se ampliaron las prácticas recomendadas y se agregaron planes de mejora.	20 de octubre de 2022

Actualización menor	Se actualizó la información de IAM para reflejar las prácticas recomendadas actuales.	28 de junio de 2022
Actualización menor	Se agregó información adicional de AWS PrivateLink y se corrigieron los enlaces que no funcionan.	19 de mayo de 2022
Actualización menor	AWS PrivateLink añadido.	6 de mayo de 2022
Actualización menor	Se eliminó el lenguaje no inclusivo.	22 de abril de 2022
Actualización menor	Se agregó información sobre el Analizador de acceso a la red de VPC.	2 de febrero de 2022
Actualización menor	Corrección del enlace que no funciona.	27 de mayo de 2021
Actualización menor	Se hicieron cambios editoriales en todo el documento.	17 de mayo de 2021
Actualización importante	Se agregó la sección de gobernanza, se detallaron varias secciones y se agregaron nuevas características y servicios en todo el documento.	7 de mayo de 2021
Actualización menor	Se actualizaron los enlaces.	10 de marzo de 2021
Actualización menor	Corrección del enlace que no funciona.	15 de julio de 2020
Actualizaciones del nuevo marco	Se actualizó la guía sobre la administración de permisos, identidades y cuentas.	8 de julio de 2020

Actualizaciones del nuevo marco	Se actualizó el documento para ampliar el asesoramiento en cada área y para agregar nuevas prácticas recomendadas, servicios y características.	30 de abril de 2020
Documento técnico actualizado	Actualizaciones para reflejar los nuevos servicios y características de AWS y poner al día las referencias.	1 de julio de 2018
Documento técnico actualizado	Se actualizó la sección Configuración y mantenimiento de seguridad del sistema para reflejar los nuevos servicios y características de AWS.	1 de mayo de 2017
Publicación inicial	Se publicó el Pilar de seguridad: Marco de AWS Well-Architected.	1 de noviembre de 2016

Avisos

Es responsabilidad de los clientes realizar su propia evaluación independiente de la información que contiene este documento. El presente documento: (a) tiene sólo fines informativos, (b) representa las ofertas y prácticas actuales de los productos de AWS, que están sujetas a cambios sin previo aviso, y (c) no supone ningún compromiso ni garantía por parte de AWS y sus filiales, proveedores o licenciantes. Los productos o servicios de AWS se proporcionan “tal cual”, sin garantías, afirmaciones ni condiciones de ningún tipo, ya sean expresas o implícitas. Las responsabilidades y obligaciones de AWS con respecto a sus clientes se controlan mediante los acuerdos de AWS y este documento no forma parte ni modifica ningún acuerdo entre AWS y sus clientes.

© 2023 Amazon Web Services, Inc. o sus filiales. Todos los derechos reservados.

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el Glosario de AWS en la Referencia de Glosario de AWS.