AWS Well-Architected Framework

Pilar de seguridad

Pilar de seguridad: AWS Well-Architected Framework

Table of Contents

Pilar de seguridad: AWS Well-Architected Framework

Fecha de publicación: 6 de diciembre de 2023 (Revisiones del documento)

Este documento se centra en el pilar de seguridad de AWS Well-Architected Framework. 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 AWS Well-Architected Framework le ayuda a comprender las compensaciones derivadas de las decisiones tomadas 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 en la nube fiables, eficaces, rentables y sostenibles. 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 buena arquitectura aumenta en gran medida la probabilidad de éxito empresarial.

El marco se basa en seis pilares:

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

El presente documento se centra en el pilar de seguridad. El mismo 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/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. Este documento no proporciona detalles de implementación ni patrones de arquitectura,

pero 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

El pilar de seguridad describe cómo sacar partido de las tecnologías de nube para proteger datos, sistemas y recursos de una forma que pueda mejorar su nivel 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:

- Implemente una base de identidad sólida: aplique el principio del privilegio mínimo y haga cumplir la separación de funciones con la autorización adecuada para cada interacción con sus recursos de AWS. Centralice la administración de identidades y busque eliminar la dependencia de las credenciales a largo plazo.
- Mantenga la trazabilidad: Monitoree, cree alertas y audite acciones y cambios en su entorno en tiempo real. Integre la recopilación de registros y métricas con sistemas para investigar y tomar medidas automáticamente.
- Implemente la seguridad en todos los niveles: aplique un enfoque de defensa exhaustivo con varios controles de seguridad. Impleméntelo en todas las capas (por ejemplo, red periférica, VPC, balanceo de carga, cada instancia y servicio de computación, sistema operativo, aplicación y código).
- Automatice las prácticas recomendadas de seguridad: los mecanismos de seguridad automatizados basados en software mejoran la capacidad de escalar de forma segura de una manera mas rápida y rentable. Cree arquitecturas seguras, como la implementación de controles definidos y administrados como código en plantillas controladas por versión.
- Cifre datos en tránsito y en reposo: clasifique sus datos en niveles de confidencialidad y utilice mecanismos como el cifrado, la tokenización y el control de acceso cuando corresponda.
- Mantenga a las personas alejadas de los datos: use mecanismos y herramientas para reducir o eliminar la necesidad de acceso directo o de procesamiento manual de datos. De esta forma, se reducen los errores humanos y el riesgo de una mala gestión o modificación al gestionar información confidencial.
- Prepárese para eventos de seguridad: prepárese para un incidente teniendo 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
- Administración de identidad y acceso
- Detección
- Protección de la infraestructura
- Protección de los datos
- Respuesta ante incidentes
- Seguridad de las aplicaciones

Modelo de responsabilidad compartida

La seguridad y la conformidad constituyen 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 el despliegue. 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: «Seguridad de la nube» – AWS es responsable de proteger la infraestructura en la que se ejecutan todos los servicios que se ofrecen en la nube de AWS. Esta infraestructura está compuesta por hardware, software, redes e instalaciones que ejecutan servicios en la nube de AWS.

Responsabilidad del cliente: «Seguridad en la nube» – La responsabilidad del cliente variará en función de los servicios en la nube de AWS que seleccione. Esto determina la cantidad de trabajo de configuración que el cliente debe realizar 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 realice todas las tareas necesarias de administración y configuración de seguridad. Los clientes que despliegan 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.

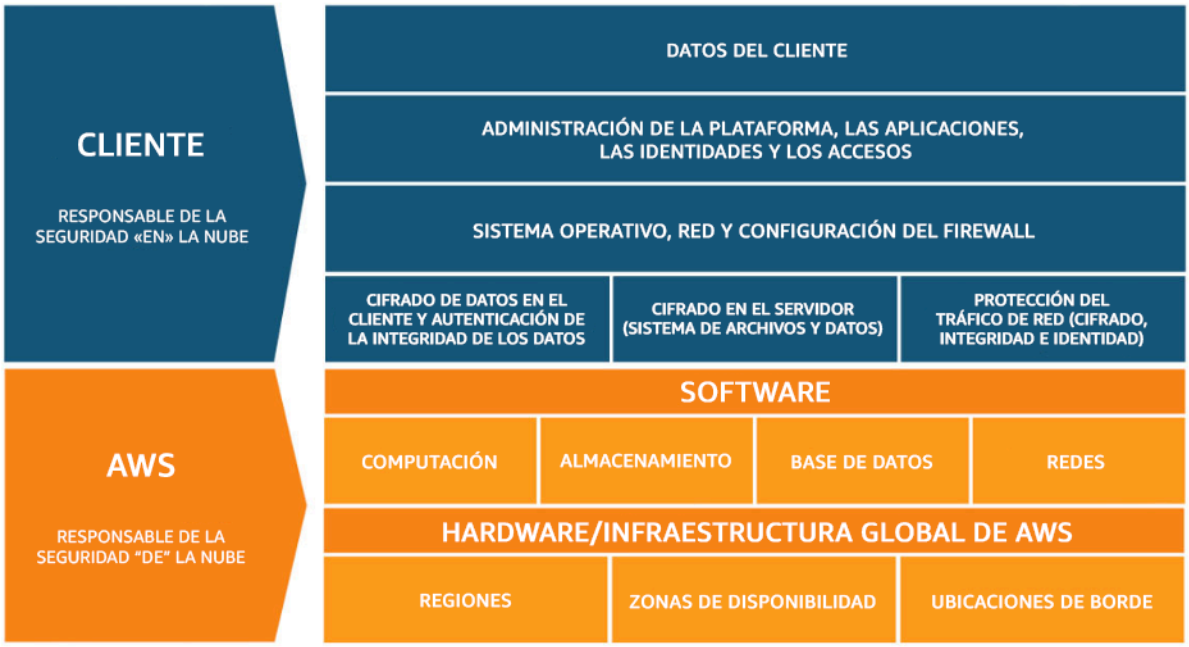


Figura 1: Modelo de responsabilidad compartida de AWS

Este modelo de responsabilidad compartida entre clientes 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, administrando los controles asociados con la infraestructura física desplegada en el entorno de

AWS, de cuya administración se encargaba el cliente anteriormente. Como el despliegue de cada cliente se realiza 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 realizar 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.
- 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 desplegando 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 enrute 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 útil 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 realiza en las aplicaciones que estos equipos controlan. Esto podría realizarse mediante la implementación de la validación de entrada en una aplicación o garantizando 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 costes financieros, relacionados con la reputación y con el tiempo invertido del evento.

Probabilidad	Nivel de riesgo				
Muy probable	Bajo	Medio	Alto	Crítico	Crítico
Probable	Bajo	Medio	Medio	Alto	Crítico
Posible	Bajo	Bajo	Medio	Medio	Alto
Poco probable	Bajo	Bajo	Medio	Medio	Alto
Muy improbable	Bajo	Bajo		Medio	Alto
Consecuencia	Mínimo	Bajo	Mediana	Alto	Grave

Figura 2: Matriz de probabilidad de nivel de riesgo

Separación y administración de cuentas de AWS

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 de cuentas de forma centralizada: AWS Organizations automatiza la administración y creación de cuentas de AWSy las controla una vez que se han creado. 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 distintos entornos en función de los requisitos y el objetivo de la carga de trabajo.

Definición de controles de forma centralizada: controle lo que pueden hacer las cuentas de AWS permitiendo 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 usted no haya permitido explícitamente. AWS Control Tower ofrece una forma simplificada de configurar y controlar varias cuentas. Automatiza la configuración de cuentas en AWS Organization, automatiza el aprovisionamiento, aplica barreras de protección (entre las que se incluyen la prevención y la detección) y le ofrece un panel para obtener visibilidad.

Configuración de servicios y recursos de forma centralizada: AWS Organizations le ayuda a configurar servicios de AWS que se aplican a todas las cuentas. Por ejemplo, puede configurar el registro central de todas las acciones realizadas en la organización con AWS CloudTrail, e impedir que las cuentas de los miembros desactiven el registro. También puede agregar de forma centralizada datos para reglas que haya definido con AWS Config, lo que le permite realizar una auditoría de las cargas de trabajo para comprobar si cumplen los requisitos y reaccionar rápidamente a 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, tales 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 Separar cargas de trabajo utilizando cuentas
- SEC01-BP02 Proteger el usuario raíz y las propiedades de la cuenta

SEC01-BP01 Separar cargas de trabajo utilizando 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 realice a nivel de 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 aísle las operaciones en la nube, las cargas de trabajo no relacionadas y los entornos en cuentas separadas para aumentar la seguridad en toda la infraestructura en la nube.

Antipatrones usuales:

- Colocar en la misma cuenta varias cargas de trabajo no relacionadas con diferentes niveles de confidencialidad de los datos.
- Estructura de la unidad organizativa (OU) mal definida.

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 sus 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 (Organización del entorno de AWS utilizando varias cuentas).

Cuando tenga varias Cuentas de AWS con una administración central, sus 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 de los servicios que puede utilizar para implementar y administrar esta estructura de varias cuentas en su entorno de AWS. AWS Organizations le permite organizar las cuentas en una jerarquía definida por una o varias capas de OU, en la que cada OU contiene una serie de cuentas miembro. Las políticas de control de servicios (SCP) permiten al administrador de la organización establecer controles preventivos detallados en las cuentas miembros y AWS Config puede utilizarse para establecer controles proactivos y de detección en las cuentas miembro. Muchos servicios de AWS se integran con AWS Organizations para proporcionar controles administrativos delegados y realizar tareas específicas del servicio en todas las cuentas miembros de la organización.

Por encima de AWS Organizations, AWS Control Tower proporciona una configuración recomendada de 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 tiene varias ventajas con respecto a AWS Organizations. Estas son tres ventajas que mejoran la gobernanza de las cuentas:

- Barreras de protección de seguridad obligatorias integradas que se aplican automáticamente a las cuentas que se admiten en la organización.
- Barreras de protección opcionales que pueden activarse o desactivarse para un conjunto determinado de OU.
- AWS Control Tower Account Factory proporciona un despliegue automatizado de cuentas que contienen bases de referencia y opciones de configuración preaprobadas dentro de su organización.

Pasos para la implementación

1. Diseñe una estructura de unidades organizativas: si la estructura de unidades organizativas está diseñada correctamente, se reduce la carga administrativa necesaria para crear y mantener las políticas de control de los servicios y otros controles de seguridad. La estructura de su unidad organizativa debe ajustarse a sus necesidades empresariales, la confidencialidad de los datos y la estructura de la carga de trabajo.
2. Cree una zona de aterrizaje para su entorno de varias cuentas: una zona de aterrizaje proporciona una base de seguridad e infraestructura uniforme desde la que su organización puede desarrollar, iniciar y desplegar cargas de trabajo rápidamente. Puede utilizar una zona de aterrizaje personalizada o AWS Control Tower para organizar su entorno.

3. Establezca barreras de protección: implemente barreras de protección de seguridad uniformes para su entorno en toda su zona de aterrizaje. AWS Control Tower proporciona una lista de controles obligatorios y opcionales que pueden desplegarse. Los controles obligatorios se despliegan 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. Restrinja el acceso a las regiones añadidas recientemente: para las nuevas Regiones de AWS, los recursos de IAM, como los usuarios y los roles, solo se propagan a las regiones que especifique. Esta acción puede realizarse a través de la consola cuando se utiliza Control Tower o ajustando las políticas de permisos de IAM en AWS Organizations.
5. Considere la posibilidad de usar AWS CloudFormation StackSets: StackSets le ayuda a desplegar recursos como 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 Recurrir a un proveedor de identidades centralizado

Documentos relacionados:

- AWS Control Tower
- AWS Security Audit Guidelines (Directivas de auditoría de seguridad de AWS)
- Prácticas recomendadas de seguridad en IAM
- Use CloudFormation StackSets to provision resources across multiple Cuentas de AWS and regions (Utilice CloudFormation StackSets para aprovisionar recursos en varias cuentas y regiones de AWS)
- Preguntas frecuentes de AWS Organizations
- Terminología y conceptos de AWS Organizations
- Best Practices for AWS Organizations Service Control Policies in a Multi-Account Environment (Prácticas recomendadas para las políticas de control de servicios de AWS Organizations en un entorno de varias cuentas)
- AWS Account Management Reference Guide (Guía de referencia para la administración de cuentas de AWS)
- Organización de su entorno de AWS mediante varias cuentas

Vídeos relacionados:

- Enable AWS adoption at scale with automation and governance (Facilitar la adopción de AWS a escala con la automatización y la gobernanza)
- Security Best Practices the Well-Architected Way (Prácticas recomendadas de seguridad al estilo de Well-Architected)
- Building and Governing Multiple Accounts using AWS Control Tower (Creación y administración de varias cuentas mediante Control Tower)
- Enable Control Tower for Existing Organizations (Habilitar Control Tower para las organizaciones existentes)

Talleres relacionados:

- Control Tower Immersion Day (Día de inmersión en Control Tower)

SEC01-BP02 Proteger el 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 uso indebido de las credenciales de usuario raíz. Establecer controles de detección también puede servir para alertar al personal adecuado cuando se realizan acciones con el usuario raíz.

Antipatrones usuales:

- Utilizar el usuario raíz para realizar 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 genera confianza, ya que las acciones en su 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 habilitadas de forma predeterminada, deberá implementarlas directamente. Considere estas recomendaciones como pasos básicos para proteger su 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 se denomina usuario raíz de la Cuenta de AWS. Puede iniciar sesión como usuario raíz con la dirección de correo electrónico y la contraseña que se ha usado para crear la cuenta. Dado el elevado nivel de acceso que se concede al usuario raíz de AWS, debe limitar el uso de este usuario de AWS a la realización de tareas que lo requieran específicamente. Las credenciales de inicio de sesión del usuario raíz deben estar muy bien protegidas y siempre se debe habilitar la autenticación multifactor (MFA) para el usuario raíz de la Cuenta de AWS.

Además del flujo de autenticación normal para iniciar sesión con su 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 su 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 añadir varias capas de cuentas miembro por debajo de esa cuenta de administración. Dé prioridad a 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 su cuenta de administración puede ser diferente a la de los usuarios raíz de sus cuentas miembro, y puede colocar controles de seguridad preventivos en los usuarios raíz de sus cuentas miembro.

Pasos para la implementación

Se recomienda realizar los siguientes pasos de implementación para establecer controles para el usuario raíz. Cuando sea oportuno, las recomendaciones hacen referencia a la referencia de CIS AWS Foundations versión 1.4.0. Además de estos pasos, consulte las prácticas recomendadas de AWS para proteger sus recursos y su Cuenta de AWS.

Controles preventivos

1. Establezca 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 para el usuario raíz, debe hacer que los procesos que utilizan dichas claves pasen a 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 está expuesto a usted. Considere la posibilidad de utilizar el flujo de restablecimiento de las contraseñas desde su cuenta de administración de AWS Organization para obtener acceso a la cuenta 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. Habilite MFA para el usuario raíz.

4. Habilite controles preventivos para usuarios raíz de cuentas miembro en entornos de varias cuentas de AWS.
   a. Considere la posibilidad de habilitar la barrera de protección preventiva No permitir la creación de claves de acceso para el usuario raíz para las cuentas miembros.
   b. Considere la posibilidad de habilitar la barrera de protección preventiva No permitir acciones como usuario raíz para las cuentas miembros.
5. Si necesita credenciales para el usuario raíz:
   a. Utilice una contraseña compleja.
   b. Habilite 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 con regularidad. (CIS 1.6)
      - Para configurar MFA para el usuario raíz, siga las instrucciones para habilitar un dispositivo MFA virtual o un dispositivo MFA físico.
   d. Considere la posibilidad de inscribir varios dispositivos MFA de reserva. Se permiten hasta 8 dispositivos MFA por cuenta.
      - Tenga en cuenta que, si inscribe más de un dispositivo MFA para el usuario raíz, se desactiva automáticamente el flujo para recuperar su cuenta si el dispositivo MFA se pierde.
   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.
   - Cambiar la contraseña del usuario raíz de forma periódica reduce el riesgo de que se utilice de forma indebida si se ha expuesto de forma inadvertida.

Controles de detección

- Cree alarmas para detectar el uso de las credenciales del usuario raíz (CIS 1.7). Si se habilita Amazon GuardDuty, este supervisará el uso de credenciales de API del usuario raíz y alertará de ese uso mediante el hallazgo de RootCredentialUsage.
- Evalúe e implemente los controles de detección que se incluyen 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 que hay 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 un único individuo, 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 realizar las tareas de AWS que requieran dicho usuario. Todas las demás acciones deben realizarlas otros usuarios que asuman los roles apropiados.
- Compruebe periódicamente que el acceso al usuario raíz funciona para poder 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 figuran en los contactos alternativos funcionan. 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 funcionan.
- Prepare procedimientos de respuesta a incidentes para responder al uso indebido de la cuenta raíz. Consulte la AWS Security Incident Response Guide (Guía de respuesta a incidentes de seguridad de AWS) y las prácticas recomendadas de la sección Incident Response (Respuesta a incidentes) del documento técnico sobre los pilares de seguridad para obtener más información sobre la creación de una estrategia de respuesta a incidentes para su Cuenta de AWS.

Recursos

Prácticas recomendadas relacionadas:

- SEC01-BP01 Separar cargas de trabajo utilizando cuentas
- SEC02-BP01 Usar mecanismos de inicio de sesión sólidos
- SEC03-BP02 Conceder acceso con privilegios mínimos
- SEC03-BP03 Establecer un proceso de acceso de emergencia
- SEC10-BP05: Aprovisionamiento previo del acceso

Documentos relacionados:

- AWS Control Tower
- AWS Security Audit Guidelines (Directivas de auditoría de seguridad de AWS)
- Prácticas recomendadas de seguridad en IAM
- Amazon GuardDuty: alerta sobre el uso de credenciales raíz
- Step-by-step guidance on monitoring for root credential use through CloudTrail (Guía paso a paso para supervisar el uso de credenciales raíz a través de Control Tower)
- MFA tokens approved for use with AWS (Tokens MFA aprobados para su uso con AWS)
- Implementación del acceso con rotura de cristales en AWS
- Top 10 security items to improve in your Cuenta de AWS (Los 10 elementos de seguridad que debe mejorar en su cuenta de AWS)
- What do I do if I notice unauthorized activity in my Cuenta de AWS? (¿Qué hago si observo actividad no autorizada en mi cuenta de AWS?

Vídeos relacionados:

- Enable AWS adoption at scale with automation and governance (Facilitar la adopción de AWS a escala con la automatización y la gobernanza)
- Security Best Practices the Well-Architected Way (Prácticas recomendadas de seguridad al estilo de Well-Architected)
- Limitación del uso de credenciales raíz de AWS de AWS re:inforce 2022 – Security best practices with AWS IAM (AWS re:inforce 2022: prácticas recomendadas de seguridad con AWS IAM)

Ejemplos relacionados y laboratorios:

- Laboratorio: Cuenta de AWS and root user (La cuenta de AWS y el usuario raíz)

Funcionamiento seguro de las cargas de trabajo

El funcionamiento seguro de las cargas de trabajo abarca todo el ciclo de vida de las mismas: 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 adoptando 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 el despliegue de cargas de trabajo y ayuda a subir el nivel de la capacidad de seguridad de la organización.

Para utilizar la carga de trabajo de forma segura, debe adoptar prácticas recomendadas globales en cada área de seguridad. Tome los requisitos y los procesos que ha definido en la excelencia operativa a nivel de organización y de carga de trabajo, y aplíquelos a todas las áreas. Mantenerse actualizado con AWS, las prácticas recomendadas del sector y la inteligencia de amenazas le ayudan a desarrollar el modelo de amenaza 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. Las gente hacen bien muchas cosas, pero hacer lo mismo de forma coherente y en repetidas ocasiones sin cometer errores no es una de ellas. Incluso con runbooks bien redactados, se corre el riesgo de que la gente no lleve acabo 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 desplegar aplicaciones es a través de la automatización. El código que ejecuta el despliegue puede probarse y utilizarse para realizar dicho proceso. 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 desplegada en un entorno de prueba y entrenamiento. De esta forma, podrá probar la automatización para demostrar que realizó correctamente todos los pasos. También puede obtener retroalimentación temprana en el ciclo de desarrollo y despliegue, lo que reduce la posibilidad de tener que volver a repetir los procesos. Para reducir la posibilidad de se produzcan

errores de despliegue, realice cambios en la configuración por código y no por persona. Si tiene que volver a desplegar una aplicación, la automatización le facilitará esta tarea. A medida que va definiendo objetivos de control adicionales, podrá ir añadiéndolos 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 Identificar y validar objetivos de control
- SEC01-BP04 Mantenerse al día de las amenazas de seguridad
- SEC01-BP05 Mantenerse al día con las recomendaciones de seguridad
- SEC01-BP06 Automatizar la comprobación y validación de controles de seguridad en canalizaciones
- SEC01-BP07 Identificar amenazas y priorizar mitigaciones con un modelo de amenazas
- SEC01-BP08 Evaluar e implementar nuevos servicios y características de seguridad de forma periódica

SEC01-BP03 Identificar y validar objetivos de control

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

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

Guía para la implementación

- Identificar los requisitos de cumplimiento: descubra los requisitos organizativos, legales y de conformidad que debe cumplir la carga de trabajo.
- Identificar los recursos de cumplimiento de AWS: identifique los recursos que AWS tiene disponibles para ayudarle en términos de cumplimiento.
  - https://aws.amazon.com/compliance/
  - https://aws.amazon.com/artifact/

Recursos

Documentos relacionados:

- Directrices de auditoría de seguridad de AWS
- Boletines de seguridad

Vídeos relacionados:

- AWS Security Hub: gestionar las alertas de seguridad y automatizar el cumplimiento
- Prácticas recomendadas de seguridad a la forma Well-Architected

SEC01-BP04 Mantenerse al día de las amenazas de seguridad

Para ayudarle a definir e implementar los controles adecuados, reconozca los vectores de ataque manteniéndose al día de las últimas amenazas de seguridad. Use AWS Managed Services para facilitar la recepción de notificaciones de comportamientos inesperados o inusuales en sus cuentas de AWS. Investigue mediante herramientas de socios de AWS o orígenes de información sobre amenazas de terceros como parte de su flujo de información de seguridad. La lista de vulnerabilidades y exposiciones comunes (CVE) contiene vulnerabilidades de ciberseguridad divulgadas públicamente que puede utilizar para estar al día.

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

Guía para la implementación

- Suscríbase a orígenes de inteligencia sobre amenazas: consulte periódicamente información de inteligencia de distintos orígenes que sean relevantes para las tecnologías que se usan en su carga de trabajo.
  - Lista de vulnerabilidades y exposiciones comunes (CVE)
- Considere AWS Shield Advanced : proporciona visibilidad casi en tiempo real sobre los orígenes de inteligencia si se puede acceder a su carga de trabajo desde Internet.

Recursos

Documentos relacionados:

- AWS Security Audit Guidelines (Directrices de auditoría de seguridad de AWS)
- AWS Shield
- Boletines de seguridad

Vídeos relacionados:

- Security Best Practices the Well-Architected Way (Prácticas recomendadas de seguridad a la forma Well-Architected)

SEC01-BP05 Mantenerse al día con las recomendaciones de seguridad

Manténgase al día de las recomendaciones de seguridad de AWS y de todo el sector para hacer evolucionar la postura de seguridad de su carga de trabajo. Los boletines de seguridad de AWS contienen información importante sobre la seguridad y las notificaciones de privacidad.

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

Guía para la implementación

- Siga las actualizaciones de AWS: suscríbase o compruebe regularmente las nuevas recomendaciones, consejos y trucos.
  - Laboratorios de AWS Well-Architected
  - Blog de seguridad de AWS

  - Documentación de servicio de AWS
- Suscríbase a las noticias del sector: consulte habitualmente noticias de distintas fuentes que sean relevantes para las tecnologías que se utilicen en su carga de trabajo.
  - Ejemplo: lista de vulnerabilidades y exposiciones comunes

Recursos

Documentos relacionados:

- Boletines de seguridad

Videos relacionados:

- Prácticas recomendadas de seguridad a la forma Well-Architected

SEC01-BP06 Automatizar la comprobación y validación de controles de seguridad en canalizaciones

Establezca referencias y plantillas seguras para mecanismos de seguridad que se comprueben y validen como parte de sus compilaciones, canalizaciones y procesos. Utilice herramientas y automatización para probar y validar todos los controles de seguridad de forma continua. Por ejemplo, escanee elementos como imágenes de máquinas y plantillas de infraestructura como código en busca de vulnerabilidades de seguridad, irregularidades y divergencias respecto de una referencia establecida en cada etapa. AWS CloudFormation Guard puede ayudarle a verificar que las plantillas de CloudFormation sean seguras, ahorrarle tiempo y reducir el riesgo de errores de configuración.

Reducir el número de configuraciones incorrectas de seguridad introducidas en un entorno de producción es fundamental. De este modo, establecer un control de calidad más exhaustivo y reducir los defectos durante el proceso de compilación facilitará obtener mejores resultados. Cuando sea posible, diseñe canalizaciones de integración e implementación continuas (CI/CD) para probar si hay problemas de seguridad. Las canalizaciones de CI/CD ofrecen la oportunidad de mejorar la seguridad en cada etapa de la compilación y la entrega. Las herramientas de seguridad de CI/CD también deben mantenerse actualizadas para mitigar las amenazas en evolución.

Realice un seguimiento de los cambios en la configuración de su carga de trabajo para ayudar con la auditoría normativa, la gestión de cambios y las investigaciones que puedan afectarle. Puede utilizar

AWS Config para registrar y evaluar sus recursos de AWS y de terceros. Le permite evaluar y auditar de forma continua el cumplimiento general de las reglas y los paquetes de conformidad, que son conjuntos de reglas con acciones de corrección.

Entre las medidas de seguimiento de los cambios deberían incluirse cambios planificados que formen parte del proceso de control de cambios de la organización (lo que a veces se denomina "MACD": "mover", "agregar", "cambiar" y "eliminar", por sus siglas en inglés), cambios ad hoc o cambios inesperados, como incidentes. Los cambios pueden producirse en la infraestructura, pero también pueden estar relacionados con otras categorías, como los cambios en los repositorios de código, en los inventarios de aplicaciones e imágenes de máquinas, en los procesos y políticas o en la documentación.

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

Guía para la implementación

- Automatice la administración de la configuración: aplique y valide configuraciones seguras de forma automática mediante el uso de un servicio o herramienta de administración de la configuración.
  - AWS Systems Manager
  - AWS CloudFormation
  - Configurar una canalización de CI/CD en AWS

Recursos

Documentos relacionados:

- Cómo utilizar las políticas de control de servicios para establecer barreras de protección de permisos entre cuentas de AWS Organizations

Videos relacionados:

- Administración de entornos de AWS con varias cuentas utilizando AWS Organizations
- Prácticas recomendadas de seguridad a la forma Well-Architected

SEC01-BP07 Identificar amenazas y priorizar 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 su carga de trabajo. Priorice sus amenazas y adapte sus mitigaciones de controles de seguridad para evitarlas, detectarlas y responder a ellas. Revise y mantenga todo esto en el contexto de su 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 mitigaciones dentro del contexto de la protección de algo de valor» – «Application Threat Modeling» de Open Web Application Security Project (OWASP)

¿Por qué debe modelar las 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 coste y un esfuerzo relativamente bajos en comparación con las fases posteriores del ciclo de vida. Este enfoque se ajusta al principio de seguridad shift-left (desplazamiento a la izquierda) del sector. 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 debe realizarse el modelado de amenazas?

Empiece a modelar las amenazas lo antes posible en el ciclo de vida de su 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 sus cargas de trabajo. Revise 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 función o servicio.

Pasos para la implementación

¿Cómo podemos realizar el modelado de amenazas?

Hay muchas formas diferentes de realizar 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 es comenzar con Shostack's 4 Question Frame for Threat Modeling (Marco de 4 preguntas para el modelado de amenazas de Shostack), que plantea preguntas abiertas para proporcionar una estructura a su modelado de amenazas:

1. ¿En qué está trabajando?

   La finalidad de esta pregunta es ayudarle a comprender y acordar el sistema que está construyendo y los detalles de ese sistema que son relevantes para la seguridad. Lo más habitual es responder que se está creando un modelo o diagrama, ya esto ayuda a visualizar lo que está construyendo, por ejemplo, con un diagrama de flujo de datos. Anotar las suposiciones y los detalles importantes sobre su 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 de su 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 usted identifica las amenazas que afectan a su sistema. Las amenazas son acciones o acontecimientos accidentales o intencionados que tienen repercusiones no deseadas y podrían afectar a la seguridad de su 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. Para crear esta lista, todos los miembros de su equipo y las personas relevantes implicadas en el modelado de amenazas deben hacer una lluvia de ideas y colaborar. Para facilitar la lluvia de ideas, puede utilizar un modelo de identificación de amenazas, como STRIDE, que sugiere diferentes categorías para evaluar las siguientes amenazas: suplantación de identidad, manipulación, repudio, divulgación de información, denegación de servicio y elevación de privilegios. Además, puede facilitar la lluvia de ideas inspirándose en listas e investigaciones existentes, como OWASP Top 10 (Los 10 principales riesgos de seguridad de OWASP), HiTrust Threat Catalog (Catálogo de amenazas de HiTrust) y el propio catálogo de amenazas 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.

   La seguridad y la conformidad constituyen una responsabilidad compartida entre usted 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 usted y AWS le ayuda a delimitar su 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 lo que se refiere a la parte de AWS de esa responsabilidad compartida, descubrirá que los servicios de AWS están dentro del ámbito de muchos programas de conformidad. Estos programas le ayudan a conocer los sólidos controles que hay en AWS para mantener la seguridad y la conformidad de la nube. Los clientes de AWS pueden descargar informes de auditoría de estos programas desde 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 su 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. En la documentación de cada servicio de AWS, hay un capítulo dedicado a la seguridad que ofrece orientación sobre los controles de seguridad que deben considerarse como mitigaciones. 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 podrían ser cosas como 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. ¿Hemos hecho 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 realizan. Estas mejoras se deben a una combinación de práctica, aprendizaje, enseñanza y revisión. Para profundizar y ponerse manos a la obra, es recomendable que usted y su equipo completen el curso de formación el taller Threat modeling the right way for builders training course (Modelado de amenazas de la forma adecuada para constructores). Además, si busca orientación sobre cómo integrar el modelado de amenazas en el ciclo de vida de desarrollo de aplicaciones de su organización, consulte la publicación How to approach threat modeling (Cómo abordar el modelado de amenazas) en el blog de seguridad de AWS.

Threat Composer

Para ayudarle y guiarle en la creación de modelos de amenazas, considere la posibilidad de utilizar la herramienta Threat Composer, que tiene como objetivo obtener valor más rápido al modelar amenazas. La herramienta le ayuda a hacer lo siguiente:

- Escribir instrucciones de amenazas útiles adaptadas a la gramática de amenazas que funcionan en un flujo de trabajo no lineal natural
- 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 Identificar y validar objetivos de control
- SEC01-BP04 Mantenerse al día de las amenazas de seguridad
- SEC01-BP05 Mantenerse al día con las recomendaciones de seguridad
- SEC01-BP08 Evaluar e implementar nuevos servicios y características de seguridad de forma periódica

Documentos relacionados:

- How to approach threat modeling (Cómo abordar el modelado de amenazas) (Blog de seguridad de AWS)
- NIST: Guide to Data-Centric System Threat Modelling (Guía para el modelado de amenazas de sistemas centrados en datos)

Vídeos relacionados:

- AWS Summit ANZ 2021 - How to approach threat modelling (AWS Summit ANZ 2021 - Cómo abordar el modelado de amenazas)
- AWS Summit ANZ 2022 - Scaling security – Optimise for fast and secure delivery (AWS Summit ANZ 2022 - Escalar la seguridad - Optimizar para una entrega rápida y segura)

Formación relacionada:

- Threat modeling the right way for builders – AWS Skill Builder virtual self-paced training (Modelado de amenazas de la forma correcta para constructores - Formación virtual autodidacta de AWS Skill Builder)
- Threat modeling the right way for builders – AWS Workshop (Modelado de amenazas de la forma correcta para constructores - Taller)

Herramientas relacionadas:

- Threat Composer

SEC01-BP08 Evaluar e implementar 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 permitan desarrollar la postura de seguridad de su carga de trabajo. En el blog de seguridad de AWS se destacan nuevos servicios y características de AWS, guías de implementación y directrices de seguridad generales. Novedades de AWS es una forma ideal de estar al día de las nuevas características, servicios y anuncios de AWS.

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

Guía para la implementación

- Planifique revisiones periódicas: cree un calendario de actividades de revisión que incluya requisitos de cumplimiento, evaluación de nuevas características y servicios de seguridad de AWS y revisión de las noticias del sector.
- Descubra servicios y características de AWS: descubra las características de seguridad disponibles para los servicios que está utilizando y las características nuevas que se vayan lanzando.
  - Blog de seguridad de AWS
  - Boletines de seguridad de AWS
  - Documentación de servicio de AWS
- Defina el proceso de incorporación de servicios de AWS: defina procesos para incorporar nuevos servicios de AWS. Incluya la forma en que evalúa los nuevos servicios de AWS en cuanto a su funcionalidad, así como los requisitos de conformidad de su carga de trabajo.
- Pruebe nuevos servicios y características: pruebe nuevos servicios y características a medida que se publiquen en un entorno que no sea de producción y que replique de forma fidedigna uno de producción.
- Implemente otros mecanismos de defensa: ponga en marcha mecanismos automatizados para defender su carga de trabajo, explore las opciones disponibles.
  - Corrección de recursos de AWS disconformes con Reglas de AWS Config

Recursos

Videos relacionados:

- Prácticas recomendadas de seguridad a la forma Well-Architected

Administración de identidad y acceso

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

Hay dos tipos de identidades que debe administrar cuando tenga que utilizar cargas de trabajo de AWS seguras.

- Identidades humanas: los administradores, desarrolladores, operadores y clientes de sus aplicaciones requieren una identidad para acceder a sus aplicaciones y entornos de AWS. Estos pueden ser miembros de la organización, o usuarios externos con los que colabora, y que interactúan con sus recursos de AWS a través de un navegador web, aplicación de cliente, aplicación para dispositivos móviles o herramientas de línea de comandos interactivas.
- Identidades de máquinas: las aplicaciones de carga de trabajo, herramientas operativas y componentes requieren una identidad para realizar solicitudes a los servicios de AWS, por ejemplo, para leer datos. Entre estas identidades se incluyen máquinas que se ejecutan en el entorno de AWS, como, por ejemplo, instancias de Amazon EC2 o funciones de AWS Lambda. También puede administrar identidades de máquinas para terceros que necesiten acceso. Además, es posible que también tenga máquinas fuera de AWS que necesiten acceso al entorno de AWS.

Prácticas recomendadas

- SEC02-BP03 Almacenar y usar secretos de forma segura
- SEC02-BP04 Recurrir a un proveedor de identidades centralizado
- SEC02-BP05 Auditar y rotar las credenciales periódicamente
- SEC02-BP06 Aprovechar los grupos y atributos de usuarios

SEC02-BP01 Usar mecanismos de inicio de sesión sólidos

Los inicios de sesión (autenticación mediante credenciales de inicio de sesión) pueden ser arriesgados 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: reducir los riesgos que supone el acceso involuntario a las credenciales en AWS utilizando 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 (sucesor de AWS Single Sign-On) y los proveedores de identidad de terceros. Esto significa exigir que se use MFA, aplicar políticas de contraseñas sólidas y detectar comportamientos de inicio de sesión anómalos.

Antipatrones usuales:

- 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 pueden iniciar sesión en AWS. Una práctica recomendada de AWS es confiar en un proveedor de identidades centralizado que utilice la federación (federación directa o mediante 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 utilizar el usuario raíz de la cuenta para configurar el acceso de sus usuarios (y para las tareas que requieran el usuario raíz). Es importante habilitar MFA para el usuario raíz de la cuenta inmediatamente después de abrir su Cuenta de AWS y proteger ese usuario utilizando la guía de prácticas recomendadas de AWS.

Si crea usuarios en AWS IAM Identity Center, asegure el proceso de inicio de sesión en ese servicio. Para las identidades de consumidor, puede utilizar Amazon Cognito user pools y proteger el proceso de inicio de sesión en ese servicio, o utilizar uno de los proveedores de identidades que admiten los Amazon Cognito user pools.

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

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 se deben establecer en la política de la empresa o se debe utilizar un estándar como NIST 800-63.

- Exija el uso de MFA. Es una práctica recomendada de IAM exigir que se utilice MFA para identidades y cargas de trabajo humanas. Si se habilita MFA, habrá una capa adicional de seguridad que requiere 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 propias 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 sobre IAM Identity Center

- IAM Identity Center proporciona una política de contraseñas predefinida cuando se utiliza el directorio predeterminado que establece los requisitos de longitud, complejidad y reutilización de las contraseñas.
- Habilite MFA y configure el ajuste contextual o continuo para MFA cuando la fuente de identidad sea el directorio predeterminado, AWS Managed Microsoft AD o AD Connector.
- Permita que los usuarios registren sus propios dispositivos MFA.

Recomendaciones sobre el directorio de Amazon Cognito user pools:

- Configure los ajustes de seguridad de la contraseña.
- Exija el uso de MFA a los usuarios.
- Utilice la configuración de seguridad avanzada de Amazon Cognito user pools para funciones como la autenticación adaptativa, que puede bloquear 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 alfanuméricos.
- Cree una política de IAM para imponer el inicio de sesión MFA de modo que los usuarios puedan administrar sus propias contraseñas y dispositivos MFA.

Recursos

Prácticas recomendadas relacionadas:

- SEC02-BP03 Almacenar y usar secretos de forma segura
- SEC02-BP04 Recurrir a un proveedor de identidades centralizado
- SEC03-BP08 Compartir recursos de forma segura en su organización

Documentos relacionados:

- Política de contraseñas de AWS IAM Identity Center (sucesor de AWS Single Sign-On)
- Política de contraseñas de 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 en IAM

Vídeos relacionados:

- Managing user permissions at scale with AWS IAM Identity Center (Administración de permisos de usuario a escala con AWS SSO)
- Mastering identity at every layer of the cake (Dominar la identidad en cada capa del pastel)

SEC02-BP02 Usar credenciales temporales

Al realizar cualquier tipo de autenticación, es mejor utilizar credenciales temporales en lugar de credenciales de larga duración para reducir o eliminar riesgos, tales como que las credenciales se divulguen, compartan o roben de forma inadvertida.

Resultado deseado: para reducir el riesgo que implican las credenciales de larga duración, utilice credenciales temporales siempre que sea posible tanto para las identidades humanas como para las de las máquinas. Las credenciales de larga duración entrañan muchos riesgos; por ejemplo, pueden subirse en el código en repositorios públicos de GitHub. Al utilizar credenciales temporales, reducirá enormemente las posibilidades de que las credenciales se vean comprometidas.

Antipatrones usuales:

- Desarrolladores que utilizan claves de acceso de larga duración de IAM users 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 CLI de AWS. Las solicitudes de la API y la CLI a los servicios de AWS deben, en prácticamente todos los casos, firmarse utilizando claves de acceso de AWS. Estas solicitudes pueden firmarse con credenciales temporales o de larga duración. El único caso en que debe utilizar credenciales de larga duración, que también se conocen como claves de acceso de larga duración, es cuando utiliza un usuario de IAM o el usuario raíz de la Cuenta de AWS. Si se federa a AWS o asume un rol de IAM a través de otros métodos, se generan credenciales temporales. Incluso cuando accede a la AWS Management Console utilizando credenciales de inicio de sesión, se generan credenciales temporales para que pueda realizar llamadas a los servicios de AWS. Hay pocas situaciones en las que necesite credenciales de larga duración y casi todas las tareas se pueden realizar utilizando 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 en 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

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

- Debe recurrir a un proveedor de identidades centralizado y exigir a los usuarios humanos que utilicen la federación con un proveedor de identidades para acceder a AWS utilizando credenciales temporales. La federación para sus usuarios puede realizarse con federación directa a cada Cuenta de AWS o mediante AWSIAM Identity Center (sucesor de AWS IAM Identity Center) y el proveedor de identidades de su elección. La federación tiene una serie de ventajas con respecto a los usuarios de IAM, además de eliminar las credenciales de larga duración. Sus 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 sus usuarios.
- Cuando conceda a terceros (por ejemplo, proveedores de software como servicio [SaaS]), acceso a los recursos de su Cuenta de AWS, puede utilizar roles entre cuentas y políticas basadas en recursos.

- Si necesita conceder acceso a sus recursos de AWS a aplicaciones para consumidores o clientes, puede utilizar grupos de identidades de Amazon Cognito o grupos de usuarios de Amazon Cognito user pools para proporcionar credenciales temporales. Los permisos para las credenciales se configuran a través de roles de IAM También puede definir un rol de IAM separado con permisos limitados para los usuarios invitados que no se hayan autenticado.

En el caso de las identidades de máquina, puede que necesite utilizar credenciales de larga duración. En estos casos, debe 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 le permite configurar un rol de ejecución de Lambda para conceder al servicio permisos para realizar acciones de AWS utilizando credenciales temporales. Existen muchos otros modelos similares para que los servicios de AWS concedan credenciales temporales utilizando roles de IAM.
- Para los dispositivos IoT, puede utilizar el proveedor de credenciales de AWS IoT Core para solicitar credenciales temporales.
- Para sistemas locales o sistemas que se ejecutan fuera de AWS que necesitan acceso a los recursos de AWS, puede utilizar Funciones de IAM en cualquier lugar.

Hay escenarios en los que las credenciales temporales no son una opción y puede que necesite utilizar credenciales de larga duración. En estas situaciones, audite y rote las credenciales periódicamente y rote las claves de acceso con regularidad para los casos de uso que requieran credenciales de larga duración. Algunos ejemplos que podrían requerir credenciales de larga duración son los plugins de WordPress y los clientes de AWS de terceros. En situaciones en las que deba utilizar credenciales de larga duración, o para credenciales que no sean claves de acceso de AWS, como inicios de sesión en bases de datos, puede utilizar un servicio diseñado para administrar secretos, como AWS Secrets Manager. Secrets Manager simplifica la administración, la rotación y el almacenamiento seguro de secretos cifrados mediante servicios compatibles. Si desea obtener más información sobre la rotación de las credenciales de larga duración, consulte Rotación de las claves de acceso.

Recursos

Prácticas recomendadas relacionadas:

- SEC02-BP03 Almacenar y usar secretos de forma segura
- SEC02-BP04 Recurrir a un proveedor de identidades centralizado
- SEC03-BP08 Compartir recursos de forma segura en su organización

Documentos relacionados:

- Credenciales de seguridad temporales
- Credenciales de AWS
- Prácticas recomendadas de seguridad en IAM
- Roles de IAM
- IAM Identity Center
- Federación y proveedores de identidades
- Rotación de las claves de acceso
- Soluciones de socios con competencia en seguridad: acceso y control de acceso
- Cuenta de AWS usuario raíz

Vídeos relacionados:

- Managing user permissions at scale with AWSIAM Identity Center (successor to AWS IAM Identity Center) (Administración de permisos de usuario a escala con AWS SSO [sucesor de AWS Single Sign-On])
- Mastering identity at every layer of the cake (Dominar la identidad en cada capa del pastel)

SEC02-BP03 Almacenar y usar secretos de forma segura

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: implementar un mecanismo para administrar de forma segura 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 hay secretos incrustados en el código fuente durante el proceso de desarrollo.
- Reducir la probabilidad de que las credenciales se divulguen de forma inadvertida.

Antipatrones usuales:

- Credenciales no rotativas.
- 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 (es algo parecido a 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 realiza 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 una clave de acceso secreta de AWS, considere la posibilidad de sustituir esa credencial de larga duración por una credencial temporal utilizando roles de IAM.

Es posible que algunos secretos de larga duración no puedan eliminarse ni sustituirse. Estos secretos pueden almacenarse en un servicio como AWS Secrets Manager, donde pueden almacenarse, administrarse y rotarse de forma centralizada y periódica.

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:

Credential type	Description	Suggested strategy
IAM access keys	AWS IAM access and secret keys used to assume IAM roles inside of a workload	Replace: Use Roles de IAM assigned to the compute instances (such as Amazon EC2 or AWS Lambda) instead. For interoperability with third parties that require access to resources in your Cuenta de AWS, ask if they support Acceso entre cuentas de AWS. For mobile apps, consider using temporary credentials through Grupos de identidades de Amazon Cognito (identidades federadas). For workloads running outside of AWS, consider Funciones de IAM

Credential type	Description	Suggested strategy
		en cualquier lugar or Activaciones híbridas de AWS Systems Manager.
SSH keys	Secure Shell private keys used to log into Linux EC2 instances, manually or as part of an automated process	Replace: Use AWS Systems Manager or EC2 Instance Connect to provide programmatic and human access to EC2 instances using IAM roles.
Application and database credentials	Passwords – plain text string	Rotate: Store credentials in AWS Secrets Manager and establish automated rotation if possible.
Amazon RDS and Aurora Admin Database credentials	Passwords – plain text string	Replace: Use the Integración de Secrets Manager con Amazon RDS or Amazon Aurora. In addition, some RDS database types can use IAM roles instead of passwords for some use cases (for more detail, see Autenticación de bases de datos de IAM).
OAuth tokens	Secret tokens – plain text string	Rotate: Store tokens in AWS Secrets Manager and configure automated rotation.
API tokens and keys	Secret tokens – plain text string	Rotate: Store in AWS Secrets Manager and establish automated rotation if possible.

Un antipatrón común es incrustar claves de acceso de IAM dentro del código fuente, los archivos de configuración o las aplicaciones móviles. Cuando se requiera 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 pueden proporcionarse a través de roles de IAM para instancias de EC2, roles de ejecución para funciones Lambda, roles de IAM de Cognito para el acceso de usuarios móviles y políticas de IoT Core para dispositivos IoT. Cuando interactúe con terceros, es preferible que delegue 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 a ese tercero la clave de acceso secreta para ese usuario.

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

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

Pasos para la implementación

1. Identifique rutas de código que contengan credenciales codificadas mediante herramientas automatizadas como Amazon CodeGuru.
   - Utilice Amazon CodeGuru para analizar sus repositorios de código. Una vez finalizada la revisión, filtre `Type=Secrets` en CodeGuru para encontrar las líneas de código problemáticas.
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 su carga de trabajo está fuera de AWS pero requiere credenciales de IAM para acceder a recursos de AWS, considere la posibilidad de usar Funciones de IAM en cualquier lugar o activaciones híbridas de AWSSystems Manager.
3. Para otros secretos de terceros de larga duración que requieran el uso de la estrategia de rotación, integre Secrets Manager en su código para recuperar secretos de terceros en tiempo de ejecución.
   a. La consola CodeGuru puede crear automáticamente un secreto en Secrets Manager utilizando las credenciales descubiertas.
   b. Integre la recuperación de secretos desde Secrets Manager en el código de su aplicación.

    - Las funciones Lambda sin servidor pueden utilizar una extensión de Lambda agnóstica del lenguaje.
    - Para instancias o contenedores EC2, AWS proporciona ejemplos de código del lado del cliente para recuperar secretos de Secrets Manager en varios lenguajes de programación populares.
4. Revise periódicamente su base de código y vuelva a analizarlo para verificar que no se hayan añadido nuevos secretos.
    - Considere la posibilidad de utilizar una herramienta como git-secrets para evitar que se envíen nuevos secretos a su repositorio de código fuente.
5. Supervise la actividad de Secrets Manager en busca de indicios de un uso inesperado, un 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 Usar credenciales temporales
- SEC02-BP05 Auditar y rotar las credenciales periódicamente

Documentos relacionados:

- Introducción a AWS Secrets Manager
- Federación y proveedores de identidades
- Amazon CodeGuru Introduces Secrets Detector (El revisor de Amazon CodeGuru presenta el detector de secretos)
- Cómo AWS Secrets Manager usa 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

Vídeos relacionados:

- Best Practices for Managing, Retrieving, and Rotating Secrets at Scale (Prácticas recomendadas para administrar, recuperar y rotar secretos a escala)
- Find Hard-Coded Secrets Using Amazon CodeGuru Secrets Detector (Encuentre secretos difíciles de descifrar utilizando el detector de secretos de Amazon CodeGuru)
- Securing Secrets for Hybrid Workloads Using AWS Secrets Manager (Asegurar secretos para cargas de trabajo híbridas utilizando AWS Secrets Manager)

Talleres relacionados:

- Almacene, recupere y administre credenciales confidenciales en AWS Secrets Manager
- Activaciones híbridas de AWS Systems Manager

SEC02-BP04 Recurrir a 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 con 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 se utiliza la federación ni el inicio de sesión único. Los usuarios de la plantilla crean cuentas de usuario y credenciales independientes en numerosas 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 con 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 de la 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 con sus sistemas de recursos humanos (RR. HH.), cuando un usuario cambia de rol, estos cambios se sincronizan con el proveedor de identidades y sus 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

Guía para el acceso a AWS de los usuarios de la plantilla

Es posible que los usuarios de la plantilla, como empleados y contratistas de su organización, tengan que acceder a AWS mediante la AWS Management Console o la AWS Command Line Interface (AWS CLI) para desempeñar sus funciones laborales. Para conceder acceso a AWS, puede federar a los usuarios de la 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 de la 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 o Open ID Connect (OIDC) para cada Cuenta de AWS y utilizar atributos de usuario federados para el control de acceso. Para iniciar sesión en el proveedor de identidades, los usuarios de la 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 AWS Management Console para permitir que el usuario haga un inicio de sesión único en la AWS Management Console asumiendo un rol de IAM. Los usuarios también pueden obtener credenciales de API de AWS temporales para usarlas en la AWS

CLI o bien SDK de AWS de AWS STS asumiendo el rol de IAM mediante una aserción SAML del proveedor de identidades.

- Para federar a los usuarios de la plantilla con varias cuentas en su organización de AWS, puede usar AWS IAM Identity Center para administrar de forma centralizada el acceso de los usuarios de la plantilla a las aplicaciones y Cuentas de AWS. Habilite el centro de identidades para su organización y configure el origen de las identidades. IAM Identity Center proporciona un directorio de orígenes de identidades predeterminado que puede usar para administrar sus usuarios y grupos. Como alternativa, puede elegir un origen de identidades externo conectándose a su proveedor de identidades externo con SAML 2.0 y aprovisionando automáticamente usuarios y grupos con SCIM, o conectándose a su directorio de Microsoft AD con AWS Directory Service. Una vez configurado un origen de identidades, puede asignar acceso a Cuentas de AWS a usuarios y grupos definiendo políticas de privilegios mínimos en sus conjuntos de permisos. Los usuarios de la plantilla pueden autenticarse a través de su proveedor de identidades central para iniciar sesión en el portal de acceso de AWS e iniciar sesión única en las aplicaciones en la nube y Cuentas de AWS que se les asignen. Los usuarios pueden configurar la AWS CLI v2 para autenticarse con el centro de identidades y obtener credenciales para ejecutar comandos de AWS CLI. El centro de identidades también permite el acceso mediante el inicio de sesión único a aplicaciones de AWS como Amazon SageMaker Studio y portales de Monitor de AWS IoT SiteWise.

Tras seguir las instrucciones anteriores, los usuarios de la plantilla ya no tendrán que usar grupos y IAM users para las operaciones normales al administrar las cargas de trabajo de 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 su proveedor de identidades centralizado. Debe identificar y eliminar los grupos de IAM, los IAM users y las credenciales de usuario de larga duración (contraseñas y claves de acceso) que ya no sean necesarios en sus cuentas de Cuentas de AWS. Puede buscar credenciales no utilizadas con informes de credenciales de IAM, eliminar los IAM users correspondientes y eliminar los grupos de IAM. Puede aplicar una política de control de servicio (SCP) a su organización, lo que ayuda a evitar la creación de nuevos grupos y IAM users. Al hacerlo, exige que el acceso a AWS tenga lugar a través de identidades federadas.

Guía para los usuarios de sus aplicaciones

Puede administrar las identidades de los usuarios de sus aplicaciones, como una aplicación móvil, mediante Amazon Cognito como su proveedor de identidades centralizado. Amazon Cognito permite la autenticación, la autorización y la administración de usuarios para sus aplicaciones web y móviles. 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 su empresa. Puede integrar su aplicación web o móvil personalizada con Amazon Cognito para añadir 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 con los recursos de desarrollo de frontend y backend.

Pasos para la implementación

Pasos para los usuarios de la plantilla que acceden a AWS

- Federe a los usuarios de la plantilla para AWS mediante un proveedor de identidades centralizado utilizando 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 IAM users 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 con 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 por Well-Architected:

- SEC02-BP06 Aprovechar los grupos y atributos de usuarios
- SEC03-BP02 Conceder acceso con privilegios mínimos
- SEC03-BP06 Administrar el acceso en función del ciclo de vida

Documentos relacionados:

- Identity federation in AWS
- Prácticas recomendadas de seguridad en IAM
- AWS Identity and Access Management Best practices
- 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: IAM Identity Center credential provider

Vídeos 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
- Workshop: Serverless identity

Herramientas relacionadas:

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

SEC02-BP05 Auditar y rotar las credenciales periódicamente

Audite y rote las credenciales periódicamente para limitar el tiempo que pueden utilizarse para acceder a sus recursos. Las credenciales de larga duración entrañan muchos riesgos, y estos riesgos pueden reducirse rotándolas regularmente.

Resultado deseado: implementar la rotación de credenciales para ayudar a reducir los riesgos asociados al uso de credenciales de larga duración. Auditar regularmente y corregir la no conformidad con las políticas de rotación de credenciales.

Antipatrones usuales:

- 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: medio

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 realizar 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. Si pasa de usuarios de AWS Identity and Access Management (IAM) a identidades centralizadas, puede generar un informe de credenciales para auditar a sus usuarios.

También recomendamos que aplique y supervise una configuración de MFA en su proveedor de identidades. Puede configurar Reglas de AWS Config o utilizar los estándares de seguridad de AWS Security Hub para supervisar si los usuarios tienen habilitado MFA. Considere la posibilidad de utilizar Funciones de IAM en cualquier lugar 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 realizar auditorías frecuentes y rotar las claves de acceso.

Pasos para la implementación

- Audite las credenciales periódicamente: 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 a 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 informes de credenciales y AWS Identity and Access Management Access Analyzer para auditar las credenciales y los permisos de IAM. Puede utilizar Amazon CloudWatch para configurar alarmas para llamadas a la API específicas que se

realicen dentro de su entorno de AWS. Amazon GuardDuty también puede alertarle de actividades inesperadas, que podrían indicar que el acceso es demasiado permisivo o que se ha producido un acceso no intencionado a las credenciales de IAM.

- Rote las credenciales periódicamente: cuando no pueda utilizar credenciales temporales, rote las claves de acceso de larga duración de IAM de forma periódica (cada 90 días como máximo). 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 sus recursos. Si desea obtener más información sobre la rotación de las claves de acceso para los usuarios de IAM, consulte Rotación de las claves de acceso.
- Revise los permisos de IAM: para mejorar la seguridad de su Cuenta de AWS, revise y supervise de forma regular cada una de sus políticas de IAM. Verifique que las políticas sigan el principio del privilegio mínimo.
- Considere la posibilidad de automatizar la creación y actualización de 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 el despliegue 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.
- Utilice Funciones de IAM en cualquier lugar para sustituir a los usuarios de IAM en las identidades de máquina: Funciones de IAM en cualquier lugar le permite utilizar roles en áreas en las que tradicionalmente no podía, como los servidores locales. Funciones de IAM en cualquier lugar utiliza un certificado X.509 de confianza para autenticarse en AWS y recibir credenciales temporales. El uso de Funciones de IAM en cualquier lugar evita la necesidad de rotar estas credenciales, ya que las credenciales de larga duración ya no se almacenan en su entorno local. 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 Usar credenciales temporales
- SEC02-BP03 Almacenar y usar secretos de forma segura

Documentos relacionados:

- Introducción a AWS Secrets Manager
- Prácticas recomendadas de seguridad en IAM

- Federación y proveedores de identidades
- Soluciones de socios con competencia en seguridad: acceso y control de acceso
- Credenciales de seguridad temporales
- Obtener informes de credenciales para su Cuenta de AWS

Vídeos relacionados:

- Best Practices for Managing, Retrieving, and Rotating Secrets at Scale (Prácticas recomendadas para administrar, recuperar y rotar secretos a escala)
- Managing user permissions at scale with AWS IAM Identity Center (Administración de permisos de usuario a escala con AWS SSO)
- Mastering identity at every layer of the cake (Dominar la identidad en cada capa del pastel)

Ejemplos relacionados:

- Well-Architected Lab - Automated IAM User Cleanup (Laboratorio de AWS Well-Architected: Limpieza automatizada de usuarios de IAM)
- Well-Architected Lab - Automated Deployment of IAM Groups and Roles (Laboratorio de AWS Well-Architected: Despliegue automatizado de grupos y roles de IAM)

SEC02-BP06 Aprovechar los grupos y atributos de usuarios

A medida que crezca el número de usuarios que administra, tendrá que determinar formas de organizarlos para que pueda administrarlos a escala. Coloque a usuarios con requisitos de seguridad comunes en grupos definidos por su proveedor de identidades, y prepare mecanismos para garantizar que los atributos de usuarios que puedan usarse para controlar el acceso (por ejemplo, los de departamento o ubicación) sean correctos y estén actualizados. Use estos grupos y atributos para controlar el acceso, en lugar de usuarios individuales. Esto le permitirá administrar el acceso de forma centralizada cambiando la pertenencia a un grupo de un usuario o sus atributos una vez con un conjunto de permisos, en lugar de actualizar muchas políticas individuales cuando el acceso de un usuario tenga que cambiarse. Puede usar AWS IAM Identity Center (IAM Identity Center) para administrar grupos y atributos de usuarios. IAM Identity Center admite los atributos de usuarios utilizados más habitualmente, ya sea mediante introducción manual durante la creación del usuario o mediante un aprovisionamiento automático con un motor de sincronización, como lo que se define en el estándar Sistema para administración de identidades entre dominios (SCIM).

Coloque a usuarios con requisitos de seguridad comunes en grupos definidos por su proveedor de identidades, y prepare mecanismos para garantizar que los atributos de usuarios que puedan usarse para controlar el acceso (por ejemplo, los de departamento o ubicación) sean correctos y estén actualizados. Use estos grupos y atributos en lugar de usuarios individuales para controlar el acceso. Esto le permite administrar el acceso de forma centralizada cambiando la pertenencia a un grupo de un usuario o sus atributos una vez, en lugar de tener que actualizar muchas políticas individuales cuando el acceso de un usuario necesita cambiarse.

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

Guía para la implementación

- Si utiliza AWS IAM Identity Center (IAM Identity Center), configure grupos: IAM Identity Center le proporciona la capacidad de configurar grupos de usuarios y asignar a los grupos el nivel deseado de permisos.
  - Inicio de sesión único de AWS: administración de identidades
- Descubra el control de acceso basado en atributos (ABAC): ABAC es una estrategia de autorización que define permisos basados en atributos.
  - ¿Qué es ABAC para AWS?
  - Laboratorio: Control de acceso basado en etiquetas de IAM para EC2

Recursos

Documentos relacionados:

- Introducción a AWS Secrets Manager
- Prácticas recomendadas de IAM
- Proveedores de identidades y federación
- Usuario raíz de una cuenta de AWS

Videos relacionados:

- Prácticas recomendadas para administrar, recuperar y rotar secretos a escala
- Administración de permisos de usuarios a escala con AWS IAM Identity Center
- Dominar la identidad en cada piso de la tarta

Ejemplos relacionados:

- Laboratorio: Control de acceso basado en etiquetas de IAM para EC2

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 controlan a qué puede acceder cada usuario y en qué condiciones. Establezca permisos para identidades específicas humanas y de máquinas a fin de conceder acceso a acciones de servicio específicas en determinados recursos. Asimismo, especifique condiciones que deben cumplirse para que se conceda el acceso. Por ejemplo, puede permitir a los desarrolladores crear nuevas funciones de Lambda, pero solo en una determinada región. Al administrar los entornos de AWS a escala, debe cumplir las siguientes prácticas recomendadas para garantizar que las identidades solo tengan acceso a lo que necesiten y a nada más.

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 en IAM están administradas o insertadas y están asociadas a identidades de IAM, como usuarios, grupos o roles. Estas políticas le permiten especificar lo que dicha identidad puede hacer (sus permisos). Las políticas basadas en la identidad también pueden clasificarse de la siguiente manera.

Políticas administradas: políticas basadas en la identidad independientes que puede asociar a varios usuarios, grupos y roles de la cuenta de AWS. Hay dos tipos de políticas administradas:

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

Las políticas administradas son el método preferido para aplicar permisos. Sin embargo, también puede usar políticas insertadas que añade 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 clientes siguiendo el principio de privilegio mínimo.

Las políticas basadas en recursos están asociadas 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 que admiten las políticas basadas en recursos, consulte Servicios de AWS que funcionan con IAM.

Los límites de permisos utilizan una política administrada para establecer los permisos máximos que un administrador puede configurar. 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) le permite conceder permisos basados en atributos. En AWS, estos se denominan etiquetas. Las etiquetas pueden asociarse a entidades principales de IAM (usuarios o roles) y a recursos de AWS. Al utilizar las políticas de IAM, los administradores pueden crear una política reutilizable que aplica permisos en función de los atributos de la entidad principal de IAM. Por ejemplo, un administrador puede usar una única política de IAM que concede a los desarrolladores de la organización acceso a los recursos de AWS que coincidan con las etiquetas de proyecto de los desarrolladores. A medida que el equipo de desarrolladores va añadiendo recursos a los proyectos, los permisos se irán aplicando automáticamente en función de los atributos. El resultado es que no es necesario actualizar ninguna política para cada nuevo recurso.

Las políticas de control de servicios de organizaciones (SCP) 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 los recursos conceden a las entidades (usuarios o roles) 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 AWS CLI o AWS API Session 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 Definir los requisitos de acceso
- SEC03-BP02 Conceder acceso con privilegios mínimos

- SEC03-BP03 Establecer un proceso de acceso de emergencia
- SEC03-BP04 Reducir continuamente los permisos
- SEC03-BP05 Definir las barreras de protección de los permisos para su organización
- SEC03-BP06 Administrar el acceso en función del ciclo de vida
- SEC03-BP07 Analizar el acceso público y entre cuentas
- SEC03-BP08 Compartir recursos de forma segura en su organización
- SEC03-BP09 Compartir recursos de forma segura con terceros

SEC03-BP01 Definir los requisitos de acceso

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

Patrones comunes de uso no recomendados:

- Codificación rígida o almacenamiento de secretos en la aplicación.
- Concesión de permisos personalizados para cada usuario.
- Uso de credenciales de larga duración.

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

Guía para la implementación

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

El acceso normal a las Cuentas de AWS en la organización debe proporcionarse mediante acceso federado o un proveedor de identidades centralizado. También debe centralizar su 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 sus 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. Las políticas administradas de AWS proporcionan políticas de IAM predefinidas que cubren los casos de uso más comunes.

Los servicios de AWS, como AWS Secrets Manager y AWS Systems Manager Parameter Store, pueden servir para desacoplar los secretos de la aplicación o de la carga de trabajo de forma segura en los casos en los que no es factible utilizar roles de IAM. En Secrets Manager, puede establecer una rotación automática de sus credenciales. Puede utilizar Systems Manager para hacer referencia a los parámetros en sus scripts, comandos, documentos SSM, configuración y flujos de trabajo de automatización con el nombre único que especificó al crear el parámetro.

Puede usar Funciones de AWS Identity and Access Management en cualquier lugar para obtener credenciales de seguridad temporales en IAM para las cargas de trabajo que se ejecutan fuera de AWS. Sus cargas de trabajo puede 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 las situaciones en las que necesite usuarios de IAM con acceso programático y credenciales a largo plazo, utilice información de la clave de acceso utilizada por última vez para rotar y retirar las claves de acceso.

Recursos

Documentos relacionados:

- Control de acceso basado en atributos (ABAC)
- AWS IAM Identity Center
- Funciones de IAM en cualquier lugar
- Políticas administradas de AWS para IAM Identity Center
- Condiciones de las políticas de AWS IAM
- Casos de uso de IAM
- Elimine credenciales innecesarias
- Administración de políticas
- How to control access to AWS resources based on Cuenta de AWS, OU, or organization (Cómo controlar el acceso a los recursos de AWS en función de la Cuenta de AWS, la unidad organizativa o la organización)

- Identify, arrange, and manage secrets easily using enhanced search in AWS Secrets Manager (Identificar, organizar y administrar fácilmente los secretos mediante la búsqueda mejorada en AWS Secrets Manager)

Vídeos relacionados:

- Become an IAM Policy Master in 60 Minutes or Less (Consiga dominar las políticas de IAM en 60 minutos o menos)
- Separation of Duties, Least Privilege, Delegation, and CI/CD (Separación de deberes, privilegio mínimo, delegación y CI/CD)
- Streamlining identity and access management for innovation (Optimizar la administración de identidades y accesos para la innovación)

SEC03-BP02 Conceder acceso con privilegios mínimos

Se recomienda conceder exclusivamente el acceso que las identidades necesitan para realizar 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 esperado: los usuarios solo tienen los permisos necesarios para desempeñar su trabajo. A los usuarios solo se les concede acceso a entornos de productos para llevar a cabo una tarea específica en un periodo de tiempo limitado y el acceso se debe revocar una vez terminada la tarea. Los permisos se deben revocar cuando no se necesiten, por ejemplo, cuando un usuario cambia de proyecto o de puesto. Los privilegios de administrador solo se deben conceder a un pequeño grupo de administradores de confianza. Los permisos se deben revisar periódicamente para evitar su acumulación. A las cuentas de máquinas o sistemas se les debe asignar el conjunto más reducido de permisos que sean necesarios para realizar sus tareas.

Antipatrones usuales:

- Concesión predeterminada de permisos de administrador a los usuarios.
- Uso del usuario raíz para las actividades cotidianas.
- Creación de políticas excesivamente permisivas, pero sin todos los privilegios de administrador.

- No revisar los permisos para averiguar si se les permite el acceso de privilegio mínimo.

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

Guía para la implementación

El principio de privilegio mínimo establece que a las identidades solo les debe permitir realizar el menor conjunto de acciones necesarias para completar 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 realizar el seguimiento de quién tiene acceso a determinados recursos. Los usuarios y roles de IAM no tienen permisos de forma predeterminada. El usuario raíz tiene acceso total de forma predeterminada y se debe controlar y supervisar de forma estricta. Únicamente se debe usar para tareas que requieran 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 le ayudarán a acotar el acceso. Por ejemplo, mediante 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 realicen los servicios de AWS en su nombre, como que AWS CloudFormation cree una función de AWS Lambda, mediante la clave de condición `CalledVia`. Debe 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 aplicaciones creen sus propias políticas de IAM para los sistemas que creen, pero también debe aplicar un límite de permiso para acotar el máximo de permisos que puede recibir el sistema.

Pasos para la implementación

- Implemente políticas de privilegio mínimo: asigne políticas de acceso con privilegio mínimo a grupos y roles de IAM para reflejar el rol o la función del usuario que haya definido.
  - Base las políticas en el uso de la API: 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 realiza realmente en AWS. IAM Access Analyzer puede generar automáticamente una política de IAM basada en la actividad. Puede usar IAM Access Advisor en el nivel de organización o de cuenta para realizar el seguimiento de la información a la que se ha accedido por última vez para una política concreta.

- Considere la utilización de políticas administradas por AWS para funciones de trabajo. Cuando empiece a crear políticas de permisos detalladas, puede ser difícil saber por dónde empezar. AWS tiene políticas administradas para roles comunes, por ejemplo, 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: elimine los permisos que no son necesarios y limite las políticas excesivamente permisivas. La generación de políticas de IAM Access Analyzer puede ser de ayuda en la optimización de las políticas de permisos.
- Garantice que los usuarios cuenten con acceso limitado a los entornos de producción: los usuarios solo deben tener acceso a los entornos de producción con un motivo 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.
- Considere el uso de límites de permisos: un límite de permisos es una característica para usar una política administrada que establece los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. El límite de permisos de una identidad le permite llevar a cabo únicamente las acciones autorizadas tanto por sus políticas basadas en la identidad como por sus límites de permisos.
- Considere el uso de etiquetas de recursos para los permisos: un modelo de control de acceso basado en atributos mediante etiquetas de recursos le permite conceder acceso según la finalidad del recurso, el propietario, el entorno u otros criterios. Por ejemplo, puede usar etiquetas de recursos para diferenciar entre los entornos de desarrollo y de producción. Con estas etiquetas, puede limitar a los desarrolladores al entorno de desarrollo. Mediante la combinación de las políticas de etiquetado y de permisos, puede conseguir un acceso detallado a los recursos sin necesidad de definir políticas complicadas y personalizadas para cada puesto.
- Use las 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 las políticas de control de servicios le permiten 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.

- Establezca una política de ciclo de vida del usuario para la organización: las políticas de este tipo definen las tareas que se realizan cuando los usuarios se incorporan en AWS, cambian de rol o ámbito, o ya no necesitan acceder a AWS. Las revisiones de permisos se deben realizar durante cada paso del ciclo de vida de un usuario para verificar son restrictivos de forma correcta y para evitar la acumulación de permisos.
- Establezca una programación periódica para revisar los permisos y eliminar los que no sean necesarios: debe revisar periódicamente el acceso de usuario para verificar que los usuarios no tengan permisos demasiado permisivos. AWS Config y IAM Access Analyzer pueden ser de ayuda al auditar los permisos de usuario.
- Establezca una matriz de roles de trabajo: con una matriz de roles de trabajo se visualizan los distintos roles y los niveles de acceso necesarios en su presencia de AWS. Con una matriz de roles de trabajo, puede definir y separar los permisos según las responsabilidades de usuario en su organización. Use grupos en vez de aplicar permisos directamente a usuarios o roles individuales.

Recursos

Documentos relacionados:

- Conceder privilegios mínimos
- Límites de permisos para las entidades de IAM
- Techniques for writing least privilege IAM policies (Técnicas para elaborar políticas de IAM de privilegio mínimo)
- IAM Access Analyzer makes it easier to implement least privilege permissions by generating IAM policies based on access activity (IAM Access Analyzer facilita la implementación de los permisos de privilegio mínimo al generar políticas de IAM basadas en la actividad de acceso)
- Delegate permission management to developers by using IAM permissions boundaries (Delegar la administración de permisos para desarrolladores mediante límites de permisos de IAM)
- Refining Permissions using last accessed information (Mejora de los permisos con la información del último acceso)
- IAM policy types and when to use them (Tipos de políticas de IAM y cuándo utilizarlas)
- Testing IAM policies with the IAM policy simulator (Prueba de las políticas de IAM con el simulador de políticas de IAM)

- Guardrails in AWS Control Tower (Barreras de protección en AWS Control Tower)
- Zero Trust architectures: An AWS perspective (Arquitecturas de confianza cero: una perspectiva de AWS)
- How to implement the principle of least privilege with CloudFormation StackSets (Cómo implementar el principio de privilegio mínimo con CloudFormation StackSets)
- Control de acceso basado en atributos (ABAC)
- Reducción del alcance de las políticas con datos de la actividad de los usuarios
- Ver accesos de rol
- Use el etiquetado para organizar el entorno y fomentar la responsabilidad
- Estrategias de etiquetado de AWS
- Etiquetado de recursos de AWS

Vídeos relacionados:

- Next-generation permissions management (Administración de permisos de nueva generación)
- Zero Trust: An AWS perspective (Confianza cero: una perspectiva de AWS)
- How can I use permissions boundaries to limit users and roles to prevent privilege escalation? (¿Cómo puedo utilizar los límites de los permisos para restringir a los usuarios y los roles para evitar la escalada de privilegios?)

Ejemplos relacionados:

- Laboratorio: Límites de permisos de IAM para delegar la creación de roles
- Laboratorio: Control de acceso basado en etiquetas de IAM para EC2

SEC03-BP03 Establecer 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. Puede que las preguntas y las prácticas recomendadas en el Pilar de fiabilidad le resulten útiles para identificar los modos de error y diseñar sistemas más resilientes para minimizar la probabilidad de que se produzcan errores.
- Ha documentado los pasos que se deben seguir para confirmar que la avería 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 de error. La especificidad puede reducir la tentación de los usuarios de abusar de un proceso general para todo tipo de emergencias. Sus 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 guías de estrategia que se pueden seguir de forma rápida y eficiente. Recuerde que un evento de emergencia puede resultar estresante para sus usuarios, ya que 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 ensayados. Sus usuarios no están preparados para emergencias y siguen procesos improvisados cuando estas se producen.
- Sus procesos de acceso de emergencia dependen 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 repercutir en su capacidad para recuperarse del error.

- Sus procesos de acceso de emergencia se utilizan 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 realizar cambios directamente que enviarlos a través de una canalización.
- Sus procesos de acceso de emergencia no generan registros suficientes para auditar los procesos, o los registros no se supervisan para alertar de un posible uso indebido de los procesos.

Beneficios de establecer esta práctica recomendada:

- Si cuenta con procesos de acceso de emergencia bien documentados y ensayados, 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 realizar un seguimiento de cada solicitud de acceso de emergencia y detectar y alertar sobre intentos no autorizados de utilizar indebidamente el proceso para eventos que no sean de emergencia.

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 desplegadas 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 supone 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 IAM users, y los roles de IAM entre cuentas en todas las cuentas de la carga de trabajo. Esto

asegura que estos recursos estén listos y disponibles cuando ocurra una emergencia. Al crear de antemano los recursos, no depende de las API del plano de control de AWS (utilizadas para crear y modificar los recursos de AWS) que podrían no estar disponibles en caso de emergencia. Además, al crear de antemano los recursos de IAM, no es necesario tener en cuenta los posibles retrasos debido a una coherencia eventual.

- Incluya los procesos de acceso de emergencia como parte de sus planes de administración de incidentes (SEC10-BP02). Documente cómo se realiza 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, realizar un seguimiento de la solicitud en cada etapa del flujo de trabajo y añadir 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 realizar un seguimiento de esas solicitudes en un solo sistema, analizar las tendencias de uso y mejorar sus procesos.
- Compruebe que solo los 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 las solicitudes de aprobación admiten aprobadores secundarios si los principales no están disponibles y cómo se escalan en la cadena de administración hasta la aprobación.
- Compruebe que el proceso genere registros y eventos de auditoría detallados para los intentos correctos e infructuosos de obtener acceso de emergencia. Supervise tanto el proceso de solicitud como el mecanismo de acceso de emergencia para detectar el uso indebido o los accesos no autorizados. Correlacione la actividad con los eventos de emergencia en curso de su sistema de administración de incidentes y alerte cuando se produzcan acciones fuera de los períodos de tiempo esperados. Por ejemplo, debe supervisar y alertar si se produce actividad en la Cuenta de AWS de acceso de emergencia, ya que nunca debe usarse en operaciones normales.
- Pruebe los procesos de acceso de emergencia de manera periódica para comprobar que los pasos estén claros y para 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 ante incidentes (SEC10-BP07) y pruebas de recuperación de desastres (REL13-BP03).

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

Como se describe en SEC02-BP04 Recurrir a 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. Puede federar varias Cuentas de AWS en su organización de AWS con IAM Identity Center, o puede federar Cuentas de AWS individuales con 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 realizar 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 período, 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 realizar 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 roles de IAM y IAM users) 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 de antemano un conjunto de IAM users para los administradores de emergencias de la cuenta de acceso de emergencia con contraseñas seguras y tokens de MFA asociados. Estos IAM users 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 realizar la acción de cambio de emergencia. La ventaja de este enfoque es que cada IAM user se asigna a un administrador de emergencias y usted puede saber qué usuario inició sesión revisando los eventos de CloudTrail. La desventaja es que hay que mantener varios IAM users con sus contraseñas de larga duración y los tokens de MFA asociados.

- Puede utilizar el usuario raíz de la 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 el IAM Identity Center con un proveedor de identidades externo o crear un proveedor de identidades de IAM (SEC02-BP04). Por lo general, se configuran importando un documento XML de metadatos de SAML proporcionado por el proveedor de identidades. El documento XML de metadatos incluye un certificado X.509 correspondiente 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. Ambos escenarios 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 importando 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 realicen 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 un IAM Identity Center o en una Región de AWS, le recomendamos que establezca una configuración que pueda utilizar para proporcionar acceso temporal a la AWS Management Console.

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 la sección sobre la configuración del acceso de emergencia a la AWS Management Console.

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 IAM users, y opcionalmente, proveedores de identidades de IAM. Además, cree de antemano roles de IAM entre cuentas en la 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 el AWS CloudFormation StackSets con AWS Organizations para crear dichos recursos en las cuentas de los miembros de su organización.

- Cree políticas de control de servicios (SCP) de AWS Organizations para denegar la eliminación y modificación de los roles de IAM entre cuentas en las Cuentas de AWS miembro.
- 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:
  - Con IAM users: cree de antemano los IAM users con contraseñas seguras y los dispositivos MFA asociados.
  - Con el 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

- Como se detalla en la configuración del acceso de emergencia a la AWS Management Console, 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 por Well-Architected:

- SEC02-BP04 Recurrir a un proveedor de identidades centralizado
- SEC03-BP02 Conceder acceso con privilegios mínimos
- SEC10-BP02: Desarrollar planes de administración de incidentes
- SEC10-BP07 Ejecutar los días de juego

Documentos relacionados:

- configuración del acceso de emergencia a la AWS Management Console
- Concesión de acceso a la AWS Management Console a los usuarios federados SAML 2.0
- Break glass access

Vídeos 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 Reducir continuamente 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 el principio del 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.

Antipatrones usuales:

- Conceder de forma predeterminada permisos de administrador a los usuarios.
- 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 realizar el trabajo actual. Recomendamos realizar 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 le permite proporcionar permisos a los usuarios utilizando sus atributos en lugar de tener que asociar políticas de permisos directamente a cada usuario.

Pasos para la implementación

- Utilice AWS Identity and Access Management Access Analyzer: IAM Access Analyzer le ayuda a identificar recursos de su organización y sus cuentas, como buckets de Amazon Simple Storage Service (Amazon S3) o roles de IAM, que se comparten con una entidad externa.

- Utilice la generación de políticas de IAM Access Analyzer: la generación de políticas de IAM Access Analyzer le ayuda a crear políticas de permisos detalladas basadas en la actividad de acceso de un usuario o rol de IAM.
- Determine un marco temporal y una política de uso aceptables para los usuarios y roles de IAM: utilice la marca de tiempo del último acceso para identificar a los usuarios y roles no utilizados y eliminarlos. Revise la información de último acceso a servicios y acciones para identificar y delimitar los permisos de 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 AWS Management Console y de manera programática para permitirle incorporarlas en sus flujos de trabajo de infraestructura y sus herramientas automatizadas.
- Considere la posibilidad de registrar eventos de datos en AWS CloudTrail: de manera predeterminada, CloudTrail no registra eventos de datos como la actividad a nivel de objeto de Amazon S3 (por ejemplo, `GetObject` y `DeleteObject`) o las actividades de tabla 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:

- Conceder privilegios mínimos
- Elimine credenciales innecesarias
- ¿Qué es AWS CloudTrail?
- Administración de políticas
- Registro y monitoreo en DynamoDB
- Habilitación del registro de eventos de CloudTrail para buckets y objetos de Amazon S3
- Obtener informes de credenciales para su Cuenta de AWS

Vídeos relacionados:

- Become an IAM Policy Master in 60 Minutes or Less (Consiga dominar las políticas de IAM en 60 minutos o menos)

- Separation of Duties, Least Privilege, Delegation, and CI/CD (Separación de deberes, privilegio mínimo, delegación y CI/CD)
- AWS re:Inforce 2022 - AWS Identity and Access Management (IAM) deep dive (AWS re:Inforce 2022: Profundización en AWS Identity and Access Management [IAM])

SEC03-BP05 Definir las barreras de protección de los permisos para su organización

Establezca controles comunes que restrinjan el acceso a todas las identidades de su organización. Por ejemplo, puede restringir el acceso a determinadas Regiones de AWS o impedir que sus operadores eliminen recursos comunes, como un rol de IAM que usa su equipo de seguridad central.

Patrones comunes de uso no recomendados:

- Ejecutar cargas de trabajo en su cuenta de administrador de la organización.
- Ejecutar cargas de trabajo de producción y de no producción en la misma cuenta.

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

Guía para la implementación

A medida que crezca y administre cargas de trabajo adicionales en AWS, deberá separarlas mediante cuentas y administrar dichas cuentas con AWS Organizations. Le recomendamos que establezca barreras de protección de permisos comunes que restrinjan el acceso a todas las identidades de su organización. Por ejemplo, puede restringir el acceso a determinadas Regiones de AWS o impedir que su equipo elimine recursos comunes, como un rol de IAM que usa su equipo de seguridad central.

Puede empezar con la implementación de ejemplos de políticas de control de servicios, como impedir que los usuarios desactiven servicios clave. Las SCP utilizan el lenguaje de las políticas de IAM y le permiten establecer controles a los que se adhieren todas las entidades principales de IAM (usuarios y roles). Puede restringir el acceso a determinadas acciones de servicio, recursos y según una condición específica para satisfacer las necesidades de control de acceso de su organización. Si es necesario, puede definir excepciones a sus barreras de protección. Por ejemplo, puede restringir las acciones de servicio para todas las entidades de IAM de la cuenta excepto para un rol de administrador específico.

Le recomendamos que evite ejecutar cargas de trabajo en su cuenta de administración. Esta cuenta debe utilizarse para controlar y desplegar las barreras de protección que afectarán a las cuentas de los miembros. Algunos servicios de AWS admiten el uso de una cuenta de administrador delegada. Cuando esté disponible, deberá utilizar esta cuenta delegada en lugar de la cuenta de administración. Debe limitar firmemente el acceso a la cuenta de administrador de la organización.

El uso de una estrategia de varias cuentas le permite tener una mayor flexibilidad a la hora de aplicar las barreras de protección a sus cargas de trabajo. La Arquitectura de referencia de Seguridad de AWS ofrece recomendaciones sobre cómo diseñar la estructura de su cuenta. Los servicios de AWS como AWS Control Tower proporcionan capacidades para administrar de forma centralizada tanto los controles preventivos como los de detección en toda la organización. Defina un propósito claro para cada cuenta o unidad organizativa en su organización y limite los controles de acuerdo con dicho propósito.

Recursos

Documentos relacionados:

- AWS Organizations
- Service control policies (SCPs) (Políticas de control de servicios [SCP])
- Get more out of service control policies in a multi-account environment (Saque más partido a las políticas de control del servicio en un entorno de varias cuentas)
- Arquitectura de referencia de AWS (AWS SRA)

Vídeos relacionados:

- Enforce Preventive Guardrails using Service Control Policies (Aplicar las barreras de protección preventivas mediante políticas de control de servicios)
- Building governance at scale with AWS Control Tower (Consolidar la gobernanza a escala con AWS Control Tower)
- AWS Identity and Access Management deep dive (Profundización en AWS Identity and Access Management)

SEC03-BP06 Administrar el acceso en función del ciclo de vida

Integre los controles de acceso con el ciclo de vida de la aplicación y el operador, el proveedor de federación centralizado. Por ejemplo, quite el acceso a un usuario cuando abandone la organización o cambie de rol.

A medida que vaya administrando las cargas de trabajo con cuentas independientes, habrá casos en los que necesite compartir recursos entre esas cuentas. Le recomendamos que comparta los recursos con AWS Resource Access Manager (AWS RAM). Este servicio le permite compartir de forma sencilla y segura recursos de AWS en su AWS Organizations y las unidades organizativas. Con AWS RAM, el acceso a los recursos compartidos se concede o revoca automáticamente a medida que las cuentas entran y salen de la organización o unidad organizativa con la que se comparten. Esto ayuda a garantizar que los recursos se comparten solo con las cuentas que pretende.

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

Guía para la implementación

Ciclo de vida de acceso de los usuarios Implemente una política de ciclo de vida de acceso de los usuarios para la incorporación de nuevos usuarios, los cambios de puesto y la salida de usuarios, de modo que solo tengan acceso los usuarios actuales.

Recursos

Documentos relacionados:

- Control de acceso basado en atributos (ABAC)
- Conceder privilegios mínimos
- Analizador de acceso de IAM
- Elimine credenciales innecesarias
- Administración de políticas de IAM

Vídeos relacionados:

- Become an IAM Policy Master in 60 Minutes or Less (Consiga dominar las políticas de IAM en 60 minutos o menos)

- Separation of Duties, Least Privilege, Delegation, and CI/CD (Separación de deberes, privilegio mínimo, delegación y CI/CD)

SEC03-BP07 Analizar el acceso público y entre cuentas

Supervise continuamente los resultados que ponen de relieve el acceso público y entre cuentas. Reduzca el acceso público y el acceso entre cuentas solo a los recursos que requieran ese acceso.

Resultado deseado: saber cuáles de sus recursos de AWS se comparten y con quién. Supervisar y auditar continuamente sus recursos compartidos para verificar que solo se compartan con las entidades principales autorizadas.

Antipatrones usuales:

- 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 directo entre cuentas utilizando políticas basadas en recursos —por ejemplo, políticas de buckets de Amazon Simple Storage Service (Amazon S3)—- o permitiendo que una 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 utiliza 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 IAM Access Analyzer con AWS Organizations para comprobar que tiene visibilidad de todas sus cuentas. IAM Access Analyzer también le permite previsualizar los resultados antes de desplegar 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 de varias cuentas, puede utilizar políticas

de confianza para controlar en qué casos se puede asumir un rol. Por ejemplo, podría utilizar la clave de condición `PrincipalOrgId` para denegar un intento de asumir un rol desde fuera de su AWS Organizations.

AWS Config puede informar de los recursos que están mal configurados y, a través de las comprobaciones de políticas de AWS Config, puede detectar los recursos que tienen configurado el acceso público. Servicios como AWS Control Tower y AWS Security Hub simplifican el despliegue de controles de detección y barreras de protección en AWS Organizations para identificar y corregir los recursos expuestos públicamente. Por ejemplo,AWS Control Tower dispone de una barrera de protección administrada que puede detectar si las Cuentas de AWS pueden restaurar alguna instantánea de Amazon EBS.

Pasos para la implementación

- Considere la posibilidad de habilitar AWS Config para AWS Organizations: AWS Config le permite agregar los hallazgos de varias cuentas que están dentro de una AWS Organizations a una cuenta de administrador delegado. Esto proporciona una visión global y le permite desplegar Reglas de AWS Config en todas las cuentas para detectar recursos de acceso público.
- Configure AWS Identity and Access Management Access Analyzer: IAM Access Analyzer le 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.
- Utilice la corrección automatizada en AWS Config para responder a los cambios en la configuración del acceso público de los buckets de Amazon S3: puede volver a habilitar automáticamente la configuración de acceso público en bloque para los buckets de Amazon S3.
- Implemente la supervisión y las alertas para identificar si los buckets de Amazon S3 se han hecho públicos: debe disponer de supervisión y alertas para identificar cuándo se desactiva el acceso público a bloques de Amazon S3 y si los buckets de Amazon S3 se hacen públicos. Además, si utiliza AWS Organizations, puede crear una política de control de servicios que impida realizar cambios en las políticas de acceso público de Amazon S3. AWS Trusted Advisor comprueba si hay buckets de Amazon S3 que tengan 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 añada, 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 sus buckets de Amazon S3 para comprobar si tienen acceso público. Para obtener más información, consulte How to Use AWS Config to Monitor for and Respond to Amazon S3 Buckets Allowing Public Access (Cómo utilizar AWS Config para supervisar y responder a los buckets

de Amazon S3 que permiten el acceso público). Al revisar el acceso, es importante tener en cuenta qué tipos de datos contienen los buckets de Amazon S3. Amazon Macie ayuda a detectar y proteger datos confidenciales, como PII, PHI y credenciales, además de claves privadas o de AWS.

Recursos

Documentos relacionados:

- Uso de AWS Identity and Access Management Access Analyzer
- AWS Control Tower controls library (Biblioteca de controles de AWS Tower Control)
- AWS Foundational Security Best Practices standard (Estándar de prácticas recomendadas de seguridad básicas de AWS)
- AWS Config Managed Rules (Reglas administradas de AWS Config)
- Referencia de verificaciones de AWS Trusted Advisor
- Supervisión de resultados de la verificación de AWS Trusted Advisor con Amazon EventBridge
- Managing AWS Config Rules Across All Accounts in Your Organization (Administración de reglas de AWS Config en todas las cuentas de su organización)
- AWS Config y AWS Organizations

Vídeos relacionados:

- Best Practices for securing your multi-account environment (Prácticas recomendadas para proteger su entorno de varias cuentas)
- Dive Deep into IAM Access Analyzer (Profundización en IAM Access Analyzer)

SEC03-BP08 Compartir 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 componentes para compartimentar el entorno, por ejemplo, en entornos de desarrollo, pruebas y producción. Sin embargo, disponer de componentes 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: reducir al mínimo el acceso involuntario mediante métodos seguros para compartir recursos dentro de su organización y facilitar su iniciativa de prevención de pérdida de datos. Reducir la sobrecarga operativa en comparación con la administración de componentes individuales, reducir los errores derivados de crear manualmente el mismo componente varias veces y aumentar la escalabilidad de las cargas de trabajo. Puede disminuir el tiempo de resolución en escenarios con varios puntos de fallo y aumentar su confianza a la hora de determinar cuándo un componente ya no es necesario. Para obtener orientación prescriptiva sobre el análisis de recursos que se comparten externamente, consulte SEC03-BP07 Analizar el acceso público y entre cuentas.

Antipatrones usuales:

- 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 ayudarle a establecer una gobernanza que reduzca el acceso externo solo a los recursos que lo requieran, además de a establecer un proceso para supervisar continuamente y alertar automáticamente.

El uso compartido entre cuentas dentro de AWS Organizations está respaldado por una serie de servicios de AWS, como AWS Security Hub, Amazon GuardDuty y AWS Backup. 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 puede transferir hallazgos desde cuentas individuales a una cuenta central en la que podrá verlos todos. AWS Backup puede realizar una copia de seguridad de un recurso y compartirlo entre varias cuentas. Puede utilizar AWS Resource Access Manager (AWS RAM) para compartir otros recursos comunes, como subredes de VPC y asociaciones de Transit Gateway, AWS Network Firewall o canalizaciones de Amazon SageMaker.

Para limitar su cuenta para que solo comparta recursos dentro de su organización, utilice políticas de control de servicios (SCP) para impedir el acceso a las entidades principales externas. Cuando comparta recursos, combine controles basados en identidades y controles de red para crear un perímetro de datos para su organización que le ayude a protegerse contra el acceso no intencionado. 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 políticas de punto de conexión de VPC y la condición `AWS:PrincipalOrgId` para asegurarse de que las identidades que acceden a sus buckets de Amazon S3 pertenecen a su organización. Es importante tener en cuenta que los SCP no se aplican a los roles vinculados al servicio (LSR) ni a las entidades principales del servicio de AWS.

Cuando utilice Amazon S3, deshabilite las ACL para 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 de 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 orientación prescriptiva sobre la administración de permisos para compartir recursos externamente, consulte Administración de permisos.

Pasos para la implementación

1. Use AWS Organizations.

   AWS Organizations es un servicio de administración de cuentas que le permite consolidar varias Cuentas de AWS en una organización que usted crea y administra de manera 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 Organizations.
2. Integre AWS Organizations con servicios de AWS.

   Cuando habilita un servicio de AWS para que realice tareas en su nombre en las cuentas miembros de su organización, AWS Organizations crea un rol vinculado al servicio de IAM para

dicho servicio en cada cuenta miembro. Debe administrar el acceso de confianza mediante la AWS Management Console, las API de AWS o la AWS CLI. Para obtener orientación prescriptiva sobre la habilitación del acceso de confianza, consulte Uso de AWS Organizations con otros servicios de AWS y Servicios de AWS que se pueden utilizar con Organizations.

3. Establezca un perímetro de datos.

   El perímetro de AWS suele representarse como una organización administrada por AWS Organizations. Junto con las redes y sistemas locales, el acceso a los recursos de AWS es lo que muchas personas consideran que es el perímetro de Mi AWS. El objetivo del perímetro 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.

   a. Defina e implemente los perímetros.

      Siga los pasos que se describen en Perimeter implementation (Implementación del perímetro) del documento técnico Building a Perimeter on AWS (Construir un perímetro en AWS) para cada condición de autorización. Para obtener orientación prescriptiva sobre la protección de la capa de red, consulte Protección de redes.

   b. Supervise y alerte continuamente.

      AWS Identity and Access Management Access Analyzer ayuda a identificar los recursos y las cuentas de su organización que se comparten con entidades externas. Puede integrar IAM Access Analyzer con AWS Security Hub para enviar y agregar los hallazgos sobre un recurso desde IAM Access Analyzer a Security Hub para ayudarle a analizar la postura de seguridad de su entorno. Para permitir la integración, habilite tanto IAM Access Analyzer como Security Hub en cada región de cada cuenta. También puede utilizar Reglas de AWS Config para auditar la configuración y alertar a quien corresponda utilizando AWS Chatbot con AWS Security Hub. A continuación, puede utilizar los documentos de AWS Systems Manager Automation para corregir los recursos no conformes.

   c. Para obtener orientación prescriptiva sobre la supervisión y alerta continua de los recursos compartidos externamente, consulte Analizar el acceso público y entre cuentas.

4. Utilice el uso compartido de recursos en los servicios de AWS y restrínjalos de la forma oportuna.

   Muchos servicios de AWS le permiten compartir recursos con otra cuenta o dirigirse a un recurso de otra cuenta, como las imágenes de máquina de Amazon (AMI) y AWS Resource Access Manager (AWS RAM). Restrinja la API `ModifyImageAttribute` para especificar las cuentas de confianza con las que compartir la AMI. Especifique la condición `ram:RequestedAllowsExternalPrincipals` cuando utilice AWS RAM para restringir el

uso compartido únicamente a su organización; de esta forma, ayuda a evitar el acceso desde identidades que no sean de confianza. Para obtener orientación prescriptiva y conocer otras consideraciones, consulte Resource sharing and external targets (Uso compartido de recursos y destinos externos).

5. Utilice AWS RAM para compartir de forma segura en una cuenta o con otras Cuentas de AWS.

   AWS RAM le 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 compartió anteriormente mediante una política basada en recursos, puede utilizar la API PromoteResourceShareCreatedFromPolicy o una equivalente para promover el recurso compartido a un recurso compartido completo de AWS RAM.

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

Recursos

Prácticas recomendadas relacionadas:

- SEC03-BP07 Analizar el acceso público y entre cuentas
- SEC03-BP09 Compartir recursos de forma segura con terceros
- SEC05-BP01 Crear capas de red

Documentos relacionados:

- Bucket owner granting cross-account permission to objects it does not own (El propietario del bucket concede permisos entre varias cuentas a objetos que no son de su propiedad)
- How to use Trust Policies with IAM (Cómo utilizar las políticas de confianza con IAM)
- Building Data Perimeter on AWS (Creación de un perímetro de datos en AWS)
- Cómo utilizar un ID externo al otorgar acceso a los recursos de AWS a terceros
- Servicios de AWS que se pueden utilizar con AWS Organizations

- Establishing a data perimeter on AWS: Allow only trusted identities to access company data (Establecer un perímetro de datos en AWS: permitir que solo las identidades de confianza accedan a los datos de la empresa)

Vídeos relacionados:

- Granular Access with AWS Resource Access Manager (Acceso detallado con AWS Resource Access Manager)
- Securing your data perimeter with VPC endpoints (Protección del perímetro de datos con puntos de conexión de VPC)
- Establishing a data perimeter on AWS (Establecer un perímetro de datos en AWS)

Herramientas relacionadas:

- Data Perimeter Policy Examples (Ejemplos de políticas del perímetro de datos)

SEC03-BP09 Compartir recursos de forma segura 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 utilizando 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: cualquiera puede utilizar las credenciales de larga duración de AWS Identity and Access Management (IAM), las claves de acceso de IAM y las claves secretas que están asociadas a un usuario siempre que las credenciales sean válidas y estén activas. El uso de un rol de IAM y credenciales temporales le ayuda a mejorar su postura de seguridad general al reducir el esfuerzo que supone mantener credenciales de larga duración, incluida la sobrecarga de administración y operativa que entrañan esos datos confidenciales. Al utilizar un identificador único universal (UUID) para el ID externo en la política de confianza de IAM y mantener bajo su control las políticas de IAM asociadas al rol de IAM, puede auditar y verificar que el acceso concedido a un tercero no sea demasiado permisivo. Para obtener orientación prescriptiva sobre el análisis de recursos que se comparten externamente, consulte SEC03-BP07 Analizar el acceso público y entre cuentas.

Antipatrones usuales:

- Utilizar la política de confianza de IAM predeterminada sin ninguna condición.
- Utilizar credenciales y claves de acceso de IAM de larga duración.
- 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. Además, defina una política de confianza utilizando la condición de ID externo. Cuando utilice un ID externo, usted o el tercero pueden 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 Funciones de IAM en cualquier lugar para administrar roles de IAM para aplicaciones fuera de AWS que utilicen API de AWS.

Si el tercero ya no necesita acceder a su entorno, elimine el rol. Procure no proporcionar credenciales de larga duración a terceros. Manténgase al tanto de otros servicios de AWS que admiten el uso compartido. Por ejemplo, AWS Well-Architected Tool permite compartir una carga de trabajo con otras Cuentas de AWS y AWS Resource Access Manager le 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 proporcionar acceso a cuentas externas.

   Los roles entre cuentas reducen la cantidad de información confidencial que almacenan las cuentas externas y terceros para dar servicio a sus clientes. Los roles entre cuentas le permiten conceder acceso a los recursos de AWS de su cuenta de forma segura a un tercero, como AWS Partner u otras cuentas de su organización, al tiempo que puede mantener la capacidad de administrar y auditar dicho acceso.

   El tercero podría estar proporcionándole un servicio desde una infraestructura híbrida o extrayendo datos a una ubicación externa. Funciones de IAM en cualquier lugar le 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 utilizar credenciales de larga duración.

No debería utilizar credenciales de larga duración 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. Utilice un ID externo con terceros.

   El uso de un ID externo le permite designar quién puede asumir un rol en una política de confianza de IAM. La política de confianza puede exigir que el usuario que asume el rol reafirme la condición y el objetivo en el que opera. También proporciona un mecanismo para que el propietario de la cuenta permita que el rol se adopte únicamente en circunstancias específicas. La función principal del ID externo es abordar y prevenir el problema del suplente confundido.

   Utilice un ID externo si es propietario de una Cuenta de AWS y ha configurado un rol para un tercero que accede a otras Cuentas de AWS además de la suya, o cuando tenga que asumir roles en nombre de diferentes clientes. Trabaje con su tercero o AWS Partner para establecer una condición de ID externo que desee incluir en la política de confianza de IAM.

3. Utilice ID externos universalmente únicos.

   Implemente un proceso que genere un valor único aleatorio para un ID externo, como un identificador universalmente único (UUID). El hecho de que un tercero reutilice los ID externos para distintos clientes no resuelve el problema del suplente confundido, ya que el cliente A podría ver los datos del cliente B utilizando el ARN de rol del cliente B junto con el ID externo duplicado. En un entorno de varios inquilinos, en el que un tercero da soporte a varios clientes con diferentes Cuentas de AWS, el tercero debe utilizar un ID único diferente como ID externo para cada Cuenta de AWS. El tercero es responsable de detectar los ID externos duplicados y de asignar de forma segura cada cliente a su ID externo correspondiente. El tercero debe realizar pruebas para verificar que solo puede asumir el rol cuando se especifica el ID externo. El tercero debería abstenerse de almacenar el ARN del rol del cliente y el ID externo hasta que se requiera el ID externo.

   El ID externo no se trata 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.

4. Declare obsoletas las credenciales de larga duración proporcionadas por el cliente.

   Declare obsoleto el uso de credenciales de larga duración y utilice roles de cuentas cruzadas o Funciones de IAM en cualquier lugar. Si debe utilizar credenciales de larga duración, establezca un plan para migrar al acceso basado en roles. Para obtener información sobre la administración de claves, consulte Administración de identidades. Trabaje también con el equipo de su Cuenta de AWS y el tercero para establecer un runbook de mitigación de riesgos. Para obtener orientación prescriptiva sobre cómo responder y mitigar el impacto potencial de un incidente de seguridad, consulte Respuesta a incidentes.

5. Verifique que la configuración tenga una orientación prescriptiva o esté automatizada.

   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 (Roles entre cuentas).

   El tercero debe proporcionar un mecanismo de configuración automatizado y auditable. Sin embargo, debería automatizar la configuración del rol con el documento de la política de roles que describe el acceso necesario. Con una plantilla de AWS CloudFormation o algo equivalente, debería supervisar los cambios y utilizar la detección de desviaciones como parte de la práctica de auditoría.

6. Tenga en cuenta los cambios.

   La estructura de su cuenta, su necesidad de utilizar al tercero o la oferta de servicios que este le proporciona 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 le alerten de cambios inesperados. Supervise y audite el uso del rol y el almacén de datos de los ID externos. Debe estar 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 realizarla, las personas implicadas, el coste y el impacto en otros recursos.

Para obtener una orientación prescriptiva sobre los métodos de detección, consulte las prácticas recomendadas en Detección.

Recursos

Prácticas recomendadas relacionadas:

- SEC02-BP02 Usar credenciales temporales
- SEC03-BP05 Definir las barreras de protección de los permisos para su organización
- SEC03-BP06 Administrar el acceso en función del ciclo de vida
- SEC03-BP07 Analizar el acceso público y entre cuentas
- SEC04 Detección

Documentos relacionados:

- Bucket owner granting cross-account permission to objects it does not own (El propietario del bucket concede permisos entre varias cuentas a objetos que no son de su propiedad)
- How to use Trust Policies with IAM roles (Cómo utilizar las políticas de confianza con roles de IAM)
- Delegación del acceso entre Cuentas de AWS mediante roles de IAM
- How do I access resources in another Cuenta de AWS using AWS IAM? (¿Cómo accedo a los recursos en otra cuenta de AWS a través de AWS 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 (Recopilación de información de recursos de AWS CloudFormation creados en cuentas externas con recursos personalizados)
- Securely Using External ID for Accessing AWS Accounts Owned by Others (Uso seguro del ID externo para acceder a cuentas de AWS propiedad de terceros)
- Extend IAM roles to workloads outside of IAM with IAM Roles Anywhere (Extienda los roles de IAM de AWS a cargas de trabajo fuera de AWS con Funciones de IAM en cualquier lugar)

Vídeos relacionados:

- How do I allow users or roles in a separate Cuenta de AWS access to my Cuenta de AWS? (¿Cómo permito que los usuarios o roles de una cuenta de AWS independiente accedan a mi cuenta de AWS?
- AWS re:Invent 2018: Become an IAM Policy Master in 60 Minutes or Less (AWS re:Invent 2018: Consiga dominar las políticas de IAM en 60 minutos o menos)
- AWS Knowledge Center Live: IAM Best Practices and Design Decisions (Centro de conocimiento de AWS en directo: Prácticas recomendadas y decisiones de diseño de IAM)

Ejemplos relacionados:

- Well-Architected Lab - Lambda cross account IAM role assumption (Level 300) (Laboratorio de Well-Architected: Asunción de roles de IAM entre cuentas de Lambda [Nivel 300])
- Configure cross-account access to Amazon DynamoDB (Configurar el acceso entre cuentas a Amazon DynamoDB)
- AWS STS Network Query Tool (Herramienta de consulta de red AWS STS)

Detección

La detección consta de dos partes: la detección de cambios de configuración inesperados o no deseados, y la detección de comportamientos inesperados. El primer caso puede ocurrir en varias ubicaciones durante el ciclo de vida de entrega de una aplicación. Al utilizar la infraestructura como código (por ejemplo, una plantilla CloudFormation), puede comprobar si hay alguna configuración no deseada antes de implementar una carga de trabajo mediante la implementación de comprobaciones en el control de código fuente o las canalizaciones de CI/CD. A continuación, a medida que va implementando una carga de trabajo en entornos de prueba y entrenamiento y de producción, puede comprobar la configuración con la infraestructura nativa de AWS, el código abierto o las herramientas de socios de AWS. Estas comprobaciones pueden realizarse en una configuración que no cumple con los principios de seguridad ni con las prácticas recomendadas, o en los cambios que se realizaron entre una configuración probada y una implementada. En una aplicación que se está ejecutando puede comprobar si la configuración se ha cambiado de una forma inesperada, como, por ejemplo, un cambio que no guarda relación con una implementación conocida ni con un evento de escalado automatizado.

En el segundo caso, comportamientos inesperados, puede utilizar herramientas o establecer alertas para avisar de un aumento de un tipo determinado de llamada a la API. Al utilizar Amazon GuardDuty, podrá recibir alertas cuando se produzca una actividad inesperada y posiblemente no autorizada o malintencionada en las cuentas de AWS. También debería supervisar de forma explícita las llamadas a la API mutantes que se supone que no deben utilizarse en la carga de trabajo, así como las llamadas a la API que cambian el nivel de seguridad.

La detección le permite identificar una posible configuración errónea de la seguridad, amenazas o comportamientos inesperados. Es parte fundamental del ciclo de vida de la 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. Hay distintos tipos de mecanismos de detección. Por ejemplo, se pueden analizar los registros de la carga de trabajo en busca de vulnerabilidades de seguridad. Debe revisar periódicamente los mecanismos de detección relacionados con la carga de trabajo con el fin de garantizar que cumple con las políticas y los requisitos internos y externos. Las notificaciones y alertas automatizadas deben basarse en condiciones definidas para permitir que los equipos o las herramientas lleven a cabo investigaciones. Estos mecanismos son factores reactivos importantes que ayudan a la organización a identificar la actividad anómala y comprender sus repercusiones.

En AWS existen varios enfoques distintos que puede utilizar en relación con los mecanismos de detección. En las siguientes secciones se describe cómo se usan estos enfoques:

Prácticas recomendadas

- SEC04-BP01 Configurar el registro de servicios y aplicaciones
- SEC04-BP02 Análisis centralizados de registros, hallazgos y métricas
- SEC04-BP03 Automatizar la respuesta a eventos
- SEC04-BP04 Implementar eventos de seguridad procesables

SEC04-BP01 Configurar el 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 forma fiable y uniforme los registros de eventos de seguridad de los servicios y aplicaciones de AWS en el momento oportuno cuando sea necesario realizar un proceso o cumplir una obligación interna (por ejemplo, la respuesta a un incidente de seguridad). Considere la posibilidad de centralizar los registros para obtener mejores resultados operativos.

Antipatrones usuales:

- Los registros se almacenan para siempre o se eliminan 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.

Ventajas de esta práctica recomendada: implementar un mecanismo de análisis de causa raíz (RCA) para los incidentes de seguridad y una fuente de pruebas para 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, habilitar, almacenar y configurar mecanismos de consulta y recuperación, así como de alerta.

Pasos para la implementación

- Seleccione y habilite las fuentes de registro. Antes de una investigación de seguridad, necesita obtener los registros relevantes para reconstruir de forma reatroctiva la actividad que se ha producido en una Cuenta de AWS. Seleccione y habilite 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 realizan en una Cuenta de AWS y captura la actividad de los servicios de AWS. Está habilitado de manera predeterminada y retiene durante 90 días los eventos de administración que se pueden recuperar a través del historial de eventos de CloudTrail mediante la AWS Management Console, la AWS CLI o un SDK de AWS. Si desea una retención y una visibilidad de los eventos de datos mayores, cree un registro de seguimiento de CloudTrail y asócielo a un bucket de Amazon S3 y, opcionalmente, a un grupo de registros de Amazon CloudWatch. Como alternativa, puede crear un CloudTrail Lake, que retiene los registros de CloudTrail hasta siete años y dispone de una utilidad de consulta basada en SQL.

  AWS recomienda a los clientes que utilizan una VPC que habiliten los registros del tráfico de red y de DNS mediante los registros de flujo de VPC y los registros de consultas de solucionador de Amazon Route 53, respectivamente, y que los transmitan por streaming 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 costes.

  Los registros de AWS CloudTrail, los registros de flujo de VPC y los registros de consulta del solucionador de Route 53 son las fuentes de registros básicas que facilitan las investigaciones

de seguridad en AWS. También puede utilizar Amazon Security Lake para recopilar, normalizar y almacenar estos datos de registros en los formatos Apache Parquet y Open Cybersecurity Schema Framework (OCSF), que están listos para su consulta. Security Lake también admite otros registros de AWS y registros de fuentes 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 hallazgos 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 Appendix A: Cloud capability definitions – Logging and Events (Apéndice A: Definiciones de las capacidades de la nube - Registro y eventos) de AWS Security Incident Response Guide (Guía de respuesta a incidentes de seguridad de AWS).

- Investigue las capacidades de registro de cada servicio y aplicación de AWS: cada servicio y aplicación de AWS le proporciona 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 Amazon CloudWatch Logs, quizá debería considerar la posibilidad de archivar los registros a los que se accede con menos frecuencia en Amazon S3.
- Seleccione el 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 con él y el coste. Las principales opciones para el almacenamiento de registros son un bucket de Amazon S3 o un grupo de CloudWatch Log.

  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 CloudWatch Logs ofrece un almacenamiento duradero y una utilidad de consulta integrada a través de CloudWatch Logs Insights.
- Identifique un periodo de retención de registros adecuado: cuando utilice un bucket de Amazon S3 o un grupo de CloudWatch Logs para almacenar registros, deberá establecer ciclos de vida adecuados para cada fuente de registros con el fin de optimizar los costes 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.

- Habilite el 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 registro específica:
  - Configuración de registros de seguimiento de AWS CloudTrail
  - Configuración de registros de flujo de VPC
  - Configuración de exportaciones de hallazgos 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 del solucionador de Amazon Route 53
  - Configuración de registros de Amazon RDS
  - Configuración de registros del plano de control de Amazon EKS
  - Configuración del agente de Amazon CloudWatch para instancias de Amazon EC2 y servidores locales
- Seleccione e implemente mecanismos de consulta para los registros: para las consultas de registros, puede utilizar CloudWatch Logs Insights para los datos almacenados en los grupos de CloudWatch Logs 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 costes.

  Por ejemplo, podría utilizar una herramienta de administración de eventos e información de seguridad (SIEM) de terceros para realizar consultas en los últimos 90 días de datos, pero utilizar Athena para realizar consultas anteriores a esos 90 días debido al coste 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.

- Utilice registros para las alertas: AWS proporciona alertas a través de varios servicios de seguridad:
  - AWS Config supervisa y registra las configuraciones de sus recursos de AWS y le permite automatizar la evaluación y la corrección con respecto a las configuraciones deseadas.
  - Amazon GuardDuty es un servicio de detección de amenazas que supervisa continuamente la actividad maliciosa y el comportamiento no autorizado para proteger sus Cuentas de AWS y cargas de trabajo. GuardDuty ingiere, agrega y analiza información de fuentes, como eventos de administración y datos de AWS CloudTrail, registros DNS, registros de flujo de VPC y registros de auditoría de Amazon EKS. GuardDuty extrae secuencias 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 proporciona un único lugar en el que se agregan, organizan y priorizan las alertas de seguridad, o los hallazgos, desde varios servicios de AWS y productos de terceros opcionales 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 la creación de estas alertas y detecciones, consulte Detection (Detección) en AWS Security Incident Response Guide (Guía de respuesta a incidentes de seguridad de AWS).

Recursos

Prácticas recomendadas relacionadas:

- SEC04-BP02 Análisis centralizados de registros, hallazgos y métricas
- SEC07-BP04 Definir la administración del ciclo de vida de los datos
- SEC10-BP06: Desplegar las herramientas con anticipación

Documentos relacionados:

- AWS Security Incident Response Guide (Guía de respuesta ante incidentes de seguridad de AWS)

- Cómo comenzar a utilizar Amazon Security Lake
- Introducción a Amazon CloudWatch Logs
- Soluciones de socios de seguridad: registro y monitorización

Vídeos relacionados:

- AWS re:Invent 2022 - Introducing Amazon Security Lake (re:Invent 2022: Introducción a Amazon Security Lake)

Ejemplos relacionados:

- Assisted Log Enabler for AWS(Habilitador de registro asistido para AWS)
- AWS Security Hub Findings Historical Export (Exportación de hallazgos históricos de AWS Security Hub)

Herramientas relacionadas:

- Snowflake for Cybersecurity

SEC04-BP02 Análisis centralizados de registros, hallazgos y métricas

Los equipos de operaciones de seguridad confían en la recopilación de registros y el uso de herramientas de búsqueda para descubrir posibles eventos de interés, que podrían indicar una actividad no autorizada o un cambio no intencionado. Sin embargo, solo con analizar los datos recopilados y procesar manualmente la información no basta para satisfacer el volumen de información procedente de arquitecturas complejas. Solo con los análisis y los informes no se facilita la asignación de los recursos adecuados para trabajar en un evento a tiempo.

Una práctica recomendada para crear un equipo de operaciones de seguridad eficaz es integrar en profundidad el flujo de hallazgos y eventos de seguridad en un sistema de flujo de trabajo y notificación, como un sistema de emisión de tiques, un sistema de errores o problemas u otro sistema de administración de eventos e información de seguridad (SIEM, por sus siglas en inglés). De esta forma, se saca el flujo de trabajo de informes estáticos y de correo electrónico, y le permite enrutar, escalar y administrar eventos o hallazgos. Numerosas organizaciones ya integran también

alertas de seguridad en sus plataformas de productividad de desarrolladores, de colaboración o de chats. Para las organizaciones que estén comenzando a incorporar la automatización, un sistema de tickets de baja latencia basado en API ofrece una flexibilidad considerable al planificar qué automatizar primero.

Esta práctica recomendada no se aplica solo a los eventos de seguridad generados a partir de mensajes de registro que muestran eventos de red o actividad del usuario, sino también a partir de cambios detectados en la propia infraestructura. La capacidad de detectar cambios, determinar su conveniencia y luego enrutar esa información al flujo de trabajo de corrección adecuado resulta esencial para mantener y validar una arquitectura segura en el contexto de los cambios en los que la naturaleza de su indeseabilidad es lo suficientemente sutil como para que su ejecución no pueda evitarse actualmente con una combinación de configuraciones de AWS Identity and Access Management (IAM) y AWS Organizations.

Amazon GuardDuty y AWS Security Hub ofrecen mecanismos de agregación, desduplicación y análisis para los registros que también están disponibles mediante otros servicios de AWS. GuardDuty ingiere, agrega y analiza información de fuentes como eventos de administración y datos de AWS CloudTrail, registros DNS de VPC y registros de flujo de VPC. Security Hub puede ingerir, agregar y analizar los resultados de GuardDuty, AWS Config, Amazon Inspector, Amazon Macie y AWS Firewall Manager, y un número significativo de productos de seguridad de terceros disponibles en AWS Marketplace y, si está convenientemente compilado, su propio código. Tanto GuardDuty como Security Hub tienen un modelo de administrador-miembro que puede combinar los hallazgos y los conocimientos de varias cuentas, los clientes con un SIEM local suelen utilizar Security Hub como registro del lado de AWS y un preprocesador y agregador de alertas a partir del que pueden ingerir Amazon EventBridge mediante un procesador y reenviador basado en AWS Lambda.

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

Guía para la implementación

- Evaluar las capacidades de procesamiento de registros: evalúe de las opciones disponibles para procesar registros.
  - Usar Amazon OpenSearch Service para registrar y supervisar (casi) todo
  - Búsqueda de un socio especializado en soluciones de registro y monitoreo
- Como punto de partida para el análisis de registros de CloudTrail, pruebe con Amazon Athena.
  - Configuración de Athena para analizar registros de CloudTrail

- Implementar el registro centralizado en AWS: consulte la siguiente solución de ejemplo de AWS para centralizar el registro procedente de varias fuentes.
  - Solución de centralización de registros
- Implementar el registro centralizado con un socio: los socios de APN tienen soluciones que le ayudarán a analizar los registros de forma centralizada.
  - Registro y supervisión

Recursos

Documentos relacionados:

- Soluciones de AWS: registro centralizado
- AWS Security Hub
- Amazon CloudWatch
- Amazon EventBridge
- Introducción: Amazon CloudWatch Logs
- Soluciones de socios de seguridad: registro y monitorización

Vídeos relacionados:

- Supervisión centralizada de la configuración de recursos y el cumplimiento
- Corrección de los hallazgos de Amazon GuardDuty y AWS Security Hub
- Administración de amenazas en la nube: Amazon GuardDuty y AWS Security Hub

SEC04-BP03 Automatizar la respuesta a eventos

El uso de la automatización para investigar y corregir eventos reduce el esfuerzo y los posibles errores humanos, y le permite escalar sus capacidades de investigación. Las revisiones frecuentes le ayudarán a ajustar sus herramientas de automatización y a aplicar iteraciones continuas.

En AWS, la investigación de eventos de interés y la información sobre cambios potencialmente inesperados en un flujo de trabajo automatizado se pueden lograr con Amazon EventBridge. Este servicio ofrece un motor de reglas escalable diseñado para gestionar tanto formatos de eventos nativos de AWS (p. ej., eventos de AWS CloudTrail) como eventos personalizados que puede generar a partir de su aplicación. Amazon GuardDuty también le permite enrutar eventos a un

sistema de flujo de trabajo para esos sistemas de respuesta a incidentes de creación (AWS Step Functions) o a una cuenta de seguridad centralizada, o a un bucket para seguir analizándolos.

La detección de cambios y el enrutamiento de esta información al flujo de trabajo correcto también se puede llevar a cabo utilizando Reglas de AWS Config y paquetes de conformidad. AWS Config detecta cambios en los servicios del ámbito (aunque con una mayor latencia que EventBridge) y genera eventos que se pueden analizar con Reglas de AWS Config para restaurar, aplicar la política de conformidad y reenviar información a sistemas, como plataformas de administración de cambios y sistemas de emisión de tiques operativos. Además de escribir sus propias funciones de Lambda para responder a eventos de AWS Config, puede utilizar el kit de desarrollo de Reglas de AWS Configy una biblioteca de código abierto Reglas de AWS Config. Los paquetes de conformidad son una colección de Reglas de AWS Config y acciones de corrección que se despliegan como una entidad única elaborada como una plantilla YAML. A plantilla de paquete de conformidad de ejemplo está disponible para el pilar de seguridad del modelo Well-Architected.

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

Guía para la implementación

- Implementar alertas automatizadas con GuardDuty: GuardDuty es un servicio de detección de amenazas que supervisa sin descanso cualquier actividad malintencionada o comportamiento no autorizado para proteger sus cargas de trabajo y sus Cuentas de AWS. Active GuardDuty y configure alertas automatizadas.
- Automatizar los procesos de investigación: desarrolle procesos automatizados que investiguen un evento y envíen la información a un administrador para ganar tiempo.
  - Laboratorio: experiencia práctica con Amazon GuardDuty

Recursos

Documentos relacionados:

- Soluciones de AWS: registro centralizado
- AWS Security Hub
- Amazon CloudWatch
- Amazon EventBridge
- Introducción: Amazon CloudWatch Logs
- Soluciones de socios de seguridad: registro y monitorización

- Configuración de Amazon GuardDuty

Vídeos relacionados:

- Supervisión centralizada de la configuración de recursos y el cumplimiento
- Corrección de los hallazgos de Amazon GuardDuty y AWS Security Hub
- Administración de amenazas en la nube: Amazon GuardDuty y AWS Security Hub

Ejemplos relacionados:

- Laboratorio: Despliegue automatizado de controles de detección

SEC04-BP04 Implementar eventos de seguridad procesables

Cree alertas que se envíen a su equipo y que este pueda actuar sobre ellas. Asegúrese de que las alertas incluyen información relevante para que el equipo pueda actuar. Para cada mecanismo de detección que tenga, también debería tener un proceso, en forma de runbook o bien manual, para realizar la investigación. Por ejemplo, cuando se activa Amazon GuardDuty, se generan diferentes resultados. Debe tener una entrada de runbook para cada tipo de resultado, por ejemplo, si se detecta un troyano , su runbook tiene instrucciones simples que indican a alguien que debe investigarlo y solucionarlo.

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

Guía para la implementación

- Descubra las métricas disponibles para los servicios de AWS: descubra las métricas disponibles a través de Amazon CloudWatch para los servicios que está utilizando.
  - Documentación de servicio de AWS
  - Uso de métricas de Amazon CloudWatch
- Configure las alarmas de Amazon CloudWatch.
  - Uso de alarmas de Amazon CloudWatch

Recursos

Documentos relacionados:

- Amazon CloudWatch
- Amazon EventBridge
- Soluciones de socios de seguridad: registro y monitorización

Vídeos relacionados:

- Centrally Monitoring Resource Configuration and Compliance (Supervisión centralizada de la configuración de recursos y el cumplimiento)
- Remediating Amazon GuardDuty and AWS Security Hub Findings (Corrección de los resultados de Amazon GuardDuty y AWS Security Hub)
- Threat management in the cloud: Amazon GuardDuty and AWS Security Hub (Administración de amenazas en la nube: Amazon GuardDuty y AWS Security Hub)

Protección de la infraestructura

La protección de la infraestructura abarca las metodologías de control, como la defensa en profundidad, que son necesarias para ajustarse a las prácticas recomendadas y las obligaciones organizativas o normativas. El uso de estas metodologías es fundamental para el éxito de las operaciones en curso 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 protección, minimización e 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 conocer bien las regiones, las zonas de disponibilidad, las zonas locales de AWSy AWS Outposts, que componen la infraestructura segura global de AWS.

AWS tiene el concepto de una región, que es una ubicación física en todo el mundo donde agrupamos centros de datos. Cada grupo de centros de datos lógicos se denomina zona de disponibilidad (AZ). Cada región de AWS consta de varias AZ aisladas y físicamente separadas dentro de un área geográfica. Si cuenta con requisitos de residencia de datos, puede elegir la región de AWS que esté cerca a la ubicación que desee. Usted conserva el control y la propiedad absolutos de la región donde se encuentran físicamente sus datos, lo cual puede ser útil para cumplir los requisitos regionales de conformidad y residencia de datos. Cada AZ dispone de seguridad física, refrigeración y alimentación eléctrica independientes. Si una aplicación está particionada en varias AZ, estará mejor aislado y contará con mayor protección frente a problemas como interrupciones de alimentación eléctrica, tormentas eléctricas, tornados, terremotos, etc. Las AZ están físicamente separadas por una distancia considerable, a muchos kilómetros de cualquier otra AZ, aunque todas se encuentran a unos 100 km (60 millas) las unas de las otras. 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 AZ. Todo el tráfico entre las AZ está cifrado. Los clientes de AWS que se centran en la alta disponibilidad pueden diseñar sus aplicaciones para que se ejecuten en varias AZ

con el fin de lograr una mejor tolerancia a los errores. Las regiones de AWS cumplen los niveles más altos de seguridad, conformidad y protección de datos.

Las zonas locales de AWS permiten que los usuarios finales accedan más fácilmente a servicios de computación, almacenamiento, bases de datos y otros servicios de AWS. Con las zonas locales de AWS, puede ejecutar fácilmente aplicaciones muy exigentes que requieren latencias inferiores a 10 milisegundos para los usuarios finales, como creación de contenido multimedia y de entretenimiento, juegos en tiempo real, simulaciones de yacimientos, automatización de diseños electrónicos y machine learning. Cada ubicación de zona local de AWS es una extensión de una región de AWS donde puede ejecutar aplicaciones sensibles a la latencia mediante servicios de AWS, tales como Amazon EC2, Amazon VPC, Amazon EBS, Amazon File Storage y Elastic Load Balancing, en zonas geográficas próximas a los usuarios finales. Las zonas locales de AWS ofrecen ancho de banda alto y conexión segura 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 en la región a través de los mismos conjuntos de herramientas y API.

AWS Outposts incorpora servicios nativos de AWS, infraestructura y modelos operativos en prácticamente cualquier centro de datos, espacio de coubicación o instalaciones locales. Puede utilizar las mismas infraestructuras, herramientas y API de AWS en instalaciones locales y en la nube de AWS para ofrecer una experiencia híbrida verdaderamente coherente. AWS Outposts se ha diseñado para entornos conectados y se puede utilizar para admitir cargas de trabajo que deben permanecer en las instalaciones con el fin de hacer frente a necesidades de baja latencia o procesamiento de datos locales.

En AWS, hay diferentes enfoques para la protección de infraestructuras. En las siguientes secciones se describe cómo se usan estos enfoques.

Temas

Protección de redes

Los usuarios, tanto los que forman parte del personal y los clientes, pueden encontrarse en cualquier lugar. Debe hacer un cambio y dejar a un lado los modelos tradicionales que confían en todos los usuarios y aplicaciones que tengan acceso a la red. Cuando sigue el principio de aplicar seguridad

en todos los niveles, está adoptando un enfoque de confianza cero . La seguridad Confianza cero es un modelo en el que los microservicios o componentes de una aplicación se consideran independientes entre ellos y ningún componente ni microservicio confían los unos de los otros.

La administración y planificación minuciosas del diseño de red conforma la base del modo de aislar y limitar los recursos en la carga de trabajo. Dado que un gran número de recursos de la carga de trabajo funcionan en una VPC y heredan las propiedades de seguridad, es fundamental que el diseño cuente con mecanismos de inspección y protección respaldados por procesos de automatización. Asimismo, en el caso de las cargas de trabajo que funcionan fuera de una VPC, que utilizan servicios fundamentalmente periféricos o sin servidor, se utilizará un enfoque más simplificado. Consulte el documento Enfoque de aplicaciones sin servidor para AWS Well-Architected Framework para obtener información sobre la seguridad sin servidor.

Prácticas recomendadas

- SEC05-BP01 Crear capas de red
- SEC05-BP02 Controlar el tráfico en todas las capas
- SEC05-BP03 Automatizar la protección de la red
- SEC05-BP04 Implementar inspección y protección

SEC05-BP01 Crear capas de red

Agrupe por capas los componentes que tienen los mismos requisitos de confidencialidad para minimizar el alcance potencial del impacto de un acceso no autorizado. Por ejemplo, un clúster de base de datos que está en una nube virtual privada (VPC) y no necesita acceso a Internet debe colocarse en subredes sin enrutamiento hacia Internet o desde Internet. El tráfico solo debe salir desde el siguiente recurso adyacente menos confidencial. Supongamos que tiene una aplicación web detrás de un equilibrador de carga. Su base de datos no debería ser accesible directamente desde este equilibrador de carga. Solo deberían tener acceso directo a su base de datos la lógica empresarial o el servidor web.

Resultado deseado: crear una red en capas. Las redes en capas ayudan a agrupar de forma lógica componentes de red similares. También reducen el alcance potencial del impacto que supondría un acceso no autorizado a la red. Una red que se haya configurado por capas de la forma adecuada hace más difícil que los usuarios no autorizados se dirijan a recursos adicionales dentro de su entorno de AWS. Además de asegurar las rutas de red internas, también debe proteger la periferia de su red, como las aplicaciones web y los puntos de conexión de API.

Antipatrones usuales:

- Crear todos los recursos en una única VPC o subred.
- Utilizar grupos de seguridad demasiado permisivos.
- No utilizar subredes.
- Permitir el acceso directo a almacenes de datos como bases de datos.

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

Guía para la implementación

Los componentes como instancias Amazon Elastic Compute Cloud (Amazon EC2), clústeres de base de datos de Amazon Relational Database Service (Amazon RDS) y funciones AWS Lambda que comparten requisitos de accesibilidad pueden segmentarse en capas formadas por subredes. Considere la posibilidad de desplegar cargas de trabajo sin servidor, como funciones Lambda, dentro de una VPC o detrás de un Amazon API Gateway. Las tareas de AWS Fargate (Fargate) que no tengan la necesidad de acceder a Internet deben colocarse en subredes sin una ruta hacia o desde Internet. Este enfoque por capas mitiga el impacto de una configuración errónea de una sola capa, que podría permitir un acceso no intencionado. Para AWS Lambda, puede ejecutar sus funciones en su VPC a fin de aprovechar los controles basados en VPC.

Si la conectividad de red incluye miles de VPC, Cuentas de AWS y redes locales, debe utilizar AWS Transit Gateway. Transit Gateway actúa como un centro que controla cómo se enruta el tráfico entre todas las redes conectadas, que actúan como radios. El tráfico entre Amazon Virtual Private Cloud (Amazon VPC) y Transit Gateway permanece en la red privada de AWS, lo que reduce la exposición externa a usuarios no autorizados y a posibles problemas de seguridad. El emparejamiento interregional de Transit Gateway también cifra el tráfico interregional sin ningún punto único de fallo ni cuello de botella en el ancho de banda.

Pasos para la implementación

- Utilice Reachability Analyzer para analizar la ruta entre un origen y un destino en función de la configuración: Reachability Analyzer le permite automatizar la verificación de la conectividad hacia y desde los recursos conectados a la VPC. Tenga en cuenta que, para realizar este análisis, se revisa la configuración (no se envían paquetes de red).
- Utilice el analizador de acceso de la red de Amazon VPC para identificar el acceso no intencionado de la red a los recursos: el analizador de acceso de la red de Amazon VPC le permite especificar sus requisitos de acceso a la red e identificar posibles rutas de la red.

- Considere si es necesario que los recursos se encuentren en una subred pública: no coloque recursos en subredes públicas de su VPC a menos que sea absolutamente necesario que reciban tráfico de red de fuentes públicas.
- Cree subredes en sus VPC: cree subredes para cada capa de red (en grupos que incluyan varias zonas de disponibilidad) para mejorar la microsegmentación. Compruebe también que ha asociado las tablas de enrutamiento correctas con sus subredes para controlar el enrutamiento y la conectividad a Internet.
- Utilice AWS Firewall Manager para administrar sus grupos de seguridad de VPC: AWS Firewall Manager ayuda a disminuir la carga de administración que supone el uso de varios grupos de seguridad.
- Utilice AWS WAF para protegerse contra vulnerabilidades web comunes: AWS WAF puede ayudar a mejorar la seguridad de la periferia inspeccionando el tráfico en busca de vulnerabilidades web comunes, como la inyección de código SQL. También le permite restringir el tráfico de direcciones IP procedentes de determinados países o ubicaciones geográficas.
- Utilice Amazon CloudFront como red de distribución de contenido (CDN): Amazon CloudFront puede ayudarle a acelerar su aplicación web al almacenar los datos más cerca de sus usuarios. También puede mejorar la seguridad de la periferia al utilizar HTTPS, restringir el acceso a zonas geográficas y garantizar que el tráfico de red solo pueda acceder a los recursos cuando se enrute a través de CloudFront.
- Utilice Amazon API Gateway cuando cree interfaces de programación de aplicaciones (API):Amazon API Gateway ayuda a publicar, supervisar y proteger las API de REST, HTTPS y WebSocket.

Recursos

Documentos relacionados:

- AWS Firewall Manager
- Amazon Inspector
- Seguridad de Amazon VPC
- Reachability Analyzer
- Amazon VPC Network Access Analyzer (Analizador de acceso de la red de Amazon Virtual Private Cloud)

Vídeos relacionados:

- AWS Transit Gateway reference architectures for many VPCs (Arquitecturas de referencia de AWS Transit Gateway para muchas VPC)
- Application Acceleration and Protection with Amazon CloudFront, AWS WAF, and AWS Shield (Aceleración y protección de aplicaciones con Amazon CloudFront, AWS WAF y AWS Shield)
- AWS re:Inforce 2022 - Validate effective network access controls on AWS (re:Inforce 2022: Validar la eficacia de los controles de acceso a la red en AWS)
- AWS re:Inforce 2022 - Advanced protections against bots using AWS WAF(re:Inforce 2022: Protecciones avanzadas contra bots con AWS WAF)

Ejemplos relacionados:

- Well-Architected Lab - Automated Deployment of VPC (Laboratorio de Well-Architected: Despliegue automatizado de VPC)
- Taller: Amazon VPC Network Access Analyzer (Analizador de acceso de la red de Amazon VPC)

SEC05-BP02 Controlar el tráfico en todas las capas

Al diseñar su topología de red, debería examinar los requisitos de conectividad de cada componente. Por ejemplo, si un componente requiere accesibilidad a Internet (entrante y saliente), conectividad a las VPC, servicios en la periferia y centros de datos externos.

Una VPC le permite definir su topología de red que abarca una Región de AWS, con un rango de direcciones IPv4 privadas que puede configurar o un rango de direcciones IPv6 que selecciona AWS. Debe aplicar 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 (firewall de inspección con estado), ACL de red, subredes y tablas de enrutamiento. Puede crear subredes en una zona de disponibilidad de una VPC. Cada subred puede tener una tabla de enrutamiento asociada que define las reglas para administrar las rutas que sigue el tráfico de la subred. Puede definir una subred que se pueda enrutar en Internet con una ruta que se dirija a una puerta de enlace de Internet o NAT asociada a la VPC o mediante otra VPC.

Cuando una instancia, una base de datos de Amazon Relational Database Service (Amazon RDS) u otro servicio se lanza en una VPC, tiene su propio grupo de seguridad por interfaz de red. Este firewall está situado fuera de la capa del sistema operativo y se puede usar para definir reglas sobre el tráfico entrante y saliente permitido. También puede definir las relaciones entre grupos de seguridad. Por ejemplo, las instancias de un grupo de seguridad de nivel de base de datos solo

aceptan tráfico de instancias de nivel de aplicación, según la referencia de los grupos de seguridad aplicados a las instancias implicadas. A no ser que utilice protocolos que no sean TCP, no debería ser necesario disponer de una instancia de Amazon Elastic Compute Cloud (Amazon EC2) que sea directamente accesible desde Internet (ni siquiera con puertos restringidos por grupos de seguridad) sin un equilibrador de carga o CloudFront. Esto ayuda en la protección ante el acceso no intencionado debido a un problema con el sistema operativo o la aplicación. Una subred también puede tener una ACL de red asociada, que actúa como firewall sin estado. Debería configurar la ACL de red para que estreche el ámbito del tráfico permitido entre capas; tenga en cuenta que tiene que definir reglas tanto para el tráfico entrante como para el saliente.

Algunos servicios de AWS requieren que los componentes accedan a Internet para realizar llamadas a la API, donde están ubicados los puntos de conexión de la API de AWS . Otros servicios de AWS usan Puntos de enlace de la VPC en sus Amazon VPC. Muchos servicios de AWS, incluidos Amazon S3 y Amazon DynamoDB, son compatibles con los puntos de conexión de VPC, y esta tecnología se ha generalizado en AWS PrivateLink. Le recomendamos que utilice este enfoque para acceder a servicios de AWS, servicios de terceros y sus propios servicios alojados en otras VPC de forma segura. Todo el tráfico de red de AWS PrivateLink permanece en la estructura global de AWS y nunca pasa por Internet. La conectividad solamente la puede iniciar el consumidor del servicio y no el proveedor de este. El uso de AWS PrivateLink para el acceso de un servicio externo le permite crear VPC aisladas por espacios vacíos sin acceso a Internet y ayuda a proteger sus VPC de vectores de amenaza externos. Los servicios de terceros pueden usar AWS PrivateLink para permitir que sus clientes se conecten a los servicios de sus VPC a través de direcciones IP privadas. Para activos de VPC que necesiten realizar conexiones salientes a Internet, se pueden establecer para que sean solo salientes (unidireccionales) mediante una puerta de enlace NAT administrada por AWS, puertas de enlace de Internet solo salientes o proxies web que cree y administre.

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

Guía para la implementación

- Controlar el tráfico de web en una VPC: implemente prácticas recomendadas de VPC para controlar el tráfico.
  - Seguridad de Amazon VPC
  - Puntos de enlace de la VPC
  - Grupo de seguridad de Amazon VPC
  - ACL de red

- Controlar el tráfico en la periferia: implemente servicios en la periferia, como Amazon CloudFront, para proporcionar una capa adicional de protección y otras características.
  - Casos de uso de Amazon CloudFront
  - AWS Global Accelerator
  - Firewall para aplicaciones web de AWS (AWS WAF)
  - Amazon Route 53
  - Enrutamiento de entrada de Amazon VPC
- Controlar el tráfico de red privado: implemente servicios que protejan el tráfico privado para su carga de trabajo.
  - Interconexión de Amazon VPC
  - Servicios de punto de conexión de Amazon VPC (AWS PrivateLink)
  - Amazon VPC Transit Gateway
  - AWS Direct Connect
  - AWS Site-to-site VPN
  - AWS Client VPN
  - Puntos de acceso de Amazon S3

Recursos

Documentos relacionados:

- AWS Firewall Manager
- Amazon Inspector
- Introducción a AWS WAF

Vídeos relacionados:

- Arquitecturas de referencia de AWS Transit Gateway para muchas VPC
- Aceleración y protección de aplicaciones con Amazon CloudFront, AWS WAF y AWS Shield

Ejemplos relacionados:

- Laboratorio: Despliegue automatizado de VPC

SEC05-BP03 Automatizar la protección de la red

Automatice los mecanismos de protección para proporcionar una red de autodefensa basada en la inteligencia de amenazas y la detección de anomalías. Por ejemplo, las herramientas de detección y prevención de intrusiones que puedan adaptarse a las amenazas actuales y reducir su impacto. Un firewall de una aplicación web es un ejemplo de dónde puede automatizar la protección de la red, por ejemplo, utilizando la solución AWS WAF Security Automations (https://github.com/awslabs/aws-waf-security-automations) para bloquear automáticamente las solicitudes que se originen en direcciones IP asociadas con actores de amenazas conocidos.

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

Guía para la implementación

- Automatice la protección para el tráfico basado en la web: AWS ofrece una solución que utiliza AWS CloudFormation para desplegar automáticamente un conjunto de reglas de AWS WAF diseñadas para filtrar ataques basados en web frecuentes. Los usuarios pueden seleccionar entre funciones de protección preconfiguradas que definen las reglas incluidas en una lista de control de acceso web de AWS WAF (ACL web).
  - Automatizaciones de seguridad de AWS WAF
- Plantéese soluciones de AWS Partner: los socios de AWS ofrecen cientos de productos destacados que son equivalentes o idénticos a los controles que ya utiliza en sus entornos locales o que pueden integrarse con ellos. Estos productos complementan a los servicios de AWS existentes y le permiten implementar una completa arquitectura de seguridad, así como disfrutar de una experiencia más coherente tanto en la nube como en los entornos locales.
  - Seguridad de la infraestructura

Recursos

Documentos relacionados:

- AWS Firewall Manager
- Amazon Inspector
- Seguridad del Amazon VPC
- Introducción a AWS WAF

Videos relacionados:

- Arquitecturas de referencia de AWS Transit Gateway para muchas VPC
- Aceleración y protección de aplicaciones con Amazon CloudFront, AWS WAF y AWS Shield

Ejemplos relacionados:

- Laboratorio: Despliegue automatizado de VPC

SEC05-BP04 Implementar inspección y protección

Inspeccione y filtre el tráfico en cada capa. Puede inspeccionar las configuraciones de VPC para buscar posibles accesos no deseados mediante Analizador de acceso de red de VPC. Puede especificar los requisitos de acceso a la red e identificar las posibles rutas de red que no los cumplan. En el caso de los componentes que realizan transacciones a través de protocolos basados en HTTP, un firewall de aplicaciones web puede ayudar a protegerlos de los ataques más habituales. AWS WAF es un firewall de aplicaciones web que le permite supervisar y bloquear las solicitudes HTTP(s) que coincidan con sus reglas configurables y que se reenvíen a una API de Amazon API Gateway, Amazon CloudFront o un Application Load Balancer. Para empezar con AWS WAF, puede usar Reglas administradas de AWS en combinación con sus propias integraciones socios o utilizar las existentes.

Para administrar AWS WAF, las protecciones de AWS Shield Advanced y los grupos de seguridad de Amazon VPC en AWS Organizations, puede utilizar AWS Firewall Manager. Le permite configurar y administrar de forma centralizada las reglas de firewall en todas sus cuentas y aplicaciones, lo que facilita escalar la aplicación de las reglas comunes. También le permite responder rápidamente a los ataques, con AWS Shield Advancedo soluciones que puede bloquear automáticamente las solicitudes no deseadas a sus aplicaciones web. Firewall Manager también funciona con AWS Network Firewall. AWS Network Firewall es un servicio administrado que utiliza un motor de reglas para ofrecerle un control detallado del tráfico de red con estado y sin estado. Es compatible con las especificaciones del sistema de prevención de intrusiones (IPS) de código abierto compatibles con Suricata para ayudar a proteger su carga de trabajo.

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

Guía para la implementación

- Configure Amazon GuardDuty: GuardDuty es un servicio de detección de amenazas que supervisa sin descanso cualquier actividad malintencionada o comportamiento no autorizado para proteger sus cargas de trabajo y sus Cuentas de AWS. Active GuardDuty y configure alertas automatizadas.
  - Amazon GuardDuty
  - Laboratorio: Despliegue automatizado de controles de detección
- Configure los registros de flujo de nube virtual privada (VPC): la característica de registros de flujo de VPC permite registrar información acerca del tráfico IP que entra y sale de las interfaces de red en la VPC. Los datos de registro de flujo se pueden publicar en Amazon CloudWatch Logs y Amazon Simple Storage Service (Amazon S3). Cuando cree un registro de flujo, podrá recuperar y ver sus datos en el destino elegido.
- Considere el reflejo de tráfico de VPC: el reflejo de tráfico es una característica de Amazon VPC que puede utilizar para copiar el tráfico de red de una interfaz de red elástica de instancias de Amazon Elastic Compute Cloud (Amazon EC2) y, a continuación, enviarlo a dispositivos de seguridad y supervisión fuera de banda para la inspección de contenido, la supervisión de amenazas y la resolución de problemas.
  - Reflejo de tráfico de VPC

Recursos

Documentos relacionados:

- AWS Firewall Manager
- Amazon Inspector
- Seguridad de Amazon VPC
- Introducción a AWS WAF

Vídeos relacionados:

- AWS Transit Gateway reference architectures for many VPCs (Arquitecturas de referencia de AWS Transit Gateway para muchas VPC)
- Application Acceleration and Protection with Amazon CloudFront, AWS WAF, and AWS Shield (Aceleración y protección de aplicaciones con Amazon CloudFront, AWS WAF y AWS Shield)

Ejemplos relacionados:

- Laboratorio: Despliegue automatizado de VPC

Protección de recursos de computación

Entre los recursos de computación se incluyen instancias de EC2, contenedores, funciones de AWS Lambda, servicios de bases de datos, dispositivos IoT, etc. Cada uno de estos tipos de recursos de computación requieren distintos enfoques para protegerlos. No obstante, comparten estrategias comunes que debe tener en cuenta: defensa en profundidad, administración de vulnerabilidades, reducción de superficie expuesta a ataques, automatización de configuraciones y operaciones, y acciones realizadas a distancia. En esta sección encontrará orientación general para proteger los recursos de computación de los servicios clave. Es importante que consulte las recomendaciones específicas de seguridad en la documentación de cada servicio de AWS que utilice.

Prácticas recomendadas

- SEC06-BP01 Administrar las vulnerabilidades
- SEC06-BP02 Reducir la superficie expuesta a ataques
- SEC06-BP03 Implementar servicios administrados
- SEC06-BP04 Automatizar la protección informática
- SEC06-BP05 Permitir que los usuarios realicen acciones a distancia
- SEC06-BP06 Validar la integridad del software

SEC06-BP01 Administrar 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: crear y mantener un programa de administración de vulnerabilidades. Analice periódicamente recursos como las instancias de Amazon EC2, los contenedores de Amazon Elastic Container Service (Amazon ECS) y las cargas de trabajo de Amazon Elastic Kubernetes Service (Amazon EKS) y aplique parches en ellos. Configure periodos de mantenimiento para los recursos administrados por AWS, como las bases de datos de Amazon Relational Database Service (Amazon RDS). Utilice el análisis de código estático para inspeccionar el código fuente de las aplicaciones

en busca de problemas comunes. Considere la posibilidad de realizar pruebas de penetración en aplicaciones web si su organización cuenta con los conocimientos necesarios o puede contratar ayuda externa.

Antipatrones usuales:

- 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.
- Desplegar código en producción antes de analizarlo en busca de problemas de seguridad.

Beneficios de establecer esta práctica recomendada:

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

Guía para la implementación

Un programa de administración de vulnerabilidades incluye la evaluación de la seguridad, la identificación de problemas, el establecimiento de prioridades y la aplicación de parches como parte de la resolución de los problemas. La automatización es la clave para analizar continuamente las cargas de trabajo en busca de problemas y exposiciones no intencionadas a la red y para realizar correcciones. La automatización de la creación y actualización de recursos ahorra tiempo y reduce el riesgo de que los errores de configuración den lugar a más problemas. En un programa de administración de vulnerabilidades bien diseñado, también se debería considerar la realización de pruebas de vulnerabilidad durante las fases de desarrollo y despliegue del ciclo de vida del software. Implementar la administración de vulnerabilidades durante el desarrollo y el despliegue ayuda a disminuir la posibilidad de que una vulnerabilidad pueda abrirse camino en su entorno de producción.

Para implementar un programa de administración de vulnerabilidades, es necesario conocer bien el modelo de responsabilidad compartida de AWS y cómo se relaciona con sus cargas de trabajo específicas. En el modelo de responsabilidad compartida, AWS es responsable de proteger la infraestructura de la Nube de AWS. Esta infraestructura está compuesta por hardware, software, redes e instalaciones que ejecutan servicios de la Nube de AWS. Usted es responsable de la seguridad en la nube, por ejemplo, de los datos reales, de la configuración de seguridad y de las tareas de administración de las instancias de Amazon EC2, así como de verificar que sus objetos de Amazon S3 estén clasificados y configurados correctamente. Su enfoque de la administración de vulnerabilidades también puede variar en función de los servicios que consuma. Por ejemplo, AWS es quien administra la aplicación de parches de nuestro servicio de base de datos relacional

administrado, Amazon RDS, pero usted es el responsable de aplicar los parches en las bases de datos autoalojadas.

AWS dispone de numerosos servicios para ayudarle con su programa de administración de vulnerabilidades. Amazon Inspector analiza continuamente las cargas de trabajo de AWS en busca de problemas de software y accesos no intencionados a la red. AWS Systems Manager Patch Manager ayuda a administrar la aplicación de parches en todas sus instancias de Amazon EC2. Amazon Inspector y Systems Manager pueden consultarse en AWS Security Hub, un servicio de administración de la postura de seguridad en la nube que ayuda a automatizar las comprobaciones de seguridad de AWS y a centralizar las alertas de seguridad.

Amazon CodeGuru puede ayudar a identificar posibles problemas en las aplicaciones Java y Python mediante el análisis estático del código.

Pasos para la implementación

- Configure Amazon Inspector: Amazon Inspector detecta automáticamente las instancias de Amazon EC2 recién lanzadas, las funciones Lambda y las imágenes de contenedor elegibles que se envían a Amazon ECR y las analiza inmediatamente en busca de problemas del software, defectos potenciales y una exposición no intencionada a la red.
- Analice el código fuente: analice bibliotecas y dependencias en busca de problemas y defectos. Amazon CodeGuru puede analizar y proporcionar recomendaciones para corregir problemas de seguridad comunes tanto para aplicaciones Java como Python. La Fundación OWASP publica una lista de herramientas de análisis del código fuente (también conocidas como herramientas SAST).
- Implemente un mecanismo para analizar y aplicar parches en su entorno existente, así como para incluir el análisis como parte de un proceso de desarrollo de la canalización CI/CD: implemente un mecanismo para analizar y aplicar parches para solucionar los problemas en sus dependencias y sistemas operativos y protegerse contra nuevas amenazas. Haga que ese mecanismo se ejecute de forma regular. La administración de vulnerabilidades de software es esencial para saber dónde hay que aplicar parches o solucionar problemas del software. Dé prioridad a la corrección de los posibles problemas de seguridad incorporando evaluaciones de vulnerabilidad en una fase temprana de la canalización de la integración continua y entrega continua (CI/CD). Su enfoque puede variar en función de los servicios de AWS que consuma. Para buscar posibles problemas en el software que se ejecuta en instancias de Amazon EC2, añada Amazon Inspector a su canalización para que le avise y detenga el proceso de desarrollo si se detectan problemas o posibles defectos. Amazon Inspector supervisa continuamente los recursos. También puede utilizar productos de código abierto como OWASP Dependency-Check, Snyk,

OpenVAS, administradores de paquetes y herramientas de AWS Partner para la administración de vulnerabilidades.

- Utilice AWS Systems Manager: usted es el responsable de la administración de parches en sus recursos de AWS, incluidas las instancias de Amazon Elastic Compute Cloud (Amazon EC2), las imágenes de máquina de Amazon (AMI) y otros recursos de computación. AWS Systems Manager Patch Manager automatiza el proceso de aplicación de parches a instancias administradas con actualizaciones de seguridad y de otro tipo. Patch Manager puede utilizarse para aplicar parches en instancias de Amazon EC2 tanto para sistemas operativos como para aplicaciones, incluidas aplicaciones de Microsoft, paquetes de servicios de Windows y actualizaciones de versiones secundarias para instancias basadas en Linux. Además de Amazon EC2, Patch Manager también puede utilizarse para aplicar parches en servidores locales.

  Para obtener una lista de los sistemas operativos compatibles, consulte Sistemas operativos compatibles en la Guía del usuario de Systems Manager. Puede analizar instancias para ver solamente un informe de los parches que faltan, o puede analizar e instalar automáticamente todos los parches que falten.
- Utilice AWS Security Hub: Security Hub proporciona una vista completa de su estado de seguridad en AWS. Recopila datos de seguridad en múltiples servicios de AWS y proporciona esos hallazgos en un formato estandarizado, que le permite priorizar los hallazgos de seguridad en todos los servicios de AWS.
- Utilice AWS CloudFormation: AWS CloudFormation es un servicio de infraestructura como código (IaC) que puede ayudarle a administrar las vulnerabilidades mediante la automatización del despliegue de recursos y la estandarización de la arquitectura de los recursos en diversas cuentas y entornos.

Recursos

Documentos relacionados:

- AWS Systems Manager
- Security Overview of AWS Lambda (Información general de seguridad de AWS Lambda)
- Amazon CodeGuru
- Improved, Automated Vulnerability Management for Cloud Workloads with a New Amazon Inspector (Administración de vulnerabilidades mejorada y automatizada para cargas de trabajo en la nube con un nuevo Amazon Inspector)

- Automate vulnerability management and remediation in AWS using Amazon Inspector and AWS Systems Manager – Part 1 (Automatice la administración y corrección de vulnerabilidades en AWS mediante Amazon Inspector y AWS Systems Manager - Primera parte)

Vídeos relacionados:

- Securing Serverless and Container Services (Protección de servicios de contenedor y sin servidor)
- Security best practices for the Amazon EC2 instance metadata service (Prácticas recomendadas de seguridad para el servicio de metadatos de instancias de Amazon EC2)

SEC06-BP02 Reducir la superficie expuesta a ataques

Reduzca su exposición al acceso no intencionado endureciendo los sistemas operativos y minimizando los componentes, bibliotecas y servicios consumibles externamente que se estén utilizando. Puede comenzar por reducir los componentes no utilizados, ya sean paquetes de sistemas operativos, aplicaciones para cargas de trabajo basadas en Amazon Elastic Compute Cloud (Amazon EC2) o módulos de software externos en su código, para todas las cargas de trabajo. Puede encontrar muchas guías de endurecimiento y configuración de seguridad para sistemas operativos y software de servidores comunes. Por ejemplo, puede empezar por el Centro para la seguridad de Internet e iterar a partir de ahí.

En Amazon EC2, puede crear sus propias imágenes de máquina de Amazon (AMI), a las que habrá aplicado parches y habrá endurecido, para ayudarle a cumplir los requisitos de seguridad específicos de su organización. Los parches y otros controles de seguridad que apliquen en la AMI serán efectivos en el momento en el que se crearon, no son dinámicos a no ser que los modifique tras el lanzamiento, por ejemplo con AWS Systems Manager.

Puede simplificar el proceso de creación de AMI seguras con EC2 Image Builder. EC2 Image Builder reduce significativamente el esfuerzo necesario para crear y mantener imágenes golden sin escribir ni mantener automatizaciones. Cuando hay disponibles actualizaciones de software, Image Builder produce automáticamente una nueva imagen sin exigir a los usuarios que inicien manualmente creaciones de imágenes. EC2 Image Builder le permite validar fácilmente la funcionalidad y seguridad de sus imágenes antes de usarlas en producción con pruebas propias o proporcionadas por AWS. También puede aplicar la configuración de seguridad facilitada por AWS para proteger aún más sus imágenes de modo que cumplan criterios de seguridad internos. Por ejemplo, puede producir imágenes que se ajusten al estándar Security Technical Implementation Guide (STIG) con plantillas proporcionadas por AWS.

Mediante el uso de herramientas de análisis de código estático de terceros, puede identificar problemas de seguridad comunes como enlaces de entrada de funciones sin comprobar, además de vulnerabilidades y exposiciones comunes aplicables (CVE). Puede usar Amazon CodeGuru para los lenguajes compatibles. Las herramientas de comprobación de dependencias también se pueden usar para determinar si las bibliotecas con las que se vincula su código están actualizadas a su última versión, si no tienen CVE y si tienen condiciones de licencia que se ajusten a sus requisitos de política del software.

Con Amazon Inspector, puede llevar a cabo evaluaciones de configuración de sus instancias en busca de CVE conocidos, evaluarlas en función de referencias de seguridad y automatizar la notificación de defectos. Amazon Inspector se ejecuta en instancias de producción o en una canalización de compilación y notifica a los desarrolladores e ingenieros cuando detecten algún hallazgo. Puede acceder a los hallazgos programáticamente y dirigir el equipo a trabajos pendientes y sistemas de seguimiento de errores. EC2 Image Builder se puede usar para mantener imágenes de servidor (AMI) con aplicación de parches automática, aplicación de políticas de seguridad proporcionadas por AWS y otras personalizaciones. Al usar 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.

Aunque Amazon Inspector y otras herramientas son eficaces a la hora de identificar configuraciones y cualquier CVE que pudiese constar, son necesarios otros métodos para comprobar su carga de trabajo en el nivel de la aplicación. El fuzzing es un método conocido de detección de errores utilizando la automatización para inyectar datos con un formato incorrecto en los campos de entrada y otras áreas de su aplicación.

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

Guía para la implementación

- Endurezca el sistema operativo: configure el sistema operativo para cumplir con las prácticas recomendadas.
  - Protección de Amazon Linux
  - Protección de Microsoft Windows Server
- Endurezca los recursos en contenedores: configure los recursos en contenedores para cumplir con las prácticas recomendadas de seguridad.
- Implemente prácticas recomendadas de AWS Lambda.
  - Prácticas recomendadas de AWS Lambda

Recursos

Documentos relacionados:

- AWS Systems Manager
- Sustitución de un host bastión con Amazon EC2 Systems Manager
- Información general de seguridad de AWS Lambda

Videos relacionados:

- Ejecución de cargas de trabajo de alta seguridad en Amazon EKS
- Protección de servicios de contenedor y sin servidor
- Prácticas recomendadas de seguridad para el servicio de metadatos de instancias Amazon EC2

Ejemplos relacionados:

- Laboratorio: Despliegue de un firewall para aplicaciones web

SEC06-BP03 Implementar servicios administrados

Implemente servicios que administren recursos, como Amazon Relational Database Service (Amazon RDS), AWS Lambda y Amazon Elastic Container Service (Amazon ECS), para reducir sus tareas de mantenimiento de seguridad como parte del modelo de responsabilidad compartida. Por ejemplo, Amazon RDS le ayuda a configurar, operar y escalar una base de datos relacional, y automatiza tareas administrativas, como el aprovisionamiento de hardware, la configuración de bases de datos, la aplicación de parches y la creación de copias de seguridad. Esto significa que tendrá más tiempo libre para centrarse en proteger su aplicación de otras maneras descritas en AWS Well-Architected Framework. Lambda le permite ejecutar código sin aprovisionar ni administrar servidores, de modo que solo tendrá que centrarse en la conectividad, invocación y seguridad en el nivel del código, y no en la infraestructura ni en el sistema operativo.

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

Guía para la implementación

- Explore los servicios disponibles: explore, pruebe e implemente servicios que administren recursos, como Amazon RDS, AWS Lambda y Amazon ECS.

Recursos

Documentos relacionados:

- Sitio web de AWS
- AWS Systems Manager
- Sustitución de un host bastión con Amazon EC2 Systems Manager
- Información general de seguridad de AWS Lambda

Vídeos relacionados:

- Ejecución de cargas de trabajo de alta seguridad en Amazon EKS
- Protección de servicios de contenedor y sin servidor
- Prácticas recomendadas de seguridad para el servicio de metadatos de instancias Amazon EC2

Ejemplos relacionados:

- Laboratorio: solicitar un certificado público en AWS Certificate Manager

SEC06-BP04 Automatizar la protección informática

Automatice sus mecanismos de protección informática, incluida la administración de vulnerabilidades, la reducción de superficies expuestas a ataques y la administración de recursos. La automatización le ayudará a dedicar tiempo a proteger otros aspectos de su carga de trabajo y a reducir el riesgo de errores humanos.

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

Guía para la implementación

- Automatizar la administración de la configuración: aplique y valide configuraciones seguras de forma automática mediante el uso de un servicio o herramienta de administración de la configuración.
  - AWS Systems Manager
  - AWS CloudFormation
  - Laboratorio: Despliegue automatizado de VPC

    - Laboratorio: Despliegue automatizado de una aplicación web en EC2

- Automatizar la aplicación de revisiones en instancias Amazon Elastic Compute Cloud (Amazon EC2): Patch Manager de AWS Systems Manager automatiza el proceso de aplicación de revisiones a instancias administradas con actualizaciones de seguridad y de otro tipo. Puede utilizar Patch Manager para aplicar revisiones tanto para sistemas operativos como para aplicaciones.
    - Patch Manager de AWS Systems Manager
    - Implementación de revisiones centralizadas para varias regiones y cuentas con Automatización de AWS Systems Manager

- Implementar la detección y prevención de intrusiones: implemente una herramienta de detección y prevención de intrusiones para supervisar y detener las actividades maliciosas en las instancias.
- Considerar soluciones de AWS Partner: los socios de AWS ofrecen cientos de productos destacados que son equivalentes o idénticos a los controles que ya utiliza en sus entornos locales o que pueden integrarse con ellos. Estos productos complementan a los servicios de AWS existentes y le permiten implementar una completa arquitectura de seguridad, así como disfrutar de una experiencia más coherente tanto en la nube como en los entornos locales.
    - Seguridad de la infraestructura

Recursos

Documentos relacionados:

- AWS CloudFormation
- AWS Systems Manager
- Patch Manager de AWS Systems Manager
- Implementación de revisiones centralizadas para varias regiones y cuentas con Automatización de AWS Systems Manager
- Seguridad de la infraestructura
- Sustitución de un host bastión con Amazon EC2 Systems Manager
- Información general de seguridad de AWS Lambda

Vídeos relacionados:

- Ejecución de cargas de trabajo de alta seguridad en Amazon EKS
- Protección de servicios de contenedor y sin servidor
- Prácticas recomendadas de seguridad para el servicio de metadatos de instancias de Amazon EC2

Ejemplos relacionados:

- Laboratorio: Despliegue de un firewall para aplicaciones web
- Laboratorio: Despliegue automatizado de una aplicación web en EC2

SEC06-BP05 Permitir que los usuarios realicen acciones a distancia

La eliminación de la capacidad de acceder de forma interactiva reduce el riesgo de errores humanos y el potencial de llevar a cabo configuración o administración manuales. Por ejemplo, utilice un flujo de trabajo de administración de cambios para desplegar instancias de Amazon Elastic Compute Cloud (Amazon EC2) utilizando infraestructura como código, y después administre instancias de Amazon EC2 utilizando herramientas como AWS Systems Manager en lugar de permitir el acceso directo o mediante un host bastión. AWS Systems Manager puede automatizar una variedad de tareas de mantenimiento y despliegue, utilizando características como automatización de automatización, documentos (guías de estrategias) y el comando de ejecución. Las pilas de AWS CloudFormation se generan a partir de las canalizaciones y pueden automatizar el despliegue de su infraestructura y las tareas de administración sin usar directamente la AWS Management Console o las API.

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

Guía para la implementación

- Sustituir el acceso a la consola: sustituya el acceso a la consola (SSH o RDP) a instancias con Run Command de AWS Systems Manager para automatizar las tareas de administración.

- Run Command de AWS Systems Manager

Recursos

Documentos relacionados:

- AWS Systems Manager
- Run Command de AWS Systems Manager
- Sustitución de un host bastión con Amazon EC2 Systems Manager
- Información general de seguridad de AWS Lambda

Vídeos relacionados:

- Ejecución de cargas de trabajo de alta seguridad en Amazon EKS
- Protección de servicios de contenedor y sin servidor
- Prácticas recomendadas de seguridad para el servicio de metadatos de instancias de Amazon EC2

Ejemplos relacionados:

- Laboratorio: Despliegue de un firewall para aplicaciones web

SEC06-BP06 Validar la integridad del software

Implemente mecanismos (por ejemplo, firma de código) para validar que el software, el código y las bibliotecas que se utilizan en la carga de trabajo procedan de fuentes de confianza y no se hayan manipulado. Por ejemplo, debería verificar el certificado de firma de código de binarios y scripts para confirmar el autor y asegurarse de que no se haya manipulado desde que el autor lo creó. AWS Signer puede ayudar a garantizar la confianza e integridad de su código administrando de forma centralizada el ciclo de vida de la firma del código, incluida la certificación de la firma y las claves públicas y privadas. Puede aprender a usar patrones avanzados y prácticas recomendadas para la firma de código con AWS Lambda. Además, comparar la suma de comprobación de un software que haya descargado con la suma de comprobación del proveedor puede ayudar a garantizar que no haya existido manipulación alguna.

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

Guía para la implementación

- Investigue mecanismos: la firma de código es un mecanismo que se puede usar para validar la integridad del software.
  - NIST: consideraciones de seguridad para la firma de código

Recursos

Documentos relacionados:

- AWS Signer
- Nuevo: Firma de código, un control de confianza e integridad para AWS Lambda

Protección de los datos

Antes de diseñar una carga de trabajo, hay que adoptar prácticas fundamentales 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 haciéndolos ininteligibles para el acceso no autorizado. Estos métodos son importantes porque respaldan los objetivos, como, por ejemplo, la prevención de una mala gestión o el cumplimiento con las obligaciones normativas.

En AWS existen varios enfoques distintos que puede utilizar en relación con la protección de datos. En la siguiente sección se describe cómo se usan estos enfoques.

Temas

Clasificación de los datos

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

Prácticas recomendadas

SEC07-BP01 Identificar los datos en su carga de trabajo

Es fundamental conocer el tipo y la clasificación de los datos que procesa su carga de trabajo, los procesos empresariales asociados, dónde se almacenan los datos y quién es su propietario. También debe conocer los requisitos legales y de conformidad aplicables a su carga de trabajo y qué controles deben aplicarse en los datos. Identificar los datos es el primer paso en el proceso de clasificación de los datos.

Beneficios de establecer esta práctica recomendada:

La clasificación de datos permite a los propietarios de las cargas de trabajo identificar las ubicaciones en las que se almacenan datos confidenciales y determinar cómo se debe acceder a esos datos y compartirlos.

La clasificación de los datos tiene como objetivo responder a las siguientes preguntas:

- ¿Qué tipo de datos tiene?

  Podrían ser datos como los siguientes:

  - Datos de propiedad intelectual (PI), como secretos comerciales, patentes o acuerdos contractuales.
  - Información sanitaria protegida (PHI), como historiales médicos que contienen información sobre la historia clínica de una persona.
  - Información de identificación personal (PII), como nombre, dirección, fecha de nacimiento y número de identificación nacional o de registro.
  - Datos de tarjetas de crédito, como el número de cuenta principal (PAN), el nombre del titular de la tarjeta, la fecha de caducidad y el número de código de servicio.
  - ¿Dónde se almacenan los datos confidenciales?
  - ¿Quién puede acceder a los datos, modificarlos y borrarlos?
  - Es esencial conocer los permisos de los usuarios para protegerse de posibles tratamientos indebidos de los datos.
- ¿Quién puede realizar operaciones de creación, lectura, actualización y eliminación (CRUD)?
  - Para tener en cuenta la posible escalada de privilegios, conozca quién puede administrar los permisos de los datos.
- ¿Qué impacto podría tener en la empresa que los datos se divulgasen involuntariamente, se alteraren o se eliminasen?
  - Conozca el riesgo que supone que los datos se modifiquen, eliminen o revelen de forma inadvertida.

Si conoce las respuestas a estas preguntas, podrá tomar las siguientes medidas:

- Reducir el alcance de los datos confidenciales (como el número de ubicaciones de datos confidenciales) y limitar el acceso a los datos confidenciales solo a los usuarios autorizados.

- Conocer los distintos tipos de datos para poder implementar los mecanismos y técnicas de protección de datos adecuados, como el cifrado, la prevención de la pérdida de datos y la administración de identidades y accesos.
- Optimizar los costes proporcionando los objetivos de control adecuados para los datos.
- Responder con confianza a las preguntas de los reguladores y auditores sobre el tipo y la cantidad de datos, y sobre cómo se aíslan entre sí los datos con distintos niveles de confidencialidad.

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

Guía para la implementación

La clasificación de los datos es el acto de identificar el nivel de confidencialidad de los datos. Podría ser necesario etiquetarlos para que la búsqueda y el seguimiento de esos datos sean más sencillos. La clasificación de los datos también reduce la duplicación de datos, lo que puede ayudar a disminuir los costes de almacenamiento y de copias de seguridad al tiempo que acelera el proceso de búsqueda.

Utilice servicios como Amazon Macie para automatizar a escala tanto la detección como la clasificación de datos confidenciales. Otros servicios, como Amazon EventBridge y AWS Config, pueden utilizarse para automatizar la corrección de problemas de seguridad de los datos, como los buckets sin cifrar de Amazon Simple Storage Service (Amazon S3) y volúmenes EBS de Amazon EC2 o recursos de datos sin etiquetar. Para obtener una lista completa de las integraciones de los servicios de AWS, consulte la documentación de EventBridge.

Es posible detectar PII en datos no estructurados, como correos electrónicos de clientes, tickets de soporte, reseñas de productos y redes sociales, mediante Amazon Comprehend, que es un servicio de procesamiento de lenguaje natural (NLP) que utiliza machine learning (ML) para encontrar información y relaciones, como personas, lugares, sentimientos y temas en un texto no estructurado. Para obtener una lista de los servicios de AWS que pueden ayudar a identificar los datos, consulte Common techniques to detect PHI and PII data using AWS services (Técnicas comunes para detectar datos PHI y PII utilizando los servicios de AWS).

Otro método que facilita la clasificación y protección de los datos es el etiquetado de recursos de AWS. El etiquetado le permite asignar metadatos a sus recursos de AWS y puede utilizarlo para administrar, identificar, organizar, buscar y filtrar recursos.

En algunos casos, puede optar por etiquetar recursos enteros (como un bucket de S3), especialmente cuando se espera que una carga de trabajo o un servicio específico almacene procesos o transmisiones de una clasificación de datos ya conocida.

Cuando sea apropiado, puede etiquetar un bucket de S3 en lugar de objetos individuales para facilitar la administración y el mantenimiento de la seguridad.

Pasos para la implementación

Detecte datos confidenciales dentro de Amazon S3:

1. Antes de empezar, asegúrese de que dispone de los permisos adecuados para acceder a la consola de Amazon Macie y a las operaciones de la API. Para obtener más información, consulte Getting started with Amazon Macie (Introducción a Amazon Macie).
2. Utilice Amazon Macie para detectar automáticamente los datos cuando los datos confidenciales residan en Amazon S3.
   - Utilice la guía Getting Started with Amazon Macie (Introducción a Amazon Macie) para configurar un repositorio de resultados de detección de datos confidenciales y crear un trabajo de detección de datos confidenciales.
   - Cómo utilizar Amazon Macie para previsualizar datos confidenciales en buckets de S3.

     De forma predeterminada, Macie analiza los objetos con el conjunto de identificadores de datos administrados que recomendamos para detectar automáticamente los datos confidenciales. Para adaptar el análisis, configure Macie para que utilice identificadores de datos administrados específicos, identificadores de datos personalizados y listas de permitidos cuando detecte automáticamente los datos confidenciales para su cuenta u organización. Para ajustar el alcance del análisis, puede excluir buckets específicos (por ejemplo, buckets de S3 que suelen almacenar datos de registro de AWS).
3. Para configurar y utilizar la detección automatizada de datos confidenciales, consulte Performing automated sensitive data discovery with Amazon Macie (Detección automática de datos confidenciales con Amazon Macie).
4. También puede consultar Automated Data Discovery for Amazon Macie (Detección automática de datos para Amazon Macie).

Detecte datos confidenciales dentro de Amazon RDS:

Para obtener más información sobre la detección de datos en bases de datos de Amazon Relational Database Service (Amazon RDS), consulte Enabling data classification for Amazon RDS database

with Macie (Habilitación de la clasificación de datos para bases de datos de Amazon RDS con Macie).

Detecte datos confidenciales dentro de DynamoDB:

- En Detecting sensitive data in DynamoDB with Macie (Detección de datos confidenciales en DynamoDB con Macie), se explica cómo utilizar Amazon Macie para detectar datos confidenciales en tablas de Amazon DynamoDB exportando los datos a Amazon S3 para analizarlos.

Soluciones de los socios de AWS

- Considere la posibilidad de utilizar nuestra amplia AWS Partner Network. Los socios de AWS disponen de exhaustivas herramientas y marcos de conformidad que se integran directamente con los servicios de AWS. Los socios pueden proporcionarle una solución de gobernanza y conformidad a medida para ayudarle a satisfacer sus necesidades organizativas.
- Para obtener soluciones personalizadas para la clasificación de datos, consulte Data governance in the age of regulation and compliance requirements (Gobernanza de datos en la era de la regulación y los requisitos de conformidad).

Para aplicar automáticamente las normas de etiquetado que adopte su organización, puede crear y desplegar políticas mediante AWS Organizations. Las políticas de etiquetado le permiten especificar reglas que definen los nombres válidos de las claves y qué valores son válidos para cada clave. Puede optar por supervisarlas únicamente, lo que le ofrece la oportunidad de evaluar y limpiar sus etiquetas existentes. Una vez que sus etiquetas cumplan las normas elegidas, puede activar la aplicación de la norma en las políticas de etiquetas para evitar que se creen etiquetas que no las cumplan. Para obtener más información, consulte Securing resource tags used for authorization using a service control policy in AWS Organizations (Proteger las etiquetas de recursos utilizadas para la autorización mediante una política de control de servicios en las organizaciones de AWS) y el ejemplo de política para evitar que las etiquetas se modifiquen, excepto por las entidades principales autorizadas.

- Para comenzar a utilizar las políticas de etiquetas en AWS Organizations, se recomienda encarecidamente seguir el flujo de trabajo de Introducción a las políticas de etiquetas antes de pasar a políticas de etiquetas más avanzadas. Conocer el efecto que tiene asociar una simple política de etiquetas a una sola cuenta antes de extenderla a toda una unidad organizativa (OU) u organización le permite ver los efectos que tiene antes de imponer su cumplimiento. En

Introducción a las políticas de etiquetas, encontrará enlaces a instrucciones de tareas relacionadas con políticas más avanzadas.

- Considere la posibilidad de evaluar otros servicios y características de AWS compatibles con la clasificación de datos, que se enumeran en el documento técnico Data Classification (Clasificación de datos).

Recursos

Documentos relacionados:

- Getting Started with Amazon Macie (Introducción a Amazon Macie)
- Automated data discovery with Amazon Macie (Detección automática de datos con Amazon Macie)
- Introducción a las políticas de etiquetas
- Detecting PII entities (Detectar entidades PII)

Blogs relacionados:

- Cómo utilizar Amazon Macie para previsualizar datos confidenciales en buckets de S3.
- Performing automated sensitive data discovery with Amazon Macie (Detección automática de datos confidenciales con Amazon Macie)
- Common techniques to detect PHI and PII data using AWS Services (Técnicas comunes para detectar datos PHI y PII utilizando los servicios de AWS)
- Detecting and redacting PII using Amazon Comprehend (Detección y ocultación de PII utilizando Amazon Comprehend)
- Securing resource tags used for authorization using a service control policy in AWS Organizations (Protección de las etiquetas de recursos utilizadas para la autorización mediante una política de control de servicios en AWS Organizations)
- Enabling data classification for Amazon RDS database with Macie (Habilitación de la clasificación de datos para la base de datos de Amazon RDS con Macie)
- Detecting sensitive data in DynamoDB with Macie (Detección de datos confidenciales en DynamoDB con Macie)
-

Vídeos relacionados:

- Event-driven data security using Amazon Macie (Seguridad de datos basada en eventos utilizando Amazon Macie)
- Amazon Macie for data protection and governance (Amazon Macie para la protección y gobernanza de datos)
- Fine-tune sensitive data findings with allow lists (Optimización de los hallazgos de datos confidenciales con listas de permitidos)

SEC07-BP02 Definir controles de protección de datos

Proteja los datos de acuerdo con su nivel de clasificación. Por ejemplo, proteja los datos clasificados como públicos utilizando recomendaciones relevantes a la vez que protege los datos confidenciales con controles adicionales.

Mediante el uso de etiquetas de recursos, separando cuentas de AWS por nivel de confidencialidad (y potencialmente también según las reservas, enclaves o comunidades de intereses), políticas de IAM, SCP de AWS Organizations, AWS Key Management Service (AWS KMS) y AWS CloudHSM, puede definir e implementar sus políticas de clasificación y protección de datos con cifrado. Por ejemplo, si tiene un proyecto con buckets de S3 que contienen datos muy críticos o instancias de Amazon Elastic Compute Cloud (Amazon EC2) que procesen información confidencial, se les puede asignar la etiqueta `Project=ABC` . Solamente su equipo inmediato sabrá qué significa el código del proyecto; también proporciona una forma de utilizar el control de acceso basado en atributos. Puede definir los niveles de acceso a las claves de cifrado de AWS KMS con políticas y concesiones de claves para garantizar que los servicios adecuados tengan acceso al contenido confidencial a través de un mecanismo seguro. Si va a tomar decisiones de autorización en función de etiquetas, debería asegurarse de que los permisos de las etiquetas se definan convenientemente con políticas de etiquetas en AWS Organizations.

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

Guía para la implementación

- Definir el esquema de identificación y clasificación de datos: la identificación y clasificación de los datos se realiza para evaluar el impacto potencial, el tipo de datos que almacena y quién debe acceder a ellos.
  - Documentación de AWS

- Detectar los controles de AWS disponibles: para los servicios de AWS que está utilizando o pretende utilizar, detecte los controles de seguridad. Muchos servicios tienen una sección de seguridad en su documentación.
  - Documentación de AWS
- Identificar los recursos de cumplimiento de AWS: identifique los recursos que AWS tiene disponibles para ayudarle.
  - https://aws.amazon.com/compliance/

Recursos

Documentos relacionados:

- Documentación de AWS
- Documento técnico sobre clasificación de datos
- Introducción a Amazon Macie
- Falta el texto

Vídeos relacionados:

- Introducción al nuevo Amazon Macie

SEC07-BP03 Automatizar 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 esto, en lugar del acceso directo de una persona, reduce el riesgo de error y exposición humanos. Debería valorar el uso de una herramienta como Amazon Macie, que usa el machine learning para detectar, clasificar y proteger automáticamente los datos confidenciales en AWS. Amazon Macie reconoce la información confidencial, como la información de identificación personal (PII) o la propiedad intelectual, y le proporciona paneles y alertas que le permiten visualizar cómo se desplazan estos datos o cómo se obtiene acceso a ellos.

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

Guía para la implementación

- Use el inventario de Amazon Simple Storage Service (Amazon S3): el inventario de Amazon S3 es una de las herramientas que puede utilizar para realizar una auditoría y elaborar informes sobre el estado de cifrado y replicación de los objetos.
  - Inventario de Amazon S3
- Plantéese usar Amazon Macie: Amazon Macie utiliza el aprendizaje automático para descubrir y clasificar automáticamente los datos almacenados en Amazon S3.
  - Amazon Macie

Recursos

Documentos relacionados:

- Amazon Macie
- Inventario de Amazon S3
- Documento técnico sobre clasificación de datos
- Introducción a Amazon Macie

Videos relacionados:

- Introducción al nuevo Amazon Macie

SEC07-BP04 Definir la administración del ciclo de vida de los datos

Su estrategia de ciclo de vida definida debería basarse en el nivel de confidencialidad, además de en los requisitos jurídicos y organizativos. Debe tener en cuenta algunos aspectos, como la duración de retención, los procesos de destrucción, la administración del acceso, la transformación o el intercambio de los datos. Al seleccionar una metodología de clasificación de los datos, valore la facilidad de uso frente al acceso. También debería dar cabida a los distintos niveles de acceso y particularidades para implementar un enfoque seguro, pero utilizable, para cada nivel. Utilice siempre un enfoque de defensa en profundidad y reduzca el acceso humano a los datos y los mecanismos de transformación, eliminación o copia de los datos. Por ejemplo, exija a los usuarios que se autentiquen en una aplicación con métodos estrictos, y otorgue a la aplicación, en lugar de a los usuarios, el requisito de permiso de acceso para llevar a cabo una acción a distancia. Además, asegúrese de que los usuarios procedan de una ruta de red de confianza y requieran acceso a las

claves de descifrado. Use herramientas como paneles e informes automáticos para proporcionar a los usuarios información de los datos en lugar de proporcionarles acceso directo a los datos.

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

Guía para la implementación

- Identifique los tipos de datos: identifique los tipos de datos que almacena o procesa en su carga de trabajo. Esos datos podrían ser textos, imágenes, bases de datos binarias, etc.

Recursos

Documentos relacionados:

- Documento técnico sobre clasificación de datos
- Introducción a Amazon Macie

Vídeos relacionados:

- Introducción al nuevo Amazon Macie

Protección de los datos en reposo

Los datos en reposo representan los datos que se conservan en un almacenamiento no volátil durante cualquier periodo de tiempo en una carga de trabajo. Esto incluye el almacenamiento en bloque, el almacenamiento de objetos, las bases de datos, los archivos, los dispositivos 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 no puede tener significado por sí mismo y no debe derivarse de los datos que se están tokenizando. Por tanto, un resumen criptográfico no puede usarse como token. Al planificar minuciosamente el enfoque de tokenización, puede proporcionar protección adicional al contenido y también asegurarse de que se cumplan los requisitos de conformidad. Por ejemplo, puede reducir el

ámbito de conformidad de un sistema de procesamiento de tarjetas de crédito si saca partido de un token en lugar de utilizar 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 la información hasta un punto en el que los datos restantes no se consideren confidenciales. Por ejemplo, PCDI-DSS permite conservar los últimos cuatro dígitos del número de una tarjeta, aunque este dato esté fuera del límite del ámbito de conformidad del proceso de indexación.

Auditar el uso de las claves de cifrado: asegúrese de entender el uso de las claves de cifrado y de realizar una auditoría en ellas, para validar que se implementen correctamente los mecanismos de control de acceso en dichas claves. Por ejemplo, un servicio de AWS que utilice una clave de AWS KMS registra cada uso en AWS CloudTrail. A continuación, puede realizar una consulta en AWS CloudTrail, mediante una herramienta como Amazon CloudWatch Insights, para garantizar que todos los usos de las claves sean válidos.

Prácticas recomendadas

- SEC08-BP01 Implementar una administración de claves segura
- SEC08-BP02 Aplicar el cifrado en reposo
- SEC08-BP03 Automatizar la protección de los datos en reposo
- SEC08-BP04: Aplicación del control de acceso
- SEC08-BP05: Uso de mecanismos para mantener a las personas alejadas de los datos

SEC08-BP01 Implementar 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: un mecanismo de administración de claves escalable, repetible y automatizado. El mecanismo debe proporcionar la capacidad de hacer cumplir el acceso con privilegios mínimos al material de claves y proporcionar el equilibrio correcto entre la disponibilidad, la confidencialidad y la integridad de las claves. Es preciso supervisar el acceso a las claves y el material de claves debe rotarse mediante un proceso automatizado. Las identidades humanas nunca deben tener acceso al material de claves.

Patrones comunes de uso no recomendados:

- Acceso humano a material de claves no cifrado.
- Creación de 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

Muchos requisitos reglamentarios y prácticas recomendadas incluyen el cifrado de los datos en reposo como un control de seguridad fundamental. Para satisfacer 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 140-2 de nivel 3 para proteger sus claves. No hay ningún mecanismo para exportar claves de AWS KMS en texto sin formato.

Si se despliegan cargas de trabajo mediante una estrategia de cuentas múltiples, se considera una práctica recomendada 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 en el equipo de aplicaciones. En otros casos de uso, las organizaciones pueden 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. Tómese tiempo para revisar las prácticas recomendadas de control de acceso a sus claves de AWS KMS.

Se recomienda supervisar el uso de claves de cifrado para detectar patrones de acceso inusuales. Las operaciones realizadas con claves administradas por AWS y claves administradas por el cliente almacenadas en AWS KMS pueden registrarse en AWS CloudTrail y deben revisarse periódicamente. Debe prestarse especial atención a la supervisión 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 período de esperapredeterminado de 30 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 para usted; 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, la práctica recomendada es utilizar cifrado de sobre para proteger los datos. La SDK de cifrado de AWS puede proporcionar a sus aplicaciones elementos básicos de cifrado del lado 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.
   - 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.
   - 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 claves 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.
   - Cómo los servicios de AWS utilizan AWS KMS

- 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.
   - Introducción: AWS Key Management Service (AWS KMS)
   - Revise las prácticas recomendadas de control de acceso a sus claves de AWS KMS.
4. Considere AWS Encryption SDK: utilice el AWS Encryption SDK con la integración de AWS KMS cuando la aplicación necesite cifrar datos en el lado del cliente.
   - AWS Encryption SDK
5. Habilite IAM Access Analyzer para revisar y notificar automáticamente si hay políticas de claves de AWS KMS demasiado amplias.
6. Habilite Security Hub 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.
   - Algunas organizaciones prefieren segregar 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
- Herramientas y servicios de criptografía de AWS
- Protección de los datos de Amazon S3 mediante el cifrado
- Cifrado de sobre
- Compromiso de soberanía digital de AWS
- Demystifying AWS KMS key operations, bring your own key, custom key store, and ciphertext portability
- Detalles criptográficos de AWS Key Management Service

Vídeos 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 Aplicar el cifrado en reposo

Debe obligar a usar el cifrado de los datos en reposo. El cifrado mantiene la confidencialidad de los datos confidenciales en caso de que se produzca un acceso no autorizado o se divulguen de manera accidental.

Resultado deseado: los datos privados deben cifrarse de forma predeterminada cuando estén en reposo. El cifrado ayuda a mantener la confidencialidad de los datos y proporciona una capa adicional de protección contra la divulgación o exfiltración de datos intencionada o inadvertida. No es posible leer los datos cifrados ni acceder a ellos sin antes descifrarlos. Hay que hacer un inventario y controlar todos los datos almacenados sin cifrar.

Antipatrones usuales:

- No utilizar configuraciones para que el cifrado se realice 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 Identificar los datos en su carga de trabajo).

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 Simple Storage Service (Amazon S3) puede establecer el cifrado predeterminado en un bucket para que todos los objetos nuevos se cifren automáticamente. Cuando utilice AWS KMS, tenga en cuenta hasta qué punto es necesario restringir los datos. AWS administra y utiliza en su nombre las claves de AWS KMS predeterminadas y controladas por el servicio. 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). Usted tiene el control total sobre las CMK, incluida la rotación y la administración del acceso mediante el uso de políticas de claves.

Además, Amazon Elastic Compute Cloud (Amazon EC2) y Amazon S3 admiten la aplicación del cifrado mediante la configuración del cifrado predeterminado. Puede utilizar Reglas de AWS Config para comprobar automáticamente que está utilizando cifrado, por ejemplo, para volúmenes de Amazon Elastic Block Store (Amazon EBS), instancias de Amazon Relational Database Service (Amazon RDS) y buckets de Amazon S3.

AWS también proporciona opciones para el cifrado del cliente, lo que le permite cifrar los datos antes de subirlos a la nube. AWS Encryption SDK proporciona una forma de cifrar sus datos mediante el cifrado de sobre. Usted 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 utilizando claves almacenadas dentro de AWS CloudHSM antes de subir sus datos a AWS. El Amazon DynamoDB Encryption Client también le permite cifrar y firmar elementos antes de subirlos a una tabla de DynamoDB.

Pasos para la implementación

- Aplique el cifrado en reposo para Amazon S3: implemente el cifrado predeterminado de buckets de Amazon S3.

Configure el 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 usted cree.

Configure imágenes de máquina de Amazon (AMI) cifradas: al copiar una AMI existente con cifrado habilitado, se cifran automáticamente las instantáneas y los volúmenes raíz.

Configure el 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.

Cree y configure 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.

Configure el 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
- Documentación de AWS
- AWS Encryption SDK
- Documento técnico Introducción a los detalles criptográficos de AWS KMS
- AWS Key Management Service
- AWS cryptographic services and tools (Herramientas y servicios criptográficos de AWS)
- Cifrado de Amazon EBS
- Cifrado predeterminado para volúmenes de Amazon EBS

- Cifrado de recursos de Amazon RDS
- Habilitación del cifrado predeterminado de bucket de Amazon S3
- Protección de datos de Amazon S3 mediante cifrado

Vídeos relacionados:

- How Encryption Works in AWS (Cómo funciona el cifrado en AWS)
- Securing Your Block Storage on AWS (Protección del almacenamiento en bloque de AWS)

SEC08-BP03 Automatizar la protección de los datos en reposo

Utilice herramientas automatizadas para validar y aplicar continuamente los controles de datos en reposo; por ejemplo, verifique que solo hay recursos de almacenamiento cifrados. Puede automatizar la validación de que todos los volúmenes de EBS están cifrados con Reglas de AWS Config. AWS Security Hub también puede verificar varios controles mediante comprobaciones automatizadas con respecto a los estándares de seguridad. Además, su Reglas de AWS Config puede corregir recursos no conformes automáticamente.

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

Guía para la implementación

Datos en reposo representan los datos que se conservan en un almacenamiento no volátil durante cualquier periodo de tiempo en una carga de trabajo. Esto incluye el almacenamiento en bloque, el almacenamiento de objetos, las bases de datos, los archivos, los dispositivos 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.

Aplique el cifrado en reposo: debe asegurarse de que la única forma de almacenar los datos sea mediante el cifrado. AWS KMS se integra perfectamente con muchos servicios de AWS para facilitarle el cifrado de todos sus datos en reposo. Por ejemplo, en Amazon Simple Storage Service (Amazon S3), puede establecer el cifrado predeterminado en un bucket de modo que todos los objetos nuevos se cifran automáticamente. Además, Amazon EC2 y Amazon S3 admiten la aplicación del cifrado mediante la configuración del cifrado predeterminado. Puede usar las reglas de administradas de AWS Config para comprobar automáticamente que está utilizando el cifrado,

por ejemplo, para volúmenes de EBS, instancias de Amazon Relational Database Service (Amazon RDS)y buckets de Amazon S3.

Recursos

Documentos relacionados:

- AWS Crypto Tools
- SDK de cifrado de AWS

Vídeos relacionados:

- How Encryption Works in AWS (Cómo funciona el cifrado en AWS)
- Securing Your Block Storage on AWS (Protección del almacenamiento en bloque de AWS)

SEC08-BP04: Aplicación del control de acceso

Para ayudarle a proteger sus datos en reposo, aplique el control de acceso mediante mecanismos como el aislamiento y el control de versiones, y utilice el principio del privilegio mínimo. Impida que se conceda acceso público a sus datos.

Resultado deseado: verificar que solo los usuarios autorizados puedan acceder a los datos en función de su necesidad de utilizarlos. Proteja sus datos con copias de seguridad periódicas y el control de versiones para evitar que se modifiquen o eliminen de forma intencionada o involuntaria. Aísle los datos críticos de otros datos para proteger su confidencialidad e integridad.

Antipatrones usuales:

- 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: bajo

Guía para la implementación

Hay muchos controles que pueden ayudar a proteger sus datos en reposo, como el control de acceso (con el privilegio mínimo), el aislamiento y el control de versiones. El acceso a sus datos debe auditarse utilizando mecanismos de detección, como AWS CloudTrail, y registros de nivel de servicio, como los registros de acceso de Amazon Simple Storage Service (Amazon S3). Debe realizar un inventario de los datos a los que se puede acceder públicamente y crear un plan para reducir la cantidad de datos disponibles públicamente a lo largo del tiempo.

El bloqueo de almacenes de Amazon S3 Glacier y el bloqueo de objetos de Amazon S3 proporcionan un control de acceso obligatorio para los objetos de Amazon S3: una vez bloqueada una política de almacenes con la opción de conformidad, ni siquiera el usuario raíz puede cambiarla hasta que venza el bloqueo.

Pasos para la implementación

- Aplique el control de acceso: aplique el control de acceso con privilegios mínimos, incluido el acceso a las claves de cifrado.
- Separe los datos en función de diferentes niveles de clasificación: utilice diferentes Cuentas de AWS para los niveles de clasificación de los datos y administre dichas cuentas mediante AWS Organizations.
- Revise las políticas de AWS Key Management Service (AWS KMS): revise el nivel de acceso concedido en las políticas de AWS KMS.
- Revise los permisos de los objetos y buckets de Amazon S3: revise periódicamente el nivel de acceso otorgado por las políticas de buckets de S3. La práctica recomendada es evitar el uso de buckets de lectura o escritura pública. Plantéese utilizar AWS Config para detectar buckets que están disponibles al 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. De manera predeterminada, todos los buckets de S3 son privados y solo permiten el acceso a los usuarios que cuentan con una autorización explícita.
- Habilite AWS IAM Access Analyzer: IAM Access Analyzer analiza los buckets de Amazon S3 y genera un hallazgo cuando una política de S3 concede acceso a una entidad externa.
- Habilite el control de versiones de Amazon S3 y el bloqueo de objetos cuando corresponda.
- Utilice el inventario de Amazon S3: el inventario de Amazon S3 puede utilizarse para auditar e informar sobre el estado de replicación y cifrado de sus objetos de S3.

- Revise los permisos de uso compartido de Amazon EBS y https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sharing-amis.html: los permisos de uso compartido pueden permitir que las imágenes y los volúmenes se compartan con Cuentas de AWS externas a su carga de trabajo.
- Revise periódicamente los recursos compartidos de AWS Resource Access Manager para determinar si los recursos deben seguir compartiéndose. Resource Access Manager le permite compartir recursos, como las políticas de AWS Network Firewall, las reglas de resolución de Amazon Route 53 y las subredes, dentro de sus Amazon VPC. Audite periódicamente los recursos compartidos y deje de compartir los recursos que ya no sea necesario.

Recursos

Prácticas recomendadas relacionadas:

- SEC03-BP01 Definir los requisitos de acceso
- SEC03-BP02 Conceder acceso con privilegios mínimos

Documentos relacionados:

- Documento técnico Introducción a los detalles criptográficos de AWS KMS
- Introducción a la administración de permisos de acceso a los recursos de Amazon S3
- Información general sobre la administración de acceso a sus recursos de AWS KMS
- Reglas de AWS Config
- Amazon S3 + Amazon CloudFront: A Match Made in the Cloud (Amazon S3 + Amazon CloudFront: una combinación perfecta en la nube)
- Uso del control de versiones
- Usar Bloqueo de objetos de Amazon S3
- Compartir una instantánea de Amazon EBS
- AMI compartidas
- Hosting a single-page application on Amazon S3 (Alojar una aplicación de una sola página en Amazon S3)

Vídeos relacionados:

- Securing Your Block Storage on AWS (Protección del almacenamiento en bloque de AWS)

SEC08-BP05: Uso de mecanismos para mantener a las personas alejadas de los datos

Impida a todos los usuarios acceder directamente a sistemas e información confidenciales en circunstancias de funcionamiento normales. Por ejemplo, utilice un flujo de trabajo de administración de cambios para administrar instancias de Amazon Elastic Compute Cloud (Amazon EC2) con herramientas en lugar de permitir el acceso directo o un host bastión. Esto se puede lograr mediante la automatización de AWS Systems Manager, que usa documentos de automatización que incluyen los pasos que han de seguirse para realizar tareas. Estos documentos se pueden almacenar en el control de código fuente, otros compañeros pueden revisarlos antes de su publicación, y pueden probarse de forma exhaustiva para reducir al mínimo el riesgo en comparación con el acceso al shell. Los usuarios empresariales podrían tener un panel en lugar de acceso directo a un almacén de datos para ejecutar consultas. Allí donde no se utilicen canalizaciones de CI/CD, determine qué controles y procesos son necesarios para ofrecer correctamente un mecanismo de acceso instantáneo que suele estar deshabilitado.

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

Guía para la implementación

- Implemente mecanismos para mantener a las personas alejadas de los datos: entre estos mecanismos se incluyen el uso de paneles, como Amazon QuickSight, para mostrar datos a los usuarios en lugar de realizar consultas directas.
  - Amazon QuickSight
- Automatice la administración de la configuración: realice acciones a distancia, y aplique y valide configuraciones seguras de forma automática mediante el uso de un servicio o herramienta de administración de la configuración. Evite usar hosts bastión o acceder directamente a instancias de EC2.
  - AWS Systems Manager
  - AWS CloudFormation
  - Canalización de CI/CD para plantillas de AWS CloudFormation en AWS

Recursos

Documentos relacionados:

- Documento técnico Detalles criptográficos de AWS KMS

Vídeos relacionados:

- Cómo funciona el cifrado en AWS
- Protección del almacenamiento en bloque de AWS

Protección de los datos en tránsito

Los datos en tránsito son todos aquellos que se envían 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, podrá proteger la confidencialidad y la integridad de los datos de la carga de trabajo.

Proteger los datos entre la VPC y las ubicaciones locales: puede usar AWS PrivateLink para crear una conexión de red segura y privada entre Amazon Virtual Private Cloud (Amazon VPC) o una conectividad local y los servicios alojados en AWS. Puede acceder a servicios de AWS, servicios externos y servicios de otras Cuentas de AWS como si estuvieran en su red privada. Con AWS PrivateLink, puede acceder a servicios de acceso en cuentas con CIDR de IP superpuestos sin necesidad de utilizar una puerta de enlace de Internet o NAT. Tampoco tiene que configurar reglas del firewall, definiciones de rutas ni 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 la conformidad con las normativas de conformidad específicas del sector, tales como HIPAA y el Escudo de la privacidad Unión Europea-Estados Unidos. AWS PrivateLink funciona a la perfección con soluciones externas para crear una red global simplificada, lo que le permite acelerar la migración a la nube y sacar partido de los servicios disponibles de AWS.

Prácticas recomendadas

- SEC09-BP01: Implementación de la administración segura de claves y certificados
- SEC09-BP02 Aplicar el cifrado en tránsito
- SEC09-BP03: Automatización de la detección del acceso involuntario a los datos
- SEC09-BP04: Autenticar 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, desplegar, 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:

- Realizar pasos manuales durante los procesos de despliegue 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 el despliegue 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, el despliegue 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 Certificate Manager y AWS Private Certificate Authority (AWS Private CA). ACM es el servicio principal que los clientes utilizan para aprovisionar, administrar y desplegar certificados para su uso tanto en cargas de trabajo de AWS tanto públicas como privadas. ACM emite certificados mediante AWS Private CA y se integra con muchos otros servicios administrados de AWS para proporcionar certificados TLS seguros para las cargas de trabajo.

AWS Private 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 Private 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 Funciones de IAM en cualquier lugar para proporcionar credenciales temporales de IAM a las cargas de trabajo locales a las que se les hayan emitido certificados X.509 firmados por su CA privada.

Además de ACM y AWS Private CA, AWS IoT Core proporciona soporte especializado para el aprovisionamiento, la administración y el despliegue de certificados de PKI en dispositivos IoT. AWS IoT Core proporciona mecanismos especializados para incorporar dispositivos IoT en su infraestructura de clave pública a escala.

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 desplegar 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 del

despliegue 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 Private 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 Certificate Manager. ACM se puede usar para desplegar certificados TLS para servidores web, equilibradores de carga u otros usos para certificados de confianza pública.
    - Considere AWS Private 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 Private 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.
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 desplegar 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 Usar credenciales temporales
- SEC08-BP01 Implementar una administración de claves segura

- SEC09-BP04: Autenticar 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
- Prácticas recomendadas de CA privada
- How to use AWS RAM to share your ACM Private CA cross-account

Vídeos relacionados:

- Activating AWS Certificate Manager Private CA (taller)

Ejemplos relacionados:

- Taller de CA privada
- Taller de IoT Device Management (incluido el aprovisionamiento de dispositivos)

Herramientas relacionadas:

- Complemento para el administrador de certificados de Kubernetes para usar AWS Private CA

SEC09-BP02 Aplicar el cifrado en tránsito

Aplique los requisitos de cifrado definidos en función de las políticas, las obligaciones reglamentarias y las normas de su organización para ayudar a cumplir los requisitos organizativos, legales y de conformidad. Utilice únicamente protocolos con cifrado cuando transmita datos confidenciales fuera de su nube virtual privada (VPC). El cifrado ayuda a mantener la confidencialidad de los datos incluso cuando transitan por redes que no son de confianza.

Resultado deseado: todos los datos deben cifrarse en tránsito utilizando protocolos TLS seguros y conjuntos de cifrado. El tráfico de red entre sus recursos e Internet debe cifrarse para mitigar el acceso no autorizado a los datos. El tráfico de red de su entorno interno de AWS únicamente debe cifrarse utilizando TLS siempre que sea posible. La red interna de AWS se cifra de manera predeterminada y el tráfico de red dentro de una VPC no se puede suplantar ni espiar a menos que una parte no autorizada haya obtenido acceso a cualquier recurso que esté generando tráfico (como

las instancias de Amazon EC2 y los contenedores de Amazon ECS). Considere la posibilidad de proteger el tráfico entre redes con una red privada virtual (VPN) IPsec.

Antipatrones usuales:

- 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 inseguros, como HTTP, se pueden auditar y bloquear en una VPC mediante el uso de grupos de seguridad. Las solicitudes HTTP también se pueden redirigir automáticamente a HTTPS en Amazon CloudFront o en un Application Load Balancer. Dispone de un control total sobre los recursos informáticos 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 realizan llamadas a las API de AWS utilizando al menos TLS 1.2, ya que AWS va a dejar de utilizar TLS 1.0 y 1.1 en junio de 2023. Hay soluciones de terceros disponibles en AWS Marketplace si tiene requisitos especiales.

Pasos para la implementación

- Aplique el 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.
- Configure protocolos seguros en los servicios de periferia: configure HTTPS con Amazon CloudFront y utilice un perfil de seguridad apropiado para su postura de seguridad y su caso de uso.
- Utilice una VPN para la conectividad externa: considere la posibilidad de utilizar una VPN IPsec para proteger las conexiones punto a punto o de red a red para ofrecer tanto privacidad como integridad de los datos.

- Configure 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 agente de escucha. Cree un agente de escucha HTTPS para su Application Load Balancer.
- Configure 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).
- Configure protocolos seguros: revise la documentación del servicio de AWS para determinar las capacidades de cifrado en tránsito.
- Configure el acceso seguro al realizar subidas en los buckets de Amazon S3: utilice los controles de políticas de buckets de Amazon S3 para aplicar el acceso seguro a los datos.
- Considere la posibilidad de utilizar AWS Certificate Manager: ACM le permite aprovisionar, administrar y desplegar certificados TLS públicos para utilizarlos con los servicios de AWS.
- Considere la posibilidad de utilizar AWS Private Certificate Authority para las necesidades de PKI privadas: AWS Private 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:

- Documentación de AWS
- 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 (Creación de un agente de escucha HTTPS para Application Load Balancer)
- Tutorial: configure SSL/TLS en Amazon Linux 2
- Uso de SSL/TLS para cifrar una conexión a una instancia de base de datos
- Configuración de las opciones de seguridad para las conexiones

SEC09-BP03: Automatización de la detección del acceso involuntario a los datos

Utilice herramientas, tales como Amazon GuardDuty, para detectar automáticamente actividades sospechosas o intentos de trasladar datos fuera de los límites definidos. Por ejemplo, GuardDuty

puede detectar actividad de lectura de Amazon Simple Storage Service (Amazon S3) que sea inusual con la búsqueda Exfiltration:S3/AnomalousBehavior. Además de GuardDuty, los registros de flujo de Amazon VPC, que capturan información sobre el tráfico de red, pueden utilizarse con Amazon EventBridge para desencadenar la detección de conexiones anómalas, tanto las que se han llegado a establecer como las denegadas. El analizador de acceso de Amazon S3 puede ayudar a evaluar a qué datos pueden acceder ciertos usuarios en los buckets de Amazon S3.

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

Guía para la implementación

- Automatización de la detección del acceso involuntario a los datos: utilice una herramienta o mecanismo de detección para detectar automáticamente los intentos de trasladar datos fuera de los límites definidos; por ejemplo, para detectar un sistema de base de datos que esté copiando datos a un host desconocido.
  - Registros de flujo de VPC
- Plantéese utilizar Amazon Macie: Amazon Macie es un servicio de privacidad y seguridad de datos totalmente administrado que utiliza el machine learning y la coincidencia de patrones para detectar y proteger los datos confidenciales en AWS.
  - Amazon Macie

Recursos

Documentos relacionados:

- Registros de flujo de VPC
- Amazon Macie

SEC09-BP04: Autenticar 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.

Antipatrones usuales:

- 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 realizan 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 deAWS 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 Private Certificate Authority (AWS Private CA). Puede utilizar servicios como Amazon API Gateway y AWS App Mesh para proporcionar autenticación mTLS para la comunicación entre cargas de trabajo o dentro de ellas. 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

- Defina y documente 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 la versión ejecutable.
  - Un diagrama de flujo de datos también puede ser útil cuando se realiza un ejercicio de modelado de amenazas, como se describe en «SEC01-BP07 Identificar amenazas y priorizar mitigaciones con un modelo de amenazas».
- Establezca 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.
- Implemente 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, considere la posibilidad de usar API Gateway o App Mesh. AWS Private CA se puede usar para establecer una jerarquía de CA privada capaz de emitir certificados para su uso con los mTLs.
  - Al realizar 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.
- Supervise el 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 de AWS Well-Architected Framework para obtener más información sobre la planificación, la simulación y la respuesta a los incidentes de seguridad.

Recursos

Prácticas recomendadas relacionadas:

- SEC03-BP07 Analizar el acceso público y entre cuentas
- SEC02-BP02 Usar credenciales temporales
- SEC01-BP07 Identificar amenazas y priorizar mitigaciones con un modelo de amenazas

Documentos relacionados:

- «Evaluating access control methods to secure Amazon API Gateway APIs»
- «Configuración de la autenticación TLS mutua para una API de REST»
- «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 (Guía de respuesta ante incidentes de seguridad de AWS)

Vídeos 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 ante 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 realizar 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, le ayudan a asegurarse de que podrá recuperarse con una interrupción mínima en el negocio.

Temas

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 formación 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 ante incidentes en la nube exitoso cuenta con Preparación, Operacionesy 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.

El siguiente diagrama 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

Aunque los mecanismos y procesos generales de respuesta ante incidentes, como los definidos en la guía de administración de incidentes de seguridad de computación NIST SP 800-61, sean válidos, le animamos a evaluar estos objetivos de diseño que son importantes a la hora de responder ante incidentes de seguridad en un entorno en la nube:

- Establecimiento de objetivos de respuesta: 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 generen 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 del despliegue: 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 del despliegue de los recursos con la configuración adecuada. En caso de que se identificara un posible compromiso, compruebe que la repetición del despliegue 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 fuera 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 despliegue. 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 realiza 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 formarlas 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, añadir 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: Desarrollar planes de administración de incidentes
- SEC10-BP03: Preparar capacidades forenses
- SEC10-BP04 Desarrollar y probar guías estratégicas de respuesta a incidentes de seguridad
- SEC10-BP05: Aprovisionamiento previo del acceso
- SEC10-BP06: Desplegar las herramientas con anticipación
- SEC10-BP07 Ejecutar simulaciones

SEC10-BP01 Identificación del personal clave y los recursos externos

Identifique las obligaciones legales, el personal y los recursos internos y externos que ayudarían a su organización a responder ante un incidente.

Al definir su enfoque a la hora de responder ante un incidente en la nube, de forma conjunta con otros equipos (como el consejo jurídico, el equipo directivo, las partes interesadas de la empresa y los servicios de asistencia de AWS, entre otros), debe identificar el personal clave, las partes interesadas y los contactos pertinentes. Con el fin de reducir la dependencia y el tiempo de respuesta, asegúrese de que su equipo, los equipos especializados en seguridad y los equipos de intervención cuenten con los conocimientos adecuados sobre los servicios que utiliza y que tengan la oportunidad de realizar una formación práctica.

Le animamos a identificar a los socios de seguridad externos de AWS que puedan ofrecerle una experiencia externa y una perspectiva diferente para aumentar sus capacidades de respuesta. Sus socios de seguridad de confianza pueden ayudarle a identificar posibles riesgos o amenazas con los que puede que no esté familiarizado.

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

Guía para la implementación

- Identifique al personal clave de la organización: Mantenga una lista de contactos del personal de su organización al que tendría que involucrar para responder y recuperarse ante un incidente.
- Identifique a los socios externos: Si es necesario, póngase en contacto con socios externos que puedan ayudarle a responder y a recuperarse ante un incidente.

Recursos

Documentos relacionados:

- AWS Incident Response Guide (Guía de respuesta ante incidentes de AWS)

Vídeos relacionados:

- Prepare for and respond to security incidents in your AWS environment (Cómo prepararse y responder ante incidentes de seguridad en el entorno de AWS)

Ejemplos relacionados:

SEC10-BP02: Desarrollar 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 le ayudará 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 y recuperarse de él. 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 local. 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, es útil cumplir con la guía de administración de seguridad informática NIST SP 800-61. Del mismo modo, cuando opere con cargas de trabajo con datos de información de identificación personal (PII) de Europa, considere situaciones como la forma en que podría proteger y responder a los problemas relacionados con la residencia de datos según lo dispuesto por la normativa del Reglamento General de Protección de Datos (RGPD).

Al diseñar 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 en la respuesta a incidentes. En este modelo, AWS administra la seguridad de la nube y usted 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 AWS Security Incident Response Guide (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, manteniéndose 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

Definición de roles y responsabilidades

La gestión de los eventos de seguridad requiere disciplina en toda la organización y una buena disposición a entrar en acción. Dentro de la estructura organizativa, debe haber muchas personas que tengan responsabilidades y obligaciones, que se consulten o que se mantengan informadas durante un incidente, como los representantes de Recursos Humanos (RR. HH.), el equipo directivo y el departamento legal. Tenga en cuenta estas funciones y responsabilidades y piense si debe participar algún tercero. Tenga en cuenta que, en muchas zonas geográficas, hay leyes locales que rigen lo que se debe y lo que no se debe hacer. Aunque parezca un mero trámite burocrático, elaborar un gráfico de las personas con responsabilidades y obligaciones, las personas que hay que consultar y las personas a las que hay que informar (RACI) para sus planes de respuesta en materia de seguridad facilita una comunicación rápida y directa y deja claro quiénes son los líderes en las diferentes etapas del evento.

Durante un incidente, es fundamental incluir a los propietarios y desarrolladores de las aplicaciones y los recursos afectados, ya que son los expertos en la materia (SME) que pueden proporcionar información y contexto para ayudar a medir el impacto. Asegúrese de establecer relaciones con los desarrolladores y propietarios de las aplicaciones antes de confiar en su experiencia para responder a los incidentes. Es posible que los propietarios de aplicaciones o SME, como los administradores o ingenieros de la nube, tengan que actuar en situaciones en las que el entorno no sea familiar o sea complejo, o a los que las personas encargadas de la respuesta no tengan acceso.

Por último, en la investigación o la respuesta pueden participar socios de confianza, ya que pueden proporcionar experiencia adicional y un control muy valioso. Si no dispone de estas habilidades en su propio equipo, tal vez sea conveniente contratar a una persona externa para que le ayude.

Conozca a los equipos de asistencia y respuesta de AWS

- AWS Support

  - AWS Support dispone de una amplia variedad de planes que ofrecen acceso a herramientas y experiencia que respalda el éxito y el buen estado operativo de sus soluciones de AWS. Si necesita asistencia técnica y más recursos para planificar, desplegar y optimizar su entorno de AWS, puede seleccionar el plan de asistencia que mejor se adapte a su caso de uso de AWS.
  - Utilice el Centro de soporte de AWS Management Console (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 AWS Support está controlado por AWS Identity and Access Management. Para obtener más información sobre el acceso a las características de AWS Support, consulte Getting started with AWS Support(Introducción a AWS Support).
- Equipo de respuesta a incidentes de clientes (CIRT) de AWS
  - 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 mejores prácticas 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 AWS Support.
- Asistencia en respuestas a DDoS
  - AWS ofrece AWS Shield, que proporciona un servicio de protección contra ataques de denegación de servicio distribuidos (DDoS) administrado que protege las aplicaciones web que se ejecutan en AWS. Shield ofrece detección permanente y mitigaciones automáticas en línea que pueden minimizar el tiempo de inactividad y la latencia de las aplicaciones, por lo que no es necesario utilizar AWS Support para beneficiarse de la protección contra ataques DDoS. Hay dos niveles 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. Al implementar las prácticas recomendadas para mantener su infraestructura, AMS ayuda a reducir sus gastos y riesgos operativos. AMS automatiza actividades comunes, como solicitudes de cambios, monitorización, administración

de parches, seguridad y servicios de copia de seguridad, y ofrece servicios de ciclo de vida completo para aprovisionar, ejecutar y ofrecer asistencia a su infraestructura.

- AMS asume la responsabilidad de desplegar 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.

Desarrolle 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. 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 a 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: se 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 (¿Cómo detecta e investiga los eventos de seguridad?)

Documentos relacionados:

- AWS Security Incident Response Guide (Guía de respuesta ante incidentes de seguridad de AWS)
- NIST: guía de administración de incidentes de seguridad informática

SEC10-BP03: Preparar capacidades forenses

Antes de que se produzca un incidente de seguridad, considere la posibilidad de desarrollar capacidades forenses que le 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 local también son aplicables a AWS Para obtener información clave 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

Prepare el entorno forense

AWS Organizations le permite administrar y gobernar 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 usar unidades organizativas (OU) para agrupar las cuentas y administrarlas como una sola unidad.

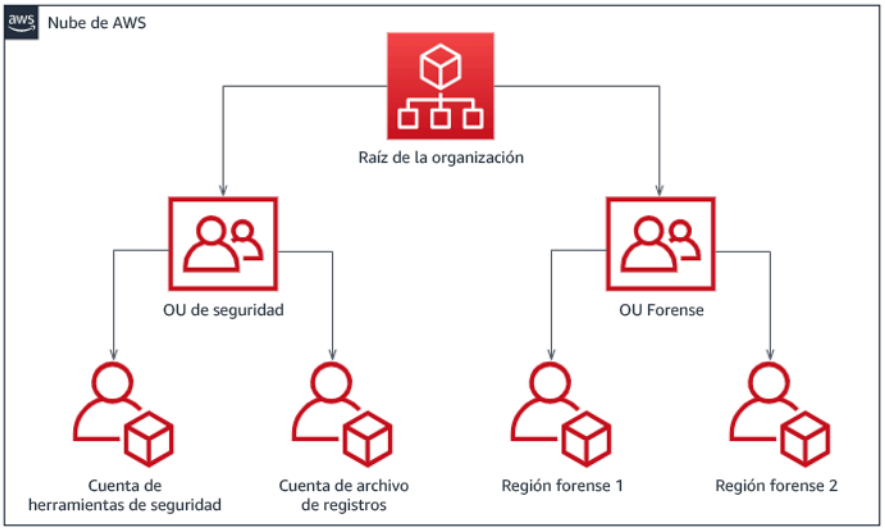
Para la respuesta a incidentes, es útil contar con una estructura de Cuenta de AWS que respalde las funciones de respuesta ante incidentes, lo que incluye una OU de seguridad y una OU forense. Dentro de la unidad organizativa de seguridad, debe tener cuentas para:

- 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 US East (N. Virginia) Region (`us-east-1`) y US West (Oregon) (`us-west-2`), entonces tendría dos cuentas en la OU 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

Capture 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 realizar 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 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 instrucciones 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.

Automatice 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 siguiente. 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

Vídeos relacionados:

- Automating Incident Response and Forensics

Ejemplos relacionados:

- Automated Incident Response and Forensics Framework
- Automated Forensics Orchestrator for Amazon EC2

SEC10-BP04 Desarrollar y probar guías estratégicas de respuesta a incidentes de seguridad

Una parte esencial de la preparación de los procesos de respuesta a incidentes es desarrollar unas guías estratégicas. Las guías estratégicas de respuesta a incidentes recogen una serie de 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, por ejemplo:

- Incidentes esperados: deben crearse guías estratégicas 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 guías estratégicas para las alertas y los resultados de seguridad conocidos, como los resultados de GuardDuty. Podría recibir un resultado de GuardDuty y pensar: «¿Y ahora qué?». Si desea evitar que un resultado de GuardDuty se ignore o no se gestione del modo correcto, cree una guía estratégica para cada posible resultado de GuardDuty. Puede encontrar información e instrucciones sobre los procesos de corrección en la documentación de GuardDuty. Conviene señalar que GuardDuty no está habilitado de forma predeterminada y que tiene un coste. Para obtener más detalles sobre GuardDuty, consulte Apéndice A: Definiciones de capacidades en la nube: visibilidad y alertas.

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.

Pasos para la implementación

Algunos de los elementos que deben incluirse en una guía estratégica son:

- 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 remisión a instancias superiores: ¿quién participa 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 por Well-Architected:

- SEC10-BP02 - Desarrolle planes de gestión 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 ha 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:

- Uso de la cuenta raíz para la respuesta ante incidentes.
- Alterar las cuentas de usuario 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 escalada de 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 de respuesta ante incidentes, le recomendamos que implemente la federación de identidades junto con el escalado temporal del 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 la solicitud es aprobada, el usuario recibe un conjunto de credenciales de AWS temporales que puede usar 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 el AWS Security Token Service y políticas de sesión para definir el alcance del 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 inmediato de emergencia configurado para permitir la investigación y la reparación puntual de los incidentes. También le recomendamos que utilice un usuario de IAM con los permisos adecuados para realizar tareas y acceder a los recursos de AWS. Utilice las credenciales del usuario raíz solo para tareas que requieren el acceso del 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 de usuario exclusivas. Las cuentas de usuario 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 realizar 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 de AWS Identity and Access Management 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 AWS Management Console, 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 usuario de IAM creadas para este fin no se compartan con otras personas y que el usuario raíz de Cuenta de AWS no se utilice a menos que se requiera para una tarea específica. 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 la contraseña y el token MFA del usuario raíz.

Para configurar las políticas de IAM de los roles de respuesta ante incidentes, utilice IAM Access Analyzer 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 realizadas. 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 guía de estrategias a fin de facilitar la administración y la auditoría. Entre los ejemplos de guías 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 usuario de respuesta ante incidentes para asumir los roles de IAM de respuesta ante incidentes exclusivas 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 `AssumeRole` para estos roles estén registradas en CloudTrail y se haya alertado de ellas y que se registre cualquier acción realizada con estos roles.

Se recomienda que tanto las cuentas de usuario 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 *<ID_USUARIO>*`-BREAK-GLASS` y los roles de IAM `BREAK-GLASS-ROLE`.

CloudTrail se utiliza para registrar la actividad de API en sus cuentas de AWS y debe utilizarse para configurar alertas sobre el uso de los roles 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 Amazon CloudWatch filtro a filtro en los eventos `AssumeRole` relacionados con el rol IAM de respuesta ante incidentes:

```
{ $.eventName = "AssumeRole" && $.requestParameters.roleArn =
 "<ARN_DE_ROL_DE_RESPUESTA_ANTE_INCIDENTES>" && $.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. Pueden ser instancias de Amazon Elastic Compute Cloud, bases de datos de Amazon Relational Database Service o plataformas de software como servicio (SaaS). Se recomienda que en lugar de utilizar protocolos nativos como SSH o RDP, se use AWS Systems Manager Session Manager 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 se podrían automatizar partes de sus guías de estrategias mediante documentos de AWS Systems Manager Run Command, lo que puede reducir los errores del usuario 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 administración de las cuentas de usuario de IAM de respuesta ante incidentes debe agregarse a sus procesos de incorporación, traslado y abandono de los empleados y revisarse y probarse periódicamente para verificar que solo se permite el acceso previsto.

Recursos

Documentos relacionados:

- Managing temporary elevated access to your AWS environment (Administrar el acceso de alto nivel temporal al entorno de AWS)
- AWS Security Incident Response Guide (Guía de respuesta ante incidentes de seguridad de AWS)
- AWS Elastic Disaster Recovery
- AWS Systems Manager Incident Manager
- Setting an account password policy for IAM users (Establecer una política de contraseñas de cuenta para los usuarios de IAM)
- Using multi-factor authentication (MFA) in AWS (Uso de la autenticación multifactor [MFA] en AWS)
- Configuring Cross-Account Access with MFA (Configuración del acceso entre cuentas con MFA)
- Using IAM Access Analyzer to generate IAM policies (Uso de IAM Access Analyzer para generar políticas de IAM)
- Best Practices for AWS Organizations Service Control Policies in a Multi-Account Environment (Prácticas recomendadas para las políticas de control de servicios de AWS Organizations en un entorno de varias cuentas)
- How to Receive Notifications When Your AWS Account's Root Access Keys Are Used (Cómo recibir notificaciones cuando se utilizan las claves de acceso raíz de su cuenta de AWS)
- Create fine-grained session permissions using IAM managed policies (Crear permisos de sesión detallados mediante políticas administradas de IAM)

Vídeos relacionados:

- Automating Incident Response and Forensics in AWS (Automatización de la respuesta ante incidentes y el análisis forense en AWS)

- DIY guide to runbooks, incident reports, and incident response (Guía paso a paso sobre runbooks, informes de incidentes y respuesta a incidentes)
- Prepare for and respond to security incidents in your AWS environment (Cómo prepararse y responder ante incidentes de seguridad en el entorno de AWS)

Ejemplos relacionados:

- Laboratorio: Configuración de la cuenta y usuario raíz de AWS
- Laboratorio: Respuesta ante incidentes con la consola de AWS y la CLI

SEC10-BP06: Desplegar las herramientas con anticipación

Asegúrese de que el personal de seguridad despliega 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 Amazon CloudWatch Anomaly Detection, 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, es necesario que pueda revisar los registros pertinentes para registrar y comprender el alcance completo y la cronología del incidente. También necesita registros para generar alertas que indiquen 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 coherente 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

Seleccione y configure registros de análisis y alertas

Consulte la siguiente documentación sobre la configuración de registros para la respuesta a incidentes:

- Estrategias de registro para la respuesta a incidentes de seguridad
- SEC04-BP01 Configurar el registro de servicios y aplicaciones

Habilite los servicios de seguridad para respaldar la detección y la respuesta

AWS ofrece funcionalidades nativas 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 las capacidades de la nube.

Desarrolle e implemente 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 detalles 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 detalles sobre la implementación y su aplicación, consulte Implement AWS resource tagging strategy using AWS Tag Policies and Service Control Policies (SCPs).

Recursos

Prácticas recomendadas por Well-Architected:

- SEC04-BP01 Configurar el registro de servicios y aplicaciones
- SEC04-BP02 Análisis centralizados de registros, hallazgos y métricas

Documentos relacionados:

- Estrategias de registro para la respuesta a incidentes de seguridad
- Incident response cloud capability definitions

Ejemplos relacionados:

- Threat Detection and Response with Amazon GuardDuty and Amazon Detective
- Security Hub Workshop
- Vulnerability Management with Amazon Inspector

SEC10-BP07 Ejecutar 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 uno de los métodos que se pueden utilizar para realizar 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.

Ventajas de aplicar esta práctica recomendada: las simulaciones brindan una serie de ventajas:

- 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 realizar una sesión de debate en la que participen las diversas partes interesadas en la respuesta a incidentes para practicar las funciones y responsabilidades, y utilizar las herramientas de comunicación y las guías estratégicas establecidas. Por lo general, este ejercicio se puede realizar 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) realiza una simulación para lograr un determinado objetivo o un conjunto de objetivos en 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 realizar 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 realizar los ejercicios de equipo rojo por su complejidad y su coste.

Pasos para la implementación

Independientemente del tipo de simulación que elija, las simulaciones suelen tener estos pasos de implementación:

1. Defina los elementos básicos del ejercicio: defina el escenario y los objetivos de la simulación. Ambos deben contar con la aceptación de los directivos.
2. Identifique a las principales partes interesadas: como mínimo, en un ejercicio se necesitan facilitadores y participantes. Dependiendo del escenario, podrían participar otras partes interesadas, como los directivos del departamento legal, de comunicaciones o ejecutivo.
3. Cree y pruebe el escenario: es posible que haya que redefinir el escenario a medida que se va creando si algunos elementos específicos no son factibles. Se espera que, al final de esta etapa, haya un escenario definitivo.

4. Facilite la simulación: el tipo de simulación determina la forma de realizarla (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. Desarrolle el 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:

- AWS Incident Response Guide

Vídeos relacionados:

- AWS GameDay - Security Edition

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, erradicacióny 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 en la sección Preparación para poder responder eficazmente a un evento de seguridad activo.

Para obtener más información, consulte la sección Operaciones de la Guía de respuestas ante incidentes de seguridad deAWS.

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, responder e investigar de forma eficaz los posibles incidentes de seguridad con el objetivo de reducir las posibles vulnerabilidades, el tiempo de respuesta y el retorno a operaciones seguras. Los siguientes mecanismos pueden ayudarle 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 Establecer 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 ayudará 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 siguientes puntos:

- ¿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 lograron escalar para responder al incidente?
- ¿Qué se puede mejorar en las siguientes áreas?:
  - Personal
    - ¿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?
  - Procesar
    - ¿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/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, despliega 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 coste 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 AppSec madura, puede aumentar la cantidad de pruebas que se llevan a cabo mediante la automatización, mejorar la fidelidad de la retroalimentación 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: organización y cultura, seguridad de la canalización, seguridad en la canalización y administración de dependencias. Cada área proporciona un conjunto de principios que puede implementar y ofrece una visión integral de cómo diseñar, desarrollar, compilar, desplegar 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 Formar en seguridad de las aplicaciones
- SEC11-BP02 Automatizar las pruebas a lo largo del ciclo de vida de desarrollo y lanzamiento
- SEC11-BP03 Realizar pruebas de penetración periódicas
- SEC11-BP04 Revisiones manuales del código
- SEC11-BP05 Centralizar los servicios para paquetes y dependencias
- SEC11-BP06 Desplegar software mediante programación
- SEC11-BP07 Evaluar periódicamente las propiedades de seguridad de las canalizaciones
- SEC11-BP08 Crear un programa que integre la propiedad de la seguridad en los equipos de la carga de trabajo

SEC11-BP01 Formar en seguridad de las aplicaciones

Ofrezca formación a los creadores de su organización sobre las prácticas habituales para el desarrollo y el funcionamiento seguros de las aplicaciones. La adopción de prácticas de desarrollo centradas en la seguridad contribuye a reducir la probabilidad de que surjan problemas que solo se detectan en la fase de revisión de la seguridad.

Resultado deseado: El software debe diseñarse y crearse teniendo en cuenta la seguridad. Cuando los creadores de una organización reciben formación sobre prácticas de desarrollo seguras que parten de un modelo de amenazas, mejora la calidad y la seguridad general del software producido. Este planteamiento puede acortar el tiempo hasta la entrega del software o de las características, ya que se reduce la necesidad de tener que volver a repetir los procesos tras la fase de revisión de la seguridad.

A efectos de esta práctica recomendada, el desarrollo seguro se refiere al software que se está escribiendo y a las herramientas o sistemas que prestan soporte al ciclo de vida de desarrollo del software (SDLC).

Patrones comunes de uso no recomendados:

- Esperar a una revisión de seguridad para estudiar las propiedades de seguridad de un sistema.
- Dejar todas las decisiones de seguridad en manos del equipo de seguridad.
- No comunicar claramente cómo se relacionan las decisiones tomadas en el SDLC con las expectativas o políticas generales de seguridad de la organización.

- Intervenir 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

Proporcione formación a los creadores de su organización. Una buena base para iniciar la formación sobre seguridad es empezar con un curso sobre modelado de amenazas. Lo ideal sería que los creadores pudieran acceder por sí mismos a la información relevante para sus cargas de trabajo. Este acceso les ayuda a tomar decisiones informadas sobre las propiedades de seguridad de los sistemas que crean sin necesidad de preguntar a otro equipo. El proceso de solicitud de revisiones al equipo de seguridad debe estar claramente definido y ser fácil de seguir. Los pasos del proceso de revisión deben incluirse en la formación sobre seguridad. Cuando se disponga de patrones o plantillas de implementación, deben ser fáciles de encontrar y vincular a los requisitos generales de seguridad. Plantéese el uso de AWS CloudFormation, Componentes de AWS Cloud Development Kit (AWS CDK), Service Catalog u otras herramientas basadas en plantillas para reducir la necesidad de configuración personalizada.

Pasos para la aplicación

- Empiece por ofrecer a los creadores un curso sobre modelado de amenazas para sentar una buena base y ayudarles a formarse en cómo pensar en la seguridad.
- Ofrezca acceso a formación para socios de AWS, sector o Formación de AWS y Certification.
- Ofrezca formación sobre el proceso de revisión de la seguridad de su organización, que aclare el reparto de responsabilidades entre el equipo de seguridad, los equipos de carga de trabajo y otras partes interesadas.
- Publique guías de autoservicio sobre cómo cumplir sus requisitos de seguridad, incluidos ejemplos de código y plantillas, si están disponibles.

- Obtenga comentarios periódicamente de los equipos de creadores sobre su experiencia con el proceso de formación y revisión de la seguridad, y utilícelos para mejorar.
- Utilice días de juegos o campañas de detección de errores para reducir el número de problemas y mejorar las competencias de los creadores.

Recursos

Prácticas recomendadas relacionadas:

- SEC11-BP08 Crear un programa que integre la propiedad de la seguridad en los equipos de la carga de trabajo

Documentos relacionados:

- Formación de AWS y Certification
- How to think about cloud security governance (Cómo concebir la gobernanza de la seguridad en la nube)
- How to approach threat modeling (Cómo abordar el modelado de amenazas)
- Accelerating training – The AWS Skills Guild (Acelere la formación: AWS Skills Guild)

Vídeos relacionados:

- Proactive security: Considerations and approaches (Seguridad proactiva: consideraciones y estrategias)

Ejemplos relacionados:

- Workshop on threat modeling (Taller de modelado de amenazas)
- Industry awareness for developers (Concienciación del sector para desarrolladores)

Servicios relacionados:

- AWS CloudFormation
- Componentes de AWS Cloud Development Kit (AWS CDK) (AWS CDK)
- Service Catalog

- AWS BugBust

SEC11-BP02 Automatizar 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 problemas de forma temprana y frecuente a lo largo del ciclo de vida de 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.
- Realizar 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:

- Menor 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 abarca 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 CodeWhisperer proporciona recomendaciones de código, incluido el análisis de seguridad, en el IDE del creador. Amazon CodeGuru Reviewer 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.

El taller de seguridad para desarrolladores usa herramientas de desarrollo de AWS, como AWS CodeBuild, AWS CodeCommit y AWS CodePipeline, para la automatización de canalizaciones de lanzamiento que incluyen 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 recogidos 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 aplicación

- 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.
- El taller de seguridad para desarrolladores ofrece un ejemplo de integración de pruebas estáticas y dinámicas en un proceso de lanzamiento.
- La realización de pruebas o análisis de código mediante herramientas automatizadas, como Amazon CodeWhisperer integrado con los IDE de los desarrolladores y Amazon CodeGuru Reviewer para escanear código al confirmar, ayuda a los desarrolladores a obtener información en el momento adecuado.
- Si usa AWS Lambda para la compilación, puede utilizar Amazon Inspector para analizar el código de la aplicación en sus funciones.
- El taller de CI/CD de AWS proporciona un punto de partida la crear canalizaciones de CI/CD en AWS.
- Cuando se incluyen pruebas automatizadas en las canalizaciones de CI/CD, es preciso utilizar un sistema de tickets para realizar un seguimiento de la notificación y corrección de problemas de software.
- En el caso de las pruebas de seguridad que puedan generar hallazgos, 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.

Recursos

Documentos relacionados:

- Entrega continua e implementación continua

- Socios con competencias en DevOps de AWS
- Socios con competencia en seguridad de AWS para la seguridad de las aplicaciones
- Choosing a Well-Architected CI/CD approach (Elección de un enfoque CI/CD bien diseñado)
- Monitoring CodeCommit events in Amazon EventBridge and Amazon CloudWatch Events (Supervisión de eventos de CodeCommit en Amazon EventBridge y Amazon CloudWatch Events)
- Secrets detection in Amazon CodeGuru Review (Revisión de la detección de secretos en Amazon CodeGuru)
- Accelerate deployments on AWS with effective governance (Acelerar los despliegues en AWS con una gobernanza eficaz)
- How AWS approaches automating safe, hands-off deployments (Cómo AWS aborda la automatización de despliegues seguros y sin intervención)

Vídeos relacionados:

- Hands-off: Automating continuous delivery pipelines at Amazon (Sin intervención: automatización de canalizaciones de entrega continua en Amazon)
- Automating cross-account CI/CD pipelines (Automatización de canalizaciones CI/CD entre cuentas)

Ejemplos relacionados:

- Industry awareness for developers (Concienciación del sector para desarrolladores)
- AWS CodePipeline Governance (Gobernanza de AWS CodePipeline) (GitHub)
- Security for Developers workshop (Taller de seguridad para desarrolladores)
- AWS CI/CD Workshop (Taller de CI/CD de AWS)

SEC11-BP03 Realizar pruebas de penetración periódicas

Realice 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 realice 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, remediar 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 hallazgos 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 violación 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 realizar 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 aplicación

- Tenga 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 realizar 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 Formar en seguridad de las aplicaciones

- SEC11-BP02 Automatizar las pruebas a lo largo del ciclo de vida de desarrollo y lanzamiento

Documentos relacionados:

- Las pruebas de penetración de AWS ofrecen orientación detallada sobre las pruebas de penetración en AWS
- Accelerate deployments on AWS with effective governance (Acelerar los despliegues en AWS con una gobernanza eficaz)
- Socios con competencia en seguridad de AWS
- Modernize your penetration testing architecture on AWS Fargate (Modernice su arquitectura de pruebas de penetración en AWS Fargate)
- AWS Fault injection Simulator

Ejemplos relacionados:

- Automate API testing with AWS CodePipeline (Automatización de las pruebas de API con AWS CodePipeline) (GitHub)
- Automated security helper (Ayudante de seguridad automatizado) (GitHub)

SEC11-BP04 Revisiones manuales del código

Realice una revisión manual del código del software que produce. Este proceso ayuda a verificar que la persona que ha escrito el código no es la única que comprueba su calidad.

Resultado deseado: La inclusión de un paso de revisión manual del código durante el desarrollo aumenta la calidad del software que se está escribiendo, ayuda a mejorar las competencias de los miembros con menos experiencia del equipo y da la oportunidad de identificar los puntos en los que se puede utilizar la automatización. Las revisiones manuales del código pueden apoyarse en herramientas y pruebas automatizadas.

Patrones comunes de uso no recomendados:

- No revisar el código antes del despliegue.
- Tener una misma persona que escriba y revise el código.
- No utilizar la automatización para ayudar u organizar las revisiones del código.
- No formar a los creadores sobre la 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

La etapa de revisión debe implementarse como parte del flujo general de gestión del código. Los pormenores dependen del planteamiento utilizado para la bifurcación, las solicitudes de incorporación de cambios y la fusión. Utilice AWS CodeCommit o soluciones de terceros como GitHub, GitLab o Bitbucket. Sea cual sea el método que utilice, es importante verificar que sus procesos requieren la revisión del código antes de desplegarlo en un entorno de producción. El uso de herramientas como Amazon CodeGuru Reviewer puede facilitar la organización del proceso de revisión del código.

Pasos para la aplicación

- Implemente un paso de revisión manual como parte del flujo de administración de código y realice esta revisión antes de continuar.
- Considere Amazon CodeGuru Reviewer para administrar y ayudar en las revisiones de código.
- Implemente un flujo de aprobación que exija que se complete una revisión del código antes de que este pueda pasar a la siguiente etapa.
- Compruebe que existe un proceso para identificar los problemas encontrados durante las revisiones manuales del código que podrían detectarse automáticamente.
- Integre el paso de revisión manual del código de forma que se ajuste a sus prácticas de desarrollo de código.

Recursos

Prácticas recomendadas relacionadas:

- SEC11-BP02 Automatizar las pruebas a lo largo del ciclo de vida de desarrollo y lanzamiento

Documentos relacionados:

- Working with pull requests in AWS CodeCommit repositories (Trabajo con solicitudes de incorporación de cambios en repositorios de AWS CodeCommit)
- Working with approval rule templates in AWS CodeCommit (Trabajar con plantillas de reglas de aprobación en AWS CodeCommit)
- About pull requests in GitHub (Acerca de las solicitudes de incorporación de cambios en GitHub)
- Automate code reviews with Amazon CodeGuru Reviewer (Revisiones automáticas de código con Amazon CodeGuru Reviewer)
- Automating detection of security vulnerabilities and bugs in CI/CD pipelines using Amazon CodeGuru Reviewer CLI (Automatización de la detección de vulnerabilidades y errores de seguridad en los procesos CI/CD mediante la CLI de Amazon CodeGuru Reviewer)

Vídeos relacionados:

- Continuous improvement of code quality with Amazon CodeGuru (Mejora continua de la calidad del código con Amazon CodeGuru)

Ejemplos relacionados:

- Security for Developers workshop (Taller de seguridad para desarrolladores)

SEC11-BP05 Centralizar los servicios para paquetes y dependencias

Proporcione servicios centralizados para que los equipos de creadores 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: El software se compone de un conjunto de otros paquetes de software además del código que se escribe. Esto facilita el consumo de implementaciones de funcionalidades que se utilizan repetidamente, como un analizador JSON o una biblioteca de cifrado. La centralización lógica

de los orígenes de estos paquetes y dependencias proporciona un mecanismo para que los equipos de seguridad validen las propiedades de los paquetes antes de utilizarlos. Este planteamiento también reduce el riesgo de que se produzca un problema inesperado debido a un cambio en un paquete existente o a la inclusión por equipos de creadores de paquetes arbitrarios directamente desde Internet. Utilice 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:

- Obtener paquetes de repositorios arbitrarios de Internet.
- No probar nuevos paquetes antes de ponerlos a disposición de los desarrolladores.

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 basándose en 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 añadir paquetes al repositorio cuando se produzcan actualizaciones o surjan nuevos requisitos. Los servicios de AWS como AWS CodeArtifact o soluciones similares de socios de AWS son una forma de ofrecer esta capacidad.

Pasos para la aplicación:

- 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 Automatizar las pruebas a lo largo del ciclo de vida de desarrollo y lanzamiento

Documentos relacionados:

- Accelerate deployments on AWS with effective governance (Acelerar los despliegues en AWS con una gobernanza eficaz)
- Tighten your package security with CodeArtifact Package Origin Control toolkit (Refuerce la seguridad de sus paquetes con el kit de herramientas de control de origen de paquetes de CodeArtifact)
- Detecting security issues in logging with Amazon CodeGuru Reviewer (Detección de problemas de seguridad en el registro con Amazon CodeGuru Reviewer)
- Supply chain Levels for Software Artifacts (SLSA) (Niveles de la cadena de suministro de artefactos de software [SLSA])

Vídeos relacionados:

- Proactive security: Considerations and approaches (Seguridad proactiva: consideraciones y estrategias)
- The AWS Philosophy of Security (re:Invent 2017) (La filosofía de seguridad de AWS [re:Invent 2017])
- When security, safety, and urgency all matter: Handling Log4Shell (Cuando la seguridad, la protección y la urgencia son importantes: gestión de Log4Shell)

Ejemplos relacionados:

- Multi Region Package Publishing Pipeline (Canalización de publicación de paquetes multirregión) [GitHub])
- Publishing Node.js Modules on AWS CodeArtifact using AWS CodePipeline (Publicación de módulos Node.js en AWS CodeArtifact con AWS CodePipeline) (GitHub)
- AWS CDK Java CodeArtifact Pipeline Sample (Ejemplo de canalización de CodeArtifact en Java en AWS CDK) (GitHub)
- Distribute private .NET NuGet packages with AWS CodeArtifact (Distribuir paquetes NuGet .NET privados con AWS CodeArtifact) (GitHub)

SEC11-BP06 Desplegar software mediante programación

Siempre que sea posible, realice los despliegues de software mediante programación. Con este enfoque se reduce la probabilidad de que se produzca un error en el despliegue o de que surja un problema inesperado debido a un error humano.

Resultado deseado: Mantener a las personas alejadas de los datos es un principio clave para crear de forma segura en la Nube de AWS. Este principio incluye la forma de desplegar el software.

La ventaja de no depender de personas para desplegar el software es que tendrá mayor confianza en que se ha probado lo que se despliega, y que el despliegue se realice siempre de forma coherente. No tendrá que modificar el software para que funcione en distintos entornos. El uso de los principios del desarrollo de aplicaciones de doce factores, en concreto la externalización de la configuración, le permite desplegar el mismo código en varios entornos sin necesidad de realizar cambios. La firma criptográfica de los paquetes de software es una buena forma de verificar que no ha cambiado nada entre entornos. El resultado general de este método es que se reduce el riesgo en el proceso de cambio y mejorar la coherencia de las versiones de software.

Patrones comunes de uso no recomendados:

- Despliegue manual del software en producción.
- Realización manual de cambios 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 el despliegue.
- Capacidad para demostrar criptográficamente que el software probado es el software desplegado.

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

Guía para la implementación

Cree su estructura de cuenta de Cuenta de AWS de forma que elimine el acceso humano persistente desde los entornos y utilice herramientas de CI/CD para realizar los despliegues. Diseñe las aplicaciones de manera que los datos de configuración específicos del entorno se obtengan de un origen externo, como el Parameter Store de AWS Systems Manager. Firme los paquetes después de probarlos y valide estas firmas durante el despliegue. Configure las canalizaciones de CI/CD para que envíen el código de la aplicación y utilice valores controlados para confirmar que el despliegue ha tenido lugar como corresponde. Utilice herramientas como AWS CloudFormation o AWS CDK para definir su infraestructura y, a continuación, use AWS CodeBuild y AWS CodePipeline para realizar las operaciones de CI/CD.

Pasos para la aplicación

- Cree canalizaciones de CI/CD bien definidas para agilizar el proceso de despliegue.
- Proporcione capacidad de CI/CD para simplificar la integración de las pruebas de seguridad en las canalizaciones con AWS CodeBuild y AWS Code Pipeline.
- Siga las directrices sobre separación de entornos del documento técnico Organizing Your AWS Environment Using Multiple Accounts (Organización del entorno de AWS con varias cuentas).
- Verifique que no haya acceso humano persistente a los entornos donde se ejecutan las cargas de trabajo de producción.
- Diseñe las aplicaciones de modo que admitan la externalización de datos de configuración.
- Piense en la posibilidad de llevar a cabo el despliegue mediante un modelo de despliegue azul-verde.
- Implemente valores controlados para validar el despliegue correcto del software.
- Utilice herramientas criptográficas como AWS Signer o AWS Key Management Service (AWS KMS) para firmar y verificar los paquetes de software que está desplegando.

Recursos

Prácticas recomendadas relacionadas:

- SEC11-BP02 Automatizar las pruebas a lo largo del ciclo de vida de desarrollo y lanzamiento

Documentos relacionados:

- AWS CI/CD Workshop (Taller de CI/CD de AWS)
- Accelerate deployments on AWS with effective governance (Acelerar los despliegues en AWS con una gobernanza eficaz)
- Automatización de implementaciones seguras y sin intervención
- Code signing using AWS Certificate Manager Private CA and AWS Key Management Service asymmetric keys (Firma de código mediante CA privada de AWS Certificate Manager y claves asimétricas deAWS Key Management Service)
- Code Signing, a Trust and Integrity Control for AWS Lambda (Firma de código, un control de confianza e integridad para AWS Lambda)

Vídeos relacionados:

- Hands-off: Automating continuous delivery pipelines at Amazon (Sin intervención: automatización de canalizaciones de entrega continua en Amazon)

Ejemplos relacionados:

- Blue/Green deployments with AWS Fargate Despliegues azul-verde AWS Fargate)

SEC11-BP07 Evaluar periódicamente las propiedades de seguridad de las canalizaciones

Aplique los principios del pilar de seguridad de Well-Architected a sus canalizaciones, prestando 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 y desplegar el software deben seguir las mismas prácticas recomendadas que cualquier otra carga de trabajo en su entorno. Los desarrolladores no deben poder editar las pruebas que se implementan en las canalizaciones que utilizan. Las canalizaciones solo deben tener los permisos necesarios para los despliegues que están realizando y debe implementar salvaguardas para evitar que se desplieguen en los entornos equivocados. Las canalizaciones no deben depender de credenciales a largo plazo; además, deben estar configuradas para emitir estado de forma 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 despliegue.
- 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 construye y despliega a través de las canalizaciones.
- Capacidad de detener un despliegue cuando hay actividades sospechosas.

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

Guía para la implementación

Comience con servicios de CI/CD administrados que admiten roles de IAM para reducir el riesgo de fuga de credenciales. La aplicación de los principios del pilar de seguridad a la infraestructura de canalización de CI/CD puede ayudarle a determinar dónde es posible realizar mejoras de seguridad. Siga la arquitectura de referencia de canalizaciones de despliegue de AWS. Es un buen punto de partida para crear entornos de CI/CD. Revise a intervalos regulares la implementación de la canalización y analice los registros para detectar comportamientos inesperados; esto puede ayudarle a comprender los patrones de uso de las canalizaciones que se utilizan para desplegar software.

Pasos para la aplicación

- Empiece con la arquitectura de referencia de canalizaciones de despliegue de AWS.
- Plantéese la posibilidad de utilizar AWS IAM Access Analyzer para generar mediante programación políticas de IAM de privilegios mínimos para las canalizaciones.
- Integre las canalizaciones con monitorización y alertas para que recibir notificaciones de actividad inesperada o anómala. Para los servicios administrados de AWS, Amazon EventBridge le permite enrutar datos a destinos como AWS Lambda o Amazon Simple Notification Service (Amazon SNS).

Recursos

Documentos relacionados:

- AWS Deployment Pipelines Reference Architecture (Arquitectura de referencia de canalizaciones de despliegue de AWS)
- Monitoring AWS CodePipeline (Monitorización de AWS CodePipeline)
- Security best practices for AWS CodePipeline (Prácticas recomendadas de seguridad de AWS CodePipeline)

Ejemplos relacionados:

- DevOps monitoring dashboard (Panel de monitorización de DevOps) (GitHub)

SEC11-BP08 Crear 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. Aún 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: Para integrar la propiedad de la seguridad y la toma de decisiones en los equipos de creación, puede formar a los creadores sobre cómo pensar en la seguridad o puede mejorar su formación con personal de seguridad integrado o asociado a los equipos de creación. Cualquiera de las dos estrategias es válida y permite al equipo tomar decisiones de seguridad de mayor calidad en una fase más temprana del ciclo de desarrollo. Este modelo de propiedad se basa en la formación para lograr la seguridad de las aplicaciones. Empiece con el modelo de amenazas para la carga de trabajo concreta, lo que ayudará a dirigir el enfoque de diseño al contexto apropiado. Otra ventaja de contar con una comunidad de desarrolladores centrados en la seguridad, o con un grupo de ingenieros de seguridad que trabajen con equipos de creadores, es que es posible comprender más a fondo cómo se escribe el software. Esta comprensión le ayuda a determinar las próximas áreas de mejora en su capacidad de automatización.

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 escribe.
- 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 hallazgos 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

Empiece con la orientación de SEC11-BP01 Formar 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 abordaje inicial, deberá realizar 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 aplicación

- Empiece por formar a los desarrolladores en la seguridad para las aplicaciones.
- Cree una comunidad y un programa de incorporación para educar a los creadores.
- Elija un nombre para el programa. Los más utilizados son «Guardians», «Champions» o «Advocates».
- Identifique el modelo 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 creadores 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 creadores y el personal de seguridad. Utilice estas métricas para acometer mejoras.

Recursos

Prácticas recomendadas relacionadas:

- SEC11-BP01 Formar en seguridad de las aplicaciones
- SEC11-BP02 Automatizar las pruebas a lo largo del ciclo de vida de desarrollo y lanzamiento

Documentos relacionados:

- How to approach threat modeling (Cómo abordar el modelado de amenazas)

- How to think about cloud security governance (Cómo concebir la gobernanza de la seguridad en la nube)

Vídeos relacionados:

- Proactive security: Considerations and approaches (Seguridad proactiva: consideraciones y estrategias)

Conclusión

La seguridad es un esfuerzo constante. Cuando se produzca un incidente, debe tratarse como una oportunidad de mejorar la seguridad de la arquitectura. Disponer de controles de identidad, automatizar las respuestas a eventos de seguridad, proteger la infraestructura en varios niveles y administrar datos bien clasificados con cifrado proporciona la defensa integral que toda organización debe implementar. Este esfuerzo es más fácil gracias a las funciones de programación y a las características y los servicios de AWS que se detallan en el presente documento.

La aspiración de AWS es ayudarle a crear y utilizar arquitecturas que protejan la información, los sistemas y los recursos mientras aumenta el valor de negocio.

Colaboradores

Las siguientes personas y organizaciones contribuyeron a redactar este documento:

- Sarita Dharankar, líder del pilar de seguridad, Well-Architected, Amazon Web Services
- Adam Cerini, arquitecto de soluciones sénior, Amazon Web Services
- Bill Shinn, director, oficina del director de seguridad de la información (CISO), Amazon Web Services
- Brigid Johnson, directora de desarrollo de software, AWS Identity, Amazon Web Services
- Byron Pogson, arquitecto de soluciones sénior, Amazon Web Services
- Charlie Hammell, arquitecto empresarial principal, Amazon Web Services
- Darran Boyd, arquitecto principal de soluciones de seguridad, servicios financieros, Amazon Web Services
- Dave Walker, arquitecto principal de soluciones especializadas, seguridad y cumplimiento, Amazon Web Services
- John Formento, arquitecto de soluciones sénior, Amazon Web Services
- Paul Hawkins, director, oficina del director de seguridad de la información (CISO), Amazon Web Services
- Sam Elmalak, líder tecnológico sénior, Amazon Web Services
- Pat Gaw, asesor principal de seguridad, Amazon Web Services
- Daniel Begimher, asesor sénior, seguridad, Amazon Web Services
- Danny Cortegaca, arquitecto sénior de soluciones de seguridad, Amazon Web Services
- Ana Malhotra, arquitecta de soluciones de seguridad, Amazon Web Services
- Debashis Das, director, oficina del director de seguridad de la información (CISO), Amazon Web Services
- Reef Dsouza, Principal Solutions Architect, Amazon Web Services
- Brad Burnett, Security Solutions Architect, Identity, Amazon Web Services
- Anna McAbee, Senior Security Solutions Architect, Threat Detection and Incident Response, Amazon Web Services
- Jason Garman, Principal Security Solutinos Architect, Amazon Web Services

Otra documentación

Para obtener ayuda adicional, consulte las siguientes fuentes:

- Documento técnico de AWS Well-Architected Framework
- Centro de arquitectura de AWS

Revisiones del documento

Para recibir notificaciones sobre las actualizaciones de este documento técnico, suscríbase al canal RSS.

Cambio	Descripción	Fecha
Actualizaciones de la guía sobre las prácticas recomendadas	Las prácticas recomendadas se han actualizado con nuevas directrices en las siguientes áreas: Funcionamiento seguro de las cargas de trabajo y Protección de los datos en tránsito.	December 6, 2023
Actualizaciones de la guía sobre las prácticas recomendadas	Actualizaciones importantes de la guía y las prácticas recomendadas en Respuesta ante incidentes. Se han actualizado varias prácticas recomendadas en Preparación. Se han añadido dos áreas nuevas a la respuesta ante incidentes: Operaciones y Actividad posterior al incidente. Se ha añadido una nueva práctica recomendada: SEC10-BP08 Establecer un marco de trabajo para aprender de los incidentes.	October 3, 2023
Actualizaciones de la guía sobre las prácticas recomendadas	Se han realizado actualizaciones de las prácticas recomendadas con nuevas	July 13, 2023

	guías en las siguientes áreas: «Prepárese» y«Simule».	
Actualizaciones del nuevo marco.	Prácticas recomendadas actualizadas con guía prescriptiva y prácticas recomendadas añadidas. Se ha añadido una nueva área de prácticas recomendadas de seguridad de aplicaciones (AppSec).	April 10, 2023
Documento técnico actualizado	Prácticas recomendadas actualizadas con nueva guía de implementación.	December 15, 2022
Documento técnico actualizado	Se han ampliado las prácticas recomendadas y se han añadido planes de mejora.	October 20, 2022
Actualización menor	Se ha actualizado la información de IAM para reflejar las prácticas recomendadas actuales.	June 28, 2022
Actualización menor	Se ha añadido información adicional de AWS PrivateLink y se han corregido los enlaces que no funcionan.	May 19, 2022
Actualización menor	Se ha añadido AWS PrivateLink.	May 6, 2022
Actualización menor	Se ha eliminado el lenguaje no inclusivo.	April 22, 2022
Actualización menor	Se ha añadido información sobre el Analizador de acceso de la red de VPC.	February 2, 2022

Actualización menor	Se ha añadido Pilar de sostenibilidad a la introducción.	December 2, 2021
Actualización menor	Se ha corregido el enlace que no funciona.	May 27, 2021
Actualización menor	Se han realizado cambios editoriales en todo el documento.	May 17, 2021
Actualización importante	Se ha añadido la sección de gobernanza, se han detallado varias secciones y se han añadido nuevas características y servicios en todo el documento.	May 7, 2021
Actualización menor	Se han actualizado los enlaces.	March 10, 2021
Actualización menor	Se ha corregido el enlace que no funciona.	July 15, 2020
Actualizaciones del nuevo marco	Se ha actualizado la guía sobre la administración de permisos, identidades y cuentas.	July 8, 2020
Actualizaciones del nuevo marco	Se ha actualizado para ampliar el asesoramiento en cada área y para añadir nuevas prácticas recomendadas, servicios y características.	April 30, 2020

Documento técnico actualizado	Actualizaciones para reflejar los nuevos servicios y características de AWS y poner al día las referencias.	July 1, 2018
Documento técnico actualizado	Se ha actualizado la sección Configuración y mantenimiento de seguridad del sistema para reflejar los nuevos servicios y características de AWS.	May 1, 2017
Publicación inicial	Publicación de Pilar de seguridad: AWS Well-Architected Framework.	November 1, 2016

Avisos

Los clientes son responsables de realizar sus propias evaluaciones de la información contenida en este documento. Este documento: (a) solo tiene fines informativos, (b) representa las prácticas y las ofertas de productos vigentes de AWS, que están sujetas a cambios sin previo aviso, y (c) no crea ningún compromiso ni garantía de AWS y sus empresas afiliadas, proveedores o concesionarios de licencias. Los productos o servicios de AWS se proporcionan «tal cual», sin garantías, declaraciones ni condiciones de ningún tipo, ya sean explícitas o implícitas. Las responsabilidades y obligaciones de AWS en relación con sus clientes se rigen por los acuerdos de AWS, y este documento no modifica ni forma parte de ningún acuerdo entre AWS y sus clientes.