AWS Guía del usuario de respuesta a incidentes de seguridad

Version December 1, 2024

AWS Guía del usuario de respuesta a incidentes de seguridad:

Table of Contents

¿Qué es AWS la respuesta a incidentes de seguridad?

AWS La respuesta a incidentes de seguridad le ayuda a prepararse, responder y recibir orientación rápidamente para recuperarse de los incidentes de seguridad. Esto incluye incidentes como la apropiación de cuentas, las filtraciones de datos y los ataques de ransomware.

AWS La respuesta a incidentes de seguridad clasifica las conclusiones, intensifica los eventos de seguridad y gestiona los casos que requieren su atención inmediata. Además, tiene acceso al equipo de respuesta a incidentes del AWS cliente (CIRT), que investigará los recursos afectados.

> **Note**
>
> No hay garantía de que los recursos afectados puedan recuperarse. Recomendamos establecer y mantener copias de seguridad de los recursos que podrían afectar a los requisitos de su empresa.

AWS La respuesta a incidentes de seguridad funciona con otros servicios AWS de detección y respuesta y lo guía a lo largo de todo el ciclo de vida del incidente, desde la detección hasta la recuperación.

Contenido

Configuraciones admitidas

AWS La respuesta a incidentes de seguridad admite las siguientes configuraciones de idioma y región:

- Idioma: AWS La respuesta a incidentes de seguridad está disponible en inglés.
- AWS Regiones compatibles:

  AWS La respuesta a incidentes de seguridad está disponible en un subconjunto de Regiones de AWS. En estas regiones compatibles, puede crear una membresía, crear y ver casos y acceder al panel de control.

- Este de EE. UU. (Ohio)
- Oeste de EE. UU. (Oregón)
- EE.UU. Este (Virginia)
- UE (Fráncfort)
- UE (Irlanda)
- UE (Londres)
- UE (Estocolmo)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Tokio)
- Canadá (centro)

Cuando habilitas la función de supervisión e investigación, AWS Security Incident Response monitorea los GuardDuty hallazgos de Amazon de todos los anuncios activos Regiones de AWS. Como práctica recomendada de seguridad, AWS recomienda habilitarla GuardDuty en todas AWS las regiones compatibles. Esta configuración permite GuardDuty generar información sobre actividades no autorizadas o inusuales, incluso Regiones de AWS cuando no se despliegan recursos de forma activa. Al hacerlo, mejora su postura general de seguridad y mantiene una cobertura integral de detección de amenazas en todo su AWS entorno.

> **Note**
>
> Amazon GuardDuty informa de los resultados de las regiones configuradas. Si decides no habilitar el servicio en una región específica, las alertas no estarán disponibles.

Resumen de las funciones

Supervisión e investigación

AWS Security Incident Response revisa rápidamente las alertas de seguridad de Amazon GuardDuty y las integraciones de terceros AWS Security Hub, lo que reduce el número de alertas que tu equipo necesita analizar. Configura las reglas de supresión en función de su entorno para reducir las alertas de baja prioridad que necesita clasificar e investigar.

Optimice la respuesta a los incidentes

Amplíe y ejecute la respuesta a los incidentes en cuestión de minutos con las partes interesadas, los servicios y las herramientas de terceros pertinentes.

Soluciones de seguridad de autoservicio

AWS La respuesta APIs a incidentes de seguridad permite integrar y crear sus propias soluciones de seguridad personalizadas.

Panel de control para mayor visibilidad

Supervise y mida la preparación para responder a incidentes.

Postura de seguridad

Acceda a las AWS mejores prácticas y a las herramientas verificadas para evaluar la seguridad e investigar rápidamente la respuesta a los incidentes.

Asistencia expedita

Conéctese con AWS el equipo de respuesta a incidentes del cliente (CIRT) para investigar, contener y recibir orientación sobre las formas de recuperarse de los eventos de seguridad.

Preparación y preparación

Implemente una notificación simplificada configurando un equipo de respuesta a incidentes que active alertas para las personas o grupos designados, con políticas de permisos predefinidas.

Conceptos y terminología

Los siguientes términos y conceptos son importantes para comprender el servicio de respuesta a incidentes de AWS seguridad y su funcionamiento.

Alcance: AWS Security Incident Response se ajusta a la Guía de gestión de incidentes de seguridad informática del Instituto Nacional de Estándares y Tecnología (NIST) 800-61, y proporciona un enfoque coherente de la gestión de eventos de seguridad en relación con las mejores prácticas del sector.

Análisis: la investigación y el examen detallados de un incidente de seguridad para comprender su alcance, impacto y causa raíz.

AWS Portal del servicio de respuesta a incidentes de seguridad: un portal de autoservicio para iniciar y gestionar los casos de eventos de seguridad. La comunicación y la presentación de informes continuas se facilitan mediante el sistema de venta de entradas, las notificaciones automatizadas y la interacción directa con el equipo de servicio.

Comunicación: el diálogo y el intercambio de información continuos entre el equipo de respuesta a incidentes de AWS seguridad y el cliente durante el proceso de respuesta a los incidentes.

Contención, erradicación y recuperación: la prevención de nuevas actividades no autorizadas (contención), junto con la eliminación de los recursos no autorizados y la vulnerabilidad original (erradicación), y la recuperación de los recursos para volver a la normalidad.

Mejora continua: la respuesta a los incidentes de AWS seguridad incorpora los comentarios y las lecciones aprendidas en proyectos anteriores para mejorar sus capacidades de detección, sus procesos de investigación y las medidas correctivas. AWS La respuesta a incidentes de seguridad también se basa en up-to-date las amenazas de seguridad más recientes y las mejores prácticas para abordar los cambiantes desafíos de seguridad.

Evento de ciberseguridad: cualquier suceso observable en un sistema o red que infrinja o amenace con infringir las políticas de seguridad, las políticas de uso aceptable o las prácticas de seguridad estándar.

Equipo de respuesta a incidentes: grupo de personas que brindan apoyo durante los eventos de seguridad activos. Para los casos AWS admitidos, este es el equipo de respuesta a incidentes del AWS cliente (CIRT).

Flujo de trabajo de respuesta a incidentes: secuencia definida de pasos y actividades que intervienen en la end-to-end gestión de un incidente de seguridad, de conformidad con la norma NIST 800-61.

Herramientas de investigación: herramientas de respuesta a incidentes de AWS seguridad y funciones vinculadas al servicio que se utilizan para revisar el estado operativo de su cuenta y sus recursos.

Lecciones aprendidas: revisión y documentación de la respuesta a un evento de seguridad para identificar áreas de mejora e informar la planificación de la respuesta a incidentes en el futuro.

Supervisión e investigación: AWS Security Incident Response revisa rápidamente las alertas de seguridad de Amazon GuardDuty y pone de relieve las alertas más importantes que su equipo necesita analizar. Configura las reglas de supresión en función de las características específicas de su entorno para evitar alertas innecesarias.

Preparación: las actividades que se llevan a cabo para preparar a una organización para responder y gestionar eficazmente los eventos de seguridad, como el desarrollo de planes de respuesta a incidentes y procedimientos de prueba.

Informes y comunicación: los procesos que se utilizan para mantenerlo informado durante todo el proceso de respuesta a los incidentes, incluidas las notificaciones automatizadas, las pasarelas de llamadas y la entrega de material de investigación. AWS La respuesta a incidentes de seguridad proporciona un panel único y centralizado AWS Management Console para gestionar todos sus esfuerzos de respuesta a incidentes de AWS seguridad.

Inteligencia generada por el personal de respuesta: indicadores de compromiso; tácticas, técnicas y procedimientos; y patrones asociados observados en AWS CIRT las investigaciones.

Experiencia en eventos de seguridad: los conocimientos y habilidades especializados necesarios para responder y gestionar eficazmente los eventos de seguridad, especialmente en el contexto de la AWS nube.

Modelo de responsabilidad compartida: división de las responsabilidades de seguridad entre AWS y el cliente, donde AWS es responsable de la seguridad de la nube y el cliente es responsable de la seguridad en la nube.

Inteligencia sobre amenazas: fuentes de datos internas y externas que contienen detalles sobre actividades no autorizadas para ayudar a identificar las amenazas de seguridad en constante evolución y responder a ellas.

Sistema de venta de entradas: una plataforma dedicada a la gestión de casos que le permite incorporar y gestionar los casos de incidentes de seguridad, añadir archivos adjuntos y realizar un seguimiento del ciclo de vida de la respuesta a los incidentes.

Clasificación: la evaluación inicial y la priorización de un evento de seguridad para determinar la respuesta adecuada y los próximos pasos.

Flujo de trabajo: secuencia definida de pasos y actividades que intervienen en la end-to-end gestión de un evento de seguridad.

Introducción

Contenido

Seleccione una cuenta de membresía

Una cuenta de membresía es la AWS cuenta que se utiliza para configurar los detalles de la cuenta, añadir y eliminar los detalles del equipo de respuesta a incidentes y donde se pueden crear y gestionar todos los eventos de seguridad activos e históricos. Se recomienda que alinee su cuenta de membresía de AWS Security Incident Response con la misma cuenta que ha habilitado para servicios como Amazon GuardDuty y AWS Security Hub.

Tiene dos opciones para seleccionar su cuenta de membresía AWS de Security Incident Response utilizando AWS Organizations. Puede crear una membresía en la cuenta de administración de Organizations o en una cuenta de administrador delegado de Organizations.

Utilice la cuenta de administrador delegado: las tareas administrativas de respuesta a incidentes de AWS seguridad y la gestión de casos se encuentran en la cuenta de administrador delegado. Le recomendamos que utilice el mismo administrador delegado que ha configurado para otros servicios de AWS seguridad y cumplimiento. Proporcione el ID de cuenta del administrador delegado de 12 dígitos y, a continuación, inicie sesión en esa cuenta para continuar.

Utilice la cuenta que ha iniciado sesión actualmente: al seleccionar esta cuenta, la cuenta actual será la cuenta de membresía central de su membresía de respuesta a incidentes AWS de seguridad. Las personas de su organización deberán acceder al servicio a través de esta cuenta para crear, acceder y gestionar los casos activos y resueltos.

Asegúrese de tener los permisos suficientes para administrar la respuesta a incidentes de AWS seguridad.

Consulte Añadir y eliminar permisos de IAM identidad para ver los pasos específicos para añadir permisos.

Consulte las políticas gestionadas de respuesta a incidentes de AWS seguridad.

Para verificar IAM los permisos, puede seguir estos pasos:

- Compruebe la IAM política: revise la IAM política asociada a su usuario, grupo o rol para asegurarse de que concede los permisos necesarios. Para ello, vaya a la opción https://console.aws.amazon.com/iam/, seleccione la `Users` opción, elija el usuario específico y, a continuación, en su página de resumen, vaya a la `Permissions` pestaña en la que encontrará una lista de todas las políticas adjuntas. Puede ampliar cada fila de la política para ver sus detalles.
- Pruebe los permisos: intente realizar la acción necesaria para verificar los permisos. Por ejemplo, si necesitas acceder a un caso, inténtaloListCases. Si no tienes los permisos necesarios, recibirás un mensaje de error.
- Usa AWS CLI oSDK: puedes usar la interfaz de línea de AWS Command Line Interface comandos (CLI) o el lenguaje AWS SDK de programación que prefieras para probar los permisos. Por ejemplo, con la AWS Command Line Interface, puede ejecutar el `aws sts get-caller-identity` comando para verificar sus permisos de usuario actuales.
- Compruebe los AWS CloudTrail registros: revise los CloudTrail registros para comprobar si se están registrando las acciones que intenta realizar. Esto puede ayudarte a identificar cualquier problema con los permisos.
- Utilice el IAM simulador de IAM políticas: el simulador de políticas es una herramienta que le permite probar IAM las políticas y ver el efecto que tienen en sus permisos.

> **Note**
>
> Los pasos específicos pueden variar según el AWS servicio y las acciones que intentes realizar.

Configura los detalles de la membresía

- Seleccione un Región de AWS lugar donde se guardarán su membresía y sus casos.

> **Warning**
>
> No puedes cambiar la configuración predeterminada Región de AWS después del registro inicial de la membresía.

- Si lo desea, puede seleccionar un nombre para esta membresía.
- Debe proporcionar un contacto principal y uno secundario como parte del flujo de trabajo para crear una membresía. Estos contactos se incluyen automáticamente como parte de su equipo de respuesta a incidentes. Debe haber al menos dos contactos para una sola membresía, lo que también garantiza la inclusión de un mínimo de dos contactos en el equipo de respuesta a incidentes.
- Defina etiquetas opcionales para su membresía. Las etiquetas le ayudan a realizar un seguimiento de AWS los costes y a buscar recursos.

Asocia cuentas con AWS Organizations

Su membresía da derecho a la cobertura en todos los enlaces Cuentas de AWS . AWS Organizations Las cuentas asociadas se actualizarán automáticamente a medida que se agreguen o eliminen cuentas de su organización.

Configure flujos de trabajo proactivos de respuesta y clasificación de alertas

El flujo de trabajo proactivo de respuesta y clasificación de alertas es una función opcional que su organización puede supervisar los servicios de seguridad habilitados. Seleccione el conmutador situado junto a la función para activarla.

Si tienes algún problema con la incorporación, crea un AWS Support caso para obtener asistencia adicional. Asegúrate de incluir detalles como el Cuenta de AWS ID y cualquier error que hayas podido observar durante el proceso de configuración.

Respuesta proactiva y clasificación de alertas: AWS Security Incident Response supervisa e investiga las alertas generadas a partir de las integraciones de Amazon GuardDuty y Security Hub. Para utilizar esta función, Amazon GuardDuty debe estar activado. AWS La respuesta a incidentes de seguridad clasifica las alertas de baja prioridad con la automatización del servicio para que su equipo pueda centrarse en los problemas más críticos. Para obtener más información sobre cómo funciona la respuesta a incidentes de AWS seguridad con Amazon GuardDuty AWS Security Hub, consulta la sección Detectar y analizar de la guía del usuario.

Esta función permite que AWS Security Incident Response supervise e investigue los hallazgos en todas las cuentas y cuenta con Regiones de AWS el apoyo activo de su organización. Para facilitar esta funcionalidad, AWS Security Incident Response crea automáticamente un rol vinculado al

servicio en todas las cuentas de los miembros de su cuenta. AWS Organizations Sin embargo, para la cuenta de administración, debe crear manualmente el rol vinculado al servicio para habilitar la supervisión.

El servicio no puede crear el rol vinculado al servicio en la cuenta de administración. Debe crear este rol manualmente en la cuenta de administración trabajando con conjuntos AWS CloudFormation apilados.

Contención: en caso de un incidente de seguridad, AWS Security Incident Response puede ejecutar acciones de contención para mitigar rápidamente el impacto, como aislar los hosts comprometidos o rotar las credenciales. La respuesta a incidentes de seguridad no habilita las capacidades de contención de forma predeterminada. Para ejecutar estas acciones de contención, primero debe conceder los permisos necesarios al servicio. Esto se puede hacer mediante la implementación de un AWS CloudFormation StackSet, que crea las funciones necesarias.

Tareas de usuario

Contenido

Panel de control

En la consola de respuesta a incidentes de AWS seguridad, el panel le ofrece una visión general de su equipo de respuesta a incidentes, su estado de respuesta proactiva y un recuento continuo de los casos durante cuatro semanas.

Seleccione esta opción `View incident response team` para acceder a los detalles de sus compañeros de equipo de respuesta a incidentes.

Seleccione esta opción `proactive response` para identificar si la clasificación de alertas está habilitada. Si no tiene activado el `alert triaging` flujo de trabajo, puede supervisar su estado y optar por `Proactive Response` habilitarlo.

En la sección Mis casos del panel de control se muestra el número de casos AWS admitidos abiertos y cerrados, además de los casos autogestionados que se te han asignado dentro de un período definido. También muestra el tiempo medio que se tardó en resolver los casos cerrados en horas.

Administrar mi equipo de respuesta a incidentes

Sus equipos de respuesta a incidentes incluyen a las partes interesadas en el proceso de respuesta a incidentes. Puede configurar hasta diez partes interesadas como parte de su membresía.

Algunos ejemplos para las partes interesadas internas son los miembros de su equipo de respuesta a incidentes, los analistas de seguridad, los propietarios de las aplicaciones y su equipo directivo de seguridad.

Entre los ejemplos de partes interesadas externas se incluyen personas de proveedores de software independientes (ISV) y proveedores de servicios gestionados (MSP) que desee incluir en un proceso de respuesta a incidentes.

> **Note**
>
> La configuración de un equipo de respuesta a incidentes no otorga automáticamente a los compañeros de equipo acceso a los recursos de servicio, como la membresía y los casos. Puedes usar políticas AWS gestionadas de respuesta a incidentes de AWS seguridad para conceder acceso de lectura y escritura a los recursos. Haga clic aquí para obtener más información.

Tus compañeros de equipo de respuesta a incidentes especificados en un nivel de membresía se añadirán automáticamente a cualquier caso. Puedes añadir o eliminar compañeros de equipo individuales en cualquier momento después de haber creado un caso.

El equipo de respuesta a incidentes recibirá una notificación por correo electrónico sobre los siguientes eventos:

- Caso (crear, eliminar, actualizar)
- Comentar (crear, eliminar, actualizar)
- Adjunto (crear, eliminar, actualizar)
- Membresía (crear, actualizar, cancelar, reanudar)

Asociación de la cuenta a AWS Organizations

Al activar la respuesta a incidentes de AWS seguridad, la membresía se creará y se alineará con la suya AWS Organizations. Todas las cuentas de sus Organizations están alineadas con su membresía AWS de Security Incident Response.

Para obtener más información, consulte Administrar las cuentas de respuesta a incidentes de AWS seguridad con AWS Organizations.

Supervisión e investigación

AWS Security Incident Response revisa y clasifica las alertas de seguridad de Amazon GuardDuty y AWS Security Hub, a continuación, configura las reglas de supresión en función de tu entorno para evitar alertas innecesarias. El AWS CIRT equipo investiga los hallazgos no clasificados y, con rapidez, clasifica y guía a su equipo para detectar rápidamente los posibles problemas. Si lo deseas, puedes conceder el permiso de respuesta a incidentes AWS de seguridad para implementar acciones de contención en tu nombre.

AWS La respuesta a incidentes de seguridad se ajusta a la Guía de gestión de eventos de seguridad informática NIST 800-61r2 para la respuesta a eventos de seguridad. Al ajustarse a este estándar del sector, AWS Security Incident Response proporciona un enfoque coherente para la gestión de eventos de seguridad y sigue las mejores prácticas para proteger y responder a los eventos de seguridad en su entorno. AWS

Cuando el servicio AWS de respuesta a incidentes de seguridad identifica una alerta de seguridad o usted solicita asistencia de seguridad, AWS CIRT investiga. El equipo recopila los eventos de registro y los datos del servicio, como las GuardDuty alertas, clasifica y analiza esos datos, lleva a cabo actividades de corrección y contención y proporciona informes posteriores a los incidentes.

Contenido

Preparación

El equipo de respuesta a incidentes de AWS seguridad investiga y colabora con usted durante todo el ciclo de vida de la respuesta a los incidentes de seguridad. Se recomienda configurar este equipo y asignar los permisos necesarios antes de que se produzca un incidente de seguridad.

Detecte y analice

AWS Security Incident Response monitorea, clasifica e investiga los hallazgos de seguridad de Amazon GuardDuty y las integraciones a través de ellos. AWS Security Hub Entre las opciones adicionales que pueden mejorar considerablemente el alcance y la eficacia de las capacidades de supervisión e investigación de AWS Security Incident Response se incluyen las siguientes:

Habilitar fuentes de detección compatibles

> **Note**
>
> AWS Los costos del servicio de respuesta a incidentes de seguridad no incluyen el uso ni otros costos y tarifas asociados con las fuentes de detección compatibles o el uso de otros AWS servicios. Consulte las páginas de funciones o servicios individuales para obtener detalles sobre los costos.

Amazon GuardDuty

GuardDuty es un servicio de detección de amenazas que monitorea, analiza y procesa de forma continua las fuentes de datos y los registros de su AWS entorno. GuardDuty La activación no es necesaria para utilizar la respuesta a incidentes de AWS seguridad; sin embargo, para utilizar la respuesta proactiva y la función de clasificación de alertas, Amazon GuardDuty debe estar habilitada.

Para activarlo GuardDuty en toda tu organización, consulta la `Setting up GuardDuty` sección de la Guía del GuardDuty usuario de Amazon.

Te recomendamos encarecidamente que actives todas GuardDuty las opciones compatibles Regiones de AWS. Esto permite GuardDuty generar información sobre actividades no autorizadas o inusuales, incluso en las regiones que no se utilizan activamente. Para obtener más información, consulta GuardDuty las regiones y puntos de conexión de Amazon

Enabling GuardDuty proporciona a la respuesta a incidentes de AWS seguridad acceso a los datos críticos de detección de amenazas, lo que mejora su capacidad para identificar y responder a posibles problemas de seguridad en su AWS entorno.

AWS Security Hub

Security Hub puede asimilar los hallazgos de seguridad de varios AWS servicios y soluciones de seguridad de terceros compatibles. Estas integraciones pueden ayudar a AWS Security Incident Response a monitorear e investigar los hallazgos provenientes de otras herramientas de detección.

Para habilitar la integración de Security Hub con Organizations, consulte la Guía del AWS Security Hub usuario.

Existen varias formas de habilitar las integraciones en Security Hub. En el caso de las integraciones de productos de terceros, es posible que tenga que comprar la integración en el y AWS Marketplace, a continuación, configurarla. La información de integración proporciona enlaces para completar estas tareas. Obtenga más información sobre cómo habilitar las AWS Security Hub integraciones.

AWS La respuesta a incidentes de seguridad puede monitorear e investigar los hallazgos de las siguientes herramientas cuando se integran con AWS Security Hub ellas:

- CrowdStrike — CrowdStrike Falcon
- Encajes — Encajes
- Trend Micro: Cloud One

Al habilitar estas integraciones, puede mejorar significativamente el alcance y la eficacia de las capacidades de supervisión e investigación de AWS Security Incident Response.

Analizar los hallazgos.

AWS El equipo de automatización y AWS CIRT servicio de respuesta a incidentes de seguridad analizará todos los hallazgos de las herramientas compatibles. Empezaremos a conocer su entorno comunicándonos con usted mediante AWS Support Cases. Por ejemplo, cuando necesitamos saber si un hallazgo es un comportamiento esperado o si debe convertirse en un incidente. A medida que obtengamos más información de su entorno, personalizaremos el servicio y reduciremos el número de comunicaciones.

Reportar un evento.

Puede generar un evento de seguridad a través del portal del servicio de respuesta a incidentes de AWS seguridad. Es importante no esperar durante un evento de seguridad. AWS La respuesta a incidentes de seguridad utiliza técnicas automatizadas y manuales para investigar los eventos de seguridad, analizar los registros y buscar patrones anómalos. Su colaboración y comprensión de su entorno aceleran este análisis.

Comuníquese.

AWS La respuesta a incidentes de seguridad lo mantiene informado durante la investigación mediante la participación de sus contactos de seguridad a través de la entrada al evento. Es posible

que varios compañeros de equipo apoyen tu evento, y todos ellos podrán utilizar la entrada del evento para acceder al contenido y AWS las actualizaciones proporcionadas por los clientes.

La comunicación puede incluir notificaciones automáticas cuando se genera una alerta de seguridad, la comunicación durante el análisis del evento, el establecimiento de puentes de llamadas, el análisis continuo de artefactos, como los archivos de registro, y la obtención de los resultados de las investigaciones durante el evento de seguridad.

AWS El servicio de respuesta a incidentes de seguridad utiliza dos tipos de casos diferentes Support para comunicarse con usted: en las comunicaciones salientes para notificarle un suceso, y en los casos de respuesta a incidentes de AWS seguridad, para comunicarse sobre un caso que usted nos haya abierto.

AWS Support Cases: El servicio utilizará AWS Support Cases para comunicarse con sus equipos. Crearemos casos de apoyo para cada uno de ellos Cuenta de AWS en los que se genere el hallazgo. Este enfoque facilita la comunicación con los múltiples equipos que poseen las cargas de trabajo específicas, ya que tendrán más conocimiento sobre los eventos que ocurren en sus áreas de responsabilidad.

AWS Casos de respuesta a incidentes de seguridad: si determinamos que un hallazgo debe convertirse en un incidente de seguridad, crearemos un caso de respuesta a incidentes AWS de seguridad. Esto garantiza que los problemas de seguridad críticos reciban el nivel de atención y respuesta adecuados.

Al participar activamente en estas comunicaciones y proporcionar respuestas oportunas, puede ayudar al servicio de respuesta a incidentes de AWS seguridad a:

- Comprenda mejor su entorno y los comportamientos esperados.
- Reduzca los falsos positivos a lo largo del tiempo.
- Mejore la precisión y la relevancia de las alertas.
- Garantice una respuesta rápida a los incidentes de seguridad genuinos.
- Recuerde que la eficacia del servicio de respuesta a incidentes de AWS seguridad mejora con su colaboración, lo que se traduce en un AWS entorno supervisado más seguro y eficiente.

Contiene

AWS Security Incident Response colabora con usted para contener los eventos. Puede configurar un rol de servicio para la respuesta a incidentes de AWS seguridad a fin de tomar medidas

automatizadas y manuales en su cuenta en respuesta a las alertas. También puede realizar la contención usted mismo o en colaboración con sus relaciones con terceros mediante el uso de SSM documentos.

Una parte esencial de la contención es la toma de decisiones, como cerrar un sistema, aislar un recurso de la red, desactivar el acceso o finalizar las sesiones. Estas decisiones son más fáciles cuando existen estrategias y procedimientos predeterminados para contener el evento. AWS La respuesta a incidentes de seguridad proporciona la estrategia de contención, le informa sobre el posible impacto y lo guía para implementar la solución solo después de haber considerado y aceptado los riesgos involucrados.

AWS Security Incident Response ejecuta en su nombre acciones de contención respaldadas para agilizar la respuesta y reducir el tiempo del que dispone un agente de amenazas para causar daños en su entorno. Esta capacidad permite mitigar más rápidamente las amenazas identificadas, minimizar el impacto potencial y mejorar su postura general de seguridad. Existen diferentes opciones de contención en función de los recursos que se analicen. Las acciones de contención compatibles son:

- EC2Contención: la automatización de la `AWSSupport-ContainEC2Instance` contención realiza una contención de red reversible de una EC2 instancia, dejando la instancia intacta y en ejecución, pero aislándola de cualquier actividad nueva de la red e impidiendo que se comunique con recursos internos y externos a la suya. VPC

  > **Important**
  >
  > Es importante tener en cuenta que las conexiones rastreadas existentes no se cerrarán como resultado de un cambio en los grupos de seguridad; solo el nuevo grupo de seguridad y este SSM documento bloquearán eficazmente el tráfico futuro. Encontrará más información en la sección de contención de fuentes de la guía técnica del servicio.

- IAMContención: la automatización de la `AWSSupport-ContainIAMPrincipal` contención realiza una contención de red reversible de un IAM usuario o rol, dejando al usuario o rol dentro de su cuentaIAM, pero aislándolo de la comunicación con los recursos de su cuenta.
- Contención de S3: la automatización de `AWSSupport-ContainS3Resource` contención realiza una contención reversible de un depósito de S3, dejando los objetos en el depósito y aislando el depósito o el objeto de Amazon S3 mediante la modificación de sus políticas de acceso.

> **Important**
>
> AWS La respuesta a incidentes de seguridad no habilita las capacidades de contención de forma predeterminada. Para ejecutar estas acciones de contención, primero debe conceder los permisos necesarios al servicio mediante funciones. Puede crear estas funciones de forma individual por cuenta o en toda la organización si trabaja con AWS CloudFormation conjuntos de pilas, que crean las funciones necesarias.

AWS Security Incident Response le anima a considerar estrategias de contención para cada tipo de evento importante que se ajusten a su apetito por el riesgo. Documente criterios claros que le ayuden a tomar decisiones durante un evento. Los criterios a tener en cuenta incluyen:

- Posibles daños a los recursos
- Preservación de las pruebas y requisitos reglamentarios
- Indisponibilidad del servicio (por ejemplo, conectividad de red, servicios prestados a terceros)
- Tiempo y recursos necesarios para implementar la estrategia
- Efectividad de la estrategia (por ejemplo, contención parcial o total)
- Permanencia de la solución (por ejemplo, reversible o irreversible)
- Duración de la solución (por ejemplo, solución alternativa de emergencia, solución temporal o solución permanente) Aplique controles de seguridad que puedan reducir el riesgo y disponer de tiempo para definir e implementar una estrategia de contención más eficaz.

AWS La respuesta a los incidentes de seguridad recomienda adoptar un enfoque gradual para lograr una contención eficiente y eficaz, que incluya estrategias a corto y largo plazo en función del tipo de recurso.

- Estrategia de contención
  - ¿Puede AWS la respuesta a incidentes de seguridad identificar el alcance del evento de seguridad?
    - En caso afirmativo, identifique todos los recursos (usuarios, sistemas, recursos).
    - Si no, investigue paralelamente a la ejecución del siguiente paso en los recursos identificados.
  - ¿Se puede aislar el recurso?
    - En caso afirmativo, proceda a aislar los recursos afectados.

    - Si la respuesta es negativa, colabore con los propietarios y administradores del sistema para determinar las medidas adicionales necesarias para solucionar el problema.
  - ¿Están todos los recursos afectados aislados de los recursos no afectados?
    - En caso afirmativo, continúe con el siguiente paso.
    - En caso negativo, continúe aislando los recursos afectados para completar la contención a corto plazo y evitar que el evento se agrave aún más.
- Respaldo del sistema
  - ¿Se crearon copias de seguridad de los sistemas afectados para su posterior análisis?
  - ¿Las copias forenses están cifradas y almacenadas en un lugar seguro?
    - En caso afirmativo, continúe con el siguiente paso.
    - Si la respuesta es negativa, cifre las imágenes forenses y guárdelas en un lugar seguro para evitar su uso accidental, daños y manipulaciones.

Erradicar

Durante la fase de erradicación, es importante identificar y abordar todas las cuentas, recursos e instancias afectados, por ejemplo, eliminando el malware, eliminando las cuentas de usuario comprometidas y mitigando cualquier vulnerabilidad descubierta, para aplicar una solución uniforme en todo el entorno.

La mejor práctica es utilizar un enfoque gradual para la erradicación y la recuperación, y priorizar las medidas de remediación. El objetivo de las primeras fases es aumentar la seguridad general rápidamente (días o semanas) con cambios de gran valor para evitar futuros eventos. Las fases posteriores pueden centrarse en los cambios a largo plazo (por ejemplo, cambios en la infraestructura) y en el trabajo continuo para mantener la empresa lo más segura posible. Cada caso es único y AWS CIRT trabajaremos con usted para evaluar las acciones necesarias.

Considere lo siguiente:

- ¿Puede cambiar la imagen del sistema y reforzarlo con parches u otras contramedidas para prevenir o reducir el riesgo de ataques?
- ¿Puede sustituir el sistema infectado por una nueva instancia o recurso que permita disponer de una base limpia y, al mismo tiempo, cerrar el elemento infectado?
- ¿Has eliminado todo el malware y otros artefactos dejados por el uso no autorizado y has reforzado los sistemas afectados para que no se produzcan nuevos ataques?
- ¿Es necesario realizar un análisis forense de los recursos afectados?

Recuperar

AWS La respuesta a incidentes de seguridad le proporciona orientación para ayudar a restablecer el funcionamiento normal de los sistemas, confirmar que funcionan correctamente y corregir cualquier vulnerabilidad para evitar eventos similares en el futuro. AWS La respuesta a incidentes de seguridad no ayuda directamente a la recuperación de los sistemas. Las principales consideraciones incluyen las siguientes:

- ¿Están los sistemas afectados parcheados y protegidos contra el ataque reciente?
- ¿Cuál es el plazo factible para restablecer la producción de los sistemas?
- ¿Qué herramientas utilizará para probar, supervisar y verificar los sistemas restaurados?

Informe posterior al incidente

AWS La respuesta a un incidente de seguridad proporciona un resumen del suceso una vez finalizadas las actividades de seguridad entre tu equipo y el nuestro.

Al final de cada mes, el servicio de respuesta a incidentes de AWS seguridad enviará informes mensuales por correo electrónico al punto de contacto principal de cada cliente. Los informes se entregarán en un PDF formato que utilice las métricas que se describen a continuación. Los clientes recibirán un informe por cada uno AWS Organizations.

Métricas de casos

- Casos creados
  - Nombre de la dimensión: tipo
  - Valores de dimensión: AWS compatibles, autocompatibles
  - Unidad: recuento
  - Descripción: el número de casos creados.
- Casos cerrados
  - Nombre de dimensión: Tipo
  - Valores de dimensión: AWS compatibles, autogestionados
  - Unidad: recuento
  - Descripción: una medida del número total de casos cerrados.
- Casos abiertos
  - Nombre de dimensión: Tipo

- Valores de dimensión: AWS compatibles, autocompatibles
- Unidad: recuento
- Descripción: El número de casos abiertos.

Métricas de clasificación

- Hallazgos recibidos
  - Unidad: recuento
  - Descripción: El número de resultados enviados a la clasificación.
- Hallazgos archivados
  - Unidad: recuento
  - Descripción: El número de hallazgos archivados tras ser procesados sin investigación manual.
- Los hallazgos se investigaron manualmente
  - Unidad: recuento
  - Descripción: El número de hallazgos con una investigación manual.
- Investigaciones archivadas
  - Unidad: recuento
  - Descripción: Número de investigaciones manuales que dieron como resultado un falso positivo y se enviaron para su archivo
- Las investigaciones se intensificaron
  - Unidad: recuento
  - Descripción: Número de investigaciones manuales que dieron lugar a un incidente de seguridad

Casos

AWS La respuesta a incidentes de seguridad le permite crear dos tipos de casos: casos AWS compatibles o autogestionados.

Cree un caso AWS compatible

Puede crear un caso AWS compatible a partir de la respuesta a un incidente de AWS seguridadAPI, la o la AWS Command Line Interface. AWS los casos admitidos le permiten recibir asistencia del equipo de respuesta a incidentes del AWS cliente (CIRT).

> **Note**
>
> AWS CIRTresponderá a su caso en un plazo de 15 minutos. El tiempo de respuesta corresponde a la primera respuesta de AWS CIRT. Haremos todos los esfuerzos razonables para responder a su solicitud inicial dentro de este plazo. Este tiempo de respuesta no se aplica a las respuestas posteriores.

El siguiente ejemplo describe el uso de la consola.

1. Inicie sesión en AWS Management Console. Abra la consola de respuesta a incidentes de seguridad en https://console.aws.amazon.com/security-ir/.
2. Seleccione Crear caso
3. Elige Resolver caso con AWS
4. Selecciona el tipo de solicitud
   a. Incidente de seguridad activo: este tipo es para asistencia y servicios de respuesta a incidentes urgentes.
   b. Investigaciones: las investigaciones le permiten obtener apoyo en caso de incidentes de seguridad percibidos, ya que AWS CIRT pueden respaldarse mediante el análisis de registros y la confirmación secundaria de la respuesta al incidente.
5. Establezca la fecha estimada de inicio como la fecha del primer indicador del incidente. Por ejemplo, cuando experimentó un comportamiento anormal por primera vez o cuando recibió la primera alerta de seguridad relacionada.
6. Defina un título para el caso
7. Proporcione una descripción detallada del caso. Tenga en cuenta los siguientes aspectos que pueden ayudar al personal de respuesta a incidentes a resolver el caso:
   a. ¿Qué ha pasado?
   b. ¿Quién descubrió y denunció el incidente?
   c. ¿A quién afecta el caso?
   d. ¿Cuál es el impacto conocido?
   e. ¿Cuál es la urgencia de este caso?
   f. Agregue uno o varios Cuenta de AWS IDs que estén dentro del ámbito del caso.
8. Añada detalles opcionales del caso:
   a. Seleccione los principales servicios que se ven afectados en la lista desplegable.

   b. Seleccione las principales regiones afectadas de la lista desplegable.
   c. Agregue una o varias direcciones IP o de amenazas que haya identificado como parte de este caso.
9. Añada al caso personal de respuesta a incidentes adicional opcional que recibirá las notificaciones. Para añadir a una persona, haga lo siguiente:
   a. Añada una dirección de correo electrónico.
   b. Agrega un nombre y apellidos opcionales.
   c. Seleccione Añadir nuevo para añadir a otra persona.
   d. Para eliminar a una persona, elija la opción Eliminar para una persona.
   e. Seleccione Añadir para añadir al caso a todas las personas incluidas en la lista.
      i. Puede seleccionar varias personas y elegir Eliminar para eliminarlas de la lista.
10. Añada etiquetas opcionales a la funda.
   a. Para añadir una etiqueta, haga lo siguiente:
   b. Elija Añadir nueva etiqueta.
   c. En Clave, escriba el nombre de la etiqueta.
   d. En Valor, escriba el valor de la etiqueta.
   e. Para eliminar una etiqueta, elija la opción Eliminar de la etiqueta correspondiente.

Una vez creado un caso AWS compatible, se notifica inmediatamente a usted AWS CIRT y a su equipo de respuesta a incidentes.

Cree un caso autogestionado

Puede crear un autogestionado a partir de la respuesta a un incidente de AWS seguridadAPI, la o la. AWS Command Line Interface Este tipo de caso DOESNOTinvolucra al AWS CIRT. El siguiente ejemplo describe el uso de la consola.

1. Inicie sesión en AWS Management Console. Abra la consola de respuesta a incidentes de seguridad en https://console.aws.amazon.com/security-ir/.
2. Elija Create Case (Crear caso).
3. Elija Resolver el caso con mi propio equipo de respuesta a incidentes.
4. Establezca la fecha estimada de inicio como la fecha del primer indicador del incidente. Por ejemplo, cuando experimentó un comportamiento anormal por primera vez o cuando recibió la primera alerta de seguridad relacionada.

5. Defina un título para el caso. Se recomienda incluir los datos en el título del caso, tal y como se sugiere al seleccionar la opción Generar título.
6. Introduzca Cuenta de AWS IDs que forman parte del caso. Para añadir un identificador de cuenta, haga lo siguiente:
   a. Introduce el ID de cuenta de 12 dígitos y selecciona Añadir cuenta.
   b. Para eliminar una cuenta, selecciona Eliminar junto a la cuenta que quieres eliminar de la funda.
7. Proporcione una descripción detallada del caso.
   a. Tenga en cuenta los siguientes aspectos que pueden ayudar al personal de respuesta a incidentes a resolver el caso:
      i. ¿Qué ha pasado?
      ii. ¿Quién descubrió y denunció el incidente?
      iii. ¿A quién afecta el caso?
      iv. ¿Cuál es el impacto conocido?
      v. ¿Cuál es la urgencia de este caso?
8. Añada detalles opcionales del caso:
   a. Seleccione los principales servicios que se ven afectados en la lista desplegable.
   b. Seleccione las principales regiones afectadas de la lista desplegable.
   c. Agregue una o varias direcciones IP o de amenazas que haya identificado como parte de este caso.
9. Añada al caso personal de respuesta a incidentes adicional opcional que recibirá las notificaciones. Para añadir a una persona, haga lo siguiente:
   a. Añada una dirección de correo electrónico.
   b. Agrega un nombre y apellidos opcionales.
   c. Seleccione Añadir nuevo para añadir a otra persona.
   d. Para eliminar a una persona, elija la opción Eliminar para una persona.
   e. Seleccione Añadir para añadir al caso a todas las personas incluidas en la lista. Puede seleccionar varias personas y elegir Eliminar para eliminarlas de la lista.
10. Añada etiquetas opcionales a la funda. Para añadir una etiqueta, haga lo siguiente:
    a. Elija Añadir nueva etiqueta.
    b. En Clave, escriba el nombre de la etiqueta.
    c. En Valor, escriba el valor de la etiqueta.

d. Para eliminar una etiqueta, elija la opción Eliminar de la etiqueta correspondiente.

El equipo de respuesta a incidentes recibirá una notificación por correo electrónico una vez creado el caso.

Responder a un caso AWS generado

AWS La respuesta a incidentes de seguridad puede crear una notificación o un caso saliente cuando necesites actuar o tener conocimiento de algo que pueda afectar a tu cuenta o tus recursos. Esto solo ocurrirá si has activado los flujos de trabajo de respuesta proactiva y clasificación de alertas habilitados como parte de tu suscripción.

Estas notificaciones aparecerán en el Support Centro. La guía del Support usuario contiene información y pasos detallados para actualizar, resolver y volver a abrir estos casos.

Gestión de casos

Contenido

Cambiar el estado del caso

Un caso estará en uno de los siguientes estados:

- Presentado: este es el estado inicial de un caso. Los casos en este estado han sido presentados por una persona solicitada, pero aún no se está trabajando en ellos.

- Detección y análisis: este estado indica que un equipo de respuesta a incidentes ha empezado a trabajar en el caso. Esta fase incluye la recopilación de datos, la clasificación del evento y la realización de análisis para sacar conclusiones basadas en los datos.
- Contención, erradicación y recuperación: en este estado, el personal de respuesta al incidente ha identificado una actividad sospechosa que requiere un esfuerzo adicional para eliminarla. El encargado de responder a los incidentes le proporcionará recomendaciones para analizar los riesgos empresariales y adoptar medidas adicionales. Si has activado las funciones de suscripción voluntaria para el servicio, un encargado de responder a las AWS incidencias solicitará tu consentimiento para llevar a cabo acciones de contención con SSM los documentos de las cuentas afectadas.
- Actividades posteriores a un incidente: en este estado, se ha contenido el evento de seguridad principal. El objetivo ahora es recuperar las operaciones comerciales y devolverlas a la normalidad. Se proporciona un resumen y un análisis de la causa raíz si el solucionador del caso cuenta con el AWS apoyo necesario.
- Cerrado: este es el estado final del flujo de trabajo. Los casos en estado cerrado indican que el trabajo se ha completado. Los casos cerrados no se pueden volver a abrir, así que asegúrese de que se hayan completado todas las acciones antes de pasar a este estado.

Seleccione Acción/Actualizar estado para cambiar el estado del caso para los casos autogestionados. En el caso de los casos AWS admitidos, el respondedor establece el estado. AWS CIRT

Cambiar el solucionador

En el caso de los casos autogestionados, su equipo de respuesta a incidentes puede solicitar ayuda a AWS. Selecciona Obtener ayuda de AWS para cambiar la resolución de este caso a AWS. Una vez que el caso se haya actualizado a AWS compatible, el estado cambiará a Enviado. El historial de casos existente estará disponible para AWS CIRT. Una vez que hayas solicitado ayuda, no AWS podrás volver a cambiarla a autogestionada.

Elementos de acción

El AWS CIRT personal de respuesta que esté trabajando en el caso puede solicitar a tu equipo interno que tome medidas.

Los elementos de acción que aparecen después de crear un caso incluyen:

- Solicitud para conceder permisos a un encargado de responder a incidentes para acceder a un caso
- Solicitud para proporcionar más información sobre el caso

Elemento de acción cuando una acción del cliente está pendiente:

- Solicitud para actuar en función de un nuevo comentario para continuar con el caso

Medidas a tomar cuando un caso esté listo para cerrarse:

- Solicitud de revisión del informe del caso
- Solicitud de cierre del caso

Edición de un caso

Seleccione Editar para cambiar los detalles de un caso.

Para los casos AWS compatibles y autogestionados:

Puede cambiar los siguientes detalles del caso una vez creado un caso:

- Título
- Descripción

Solo para casos AWS admitidos:

Puede cambiar los campos adicionales:

- Tipo de solicitud:
  - Incidente de seguridad activo: este tipo es para asistencia y servicios de respuesta a incidentes urgentes.
  - Investigaciones: las investigaciones le permiten obtener apoyo en caso de incidentes de seguridad percibidos, ya que AWS CIRT pueden respaldar el registro y la confirmación secundaria de la respuesta al incidente, investigar el suceso.
- Fecha de inicio estimada: cambie este campo si ha recibido indicadores para este caso anteriores a la fecha de inicio proporcionada inicialmente. Considere la posibilidad de proporcionar detalles

adicionales sobre el indicador recién detectado en el campo de descripción o añadir un comentario en la pestaña de comunicaciones.

Comunicación

AWS CIRTpueden añadir comentarios para documentar sus actividades cuando estén trabajando en un caso. Diferentes AWS CIRT socorristas pueden trabajar en un caso al mismo tiempo. Se representan como AWS Respondedores en el registro de comunicaciones.

Permisos

La pestaña de permisos muestra una lista de todas las personas a las que se les notificará cualquier cambio en el caso. Puede añadir y eliminar personas de la lista hasta que se cierre el caso.

> **Note**
>
> Los casos individuales le permiten incluir hasta 30 partes interesadas en total. Se requiere una configuración de permisos adicional para conceder acceso a estas partes interesadas a nivel de caso.

Proporcione acceso a una funda en la consola

Para proporcionar acceso al caso de AWS Management Console, puede copiar la plantilla de política de IAM permisos y añadir este permiso a un usuario o rol.

Añadir la IAM política a un usuario o un rol:

1. Copie la política de IAM permisos.
2. Abre IAM en la vía https://console.aws.amazon.com/iam/.
3. En el panel de navegación, selecciona Usuario o Funciones.
4. Seleccione un usuario o un rol para abrir la página de detalles.
5. En la pestaña de permisos, selecciona Añadir permisos.
6. Elija Asociar política.
7. Seleccione la política gestionada de respuesta a incidentes de AWS seguridad adecuada.
8. Elija Add Policy (Agregar política).

Archivos adjuntos

El personal de respuesta a incidentes puede añadir archivos adjuntos a un caso para ayudar a otros equipos de respuesta a incidentes a investigar los casos de forma autogestionada.

> **Note**
>
> Si elige un caso AWS compatible, AWS no podrá ver los archivos adjuntos. Todos los detalles de los casos AWS admitidos deben compartirse a través de los comentarios de los casos o a través de una pantalla compartida mediante la tecnología de comunicación que prefieras.

Selecciona Cargar para seleccionar un archivo de tu ordenador y añadirlo al caso.

> **Note**
>
> Todos los archivos adjuntos cargados se eliminan siete días después de la finalización del caso`Closed`.

Tags

Una etiqueta es una etiqueta opcional que puedes asignar a tus casos para almacenar metadatos sobre ese recurso. Cada etiqueta es una marca que consta de una clave y un valor opcional. Puede usar la etiqueta para buscar, asignar costos y autenticar los permisos del recurso.

Para añadir una etiqueta, haga lo siguiente:

1. Elija Añadir nueva etiqueta.
2. En Clave, escriba el nombre de la etiqueta.
3. En Valor, escriba el valor de la etiqueta.

Para eliminar una etiqueta, elija la opción Eliminar de la etiqueta correspondiente.

Actividades del caso

Los registros de auditoría proporcionan registros cronológicos detallados de todas las actividades de los casos. Proporcionan información importante en las actividades posteriores al evento y ayudan

a identificar posibles mejoras. La hora, el usuario, la acción y los detalles de cualquier cambio en el caso se registran en el registro de auditoría del caso.

Cerrar un caso

En el caso de los casos AWS admitidos, selecciona Cerrar caso en la página de detalles del caso para cerrar el caso de forma permanente en cualquier estado. Por lo general, un caso alcanza el estado Listo para cerrar antes de cerrarse permanentemente. Si cierra un caso de forma prematura con un estado distinto al de Listo para cerrar, está solicitando que AWS CIRT se deje de funcionar en este caso AWS admitido.

Si tu equipo de respuesta a incidentes es el encargado de responder, selecciona Acción/Cerrar caso en la página de detalles del caso.

> **Note**
>
> El estado «Listo para cerrar» significa que un caso se puede cerrar permanentemente y que no hay trabajo adicional por hacer al respecto.

Un caso no se puede volver a abrir después de haber sido cerrado permanentemente. Toda la información estará disponible en modo de solo lectura. Para evitar un cierre accidental, se le pedirá que confirme que desea cerrar la funda.

Trabajando con conjuntos AWS CloudFormation de pilas

> **Important**
>
> AWS La respuesta a incidentes de seguridad no habilita las capacidades de contención de forma predeterminada. Para ejecutar estas acciones de contención, primero debe conceder los permisos necesarios al servicio mediante funciones. Puede crear estas funciones de forma individual por cuenta o en toda la organización mediante la implementación AWS CloudFormation StackSets, lo que crea las funciones necesarias.

Encontrarás instrucciones específicas sobre cómo crear un conjunto de pilas con permisos gestionados por el servicio.

A continuación, se muestran conjuntos de plantillas para crear los roles y. AWSSecurityIncidentResponseContainmentAWSSecurityIncidentResponseContainmentExecution

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'Template for AWS Security Incident Response containment roles'

Resources:
  AWSSecurityIncidentResponseContainment:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSSecurityIncidentResponseContainment
      AssumeRolePolicyDocument:
        {
          'Version': '2012-10-17',
          'Statement':
            [
              {
                'Effect': 'Allow',
                'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
                'Action': 'sts:AssumeRole',
                'Condition': { 'StringEquals': { 'sts:ExternalId': !Sub
 '${AWS::AccountId}' } },
              },
              {
                'Effect': 'Allow',
                'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
                'Action': 'sts:TagSession',
              },
            ],
        }
      Policies:
        - PolicyName: AWSSecurityIncidentResponseContainmentPolicy
          PolicyDocument:
            {
              'Version': '2012-10-17',
              'Statement':
                [
                  {
                    'Effect': 'Allow',
                    'Action': ['ssm:StartAutomationExecution'],
                    'Resource':
                      [
```

```
                        !Sub 'arn:${AWS::Partition}:ssm:*:*:automation-definition/
AWSSupport-ContainEC2Instance:$DEFAULT',
                        !Sub 'arn:${AWS::Partition}:ssm:*:*:automation-definition/
AWSSupport-ContainS3Resource:$DEFAULT',
                        !Sub 'arn:${AWS::Partition}:ssm:*:*:automation-definition/
AWSSupport-ContainIAMPrincipal:$DEFAULT',
                      ],
                },
                {
                  'Effect': 'Allow',
                  'Action':
                    ['ssm:DescribeInstanceInformation', 'ssm:GetAutomationExecution',
 'ssm:ListCommandInvocations'],
                  'Resource': '*',
                },
                {
                  'Effect': 'Allow',
                  'Action': ['iam:PassRole'],
                  'Resource': !GetAtt
 AWSSecurityIncidentResponseContainmentExecution.Arn,
                  'Condition': { 'StringEquals': { 'iam:PassedToService':
 'ssm.amazonaws.com' } },
                },
              ],
          }
 AWSSecurityIncidentResponseContainmentExecution:
   Type: 'AWS::IAM::Role'
   Properties:
     RoleName: AWSSecurityIncidentResponseContainmentExecution
     AssumeRolePolicyDocument:
       {
         'Version': '2012-10-17',
         'Statement':
           [{ 'Effect': 'Allow', 'Principal': { 'Service': 'ssm.amazonaws.com' },
 'Action': 'sts:AssumeRole' }],
       }
     ManagedPolicyArns:
       - !Sub arn:${AWS::Partition}:iam::aws:policy/SecurityAudit
     Policies:
       - PolicyName: AWSSecurityIncidentResponseContainmentExecutionPolicy
         PolicyDocument:
           {
             'Version': '2012-10-17',
             'Statement':
```

```
                [
                  {
                    'Sid': 'AllowIAMContainment',
                    'Effect': 'Allow',
                    'Action':
                      [
                        'iam:AttachRolePolicy',
                        'iam:AttachUserPolicy',
                        'iam:DeactivateMFADevice',
                        'iam:DeleteLoginProfile',
                        'iam:DeleteRolePolicy',
                        'iam:DeleteUserPolicy',
                        'iam:GetLoginProfile',
                        'iam:GetPolicy',
                        'iam:GetRole',
                        'iam:GetRolePolicy',
                        'iam:GetUser',
                        'iam:GetUserPolicy',
                        'iam:ListAccessKeys',
                        'iam:ListAttachedRolePolicies',
                        'iam:ListAttachedUserPolicies',
                        'iam:ListMfaDevices',
                        'iam:ListPolicies',
                        'iam:ListRolePolicies',
                        'iam:ListUserPolicies',
                        'iam:ListVirtualMFADevices',
                        'iam:PutRolePolicy',
                        'iam:PutUserPolicy',
                        'iam:TagMFADevice',
                        'iam:TagPolicy',
                        'iam:TagRole',
                        'iam:TagUser',
                        'iam:UntagMFADevice',
                        'iam:UntagPolicy',
                        'iam:UntagRole',
                        'iam:UntagUser',
                        'iam:UpdateAccessKey',
                        'identitystore:CreateGroupMembership',
                        'identitystore:DeleteGroupMembership',
                        'identitystore:IsMemberInGroups',
                        'identitystore:ListUsers',
                        'identitystore:ListGroups',
                        'identitystore:ListGroupMemberships',
                      ],
```

```
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowOrgListAccounts',
                    'Effect': 'Allow',
                    'Action': 'organizations:ListAccounts',
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowSSOContainment',
                    'Effect': 'Allow',
                    'Action':
                      [
                        'sso:CreateAccountAssignment',
                        'sso:DeleteAccountAssignment',
                        'sso:DeleteInlinePolicyFromPermissionSet',
                        'sso:GetInlinePolicyForPermissionSet',
                        'sso:ListAccountAssignments',
                        'sso:ListInstances',
                        'sso:ListPermissionSets',
                        'sso:ListPermissionSetsProvisionedToAccount',
                        'sso:PutInlinePolicyToPermissionSet',
                        'sso:TagResource',
                        'sso:UntagResource',
                      ],
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowSSORead',
                    'Effect': 'Allow',
                    'Action': ['sso-directory:SearchUsers', 'sso-
directory:DescribeUser'],
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowS3Read',
                    'Effect': 'Allow',
                    'Action':
                      [
                        's3:GetAccountPublicAccessBlock',
                        's3:GetBucketAcl',
                        's3:GetBucketLocation',
                        's3:GetBucketOwnershipControls',
                        's3:GetBucketPolicy',
```

```
                's3:GetBucketPolicyStatus',
                's3:GetBucketPublicAccessBlock',
                's3:GetBucketTagging',
                's3:GetEncryptionConfiguration',
                's3:GetObject',
                's3:GetObjectAcl',
                's3:GetObjectTagging',
                's3:GetReplicationConfiguration',
                's3:ListBucket',
                's3express:GetBucketPolicy',
              ],
            'Resource': '*',
          },
          {
            'Sid': 'AllowS3Write',
            'Effect': 'Allow',
            'Action':
              [
                's3:CreateBucket',
                's3:DeleteBucketPolicy',
                's3:DeleteObjectTagging',
                's3:PutAccountPublicAccessBlock',
                's3:PutBucketACL',
                's3:PutBucketOwnershipControls',
                's3:PutBucketPolicy',
                's3:PutBucketPublicAccessBlock',
                's3:PutBucketTagging',
                's3:PutBucketVersioning',
                's3:PutObject',
                's3:PutObjectAcl',
                's3express:CreateSession',
                's3express:DeleteBucketPolicy',
                's3express:PutBucketPolicy',
              ],
            'Resource': '*',
          },
          {
            'Sid': 'AllowAutoScalingWrite',
            'Effect': 'Allow',
            'Action':
              [
                'autoscaling:CreateOrUpdateTags',
                'autoscaling:DeleteTags',
                'autoscaling:DescribeAutoScalingGroups',
```

```
                'autoscaling:DescribeAutoScalingInstances',
                'autoscaling:DescribeTags',
                'autoscaling:EnterStandby',
                'autoscaling:ExitStandby',
                'autoscaling:UpdateAutoScalingGroup',
              ],
            'Resource': '*',
          },
          {
            'Sid': 'AllowEC2Containment',
            'Effect': 'Allow',
            'Action':
              [
                'ec2:AuthorizeSecurityGroupEgress',
                'ec2:AuthorizeSecurityGroupIngress',
                'ec2:CopyImage',
                'ec2:CreateImage',
                'ec2:CreateSecurityGroup',
                'ec2:CreateSnapshot',
                'ec2:CreateTags',
                'ec2:DeleteSecurityGroup',
                'ec2:DeleteTags',
                'ec2:DescribeImages',
                'ec2:DescribeInstances',
                'ec2:DescribeSecurityGroups',
                'ec2:DescribeSnapshots',
                'ec2:DescribeTags',
                'ec2:ModifyNetworkInterfaceAttribute',
                'ec2:RevokeSecurityGroupEgress',
              ],
            'Resource': '*',
          },
          {
            'Sid': 'AllowKMSActions',
            'Effect': 'Allow',
            'Action':
              [
                'kms:CreateGrant',
                'kms:DescribeKey',
                'kms:GenerateDataKeyWithoutPlaintext',
                'kms:ReEncryptFrom',
                'kms:ReEncryptTo',
              ],
            'Resource': '*',
```

```
                },
                {
                  'Sid': 'AllowSSMActions',
                  'Effect': 'Allow',
                  'Action': ['ssm:DescribeAutomationExecutions'],
                  'Resource': '*',
                },
            ],
        }
```

Cancelar la membresía

Un rol que tenga el CancelMembership permiso de respuesta a incidentes de AWS seguridad puede cancelar la membresía desde la consolaAPI, el o AWS Command Line Interface.

> **Important**
>
> Una vez cancelada la membresía, no podrás ver los datos históricos de los casos. Las cancelaciones se producen al final del ciclo de facturación. Si cancelas durante el mes, tu membresía estará disponible hasta fin de mes. Cualquier recurso o investigación que se cancele `Active` o `ready to close` vaya a darse por terminado tras la cancelación definitiva de la membresía al final del ciclo de facturación.

> **Important**
>
> Si vuelves a suscribirte al servicio, se creará una nueva membresía y solo podrás acceder a los recursos de casos que estaban bajo la membresía anterior si los descargaste antes de la cancelación.

Una vez cancelada la membresía, todos los miembros del equipo de respuesta a incidentes relacionados con la membresía recibirán una notificación por correo electrónico.

> **Important**
>
> Si ha creado una membresía con una cuenta de administrador delegado y la utiliza AWS Organizations API para eliminar la designación de administrador delegado de la cuenta, la membresía se cancelará inmediatamente.

Etiquetado de los recursos AWS de respuesta a incidentes de seguridad

Una etiqueta es una etiqueta de metadatos que se asigna o que se AWS asigna a un AWS recurso. Cada etiqueta consta de una clave y un valor. En el caso de etiquetas que usted asigna, debe definir la clave y el valor. Por ejemplo, puede definir la clave como `stage` y el valor de un recurso como `test`.

Las etiquetas le ayudan a hacer lo siguiente:

- Identifique y organice sus AWS recursos. Muchos Servicios de AWS admiten el etiquetado, por lo que puede asignar la misma etiqueta a los recursos de diferentes servicios para indicar que los recursos están relacionados.
- Realice un seguimiento de sus AWS costes. Estas etiquetas se activan en el AWS Billing panel de control. AWS utiliza las etiquetas para clasificar los costes y entregarle un informe mensual de asignación de costes. Para obtener más información, consulte Uso de etiquetas de asignación de costes en la Guía del usuario de AWS facturación.
- Controle el acceso a sus AWS recursos. Para obtener más información, consulte Controlar el acceso mediante etiquetas en la Guía del IAM usuario.

Consulte la APIreferencia de respuesta a incidentes AWS de seguridad para obtener información sobre el etiquetado.

Utilización AWS CloudShell para trabajar con AWS Security Incident Response

AWS CloudShell es un shell preautenticado y basado en un navegador que se puede iniciar directamente desde. AWS Management Console Puede ejecutar AWS CLI comandos en los AWS servicios (incluida la respuesta a incidentes AWS de seguridad) mediante el shell que prefiera (Bash o Z shell). PowerShell Y puede hacerlo sin necesidad de descargar o instalar herramientas de línea de comandos.

Si lo AWS CloudShell ejecutas desde la consola AWS Management Console, las AWS credenciales que usaste para iniciar sesión en la consola estarán disponibles automáticamente en una nueva sesión de shell. Esta autenticación previa de AWS CloudShell los usuarios permite omitir la configuración de las credenciales al interactuar con AWS servicios como la respuesta a incidentes de seguridad mediante la AWS CLI versión 2 (preinstalada en el entorno informático del shell).

Contenido

Obtener permisos para IAM AWS CloudShell

Con los recursos de administración de acceso proporcionados por AWS Identity and Access Management, los administradores pueden conceder permisos a IAM los usuarios para que puedan acceder a las funciones del entorno AWS CloudShell y utilizarlas.

La forma más rápida para que un administrador conceda acceso a los usuarios es mediante una política AWS administrada. Una política administrada de AWS es una política independiente creada y administrada por AWS. La siguiente política AWS administrada para se CloudShell puede adjuntar a IAM las identidades:

- `AWSCloudShellFullAccess`: Concede permiso de uso AWS CloudShell con acceso completo a todas las funciones.

Si desea limitar el alcance de las acciones que un IAM usuario puede realizar AWS CloudShell, puede crear una política personalizada que utilice la política `AWSCloudShellFullAccess` gestionada como plantilla. Para obtener más información sobre cómo limitar las acciones que están

disponibles para los usuarios CloudShell, consulte Administrar el AWS CloudShell acceso y el uso con IAM políticas en la Guía del AWS CloudShell usuario.

> **Note**
>
> Su IAM identidad también requiere una política que otorgue permiso para realizar llamadas a Security Incident Response.

Interactuar con Security Incident Response mediante AWS CloudShell

Tras iniciar AWS CloudShell desde el AWS Management Console, podrá empezar a interactuar inmediatamente con Security Incident Response mediante la interfaz de línea de comandos.

> **Note**
>
> AWS CLI Al usarlo AWS CloudShell, no es necesario descargar ni instalar ningún recurso adicional. Además, dado que ya está autenticado en el intérprete de comandos, no tiene que configurar las credenciales antes de realizar llamadas.

¿Cómo trabajar con AWS CloudShell ellos y responder a los incidentes de seguridad

- Desde el AWS Management Console, puede iniciar CloudShell seleccionando las siguientes opciones disponibles en la barra de navegación:
  - Selecciona el CloudShell icono.
  - Comience a escribir «cloudshell» en el cuadro de búsqueda y, a continuación, elija la CloudShell opción.

Registro AWS de API llamadas de respuesta a incidentes de seguridad mediante AWS CloudTrail

AWS La respuesta a incidentes de seguridad está integrada con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en relación con la respuesta a incidentes de seguridad. CloudTrail captura todas las API llamadas de respuesta a incidentes de seguridad como eventos. Las llamadas capturadas incluyen las llamadas de la consola de respuesta a incidentes de seguridad y las llamadas en código a las API operaciones de respuesta a incidentes de seguridad. Si crea un registro, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de respuesta a incidentes de seguridad. Si no configura un registro, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Security Incident Response, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía AWS CloudTrail del usuario.

Información sobre la respuesta a incidentes de seguridad en CloudTrail

CloudTrail está habilitada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en la respuesta a un incidente de seguridad, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para obtener un registro continuo de los eventos de Cuenta de AWS los últimos 90 días, cree un banco de datos de eventos de senderos o CloudTraillagos.

CloudTrail senderos

> Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. Todos los senderos creados con él AWS Management Console son multirregionales. Puede crear un registro de seguimiento de una sola región o de varias regiones mediante la AWS CLI. Se recomienda crear un sendero multirregional, ya que puedes capturar toda la actividad de tu Regiones de AWS cuenta. Si crea un registro de seguimiento de una sola región, solo podrá ver los eventos registrados en la Región de AWS del registro de seguimiento. Para obtener

más información acerca de los registros de seguimiento, consulte Creación de un registro de seguimiento para su Cuenta de AWS y Creación de un registro de seguimiento para una organización en la Guía del usuario de AWS CloudTrail .

Puede enviar una copia de sus eventos de administración en curso a su bucket de Amazon S3 sin coste alguno CloudTrail mediante la creación de una ruta; sin embargo, hay cargos por almacenamiento en Amazon S3. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios. Para obtener información acerca de los precios de Amazon S3, consulte Precios de Amazon S3.

CloudTrail Almacenes de datos de eventos en Lake

CloudTrail Lake le permite ejecutar consultas SQL basadas en sus eventos. CloudTrail Lake convierte los eventos existentes en JSON formato basado en filas al ORC formato Apache. ORCes un formato de almacenamiento en columnas que está optimizado para una rápida recuperación de datos. Los eventos se agregan en almacenes de datos de eventos, que son recopilaciones inmutables de eventos en función de criterios que se seleccionan aplicando selectores de eventos avanzados. Los selectores que se aplican a un almacén de datos de eventos controlan los eventos que perduran y están disponibles para la consulta. Para obtener más información acerca de CloudTrail Lake, consulte Cómo trabajar con AWS CloudTrail Lake en la Guía del AWS CloudTrail usuario.

CloudTrail Los almacenes de datos y las consultas sobre eventos de Lake conllevan costes. Cuando crea un almacén de datos de eventos, debe elegir la opción de precios que desee utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el periodo de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios.

Todas las acciones de respuesta a incidentes de seguridad se registran CloudTrail y se documentan en la APIReferencia de respuesta a incidentes de AWS seguridad. Por ejemplo, las llamadas a `CreateCase` y `UpdateCase` las acciones generan entradas en los archivos de CloudTrail registro. `CreateMembership`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM).

- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el CloudTrail userIdentityelemento.

Descripción de las entradas del archivo de registro de respuesta a incidentes de seguridad

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las API llamadas públicas, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la CreateCase acción.


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA00000000000000000:user",
        "arn": "arn:aws:sts::123412341234:assumed-role/Admin/user",
        "accountId": "123412341234",
        "accessKeyId": "****",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA00000000000000000",
                "arn": "arn:aws:iam::123412341234:role/Admin",
                "accountId": "123412341234",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2024-10-13T06:32:53Z",
                "mfaAuthenticated": "false"
            }
        }
```

```
    },
    "eventTime": "2024-10-13T06:40:45Z",
    "eventSource": "security-ir.amazonaws.com",
    "eventName": "CreateCase",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "1.2.3.4",
    "userAgent": "aws-cli/2.17.23 md/awscrt#0.20.11 ua/2.0 os/macos#23.6.0 md/
arch#x86_64 lang/python#3.11.9 md/pyimpl#CPython cfg/retry-mode#standard md/
installer#exe md/prompt#off md/command#security-ir.create-case",
    "requestParameters": {
        "impactedServices": [
            "Amazon GuardDuty"
        ],
        "impactedAccounts": [],
        "clientToken": "testToken112345679",
        "resolverType": "Self",
        "description": "***",
        "engagementType": "Investigation",
        "watchers": [
            {
                "email": "***",
                "name": "***",
                "jobTitle": "***"
            }
        ],
        "membershipId": "m-r1abcdabcd",
        "title": "***",
        "impactedAwsRegions": [
            {
                "region": "ap-southeast-1"
            }
        ],
        "reportedIncidentStartDate": 1711553521,
        "threatActorIpAddresses": [
            {
                "ipAddress": "***",
                "userAgent": "browser"
            }
        ]
    },
    "responseElements": {
        "caseId": "0000000001"
    },
    "requestID": "2db4b08d-94a9-457a-9474-5892e6c8191f",
```

```
    "eventID": "b3fa3990-db82-43be-b120-c81262cc2f19",
    "readOnly": false,
    "resources": [
        {
            "accountId": "123412341234",
            "type": "AWS::SecurityResponder::Case",
            "ARN": "arn:aws:security-ir:us-east-1:123412341234:case/*"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123412341234",
    "eventCategory": "Management"
}
```

Administrar cuentas de respuesta a incidentes de AWS seguridad con AWS Organizations

AWS La respuesta a incidentes de seguridad está integrada con. AWS Organizations La cuenta AWS Organizations de administración de la organización puede designar una cuenta como administradora delegada para la respuesta a incidentes AWS de seguridad. Esta acción habilita AWS la respuesta a incidentes de seguridad como un servicio de confianza en AWS Organizations. Para obtener información sobre cómo se conceden estos permisos, consulte AWS Organizations Utilización con otros AWS servicios.

En las siguientes secciones se explican diversas tareas que puede realizar como cuenta de administrador delegada de respuesta a incidentes de seguridad.

Contenido

Consideraciones y recomendaciones para utilizar la respuesta a incidentes AWS de seguridad con AWS Organizations

Las siguientes consideraciones y recomendaciones pueden ayudarle a entender cómo funciona una cuenta de administrador delegada en Security Incident Response en AWS Security Incident Response:

Una cuenta de administrador delegada de respuesta a incidentes de seguridad es regional.

> La cuenta de administrador delegada de Security Incident Response y las cuentas de los miembros deben agregarse directamente. AWS Organizations

Cuenta de administrador delegada para la respuesta a incidentes AWS de seguridad.

Puede designar una cuenta de miembro como cuenta de administrador delegada de respuesta a incidentes de seguridad. Por ejemplo, si designa una cuenta de miembro *111122223333* en*Europe (Ireland)*, no podrá designar otra cuenta *555555555555* de miembro. *Canada (Central)* Es obligatorio que utilices la misma cuenta que la cuenta de administrador delegado de respuesta a incidentes de seguridad en todas las demás regiones.

No se recomienda configurar la administración de su organización como la cuenta de administrador delegada de respuesta a incidentes de seguridad.

La administración de su organización puede ser la cuenta de administrador delegada de Security Incident Response. Sin embargo, las prácticas recomendadas de seguridad de AWS siguen el principio de privilegios mínimos y no recomiendan esta configuración.

Al eliminar una cuenta de administrador delegada de Security Incident Response de una suscripción activa, la suscripción se cancela inmediatamente.

Si eliminas una cuenta de administrador delegada de Security Incident Response, AWS Security Incident Response elimina todas las cuentas de miembros asociadas a esta cuenta de administrador delegada de Security Incident Response. AWS La respuesta a incidentes de seguridad dejará de estar habilitada para todas estas cuentas de miembros.

Habilitar el acceso confiable para AWS Account Management

Al habilitar el acceso confiable para la respuesta a incidentes de AWS seguridad, el administrador delegado de la cuenta de administración puede modificar la información y los metadatos (por ejemplo, los detalles de contacto principales o alternativos) específicos de cada cuenta de miembro. AWS Organizations

Utilice el siguiente procedimiento para habilitar el acceso confiable a la respuesta a incidentes de AWS seguridad en su organización.

Permisos mínimos

Para realizar estas tareas, debe cumplir con los siguientes requisitos:

- Puede realizar esto únicamente desde la cuenta de administración de la organización.
- Su organización debe tener habilitadas todas las características.

Console

Para habilitar el acceso confiable para la respuesta a incidentes de AWS seguridad

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. Seleccione Respuesta a incidentes de AWS seguridad en la lista de servicios.
4. Elija Habilitar acceso de confianza.
5. En el cuadro de diálogo Habilitar el acceso de confianza para la respuesta a incidentes de AWS seguridad, escriba habilitar para confirmarlo y, a continuación, elija Habilitar el acceso de confianza.

API/CLI

Para habilitar el acceso de confianza para AWS Account Management

Tras ejecutar el siguiente comando, puede usar las credenciales de la cuenta de administración de la organización para llamar a API las operaciones de administración de cuentas que utilizan el `--accountId` parámetro para hacer referencia a las cuentas de los miembros de una organización.

- AWS CLI: enable-aws-service-access

  El siguiente ejemplo permite un acceso confiable para la respuesta a incidentes de AWS seguridad en la organización de la cuenta que realiza la llamada.

```
$ aws organizations enable-aws-service-access \
                                        --service-principal security-
ir.amazonaws.com
```

  Este comando no genera ningún resultado si se utiliza correctamente.

Permisos necesarios para designar una cuenta de administrador delegada en Security Incident Response

Puede optar por configurar su membresía en respuesta a incidentes de AWS seguridad mediante un administrador delegado para. AWS Organizations Para obtener información sobre cómo se conceden estos permisos, consulte Utilización AWS Organizations con otros AWS servicios.

> **Note**
>
> AWS La respuesta a incidentes de seguridad activa automáticamente la relación de AWS Organizations confianza cuando se utiliza la consola para la configuración y la administración. Si usaCLI/SDK, debe habilitarlo manualmente mediante el EnableAWSService Access API to trust`security-ir.amazonaws.com`.

Como AWS Organizations gerente, antes de designar la cuenta de administrador de respuesta a incidentes de seguridad delegada para su organización, compruebe que puede realizar las siguientes acciones de respuesta a incidentes de AWS seguridad: `sir:CreateMembership` y`sir:UpdateMembership`. Estas acciones le permiten designar la cuenta de administrador delegada de Security Incident Response para su organización mediante AWS Security Incident Response. También debe asegurarse de que está autorizado a realizar las AWS Organizations acciones que le ayuden a recuperar información sobre su organización.

Para conceder estos permisos, incluye la siguiente declaración en una política AWS Identity and Access Management (IAM) de tu cuenta:

```
{
    "Sid": "PermissionsForSIRAdmin",
    "Effect": "Allow",
    "Action": [
        "security-ir:CreateMembership",
        "security-ir:UpdateMembership",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
```

```
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
    ],
    "Resource": "*"
}
```

Si desea designar a su AWS Organizations dirección como la cuenta de administrador delegada de Security Incident Response, su cuenta también necesitará la siguiente IAM acción:`CreateServiceLinkedRole`. Esta acción le permite inicializar la respuesta a incidentes AWS de seguridad para la administración. Sin embargo, revise Consideraciones y recomendaciones para utilizar la respuesta a incidentes AWS de seguridad con AWS Organizations antes de proceder a agregar los permisos.

Para seguir designando a la dirección como la cuenta de administrador delegada de la respuesta a incidentes de seguridad, añada la siguiente declaración a la IAM política y *111122223333* sustitúyala por el Cuenta de AWS identificador de la administración de su organización:

```
{
 "Sid": "PermissionsToEnablesir"
 "Effect": "Allow",
 "Action": [
  "iam:CreateServiceLinkedRole"
 ],
 "Resource": "arn:aws:iam::111122223333:role/aws-service-role/security-
ir.amazonaws.com/AWSServiceRoleForAmazonsir",
 "Condition": {
  "StringLike": {
   "iam:AWSServiceName": "security-ir.amazonaws.com"
  }
 }
}
```

Designación de un administrador delegado para la respuesta a los incidentes de seguridad AWS

En esta sección se proporcionan los pasos para designar un administrador delegado en la organización de respuesta a incidentes de AWS seguridad.

Como director de la AWS organización, asegúrese de leer detenidamente el funcionamiento de una cuenta Recomendaciones y consideraciones de administrador delegado de respuesta a incidentes de seguridad. Antes de continuar, asegúrese de contar con Permisos necesarios para designar una cuenta de administrador delegada en Security Incident Response.

Elija un método de acceso preferido para designar una cuenta de administrador delegada de respuesta a incidentes de seguridad para su organización. Solo una administración puede realizar este paso.

Console

1. Abra la consola de respuesta a incidentes de seguridad en https://console.aws.amazon.com/security-ir/

   Para iniciar sesión, utilice las credenciales de administración de su AWS Organizations organización.
2. Con el Región de AWS selector situado en la esquina superior derecha de la página, seleccione la región en la que desee designar la cuenta de administrador delegado de respuesta a incidentes de seguridad de su organización.
3. Siga las instrucciones del asistente de configuración para crear su membresía, incluida la cuenta de administrador delegado.

API/CLI

- Ejecute CreateMembership con las credenciales de la dirección Cuenta de AWS de la organización.
  - Alternativamente, puede usarlo AWS Command Line Interface para hacer esto. El siguiente AWS CLI comando designa una cuenta de administrador delegada en Security Incident Response. Las siguientes son las opciones de cadena disponibles para configurar su membresía:

```
{
  "customerAccountId": "stringstring",
  "membershipName": "stringstring",
  "customerType": "Standalone",
  "organizationMetadata": {
    "organizationId": "string",
    "managementAccountId": "stringstring",
```

```
      "delegatedAdministrators": [
        "stringstring"
      ]
    },
    "membershipAccountsConfigurations": {
      "autoEnableAllAccounts": true,
      "organizationalUnits": [
        "string"
      ]
    },
    "incidentResponseTeam": [
      {
        "name": "string",
        "jobTitle": "stringstring",
        "email": "stringstring"
      }
    ],
    "internalIdentifier": "string",
    "membershipId": "stringstring",
    "optInFeatures": [
      {
        "featureName": "RuleForwarding",
        "isEnabled": true
      }
    ]
  }
```

Si AWS la respuesta a incidentes de seguridad no está habilitada en su cuenta de administrador delegada de respuesta a incidentes de seguridad, no podrá realizar ninguna acción. Si aún no lo ha hecho, asegúrese de habilitar la respuesta a incidentes de AWS seguridad en la cuenta de administrador delegada de respuesta a incidentes de seguridad recién designada.

Añadir miembros a AWS Security Incident Response

Existe una relación individual con AWS Organizations su membresía en AWS Security Incident Response. A medida que se agreguen (o eliminen) cuentas de sus Organizaciones, esto se reflejará en las cuentas cubiertas de su membresía de AWS Security Incident Response.

Para añadir una cuenta a tu membresía, sigue una de las opciones para administrar las cuentas de una organización con AWS Organizations.

Eliminar miembros de AWS Security Incident Response

Para eliminar una cuenta de su membresía, siga los procedimientos para eliminar una cuenta de miembro de una organización.

Resolución de problemas

Cuando tenga problemas relacionados con la realización de una acción específica de la respuesta a incidentes de AWS seguridad, consulte los temas de esta sección.

Un ERROR es el estado de una operación que indica un fallo en algunas o en todas las operaciones. Como alternativa, recibirá advertencias cuando se produzca un problema, pero la tarea aún se complete.

Contenido

Problemas

No se envían solicitudes desde el contexto correcto.

Todas las llamadas a AWS Security Incident Response APIs deben proceder de IAM un responsable de la cuenta de miembro o administrador delegado del servicio. Asegúrese de operar desde la cuenta IAM principal correcta, es Cuenta de AWS decir, la cuenta de administrador delegado o de membresía de su organización, en materia de respuesta a incidentes de AWS seguridad.

Errores

AccessDeniedException

No tiene acceso suficiente para realizar esta acción.

Póngase en contacto con su AWS administrador para asegurarse de que tiene permiso para asumir un IAM rol en su cuenta de administrador delegado o miembro de AWS Security Incident Response. Compruebe también que el rol tenga una IAM política que permita la acción solicitada. Para obtener más información, consulte Respuesta a incidentes de AWS seguridad IAM.

ConflictException

La solicitud provoca un estado incoherente.

Compruebe que los nombres de los archivos adjuntos o los miembros predeterminados del equipo de respuesta que haya especificado sean únicos en cada caso. Compruebe también que su suscripción al servicio de respuesta a incidentes de AWS seguridad aún no esté configurada. Abra la consola de respuesta a incidentes de seguridad en https://console.aws.amazon.com/security-ir/ y navegue hasta`Membership Details`.

InternalServerException

Se ha producido un error inesperado durante el procesamiento de la solicitud. Vuelva a intentarlo en unos minutos. Si el problema persiste, presenta un caso con Support.

ResourceNotFoundException

La solicitud hace referencia a un recurso que no existe.

Uno o más de los recursos especificados en la solicitud no existen. Compruebe que todos los recursos proporcionados ARNs o IDs sean correctos. Esto se aplica a la cuenta AWS Organizations IDs, las IAM funcionesIDs, las membresías, los casos, los miembros del equipo de respuesta, los casos, los socorristas, los archivos adjuntos de casos y los comentarios de los casos.

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Su IAM director ha realizado demasiadas solicitudes para esa API función en un período específico. Espere un minuto e inténtelo de nuevo. Si el problema persiste, considere implementar un algoritmo de retroceso exponencial y reintento.

ValidationException

La entrada no cumple las restricciones especificadas por un. Servicio de AWS

Uno o más de los campos de datos de su solicitud no cumplían con los requisitos de validación o combinación lógica. Compruebe que todos los recursos estén ARNs completos y que los valores del texto cumplan con las restricciones de tamaño y formato de la Guía de API referencia sobre respuesta a incidentes de AWS seguridad. Compruebe también que se permita cualquier actualización de valores. Por ejemplo, no es posible cambiar un caso de AWS compatible a autogestionado.

Support

Si necesita ayuda adicional, póngase en contacto con Support el Centro para solucionar problemas. Tenga a mano la siguiente información:

- La Región de AWS que usaste
- El Cuenta de AWS ID de la membresía
- Tu contenido fuente, si corresponde y está disponible
- Cualquier otra información sobre el problema que tenga que puedan contribuir a la resolución de problemas

Seguridad

Contenido

Protección de datos en la respuesta a incidentes de AWS seguridad

Contenido

El modelo de responsabilidad AWS compartida se aplica a la protección de datos para el servicio de respuesta a incidentes de AWS seguridad. Como se describe en este modelo, AWS es responsable de proteger la infraestructura que ejecuta los servicios ofrecidos en la AWS nube. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También es responsable de las tareas de configuración y administración de la seguridad de AWS los servicios que utiliza. Para obtener más información sobre la privacidad de los datos, consulte la sección Privacidad de datos FAQ. Para obtener información sobre la protección de datos en Europa, consulte el modelo de responsabilidad AWS compartida y la entrada del GDPR blog sobre AWS seguridad.

Con fines de protección de datos, las mejores prácticas de AWS seguridad establecen que debe proteger las credenciales de las AWS cuentas y configurar los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta forma, a cada usuario se le otorgan únicamente los permisos necesarios para cumplir con sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactorial (MFA) con cada cuenta.
- UseSSL/TLSpara comunicarse con AWS los recursos. Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Configure API y registre la actividad del usuario con AWS CloudTrail.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados de AWS los servicios.
- FIPSActualmente, el servicio no admite el 140-3.

Nunca debe incluir información confidencial o delicada, como sus direcciones de correo electrónico, en etiquetas o campos de texto de formato libre, como un campo de nombre. Esto incluye cuando trabaja con AWS Support u otros AWS servicios mediante la consolaAPI, AWS CLI, o AWS SDKs. Todos los datos que introduzca, las etiquetas o los campos de texto de formato libre utilizados para los nombres se pueden utilizar para los registros de facturación o diagnóstico. Si los proporciona URL a un servidor externo, le recomendamos encarecidamente que no incluya información sobre las credenciales en él URL para validar su solicitud a ese servidor.

Cifrado de datos

Contenido

Cifrado en reposo

Los datos se cifran en reposo mediante cifrado transparente del lado del servidor. Esto ayuda a reducir la carga y la complejidad operativas que conlleva la protección de información confidencial. Con el cifrado en reposo, puede crear aplicaciones sensibles a la seguridad que cumplen los requisitos de cifrado y normativos.

Cifrado en tránsito

Los datos recopilados y accedidos por AWS Security Incident Response se realizan exclusivamente a través de un canal protegido por Transport Layer Security (TLS).

Administración de claves

AWS Security Incident Response implementa integraciones AWS KMS para proporcionar un cifrado inactivo para los datos de las cajas y los archivos adjuntos.

AWS La respuesta a incidentes de seguridad no admite las claves administradas por el cliente.

Privacidad del tráfico entre redes

Tráfico entre el servicio y las aplicaciones y clientes locales

Dispone de dos opciones de conectividad entre su red privada y AWS:

- Una AWS Site-to-Site VPN conexión. Para obtener más información, consulte ¿Qué es AWS Site-to-Site VPN? en la Guía del usuario de AWS Site-to-Site VPN .
- Una AWS Direct Connect conexión. Para obtener más información, consulte ¿Qué es AWS Direct Connect? en la Guía del usuario de AWS Direct Connect .

El acceso a AWS Security Incident Response a través de la red se realiza mediante una AWS publicaciónAPIs. Los clientes deben ser compatibles con Transport Layer Security (TLS) 1.2. Recomendamos la versión TLS 1.3. Los clientes también deben admitir conjuntos de cifrado con Perfect Forward Secrecy (PFS), como Ephemeral Diffie-Hellman () o Elliptic Curve Diffie-Hellman Ephemeral (DHE). ECDHE La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos. Además, debe firmar las solicitudes con un ID de clave de acceso y una clave de acceso secreta que estén asociados a una entidad principal de IAM, o bien puede usar AWS Security Token Service (STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Tráfico entre recursos de AWS en la misma región

Un punto final de Amazon Virtual Private Cloud (AmazonVPC) para la respuesta a incidentes de AWS seguridad es una entidad lógica dentro de una VPC que permite la conectividad únicamente a la respuesta a incidentes de AWS seguridad. Amazon VPC dirige las solicitudes a AWS Security Incident Response y redirige las respuestas aVPC. Para obtener más información, consulta los

VPCpuntos finales en la Guía del VPC usuario de Amazon. Para ver ejemplos de políticas que puede usar para controlar el acceso desde los VPC puntos de conexión, consulte Uso de IAM políticas para controlar el acceso a DynamoDB.

> **Note**
>
> No se puede acceder a VPC los puntos de enlace de Amazon a través de AWS Site-to-Site VPN o AWS Direct Connect.

Identity and Access Management

AWS Identity and Access Management (IAM) es un AWS servicio que ayuda al administrador a controlar el acceso a AWS los recursos. IAMlos administradores controlan a los directores autenticados (con sesión iniciada) y autorizados (con permisos) para que utilicen los recursos de respuesta a incidentes AWS de seguridad. IAMes un AWS servicio que puede utilizar sin coste adicional.

Contenido

Audiencia

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que se realice en AWS Security Incident Response.

Administradores de seguridad

Se sugiere a estos usuarios que utilicen la política AWSSecurityIncidentResponseFullAccessadministrada para asegurarse de que tienen acceso de lectura y escritura a los recursos de membresías y casos.

Observadores de casos

Estas personas no tienen acceso autorizado a todos los casos, excepto a los casos individuales para los que usted otorga un permiso explícito.

Miembros del equipo de respuesta a incidentes

Los miembros del equipo pueden ser miembros de pleno derecho y tener acceso a los casos. Se recomienda que no todas las personas puedan tomar medidas autorizadas al ser miembros del servicio, sino que tengan acceso a todos y cada uno de los casos que se creen y gestionen a través del servicio. Para obtener más información, consulte las políticas gestionadas de respuesta a incidentes de AWS seguridad.

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario raíz de la AWS cuenta, como IAM usuario o asumiendo un IAM rol.

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Los usuarios de IAM Identity Center (Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en la consola de AWS administración o en el portal de AWS acceso. Para obtener más información sobre cómo iniciar sesión en su cuenta AWS, consulte Cómo iniciar sesión en su AWS cuenta en la Guía del usuario de AWS inicio de sesión.

Si accedes AWS mediante programación, AWS incluye un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente tus solicitudes con tus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar AWS API las solicitudes en la Guía del IAM usuario.

Independientemente del método de autenticación que utilices, es posible que tengas que proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactorial (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactorial en la Guía del usuario de AWS IAM Identity Center y Uso de la autenticación multifactorial (MFA) AWS en la Guía del IAM usuario.

AWS usuario raíz de la cuenta

Al crear una AWS cuenta, comienza con una identidad de inicio de sesión que tiene acceso completo a todos los AWS servicios y recursos de la cuenta. Esta identidad se denomina usuario raíz de la

AWS cuenta y se accede a ella iniciando sesión con la dirección 8 y la contraseña que utilizaste para crear la cuenta. No utilice nunca al usuario root para sus tareas diarias y tome medidas para proteger sus credenciales de usuario root. Úselas únicamente para realizar tareas que solo el usuario root puede realizar. Para obtener la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Se recomienda exigir a los usuarios humanos, incluidos los que necesitan acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder a AWS los servicios mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios empresarial, un proveedor de identidades web, AWS Directory Service, el directorio Identity Center o cualquier usuario que acceda a los AWS servicios mediante credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden a AWS las cuentas, asumen funciones y las funciones proporcionan credenciales temporales.

Para la administración centralizada del acceso, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en IAM Identity Center, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus AWS cuentas y aplicaciones. Para obtener información sobre IAM Identity Center, consulte ¿Qué es IAM Identity Center? en la Guía del usuario de AWS IAM Identity Center.

IAMusuarios y grupos

Un IAMusuario es una identidad de tu AWS cuenta que tiene permisos específicos para una sola persona o aplicación. Te recomendamos que utilices credenciales temporales en lugar de crear IAM usuarios con credenciales de larga duración, como contraseñas y claves de acceso. Si tiene un caso de uso específico que requiere credenciales a largo plazo con IAM los usuarios, le recomendamos que rote las claves de acceso. Para obtener más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un IAMgrupo es una identidad que especifica un conjunto de IAM usuarios. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar IAM los recursos.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Cuándo crear un IAM usuario (en lugar de un rol) en la Guía del IAM usuario.

Roles de IAM

Un IAMrol es una identidad de tu AWS cuenta que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente un IAM rol en la consola AWS de administración cambiando de rol. Puede asumir un rol mediante una llamada a una AWS API operación AWS CLI o mediante una operación personalizadaURL. Para obtener más información acerca de los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, debe crear un rol y definir los permisos para el rol. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información sobre los roles para la federación, consulte Creación de un rol para un proveedor de identidades externo en la Guía del IAMusuario. Si usa IAM Identity Center, configura un conjunto de permisos. Para controlar a qué pueden acceder sus identidades después de autenticarse, IAM Identity Center correlaciona el conjunto de permisos con un rol en. IAM Para obtener información sobre los conjuntos de permisos, consulte los conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center.
- Permisos de IAM usuario temporales: un IAM usuario o rol puede asumir un IAM rol para asumir temporalmente diferentes permisos para una tarea específica.
- Acceso multicuenta: puedes usar un IAM rol para permitir que alguien (un responsable de confianza) de una cuenta diferente acceda a los recursos de tu cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunos AWS servicios, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información sobre la diferencia entre las funciones y las políticas basadas en recursos para el acceso multicuenta, consulte el acceso a los recursos entre cuentas IAM en la Guía del IAM usuario.
- Acceso entre servicios: algunos AWS servicios utilizan funciones de otros servicios. AWS Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio

haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.

- Función de servicio: una función de servicio es una IAMfunción que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un servicio de AWS en la Guía del usuario de IAM.
- Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un servicio. AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en su AWS cuenta y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un IAM rol para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y que realizan AWS CLI o AWS API solicitan. Es preferible hacerlo de este modo a almacenar claves de acceso dentro de la instancia EC2. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para obtener más información, consulte Uso de un IAM rol para conceder permisos a aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del IAM usuario.

Para saber si se deben usar IAM roles o IAM usuarios, consulte Cuándo crear un IAM rol (en lugar de un usuario) en la Guía del IAM usuario.

Cómo funciona la respuesta a incidentes de AWS seguridad con IAM

AWS Identity and Access Management (IAM) es un AWS servicio que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. IAMlos administradores controlan quién puede autenticarse (iniciar sesión) y quién está autorizado (tiene permisos) para usar los recursos de respuesta a incidentes de AWS seguridad. IAMes un AWS servicio que puede utilizar sin coste adicional.

IAMfunciones que puede utilizar con la respuesta a incidentes AWS de seguridad	
IAMcaracterística	Alineación de servicios
Políticas basadas en identidades	Sí

IAMfunciones que puede utilizar con la respuesta a incidentes AWS de seguridad	
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Condiciones de la política: claves	Sí (global)
ACLs	No
ABAC(etiquetas en las políticas)	Sí
Credenciales temporales	Sí
Sesiones de acceso directo () FAS	Sí
Roles de servicio	No
Roles vinculados al servicio	Sí

Contenido

Políticas basadas en la identidad para la respuesta a incidentes de seguridad AWS

Las políticas basadas en la identidad son documentos de política de JSON permisos que se pueden adjuntar a una identidad, como un IAM usuario, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones permitidas o denegadas, así como los recursos y las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociada. Para obtener más información sobre todos los elementos que

puede usar en una JSON política, consulte la referencia sobre los elementos de la IAM JSON política en la Guía del IAMusuario.

Contenido

Ejemplos de políticas basadas en identidades

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de respuesta a incidentes de AWS seguridad. Tampoco pueden realizar tareas mediante la consola de AWS administración, la interfaz de línea de AWS comandos (AWS CLI) o AWS API. Un IAM administrador puede crear IAM políticas para conceder a los usuarios permisos para realizar acciones con los recursos que necesitan. A continuación, el administrador puede agregar las políticas de IAM a los roles y los usuarios pueden asumirlos.

Para obtener información sobre cómo crear una política IAM basada en la identidad mediante estos documentos de JSON política de ejemplo, consulte Creación de IAM políticas en la Guía del IAMusuario.

Para obtener más información sobre las acciones y los tipos de recursos definidos por la respuesta a incidentes de AWS seguridad, incluido el ARNs formato de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de la respuesta a incidentes de AWS seguridad en la Referencia de autorización del servicio.

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear los recursos de respuesta a incidentes de AWS seguridad de su cuenta, acceder a ellos o eliminarlos. Estas acciones pueden suponer costes para tu cuenta. AWS Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS

administradas que otorgan permisos en muchos casos de uso comunes. Están disponibles en su cuenta de AWS . Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía de usuario de IAM.

Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se puedes llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía de usuario de IAM.

Use condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de política para especificar que todas las solicitudes deben enviarse medianteSSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de un AWS servicio específico, por ejemplo AWS CloudFormation. Para obtener más información, consulte los elementos IAM JSON de la política: Condición en la Guía del IAM usuario.

Utilice IAM Access Analyzer para validar sus IAM políticas y garantizar permisos seguros y funcionales: IAM Access Analyzer valida las políticas nuevas y existentes para que se ajusten al lenguaje de las políticas (JSON) y IAM a las IAM mejores prácticas. IAM Access Analyzer proporciona más de 100 comprobaciones de políticas y recomendaciones prácticas para ayudarlo a crear políticas seguras y funcionales. Para obtener más información, consulte la validación de políticas de IAM Access Analyzer en la Guía del IAM usuario.

Requerir autenticación multifactorial (MFA): si hay una situación en la que se requieren IAM usuarios o un usuario raíz en su AWS cuenta, actívela MFA para aumentar la seguridad. Para solicitarla MFA cuando se convoque a API las operaciones, añada MFA condiciones a sus políticas. Para obtener más información, consulte Configuración del API acceso MFA protegido en la Guía del IAM usuario.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía de usuario de IAM.

Uso de la consola AWS de respuesta a incidentes de seguridad

Para acceder https://console.aws.amazon.com/security-ir/, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de respuesta a incidentes de AWS seguridad de su AWS cuenta. Si crea una política basada en identidades que sea

más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas al AWS CLI o al AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la API operación que están intentando realizar.

Adjunte la política de acceso ReadOnly AWS gestionado o de respuesta a incidentes de AWS seguridad para garantizar que los usuarios y los roles puedan usar la consola de servicio. Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la AWS CLI tecla o. AWS API

```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "ViewOwnUserInfo",
"Effect": "Allow",
"Action": [
"iam:GetUserPolicy",
"iam:ListGroupsForUser",
"iam:ListAttachedUserPolicies",
"iam:ListUserPolicies",
"iam:GetUser"
],
"Resource": ["arn:AWS:iam::*:user/${AWS:username}"]
},
{
"Sid": "NavigateInConsole",
"Effect": "Allow",
"Action": [
"iam:GetGroupPolicy",
"iam:GetPolicyVersion",
"iam:GetPolicy",
"iam:ListAttachedGroupPolicies",
"iam:ListGroupPolicies",
"iam:ListPolicyVersions",
```

```
"iam:ListPolicies",
"iam:ListUsers"
],
"Resource": "*"
}
]
}
```

Políticas basadas en recursos dentro de la respuesta a incidentes de seguridad AWS

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son JSON documentos de políticas que se adjuntan a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de buckets de Amazon S3. En los servicios que admiten políticas basadas en recursos, los gestionadores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política basada en recursos. Las entidades principales pueden incluir cuentas, usuarios, roles, usuarios federados o servicios de AWS .

Para obtener más información, consulte el acceso a los recursos entre cuentas IAM en la Guía del IAMusuario.

Acciones políticas para la respuesta a incidentes de AWS seguridad

Support policy actions: Sí

Los administradores pueden usar AWS JSON políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento Acción de una JSON política describe las acciones que puede utilizar para permitir o denegar el acceso a una política. Las acciones de política suelen tener el mismo nombre que la AWS API operación asociada. Hay algunas excepciones, como las acciones que solo permiten permisos y que no tienen una operación coincidente. API También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de respuesta a incidentes de AWS seguridad, consulte las acciones definidas por la respuesta a incidentes AWS de seguridad en la Referencia de autorización del servicio.

Las acciones políticas de respuesta a incidentes de AWS seguridad utilizan el siguiente prefijo antes de la acción:

AWS Respuesta a incidentes de seguridad: identidad

Para especificar varias acciones en una única instrucción, sepárelas con comas.

«Acción»: ["Respuesta a un incidente de AWS seguridad -identity:action1"," Respuesta a un incidente de seguridad -identity:action2"]AWS

Recursos de políticas para Amazon AWS Security Incident Response

Recursos de políticas compatibles: Sí, los administradores pueden usar AWS JSON las políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento JSON de política de recursos especifica el objeto o los objetos a los que se aplica la acción. Las declaraciones deben incluir un recurso o un NotResource elemento. Como práctica recomendada, especifique un recurso mediante su nombre de recurso de Amazon (ARN). Puedes hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utiliza un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

"Resource": "*"

Claves de condición de la política para AWS la respuesta a incidentes de seguridad

Admite claves de condición de política específicas del servicio: No

Los administradores pueden usar AWS JSON políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento Condición (o bloque Condición) permite especificar las condiciones en las que entra en vigor una sentencia. El elemento Condition es opcional. Puedes crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de condición en una sentencia o varias claves en un único elemento de condición, AWS los evalúa mediante una AND operación lógica. Si especifica varios valores para

una sola clave de condición, AWS evalúa la condición mediante una operación OR lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para obtener más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del IAMusuario.

Listas de control de acceso (ACLs) en AWS Security Incident Response

SoportaACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLsson similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de JSON políticas.

Control de acceso basado en atributos (ABAC) con respuesta a incidentes de seguridad AWS

Soportes ABAC (etiquetas en las políticas): Sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define los permisos en función de los atributos. En AWS, estos atributos se denominan etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a muchos recursos de AWS . Etiquetar entidades y recursos es el primer paso deABAC. Luego, diseñe ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso al que está intentando acceder. ABACes útil en entornos de rápido crecimiento y ayuda en situaciones en las que la administración de políticas se vuelve engorrosa.

Para controlar el acceso en función de las etiquetas, se proporciona información sobre las etiquetas en el elemento de condición de una política mediante las claves AWS: ResourceTag /key-name,: / key-name RequestTag o AWS: condition. AWS TagKeys Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial. Para obtener más información al respectoABAC, consulte ¿Qué esABAC? en la Guía IAM del usuario. Para ver un tutorial con los pasos de configuraciónABAC, consulte Usar el control de acceso basado en atributos (ABAC) en la Guía del IAMusuario.

Credenciales temporales con Amazon AWS Security Incident Response

Compatibilidad con credenciales temporales: sí

AWS los servicios no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluidos AWS los servicios que funcionan con credenciales temporales, consulte AWS los servicios con los que funcionan IAM en la Guía del IAM usuario. Está utilizando credenciales temporales si inicia sesión en la consola de AWS administración mediante cualquier método, excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accede AWS mediante el enlace de inicio de sesión único (SSO) de su empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información acerca del cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puede crear credenciales temporales manualmente con la AWS CLI tecla o. AWS API A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Sesiones de acceso directo para responder a incidentes de AWS seguridad

Admite sesiones de acceso directo (FAS): Sí

Cuando utilizas un IAM usuario o un rol para realizar acciones en AWSél, se te considera director. Al utilizar algunos servicios, es posible que realice una acción que, a continuación, inicie otra acción en un servicio diferente. FASutiliza los permisos del principal que llama a un AWS servicio, junto con los del AWS servicio solicitante para realizar solicitudes a los servicios descendentes. FASlas solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros AWS servicios o recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información detallada sobre la política a la hora de realizar FAS solicitudes, consulte Reenviar las sesiones de acceso.

Solución de problemas AWS de identidad y acceso a la respuesta a incidentes de seguridad

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas más comunes que pueden surgir al trabajar con AWS Security Incident Response yIAM.

Temas

- No tengo autorización para realizar una acción
- No estoy autorizado a realizar iam: PassRole
- Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis recursos de respuesta a incidentes AWS de seguridad

No estoy autorizado a realizar ninguna acción

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

El siguiente ejemplo de error se produce cuando el IAM usuario de mateojackson intenta usar la consola para ver detalles sobre un my-example-widget recurso ficticio, pero no tiene los permisos ficticios de Respuesta a un incidente de AWS seguridad:GetWidget .

Usuario: arn ::iam: :123456789012:user/mateojackson no está autorizado a actuar AWS: Respuesta a un incidente de seguridad: en el recurso: my -example-widget AWS GetWidget

En este caso, la política del usuario de mateojackson debe actualizarse para permitir el acceso al recurso mediante la acción Respuesta a incidentes de seguridad:. my-example-widget AWS GetWidget

Si necesita ayuda, póngase en contacto con su administrador. AWS El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar la acción iam: PassRole si recibes un error que indica que no estás autorizado a realizar la PassRole acción iam:, tus políticas deben actualizarse para que puedas transferir una función a AWS Security Incident Response.

Algunos AWS servicios le permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

El siguiente ejemplo de error se produce cuando un IAM usuario llamado marymajor intenta usar la consola para realizar una acción en respuesta a incidentes de AWS seguridad. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

Usuario: arn ::iam: :123456789012:user/marymajor no está autorizado a realizar AWS: iam: PassRole

En este caso, las políticas de Mary deben actualizarse para que pueda realizar la acción iam:. PassRole Si necesitas ayuda, ponte en contacto con tu AWS administrador. El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis recursos de respuesta a incidentes de AWS seguridad

Puedes crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puedes especificar una persona de confianza para que asuma el rol.

Para obtener más información, consulte lo siguiente:

- Para saber si Amazon AWS Security Incident Response admite estas funciones, consulte Cómo funciona AWS Security Incident Response conIAM.
- Para obtener información sobre cómo proporcionar acceso a sus recursos en todas AWS las cuentas de su propiedad, consulte Proporcionar acceso a un IAM usuario de otra AWS cuenta de su propiedad en la Guía del IAM usuario.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a AWS cuentas de terceros, consulta Cómo proporcionar acceso a AWS cuentas propiedad de terceros en la Guía del IAM usuario.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticadoPara que su aplicación pueda acceder a s externamente (federación de identidades) en la Guía del usuario de IAM.
- Para saber la diferencia entre usar roles y políticas basadas en recursos para el acceso entre cuentas, consulta el tema sobre el acceso a recursos entre cuentas IAM en la Guía del IAM usuario.

Uso de roles de servicio

Soporta funciones de servicio: No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Crear un rol para delegar permisos a un AWS servicio en la Guía del IAM usuario.

Uso de roles vinculados a servicios

Funciones vinculadas al servicio para la respuesta a incidentes AWS de seguridad

Contenido

Admite roles vinculados a servicios: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un servicio. AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en la cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Un rol vinculado a un servicio facilita la configuración de la respuesta a incidentes de AWS seguridad, ya que no es necesario añadir manualmente los permisos necesarios. AWS Security Incident Response define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AWS Security Incident Response puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda asociar a ninguna otra entidad de IAM.

Para obtener información sobre otros servicios que admiten funciones vinculadas a servicios, consulte los AWS servicios que funcionan con funciones vinculadas al servicio IAM y busque los servicios que tengan la palabra Sí en la columna Funciones vinculadas al servicio. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

AWS SLR: AWSServiceRoleForSecurityIncidentResponse

AWS La respuesta a incidentes de seguridad utiliza la función vinculada al servicio (SLR) denominada AWSServiceRoleForSecurityIncidentResponse política de respuesta a incidentes de AWS seguridad para identificar las cuentas suscritas, crear casos y etiquetar los recursos relacionados.

Permisos

El rol AWSServiceRoleForSecurityIncidentResponse vinculado al servicio confía en que el siguiente servicio asuma el rol:

- `triage.security-ir.amazonaws.com`

A esta función se adjunta la política AWS gestionada denominada. AWSSecurityIncidentResponseServiceRolePolicy El servicio usa el rol para realizar acciones en los siguientes recursos:

- AWS Organizations: Permite que el servicio busque cuentas de membresía para usarlas con el servicio.
- CreateCase: Permite que el servicio cree casos de servicio en nombre de las cuentas de membresía.
- TagResource: Permite que los recursos de etiquetas de servicio estén configurados como parte del servicio.

Administrar el rol

No necesita crear manualmente un rol vinculado a servicios. Cuando te incorporas a la respuesta a incidentes de AWS seguridad en el AWS Management Console servicio AWS CLI AWS API, el o el servicio crea el rol vinculado al servicio para ti.

> **Note**
>
> Si creó una membresía con una cuenta de administrador delegado, los roles vinculados al servicio deberán crearse manualmente en las cuentas de administración. AWS Organizations

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando te incorporas al servicio, se vuelve a crear el rol vinculado al servicio para ti.

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o función) crear, editar o eliminar la descripción de una función vinculada a un servicio. Para obtener más información, consulta los permisos de los roles vinculados al servicio en la Guía del usuario. IAM

AWS SLR: AWSServiceRoleForSecurityIncidentResponse_Triage

AWS La respuesta a incidentes de seguridad utiliza la función vinculada al servicio (SLR) denominada AWSServiceRoleForSecurityIncidentResponse_Triage política de respuesta a incidentes de AWS seguridad para supervisar continuamente su entorno en busca de amenazas a la seguridad, ajustar los servicios de seguridad para reducir el ruido de las alertas y recopilar información para investigar posibles incidentes.

Permisos

El rol AWSServiceRoleForSecurityIncidentResponse_Triage vinculado al servicio confía en que el siguiente servicio asuma el rol:

- `triage.security-ir.amazonaws.com`

La política administrada de AWSSecurityIncidentResponseTriageServiceRolePolicy AWS está asociada a este rol. El servicio utiliza la función para realizar acciones en los siguientes recursos:

- Eventos: permite al servicio crear una regla Amazon EventBridge administrada. Esta regla es la infraestructura necesaria en su AWS cuenta para enviar los eventos de su cuenta al servicio. Esta acción se realiza en cualquier AWS recurso gestionado por`triage.security-ir.amazonaws.com`.
- Amazon GuardDuty: permite al servicio ajustar los servicios de seguridad para reducir el ruido de las alertas y recopilar información para investigar posibles incidentes. Esta acción se realiza en cualquier AWS recurso.
- AWS Security Hub: Permite al servicio ajustar los servicios de seguridad para reducir el ruido de las alertas y recopilar información para investigar posibles incidentes. Esta acción se realiza en cualquier AWS recurso.

Administrar el rol

No necesita crear manualmente un rol vinculado a servicios. Cuando te incorporas a la respuesta a incidentes de AWS seguridad en el AWS Management Console servicio AWS CLI AWS API, el o el servicio crea el rol vinculado al servicio para ti.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando te incorporas al servicio, se vuelve a crear el rol vinculado al servicio para ti.

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o función) crear, editar o eliminar la descripción de una función vinculada a un servicio. Para obtener más información, consulta los permisos de los roles vinculados al servicio en la Guía del usuario. IAM

Regiones compatibles con las funciones vinculadas al servicio de respuesta a incidentes de AWS seguridad

AWS La respuesta a incidentes de seguridad permite el uso de funciones vinculadas al servicio en todas las regiones en las que el servicio está disponible.

- Este de EE. UU. (Ohio)
- Oeste de EE. UU. (Oregón)
- EE.UU. Este (Virginia)
- UE (Fráncfort)
- UE (Irlanda)
- UE (Londres)
- UE (Estocolmo)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Tokio)
- Canadá (centro)

AWS Políticas gestionadas

Una política AWS administrada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Para añadir permisos a usuarios, grupos y roles, es más fácil usar políticas AWS administradas que escribirlas tú mismo. Se necesita tiempo y experiencia para crear políticas administradas por el cliente de IAM que le proporcionen al equipo solo los permisos necesarios. Para empezar rápidamente, puedes usar nuestras políticas AWS gestionadas. Estas políticas cubren casos de uso comunes y están disponibles en tu AWS cuenta. Para obtener más información sobre las políticas AWS administradas, consulte las políticas AWS administradas en la Guía del IAM usuario.

AWS los servicios mantienen y actualizan las políticas AWS gestionadas asociadas. No puede cambiar los permisos en las políticas AWS administradas. En ocasiones, los servicios agregan permisos adicionales a una política administrada de AWS para admitir características nuevas. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Es más probable que los servicios actualicen una política gestionada por AWS cuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no afectarán a los permisos existentes.

Además, AWS admite políticas administradas para funciones laborales que abarcan varios servicios. Por ejemplo, la política ReadOnlyAccess AWS gestionada proporciona acceso de solo lectura a todos los AWS servicios y recursos. Cuando un servicio lanza una nueva función, AWS agrega permisos de solo lectura para nuevas operaciones y recursos. Para obtener una lista y una descripción de las políticas de funciones laborales, consulte las políticas AWS gestionadas para las funciones laborales en la Guía del IAMusuario.

Contenido

AWS política gestionada: AWSSecurityIncidentResponseServiceRolePolicy

AWS La respuesta a incidentes de seguridad utiliza la política AWSSecurityIncidentResponseServiceRolePolicy AWS gestionada. Esta política AWS gestionada está asociada a la función AWSServiceRoleForSecurityIncidentResponsevinculada al servicio. La política proporciona acceso a la respuesta a incidentes de AWS seguridad para identificar las cuentas suscritas, crear casos y etiquetar los recursos relacionados.

> **Important**
>
> No almacene información de identificación personal (PII) u otra información confidencial o sensible en las etiquetas. AWS Security Incident Response utiliza etiquetas para

proporcionarle servicios de administración. Las etiquetas no están diseñadas para usarse con datos privados o confidenciales

Detalles de los permisos

El servicio usa esta política para realizar acciones en los siguientes recursos:

- AWS Organizations: Permite que el servicio busque cuentas de membresía para usarlas con el servicio.
- CreateCase: Permite que el servicio cree casos de servicio en nombre de las cuentas de membresía.
- TagResource: Permite que los recursos de etiquetas de servicio estén configurados como parte del servicio.

Puede ver los permisos asociados a esta política en las políticas AWS administradas de AWSSecurityIncidentResponseServiceRolePolicy.

AWS política gestionada: AWSSecurityIncidentResponseFullAccess

AWS La respuesta a incidentes de seguridad utiliza la política AWSSecurityIncidentResponseAdmin AWS gestionada. Esta política otorga acceso total a los recursos del servicio y acceso a los relacionados Servicios de AWS. Puede utilizar esta política con sus IAM directores para añadir rápidamente permisos para la respuesta a incidentes AWS de seguridad.

Important

No almacene información de identificación personal (PII) u otra información confidencial o sensible en las etiquetas. AWS Security Incident Response utiliza etiquetas para proporcionarle servicios de administración. Las etiquetas no están diseñadas para usarse con datos privados o confidenciales

Detalles de los permisos

El servicio usa esta política para realizar acciones en los siguientes recursos:

- IAMacceso principal de solo lectura: otorga al usuario del servicio la posibilidad de realizar acciones de solo lectura contra los recursos de respuesta a incidentes de AWS seguridad existentes.
- IAMacceso de escritura principal: otorga al usuario del servicio la posibilidad de actualizar, modificar, eliminar y crear recursos de respuesta a incidentes de AWS seguridad.

Puede ver los permisos asociados a esta política en las políticas AWS gestionadas de AWSSecurityIncidentResponseFullAccess.

AWS política gestionada: AWSSecurityIncidentResponseReadOnlyAccess

AWS La respuesta a incidentes de seguridad utiliza la política AWSSecurityIncidentResponseReadOnlyAccess AWS gestionada. La política otorga acceso de solo lectura a los recursos de casos de servicio. Puede utilizar esta política con sus IAM directores para añadir rápidamente permisos para la respuesta a incidentes de AWS seguridad.

> **Important**
>
> No almacene información de identificación personal (PII) u otra información confidencial o sensible en las etiquetas. AWS Security Incident Response utiliza etiquetas para proporcionarle servicios de administración. Las etiquetas no están diseñadas para usarse con datos privados o confidenciales

Detalles de los permisos

El servicio usa esta política para realizar acciones en los siguientes recursos:

- IAMacceso principal de solo lectura: otorga al usuario del servicio la posibilidad de realizar acciones de solo lectura contra los recursos de respuesta a incidentes de AWS seguridad existentes.

Puede ver los permisos asociados a esta política en AWS las políticas gestionadas de. AWSSecurityIncidentResponseReadOnlyAccess

AWS política gestionada: AWSSecurityIncidentResponseCaseFullAccess

AWS La respuesta a incidentes de seguridad utiliza la política AWSSecurityIncidentResponseCaseFullAccess AWS gestionada. La política otorga acceso total a

los recursos de los casos de servicio. Puede utilizar esta política con sus IAM directores para añadir rápidamente permisos para la respuesta a incidentes AWS de seguridad.

> **Important**
>
> No almacene información de identificación personal (PII) u otra información confidencial o sensible en las etiquetas. AWS Security Incident Response utiliza etiquetas para proporcionarle servicios de administración. Las etiquetas no están diseñadas para usarse con datos privados o confidenciales

Detalles de los permisos

El servicio usa esta política para realizar acciones en los siguientes recursos:

- IAMacceso de solo lectura en mayúsculas y minúsculas: otorga al usuario del servicio la posibilidad de realizar acciones de solo lectura en casos de respuesta a incidentes de AWS seguridad existentes.
- IAMacceso de escritura en mayúsculas y minúsculas: otorga al usuario del servicio la posibilidad de actualizar, modificar, eliminar y crear casos de respuesta a incidentes de AWS seguridad.

Puede ver los permisos asociados a esta política en las políticas AWS gestionadas de AWSSecurityIncidentResponseCaseFullAccess.

AWS política gestionada: AWSSecurityIncidentResponseTriageServiceRolePolicy

AWS La respuesta a incidentes de seguridad utiliza la política AWSSecurityIncidentResponseTriageServiceRolePolicy AWS gestionada.
Esta política AWS gestionada está asociada a la función vinculada al servicio AWSServiceRoleForSecurityIncidentResponse_Triage.

La política proporciona acceso a la respuesta a incidentes de AWS seguridad para monitorear continuamente su entorno en busca de amenazas a la seguridad, ajustar los servicios de seguridad para reducir el ruido de las alertas y recopilar información para investigar posibles incidentes. No puede adjuntar esta política a sus entidades de IAM.

> **Important**
>
> No almacene información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada en las etiquetas. AWS Security Incident Response utiliza etiquetas para proporcionarle servicios de administración. Las etiquetas no están diseñadas para usarse con datos privados o confidenciales

Detalles de los permisos

El servicio usa esta política para realizar acciones en los siguientes recursos:

- Eventos: permite al servicio crear una regla EventBridge gestionada por Amazon. Esta regla es la infraestructura necesaria en tu AWS cuenta para enviar los eventos de tu cuenta al servicio. Esta acción se realiza en cualquier AWS recurso gestionado por`triage.security-ir.amazonaws.com`.
- Amazon GuardDuty: permite al servicio ajustar los servicios de seguridad para reducir el ruido de las alertas y recopilar información para investigar posibles incidentes. Esta acción se realiza en cualquier AWS recurso.
- AWS Security Hub: Permite al servicio ajustar los servicios de seguridad para reducir el ruido de las alertas y recopilar información para investigar posibles incidentes. Esta acción se realiza en cualquier AWS recurso.

Puede ver los permisos asociados a esta política en las políticas AWS administradas de AWSSecurityIncidentResponseTriageServiceRolePolicy.

AWS Respuesta a incidentes de seguridad: actualizaciones SLRs y políticas gestionadas

Consulte los detalles sobre las actualizaciones de las funciones de respuesta a incidentes de AWS seguridad SLRs y políticas gestionadas desde que este servicio comenzó a realizar el seguimiento de estos cambios.

Cambio	Descripción	Fecha
NuevoSLR: AWSServiceRoleForSecurityIncidentResponse Nueva política gestionada — AWSSecurityIncidentResponseServiceRolePolicy.	Nuevo rol vinculado al servicio y política adjunta que permite el acceso al servicio a sus AWS Organizations cuentas para identificar la membresía.	1 de diciembre de 2024
NuevoSLR: AWSServiceRoleForSecurityIncidentResponse_Triage Nueva política gestionada — AWSSecurityIncidentResponseTriageServiceRolePolicy	Nueva función vinculada al servicio y política adjunta que permite el acceso del servicio a sus AWS Organizations cuentas para clasificar los eventos de seguridad.	1 de diciembre de 2024
Nueva política gestionada: AWSSecurityIncidentResponseFullAccess	AWS La respuesta a incidentes de seguridad agrega una nueva SLR para IAM adjuntarla a las principales acciones de lectura y escritura del servicio.	1 de diciembre de 2024

Cambio	Descripción	Fecha
Nueva función de política gestionada: AWSSecurityIncidentResponseReadOnlyAccess	AWS Respuesta a incidentes de seguridad: añada una nueva SLR acción para adjuntarla a IAM los directores y leerla	1 de diciembre de 2024
Nueva función de política gestionada: AWSSecurityIncidentResponseCaseFullAccess	AWS La respuesta a incidentes de seguridad agrega una nueva SLR para adjuntarla a IAM las principales acciones de lectura y escritura en los casos de servicio.	1 de diciembre de 2024
Comenzó a rastrear los cambios.	Comenzó a rastrear los cambios en las políticas gestionadas SLRs y de respuesta a incidentes de AWS seguridad	1 de diciembre de 2024

Respuesta a incidentes

La seguridad y el cumplimiento son una responsabilidad compartida entre el cliente AWS y el cliente. Este modelo compartido puede ayudar a aliviar la carga operativa del cliente, ya que AWS opera, administra y controla los componentes desde el sistema operativo anfitrión y la capa de virtualización hasta la seguridad física de las instalaciones en las que opera el servicio. El cliente asume la responsabilidad y la administración del sistema operativo huésped (incluidas las actualizaciones y los parches de seguridad), del resto del software de aplicación asociado, así como de la configuración del firewall del grupo de seguridad AWS suministrado. Para obtener información adicional, consulte el modelo de responsabilidad AWS compartida.

Al establecer una base de seguridad que cumpla con los objetivos de las aplicaciones que se ejecutan en la nube, puede detectar las desviaciones a las que puede responder. Dado que la respuesta a los incidentes de seguridad puede ser un tema complejo, le recomendamos que consulte los siguientes recursos para que pueda comprender mejor el impacto que la respuesta a

los incidentes y sus elecciones tienen en sus objetivos corporativos: el documento técnico sobre las mejores prácticas de AWS seguridad y el documento técnico Perspectiva de seguridad del marco de adopción de la AWS nube (CAF).

Validación de conformidad

Los auditores externos evalúan la seguridad y el cumplimiento de AWS los servicios como parte de varios programas de AWS cumplimiento. Estos incluyen SOC PCI la Reserva Federal RAMP HIPAA y otros.

AWS No se ha evaluado la conformidad de la respuesta a los incidentes de seguridad con los programas antes mencionados.

Para obtener una lista de AWS los servicios incluidos en el ámbito de los programas de cumplimiento específicos, consulte AWS los servicios incluidos en el ámbito de aplicación por programa de cumplimiento. Para obtener información general, consulte los programas AWS de conformidad.

Puedes descargar informes de auditoría de terceros mediante AWS Artifact. Para obtener más información, consulta Descarga de informes en AWS Artifact.

Su responsabilidad en materia de cumplimiento al utilizar AWS los servicios viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las normas AWS y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en la seguridad y el cumplimiento. AWS
- Documento técnico sobre cómo diseñar una arquitectura basada en HIPAA la seguridad y el cumplimiento: este documento técnico describe cómo las empresas pueden utilizar para crear aplicaciones que cumplan con los requisitos. AWS HIPAA
- AWS recursos de cumplimiento: una colección de libros de trabajo y guías que se aplican por sector o ubicación.
- La evaluación de los recursos con AWS las reglas de AWS Config en la Guía para desarrolladores de AWS Config: Config; evalúa en qué medida las configuraciones de sus recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub: este AWS servicio proporciona una visión integral del estado de seguridad interno AWS. Security Hub utiliza controles de seguridad para evaluar sus AWS recursos y comprobar su conformidad con los estándares y las mejores prácticas del sector de la seguridad.

Para obtener una lista de los servicios y controles compatibles, consulta la Referencia de controles de Security Hub.

- Amazon GuardDuty: este AWS servicio detecta posibles amenazas para sus AWS cuentas, cargas de trabajo, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarle a cumplir diversos requisitos de conformidad, por ejemplo PCIDSS, cumpliendo con los requisitos de detección de intrusiones exigidos por determinados marcos de conformidad.
- AWS Audit Manager: este AWS servicio le ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Registro y supervisión en AWS Security Incident Response

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de AWS Security Incident Response y del resto de sus AWS soluciones. AWS En la actualidad, Security Incident Response admite los siguientes AWS servicios para supervisar su organización y la actividad que se lleva a cabo en ella.

AWS CloudTrail — Con ella CloudTrail puede capturar API llamadas desde la consola de respuesta a incidentes de AWS seguridad. Por ejemplo, cuando un usuario se autentica, CloudTrail puede registrar detalles como la dirección IP de la solicitud, quién la realizó y cuándo se realizó.

Amazon CloudWatch Metrics: con CloudWatch las métricas, puedes monitorear, informar y tomar acciones automáticas en caso de que se produzca un evento casi en tiempo real. Por ejemplo, puede crear CloudWatch paneles con las métricas proporcionadas para monitorear su uso de la respuesta a incidentes de AWS seguridad, o puede crear CloudWatch alarmas en las métricas proporcionadas para notificarle si se incumple un umbral establecido.

El espacio de nombres del servicio es /Usage/. AWS ServiceName Los nombres de las métricas disponibles son y. ActiveManagedCases SelfManagedCases

De conformidad con las condiciones del AWS servicio, el equipo de respuesta a incidentes de AWS seguridad tendrá acceso a su historial DNS y a los datos de CloudTrail registro de S3. VPC Estos datos se pueden utilizar durante los incidentes de seguridad activos cuando hay un caso abierto en el portal del servicio de respuesta a incidentes de AWS seguridad.

Resiliencia

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja demora. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte la infraestructura AWS global.

Seguridad de la infraestructura

AWS La respuesta a incidentes de seguridad está protegida por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

APILas llamadas AWS publicadas se utilizan para acceder a AWS Security Incident Response a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Cifre suites con perfecto secreto (PFS), como (Ephemeral Diffie-Hellman) o DHE ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. O bien, puede usar el servicio de token de seguridad () para generar credenciales de seguridad temporales para firmar AWS solicitudes.AWS STS

Configuración y análisis de vulnerabilidades

Usted es responsable de administrar las funciones de contención del servicio y los conjuntos de AWS CloudFormation pilas asociados.

AWS se encarga de las tareas de seguridad básicas, como la aplicación de parches al sistema operativo (SO) huésped y a las bases de datos, la configuración del firewall y la recuperación ante desastres. Estos procedimientos han sido revisados y certificados por los terceros pertinentes. Para obtener más detalles, consulte los siguientes recursos de AWS :

- Modelo de responsabilidad compartida
- Prácticas recomendadas para seguridad, identidad y conformidad

Prevención de la sustitución confusa entre servicios

El problema de la sustitución confusa es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En este AWS caso, la suplantación de identidad entre servicios puede provocar el confuso problema de un diputado. La suplantación entre servicios puede producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a cabo las llamadas se puedes manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que le ayudan a proteger los datos de todos los servicios cuyos directores de servicio tengan acceso a los recursos de su cuenta.

Recomendamos utilizar las claves de contexto de condición SourceAccount global AWSAWS: SourceArn y: en las políticas de recursos para limitar los permisos que Amazon Connect concede a otro servicio al recurso. Si usa ambas claves de contexto de condición globales, el SourceAccount valor AWS: y la cuenta del SourceArn valor AWS: deben usar el mismo ID de cuenta cuando se usen en la misma declaración de política.

La forma más eficaz de protegerse contra el confuso problema de los diputados es utilizar el nombre exacto del recurso de Amazon (ARN) del recurso que quieres permitir. Si no conoce la totalidad ARN del recurso o si está especificando varios recursos, utilice la AWS clave de condición de contexto SourceArn global con caracteres comodín (*) para las partes desconocidas del ARN recurso. Por ejemplo, arn ::servicename: :region-name: :tu ID de cuenta AWS: *. AWS

Para ver un ejemplo de política de suplantación de cargos que muestre cómo se puede evitar un problema de subdirector confuso, consulte Política de prevención de suplentes confusos.

Service Quotas

AWS Respuesta a incidentes de seguridad

En las siguientes tablas se enumeran las cuotas de los recursos de respuesta a incidentes de AWS seguridad para su AWS cuenta;. Algunas cuotas pueden aumentarse por encima de las que se indican a continuación con la aprobación del administrador del servicio. A menos que se indique lo contrario, estas cuotas son por región.

	Nombre	Valor predeterminado	Ajustable	Comentarios
1	Casos AWS compatibles activos	10	Sí (hasta 50)	El número de casos activos en los que se solicita asistencia AWS CIRT.
2	Casos activos autogestionados	50	Sí (hasta 100)	El número de casos activos que utilizan la plataforma sin la ayuda de AWS CIRT.
3	El servicio admite casos creados en 24 horas	10	No	El número de casos creados para solicitar asistencia AWS CIRT se creó en un período continuo de 24 horas.
4	Número máximo de entidades en el equipo	10	No	El número máximo de entidades

	Nombre	Valor predeterminado	Ajustable	Comentarios
	de respuesta a incidentes predeterminado			del equipo de respuesta a incidentes predeterminado.
5	Número máximo de miembros adicionales en un caso	30	No	El número máximo de entidades asociadas a un caso. Inicialmente, se rellenará con las entidades de tu equipo de respuesta a incidentes predeterminado.
6	Número máximo de casos adjuntos	50	Sí (hasta 100)	El número máximo de archivos que se pueden adjuntar a un caso.
7	Tamaño máximo de los comentarios de un caso	1 000	No	El número máximo de caracteres de un comentario de caso.
8	Tamaño máximo del nombre del archivo adjunto en mayúsculas y	255	No	El número máximo de caracteres de un nombre de archivo.

AWS Guía técnica de respuesta a incidentes de seguridad

Contenido

Resumen

Esta guía presenta una descripción general de los aspectos básicos de la respuesta a los incidentes de seguridad en el entorno de nube Amazon Web Services (AWS) de un cliente. Se proporciona información general sobre los conceptos de seguridad en la nube y respuesta a incidentes y se identifican las capacidades, los servicios y los mecanismos de la nube que están disponibles para los clientes que responden a problemas de seguridad.

Esta guía está destinada a quienes desempeñan funciones técnicas y supone que están familiarizados con los principios generales de la seguridad de la información, que tienen conocimientos básicos sobre la respuesta a los incidentes de seguridad en sus entornos locales actuales y que están familiarizados con los servicios en la nube.

¿Usa Well-Architected?

El marco de AWS Well-Architected le ayuda a entender las ventajas y desventajas de las decisiones que toma al crear sistemas en la nube. Los seis pilares del marco le permitirán aprender las prácticas recomendadas de arquitectura para diseñar y utilizar sistemas fiables, seguros, eficientes,

rentables y sostenibles. Con la AWS Well-Architected Tool consola AWS Well-Architected Tool, que está disponible de forma gratuita, puede comparar sus cargas de trabajo con estas prácticas recomendadas respondiendo a una serie de preguntas para cada pilar.

Para obtener más orientación experta y prácticas recomendadas para la arquitectura de la nube (implementaciones de arquitectura de referencia, diagramas y documentos técnicos), consulte el Centro de arquitectura de AWS.

Introducción

La seguridad es la principal prioridad en AWS. AWS los clientes se benefician de los centros de datos y la arquitectura de red diseñados para ayudar a satisfacer las necesidades de las organizaciones más sensibles a la seguridad. AWS tiene un modelo de responsabilidad compartida: AWS gestiona la seguridad de la nube y los clientes son responsables de la seguridad en la nube. Esto significa que usted tiene el control total de su implementación de seguridad, incluido el acceso a varias herramientas y servicios que le ayudarán a cumplir sus objetivos de seguridad. Estas capacidades le ayudan a establecer una base de seguridad para las aplicaciones que se ejecutan en Nube de AWS.

Si se produce una desviación de la línea base, por ejemplo, debido a un error de configuración o a un cambio de factores externos, tendrá que responder e investigar. Para hacerlo correctamente, debe comprender los conceptos básicos de la respuesta a los incidentes de seguridad en su AWS entorno y los requisitos para preparar, formar y capacitar a los equipos de la nube antes de que se produzcan problemas de seguridad. Es importante saber qué controles y capacidades puede utilizar, revisar los ejemplos de actualidad para resolver posibles problemas e identificar los métodos de remediación que utilizan la automatización para mejorar la velocidad y la coherencia de la respuesta. Además, debe comprender sus requisitos normativos y de cumplimiento en lo que respecta a la creación de un programa de respuesta a incidentes de seguridad que cumpla con esos requisitos.

La respuesta a los incidentes de seguridad puede ser compleja, por lo que le recomendamos que adopte un enfoque iterativo: comience con los servicios de seguridad básicos, desarrolle las capacidades fundamentales de detección y respuesta y, a continuación, desarrolle manuales para crear una biblioteca inicial de mecanismos de respuesta a los incidentes sobre los que pueda iterar y mejorar.

Antes de empezar

Antes de empezar a aprender sobre la respuesta a los incidentes de seguridad AWS, familiarícese con los estándares y marcos pertinentes en materia de AWS seguridad y respuesta a incidentes.

Estos fundamentos le ayudarán a comprender los conceptos y las mejores prácticas que se presentan en esta guía.

AWS estándares y marcos de seguridad

Para empezar, le recomendamos que consulte el documento técnico Best Practices for Security, Identity and Compliance, Security Pillar: AWS Well-Architected Framework y Security Perspective of the Overview of AWS the Cloud Adoption Framework AWS CAF ().

En él se AWS CAF proporcionan directrices que respaldan la coordinación entre las distintas partes de las organizaciones que se están migrando a la nube. La AWS CAF guía se divide en varias áreas de enfoque, denominadas perspectivas, que son relevantes para crear sistemas de TI basados en la nube. La perspectiva de seguridad describe cómo implementar un programa de seguridad en todos los flujos de trabajo, uno de los cuales es la respuesta a incidentes. Este documento es el resultado de nuestra experiencia trabajando con los clientes para ayudarlos a crear programas y capacidades de respuesta a incidentes de seguridad efectivos y eficientes.

Estándares y marcos de respuesta a incidentes de la industria

Este documento técnico sigue los estándares de respuesta a incidentes y las mejores prácticas de la Guía de manejo de incidentes de seguridad informática SP 800-61 r2, creada por el Instituto Nacional de Estándares y Tecnología (). NIST Leer y comprender los conceptos introducidos por la guía NIST es un requisito previo útil. Los conceptos y las mejores prácticas de esta NIST guía se aplicarán a AWS las tecnologías en este paper. Sin embargo, los escenarios de incidentes locales están fuera del ámbito de aplicación de esta guía.

AWS descripción general de la respuesta a incidentes

Para empezar, es importante entender en qué se diferencian las operaciones de seguridad y la respuesta a los incidentes en la nube. Para desarrollar capacidades de respuesta que sean eficaces AWS, necesitará comprender las diferencias con respecto a la respuesta local tradicional y su impacto en su programa de respuesta a incidentes. Cada una de estas diferencias, así como los principios básicos del diseño de la respuesta a los AWS incidentes, se detallan en esta sección.

Aspectos de la respuesta a los AWS incidentes

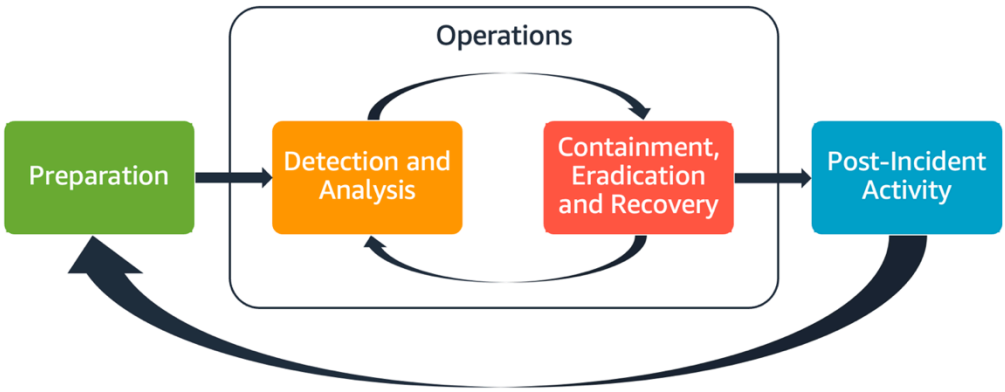
Todos AWS los usuarios de una organización deben tener un conocimiento básico de los procesos de respuesta a los incidentes de seguridad, y el personal de seguridad debe saber cómo responder a los problemas de seguridad. La educación, la capacitación y la experiencia son fundamentales para el éxito de un programa de respuesta ante incidentes en la nube y, en un escenario ideal, deben

implementarse mucho antes de tener que gestionar un posible incidente de seguridad. La base de un programa de respuesta a incidentes exitoso en la nube son la preparación, las operaciones y la actividad posterior a los incidentes.

A continuación se describe cada uno de estos aspectos para que los entienda mejor:

- Preparación: prepare a su equipo de respuesta a incidentes para detectar y responder a los incidentes internos, AWS habilitando los controles de detección y verificando 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: aborde los eventos de seguridad y los posibles incidentes siguiendo las fases NIST de respuesta a los incidentes: detectar, analizar, contener, erradicar y recuperar.
- Actividad posterior a un incidente: analice el resultado de sus simulaciones y eventos 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.

Cada uno de estos aspectos se analiza y detalla en esta guía. El siguiente diagrama muestra el flujo de estos aspectos, alineándose con el ciclo de vida de respuesta a los NIST incidentes mencionado anteriormente, pero con operaciones que abarcan la detección y el análisis, además de la contención, la erradicación y la recuperación.



Aspectos de la respuesta a los AWS incidentes

AWS principios de respuesta a incidentes y objetivos de diseño

Si bien los procesos y mecanismos generales de respuesta a los incidentes, tal como se definen en la Guía de gestión de incidentes de seguridad informática NIST SP 800-61, son sólidos, le

recomendamos que también tenga en cuenta estos objetivos de diseño específicos que son relevantes para responder a los incidentes de seguridad en un entorno de nube:

- Establezca los objetivos de respuesta: trabaje con las partes interesadas, los asesores legales y los líderes de la organización para determinar el objetivo de la respuesta a un incidente. Algunos objetivos comunes incluyen contener y mitigar el problema, recuperar los recursos afectados, conservar los datos para el análisis forense, volver a las operaciones seguras y, en última instancia, aprender de los incidentes.
- Responda mediante la nube: implemente patrones de respuesta dentro de la nube, donde se producen el evento y los datos.
- Sepa lo que tiene y lo que necesita: conserve los registros, los recursos, las instantáneas y otras pruebas copiándolos y almacenándolos en una cuenta centralizada en la nube dedicada a responder. Utilice etiquetas, metadatos y mecanismos que cumplan las políticas de retención. Deberá comprender qué servicios utiliza y, a continuación, identificar los requisitos para investigar esos servicios. Para ayudarle a entender su entorno, también puede utilizar el etiquetado, que se describe más adelante en esta the section called “Desarrollo e implementación de una estrategia de etiquetado” sección de este documento.
- Utilice mecanismos de redistribución: si una anomalía de seguridad puede atribuirse a una configuración incorrecta, la solución podría ser tan sencilla como eliminar la variación mediante la redistribución de los recursos con la configuración adecuada. Si se identifica un posible problema, compruebe que la redistribución incluya una mitigación correcta y verificada de las causas fundamentales.
- Automatice siempre que sea posible: a medida que surjan problemas o se repitan los incidentes, cree mecanismos para clasificar y responder a los eventos comunes mediante programación. Utilice respuestas humanas para incidentes únicos, complejos o delicados en los que las automatizaciones no sean suficientes.
- Elija 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.
- Aprenda y mejore sus procesos: sea proactivo a la hora de identificar las brechas en sus procesos, herramientas o personas e implemente un plan para solucionarlas. Las simulaciones son métodos seguros para detectar brechas y mejorar los procesos. Consulte la the section called “Actividad posterior al incidente” sección de este documento para obtener detalles sobre cómo iterar sus 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, idealmente con una metodología de respuesta sólida desde el punto de vista forense. En algunos casos, esto significa que puede tener varias organizaciones, cuentas y herramientas configuradas específicamente para estas tareas de respuesta. Estas herramientas y funciones deben ponerse a disposición del personal de respuesta ante incidentes mediante una canalización de implementación. No deben ser estáticas porque pueden causar un riesgo mayor.

Dominios de incidentes de seguridad en la

Para prepararse y responder eficazmente a los eventos de seguridad en su AWS entorno, debe comprender los tipos más comunes de incidentes de seguridad en la nube. Hay tres ámbitos de responsabilidad del cliente en los que pueden producirse incidentes de seguridad: el servicio, la infraestructura y la aplicación. Los diferentes dominios requieren diferentes conocimientos, herramientas y procesos de respuesta. Considere estos dominios:

- Dominio de servicio: los incidentes en el dominio de servicio pueden afectar a tus Cuenta de AWS permisos, metadatos de recursos, facturación u otras áreas. AWS Identity and Access ManagementIAM Un evento del dominio de servicio es aquel al que respondes exclusivamente con AWS API mecanismos, o en el que las causas principales están asociadas a la configuración o a los permisos de los recursos, y que pueden tener un registro relacionado orientado a los servicios.
- Dominio de infraestructura: los incidentes en el dominio de infraestructura incluyen datos o actividad relacionada con la red, como los procesos y datos de sus instancias de Amazon Elastic Compute Cloud (AmazonEC2), el tráfico a sus EC2 instancias de Amazon dentro de la nube privada virtual (VPC) y otras áreas, como contenedores u otros servicios futuros. Su respuesta a los eventos del dominio de la infraestructura suele implicar la adquisición de datos relacionados con los incidentes para su análisis forense. Es probable que incluya la interacción con el sistema operativo de una instancia y, en varios casos, también pueda implicar AWS API mecanismos. En el ámbito de la infraestructura, puede utilizar una combinación de AWS APIs herramientas forenses o de respuesta a incidentes (DFIR) digitales dentro de un sistema operativo huésped, como una EC2 instancia de Amazon dedicada a realizar análisis e investigaciones forenses. Los incidentes en el dominio de infraestructura pueden implicar el análisis de capturas de paquetes de red, bloques de discos en un volumen de Amazon Elastic Block Store (AmazonEBS) o memoria volátil adquirida de una instancia.
- Dominio de la aplicación: los incidentes en el dominio de la aplicación se producen en el código de la aplicación o en el software implementado en los servicios o la infraestructura. Este dominio debería incluirse en sus manuales de estrategias de detección y respuesta a las amenazas en

la nube y podría incorporar respuestas similares a las del dominio de la infraestructura. Con una arquitectura de aplicaciones adecuada y bien pensada, puede administrar este dominio con herramientas en la nube mediante la adquisición, la recuperación y el despliegue automatizados.

En estos ámbitos, considere los actores que podrían actuar en contra de AWS las cuentas, los recursos o los datos. Ya sea interno o externo, utilice un marco de riesgos para determinar los riesgos específicos para la organización y prepárese en consecuencia. Además, debe desarrollar modelos de amenazas que le ayuden a planificar la respuesta a los incidentes y a desarrollar una arquitectura cuidadosa.

Las principales diferencias en la respuesta a los incidentes en AWS

La respuesta a los incidentes es una parte integral de una estrategia de ciberseguridad, ya sea en las instalaciones o en la nube. Los principios de seguridad, como el mínimo privilegio y la defensa en profundidad, tienen por objeto proteger la confidencialidad, la integridad y la disponibilidad de los datos tanto en las instalaciones como en la nube. Son varios los patrones de respuesta a incidentes que respaldan estos principios de seguridad, como la retención de registros, la selección de alertas a partir del modelado de amenazas, la elaboración de manuales de estrategias y la integración de la información de seguridad y la gestión de eventos (SIEM). Las diferencias comienzan cuando los clientes comienzan a diseñar y diseñar estos patrones en la nube. Las siguientes son las principales diferencias en la respuesta a los incidentes en AWS.

Diferencia #1: La seguridad como responsabilidad compartida

La responsabilidad de la seguridad y el cumplimiento es compartida entre sus clientes AWS y sus clientes. Este modelo de responsabilidad compartida alivia parte de la carga operativa del cliente, ya que AWS opera, administra y controla los componentes desde el sistema operativo anfitrión y la capa de virtualización hasta la seguridad física de las instalaciones en las que opera el servicio. Para obtener más información sobre el modelo de responsabilidad compartida, consulte la documentación del modelo de responsabilidad compartida.

A medida que cambia su responsabilidad compartida en la nube, también cambian sus opciones de respuesta a los incidentes. Planificar y comprender estas compensaciones y adaptarlas a sus necesidades de gobierno es un paso crucial en la respuesta a los incidentes.

Además de la relación directa con la que tiene AWS, es posible que haya otras entidades que tengan responsabilidades en su modelo de responsabilidad particular. Por ejemplo, es posible que tengas unidades organizativas internas que asuman la responsabilidad de algunos aspectos de tus

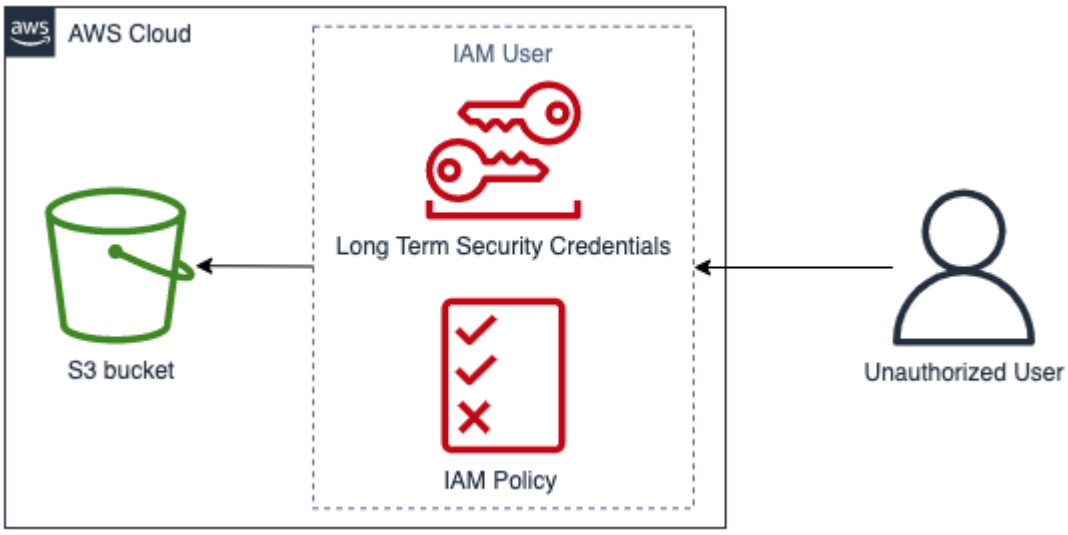
operaciones. Es posible que también tengas relaciones con otras partes que desarrollen, administren u operen parte de tu tecnología de nube.

Es sumamente importante crear y probar un plan de respuesta a incidentes adecuado y manuales adecuados que se adapten a su modelo operativo.

Diferencia #2: dominio de servicios en la nube

Debido a las diferencias en la responsabilidad de seguridad que existen entre los servicios en la nube, se introdujo un nuevo dominio para los incidentes de seguridad: el dominio del servicio, que se explicó anteriormente en la sección sobre el dominio de los incidentes. El dominio del servicio abarca la AWS cuenta del cliente, IAM los permisos, los metadatos de los recursos, la facturación y otras áreas. Este dominio es diferente para la respuesta a incidentes debido a la forma en que usted responde. La respuesta dentro del dominio del servicio generalmente se realiza mediante la revisión y emisión de API llamadas, en lugar de la respuesta tradicional basada en el host y la red. En el dominio del servicio, no interactuarás con el sistema operativo de un recurso afectado.

En el siguiente diagrama se muestra un ejemplo de un evento de seguridad en el dominio del servicio basado en un antipatrón arquitectónico. En este caso, un usuario no autorizado obtiene las credenciales de seguridad a largo plazo de un IAM usuario. El IAM usuario tiene una IAM política que le permite recuperar objetos de un bucket de Amazon Simple Storage Service (Amazon S3). Para responder a este evento de seguridad, utilizaría AWS APIs analizar AWS registros como los registros AWS CloudTrailde acceso a Amazon S3. También los utilizaría AWS APIs para contener el incidente y recuperarse de él.



Ejemplo de dominio de servicio

Diferencia #3: APIs para el aprovisionamiento de infraestructura

Otra diferencia proviene de la característica de la nube del autoservicio bajo demanda. Las principales instalaciones con las Nube de AWS que los clientes interactúan RESTful API a través de terminales públicos y privados disponibles en muchos lugares geográficos de todo el mundo. Los clientes pueden acceder a ellos APIs con AWS credenciales. A diferencia del control de acceso local, estas credenciales no están necesariamente vinculadas a una red o a un dominio de Microsoft Active Directory. En cambio, las credenciales se asocian a un IAM principal dentro de una AWS cuenta. Se puede acceder a estos API puntos de conexión desde fuera de la red corporativa, lo cual es importante tener en cuenta al responder a un incidente en el que las credenciales se utilizan fuera de la red o la zona geográfica en la que se espera.

Debido a su naturaleza API basada en datos AWS, una fuente de registro importante para responder a los eventos de seguridad es AWS CloudTrail la que permite hacer un seguimiento de las API llamadas de la administración realizadas en sus AWS cuentas y encontrar información sobre la ubicación de origen de las API llamadas.

Diferencia #4: La naturaleza dinámica de la nube

La nube es dinámica; le permite crear y eliminar recursos rápidamente. Con el escalado automático, los recursos se pueden aumentar y reducir en función del aumento del tráfico. Con una infraestructura de corta duración y cambios rápidos, es posible que un recurso que esté investigando ya no exista o se haya modificado. Para analizar los incidentes, será importante comprender la naturaleza efímera de AWS los recursos y saber cómo hacer un seguimiento de AWS su creación y eliminación. Puede utilizarlos AWS Configpara realizar un seguimiento del historial de configuración de sus AWS recursos.

Diferencia #5: acceso a los datos

El acceso a los datos también es diferente en la nube. No puedes conectarte a un servidor para recopilar los datos que necesitas para una investigación de seguridad. Los datos se recopilan por cable y mediante API llamadas. Tendrá que practicar y comprender cómo realizar la recopilación de datos a APIs fin de estar preparado para este cambio y verificar el almacenamiento adecuado para una recopilación y un acceso efectivos.

Diferencia #6: importancia de la automatización

Para que los clientes se den cuenta plenamente de los beneficios de la adopción de la nube, su estrategia operativa debe incluir la automatización. La infraestructura como código (IaC) es un patrón de entornos automatizados altamente eficientes en AWS los que los servicios se despliegan,

configuran, reconfiguran y destruyen mediante código facilitado por servicios de IaC nativos, como AWS CloudFormationsoluciones de terceros. Esto hace que la implementación de la respuesta a los incidentes sea altamente automatizada, lo que es deseable para evitar errores humanos, especialmente cuando se manejan pruebas. Si bien la automatización se usa en las instalaciones, es esencial y más simple en el. Nube de AWS

Abordar estas diferencias

Para abordar estas diferencias, siga los pasos que se describen en la siguiente sección para comprobar que su programa de respuesta a incidentes, tanto en lo que respecta a las personas, los procesos y la tecnología, esté bien preparado.

Preparación

Prepararse para un incidente es fundamental para ofrecer una respuesta oportuna y eficaz ante el incidente. La preparación se hace en tres dominios:

- Personas: preparar a su personal para un incidente de seguridad implica identificar a las partes interesadas pertinentes para la respuesta a los incidentes y capacitarlas en materia de respuesta a incidentes y tecnologías en la nube.
- Proceso: preparar los procesos para un incidente de seguridad implica documentar las arquitecturas, desarrollar planes exhaustivos de respuesta a los incidentes y crear guías para responder de manera coherente a los eventos de seguridad.
- Tecnología: preparar la tecnología para un incidente de seguridad implica configurar el acceso, agregar y monitorear 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.

Personas

Para responder a un evento de seguridad, es necesario identificar a las partes interesadas que apoyarían la respuesta a un evento de seguridad. Además, para una respuesta eficaz, es fundamental capacitarlos sobre AWS las tecnologías y su AWS entorno.

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 muchos lugares hay leyes locales que rigen lo que se debe y lo que no se debe hacer. Si bien puede parecer burocrático elaborar un diagrama responsable, responsable, consultado e informado (RACI) para sus planes de respuesta en materia de seguridad, hacerlo permite una comunicación rápida y directa y describe claramente a los líderes en las diferentes etapas del evento.

Durante un incidente, es fundamental incluir a los propietarios o desarrolladores de las aplicaciones y los recursos afectados, ya que son expertos en la materia (SMEs) 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 las aplicaciones oSMEs, por ejemplo, los administradores o ingenieros de la nube, tengan que actuar en situaciones en las que el entorno no sea familiar o sea complejo, o en las que los responsables de la respuesta no tengan acceso a él.

Por último, las relaciones de confianza pueden estar implicadas en la investigación o la respuesta, ya que pueden aportar conocimientos adicionales y un análisis valioso. Si no dispone de estas habilidades en su propio equipo, tal vez sea conveniente contratar a una persona externa para que le ayude.

Capacite al personal de respuesta a incidentes

Capacitar al personal de respuesta a incidentes sobre las tecnologías que utiliza su organización será crucial para que puedan responder adecuadamente a un incidente de seguridad. Las respuestas pueden prolongarse si los miembros de su personal no comprenden las tecnologías subyacentes. Además de los conceptos tradicionales de respuesta a incidentes, también es importante que comprendan AWS los servicios y su AWS entorno. Existen varios mecanismos tradicionales para formar al personal encargado de los incidentes, como la formación en línea y la formación presencial. También deberías considerar la posibilidad de organizar jornadas de juego o simulaciones como mecanismo de entrenamiento. Para obtener más información sobre cómo ejecutar simulaciones, consulta la the section called “Ejecute simulaciones periódicas” sección de este documento.

Comprenda Nube de AWS las tecnologías

Para reducir las dependencias y reducir el tiempo de respuesta, asegúrese de que sus equipos de seguridad y el personal de respuesta estén informados sobre los servicios en la nube y tengan la oportunidad de practicar de forma práctica con el entorno de nube específico que utilice su organización. Para que el personal de respuesta a incidentes sea eficaz, es importante comprender los AWS fundamentos IAM AWS Organizations, los servicios de AWS registro y supervisión y los servicios de seguridad. AWS

AWS ofrece talleres de seguridad en línea (consulte los talleres AWS de seguridad) en los que puede adquirir experiencias prácticas con los servicios de AWS seguridad y monitoreo. AWS también ofrece una serie de opciones de formación e itinerarios de aprendizaje a través de la formación digital, la formación presencial, los socios de AWS formación y las certificaciones. Para obtener más información, consulte AWS Capacitación y certificación.

Comprenda su AWS entorno

Además de entender AWS los servicios, sus casos de uso y cómo se integran entre sí, es igual de importante entender cómo se diseña realmente el AWS entorno de su organización y qué procesos operativos están implementados. A menudo, este tipo de conocimiento interno no está documentado y solo lo comprenden unos pocos expertos en el campo, lo que puede crear dependencias, dificultar la innovación y retrasar el tiempo de respuesta.

Para evitar estas dependencias y acelerar los tiempos de respuesta, los analistas de seguridad deben documentar, tener acceso a ellos y comprender el conocimiento interno del AWS entorno. Para comprender su presencia total en la nube, será necesaria la colaboración entre las partes interesadas en materia de seguridad pertinentes y los administradores de la nube. Parte de la preparación de los procesos para la respuesta a los incidentes incluye la documentación y la centralización de los diagramas de arquitectura, que se incluyen the section called “Documente y centralice los diagramas de arquitectura” más adelante en este documento técnico. Sin embargo, desde la perspectiva de las personas, es importante que sus analistas puedan acceder a los diagramas y los procesos operativos relacionados con su entorno y comprenderlos. AWS

Comprenda los equipos de AWS respuesta y el soporte

Support

Supportofrece una gama de planes que proporcionan acceso a las herramientas y la experiencia que respaldan el éxito y la salud operativa de sus AWS soluciones. Si necesita soporte técnico y

más recursos para planificar, implementar y optimizar su AWS entorno, puede seleccionar el plan de soporte que mejor se adapte a su caso de AWS uso.

Considere el Support Center del AWS Management Console (es necesario iniciar sesión) como el punto de contacto central para obtener asistencia en caso de problemas que afecten a sus AWS recursos. El acceso a Support está controlado porIAM. Para obtener más información sobre cómo obtener acceso a las funciones de AWS Support, consulte Cómo empezar con Support.

Además, si necesitas denunciar un abuso, ponte en contacto con el equipo de AWS confianza y seguridad.

AWS Equipo de respuesta a incidentes del cliente () CIRT

El equipo de respuesta a incidentes del AWS cliente (CIRT) es un AWS equipo global especializado y siempre disponible que brinda apoyo a los clientes durante los eventos de seguridad activa desde el punto de vista del cliente en el marco del modelo de responsabilidad AWS compartida.

Cuando lo AWS CIRT apoyen, recibirá asistencia para clasificar y recuperar un incidente de seguridad activo el día de hoy. AWS Le ayudarán a analizar la causa raíz mediante el uso de registros de AWS servicio y le ofrecerán recomendaciones para la recuperación. También le proporcionarán recomendaciones de seguridad y mejores prácticas para ayudarlo a evitar eventos de seguridad en el futuro.

AWS los clientes pueden contactarlos a AWS CIRT través de un caso de AWS soporte.

- Todos los clientes:
  1. Cuenta y facturación
  2. Servicio: Cuenta
  3. Categoría: Seguridad
  4. Gravedad: pregunta general

- Clientes con Support planes de desarrollador:
  1. Cuenta y facturación
  2. Servicio: Cuenta
  3. Categoría: Seguridad
  4. Gravedad: pregunta importante

- Clientes con Support planes empresariales:

1. Cuenta y facturación
2. Servicio: Cuenta
3. Categoría: Seguridad
4. Gravedad: pregunta urgente que afecta al negocio

- Clientes con Support planes empresariales:
  1. Cuenta y facturación
  2. Servicio: Cuenta
  3. Categoría: Seguridad
  4. Gravedad: cuestión crítica sobre el riesgo empresarial

- Clientes con suscripciones a AWS Security Incident Response: abran la consola de Security Incident Response en https://console.aws.amazon.com/security-ir/

DDoSsoporte de respuesta

AWS ofrece AWS Shield, que proporciona un servicio de protección gestionado y distribuido contra la denegación de servicio (DDoS) que protege las aplicaciones web que se ejecutan en ellas AWS. AWS Shield proporciona una detección permanente y mitigaciones automáticas integradas que pueden minimizar el tiempo de inactividad y la latencia de las aplicaciones, por lo que no es necesario recurrir Support a ellos para beneficiarse de la protección. DDoS Hay dos niveles AWS Shield: Shield Standard y Shield Advanced. Para obtener más información sobre las diferencias entre estos dos niveles, consulta la documentación sobre las funciones de Shield.

AWS Managed Services (AMS)

AWS Managed Services(AMS) proporciona una administración continua de su AWS infraestructura para que pueda centrarse en sus aplicaciones. Al implementar las mejores prácticas para mantener su infraestructura, AMS ayuda a reducir sus gastos operativos y sus riesgos. AMSautomatiza las actividades habituales, como las solicitudes de cambios, la supervisión, la administración de parches, la seguridad y los servicios de respaldo, y proporciona servicios de ciclo de vida completo para aprovisionar, ejecutar y dar soporte a su infraestructura.

AMSasume la responsabilidad de implementar un conjunto de controles de detección de seguridad y proporciona una primera línea de respuesta diaria a las alertas. Cuando se inicia una alerta, AMS sigue un conjunto estándar de guías automatizadas y manuales para verificar una respuesta

coherente. Estos manuales se comparten con AMS los clientes durante la incorporación para que puedan desarrollar y coordinar una respuesta con ellos. AMS

Proceso

Desarrollar procesos de respuesta a incidentes exhaustivos y claramente definidos es clave para un programa de respuesta a incidentes exitoso y escalable. Cuando se produce un incidente de seguridad, unos pasos y flujos de trabajo claros le ayudarán a responder de manera oportuna. Es posible que ya tenga un proceso de respuesta a incidentes existente. Independientemente de su estado actual, es importante actualizar, iterar y probar sus procesos de respuesta a incidentes con regularidad.

Desarrolle y pruebe un plan de respuesta a incidentes

El primer documento que se debe desarrollar para la respuesta a los incidentes es el plan de respuesta a los incidentes. El plan de respuesta a incidentes está diseñado para ser la base de su programa y estrategia de respuesta a incidentes. Un plan de respuesta a incidentes es un documento de alto nivel que normalmente incluye estas 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 en la respuesta a los incidentes y detalla sus funciones cuando se produce un incidente
- Un plan de comunicación: detalla la información de contacto y la forma en que se comunicará durante un incidente

  Se recomienda tener la out-of-band comunicación como respaldo para la comunicación de incidentes. Un ejemplo de aplicación que proporciona un canal de out-of-band comunicación seguro es AWS Wickr.
- Fases de la respuesta a los incidentes y acciones a tomar: enumera las fases de la respuesta a los incidentes (por ejemplo, detectar, analizar, erradicar, contener y recuperar), incluidas las acciones de alto nivel que se deben tomar dentro de esas fases
- Definiciones de gravedad y priorización de los incidentes: detalla cómo clasificar la gravedad de un incidente, cómo priorizarlo y, luego, 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. Deberá crear un plan de respuesta a incidentes que funcione mejor para su organización.

Documente y centralice los diagramas de arquitectura

Para responder de forma rápida y precisa a un incidente de seguridad, debe comprender la arquitectura de sus sistemas y redes. Comprender estos patrones internos no solo es importante para responder a los incidentes, sino también para verificar la coherencia entre las aplicaciones con las que se diseñan los patrones, de acuerdo con las mejores prácticas. También debe comprobar que esta documentación esté actualizada y se actualice periódicamente de acuerdo con los nuevos patrones de arquitectura. Debe desarrollar documentación y repositorios internos que detallen elementos como:

- AWS estructura contable: necesita saber:
  - ¿Cuántas AWS cuentas tienes?
  - ¿Cómo están organizadas esas AWS cuentas?
  - ¿Quiénes son los propietarios comerciales de las AWS cuentas?
  - ¿Utilizas las políticas de control de servicios (SCPs)? Si es así, ¿qué barreras organizativas se implementan mediante el uso? SCPs
  - ¿Limitan las regiones y los servicios que se pueden usar?
  - ¿Qué diferencias existen entre las unidades de negocio y los entornos (dev/test/prod)?
- AWS patrones de servicio
  - ¿Qué AWS servicios utilizas?
  - ¿Cuáles son los AWS servicios más utilizados?
- Patrones de arquitectura
  - ¿Qué arquitecturas de nube utiliza?
- AWS patrones de autenticación
  - ¿Cómo se autentican normalmente sus desarrolladores? AWS
  - ¿Utilizas IAM roles o usuarios (o ambos)? ¿Su autenticación está AWS conectada a un proveedor de identidad (IdP)?
  - ¿Cómo se asigna un IAM rol o un usuario a un empleado o un sistema?
  - ¿Cómo se revoca el acceso cuando alguien ya no está autorizado?
- AWS patrones de autorización

  - ¿Qué IAM políticas utilizan sus desarrolladores?
  - ¿Utilizas políticas basadas en recursos?
- Registro y monitoreo
  - ¿Qué fuentes de registro utiliza y dónde se almacenan?
  - ¿Agregan AWS CloudTrail registros? Si es así, ¿dónde se almacenan?
  - ¿Cómo se consultan CloudTrail los registros?
  - ¿Tienes Amazon GuardDuty activado?
  - ¿Cómo se accede a GuardDuty los resultados (por ejemplo, a la consola, al sistema de venta de entradasSIEM)?
  - ¿Los hallazgos o los eventos se agrupan en un? SIEM
  - ¿Los tickets se crean automáticamente?
  - ¿Qué herramientas se utilizan para analizar los registros para una investigación?
- Topología de red
  - ¿Cómo se organizan física o lógicamente los dispositivos, los puntos finales y las conexiones de la red?
  - ¿Cómo se conecta su red? AWS
  - ¿Cómo se filtra el tráfico de red entre entornos?
- Infraestructura externa
  - ¿Cómo se implementan las aplicaciones orientadas al exterior?
  - ¿Qué AWS recursos son de acceso público?
  - ¿Qué AWS cuentas contienen una infraestructura orientada al exterior?
  - ¿Qué DDoS es lo que existe? ¿Existe un filtrado externo?

La documentación de los diagramas y procesos técnicos internos facilita el trabajo del analista de respuesta a incidentes, ya que le ayuda a obtener rápidamente los conocimientos institucionales necesarios para responder a un incidente de seguridad. La documentación exhaustiva de los procesos técnicos internos no solo simplifica las investigaciones de seguridad, sino que también permite racionalizar y evaluar los procesos.

Desarrolle manuales de respuesta a incidentes

Una parte esencial de la preparación de los procesos de respuesta a incidentes consiste en desarrollar manuales de estrategias. Los manuales de estrategias de respuesta a incidentes ofrecen

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.

¿Para qué crear manuales de estrategias

Deben crearse guías estratégicas para escenarios de incidentes, como, por ejemplo:

- Incidentes esperados: se deben crear manuales de estrategias para los incidentes que anticipe. Esto puede incluir amenazas como la denegación de servicio (DoS), el ransomware y las amenazas de las credenciales.
- Hallazgos o alertas de seguridad conocidos: se deben crear manuales para sus hallazgos y alertas de seguridad conocidos, como GuardDuty los hallazgos. Es posible que reciba un GuardDuty hallazgo y piense: «¿Y ahora qué?» Para evitar que se maneje mal un GuardDuty hallazgo o se lo ignore, cree un manual de estrategias para cada posible hallazgo. GuardDuty En la documentación se pueden encontrar algunos detalles y directrices sobre la remediación. GuardDuty Vale la pena señalar que no GuardDuty está activado de forma predeterminada y conlleva un coste. GuardDuty Puede encontrar más información al respecto en el Apéndice A: Definiciones de capacidad en la nube -the section called “Visibilidad y alertas”.

¿Qué incluir en los manuales

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.

Algunos de los elementos que deben incluirse en un manual de estrategias son los siguientes:

- Descripción general del manual: ¿Qué escenario de riesgo o incidente aborda este manual? ¿Cuál es el objetivo del manual de estrategias?
- Requisitos previos: ¿Qué registros y mecanismos de detección se requieren en este escenario de incidente? ¿Cuál es la notificación esperada?
- Información sobre las partes interesadas: ¿quiénes participan y cuál es su información de contacto? ¿Cuáles son las responsabilidades de cada una de las partes interesadas?
- Pasos de respuesta: en todas las fases de la 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?
  - Detectar: ¿cómo se detectará el incidente?
  - Analizar: ¿cómo se determinará el alcance del impacto?

  - Contener: ¿cómo se aislará el incidente para limitar su alcance?
  - Erradicar: ¿cómo se eliminará la amenaza del medio ambiente?
  - Recuperación: ¿cómo se volverá a poner en producción el sistema o recurso afectado?
- Resultados esperados: una vez ejecutadas las consultas y el código, ¿cuál es el resultado esperado del manual de estrategias?

Para comprobar que la información de cada manual es coherente, puede resultar útil crear una plantilla de manual de estrategias para utilizarla en los demás manuales de estrategias de seguridad. Algunos de los elementos enumerados anteriormente, como la información de las partes interesadas, se pueden compartir en varios manuales de estrategias. Si ese es el caso, puede crear una documentación centralizada para esa información y consultarla en el manual y, a continuación, enumerar las diferencias explícitas en el manual. Esto evitará que tenga que actualizar la misma información en todos sus manuales de estrategias individuales. Al crear una plantilla e identificar la información común o compartida en los manuales de estrategias, puede simplificar y acelerar el desarrollo de los manuales de estrategias. Por último, es probable que sus manuales de estrategias evolucionen con el tiempo; una vez que haya confirmado que los pasos son coherentes, estos son los requisitos para la automatización.

Ejemplos de manuales de estrategias

Se pueden encontrar varios ejemplos de manuales de estrategias en el Apéndice B en. the section called “Recursos del manual” Los ejemplos que aparecen aquí se pueden usar para guiarlo sobre qué libros de jugadas crear y qué incluir en sus libros de jugadas. Sin embargo, es importante que elabore manuales que incorporen los riesgos más relevantes para su negocio. Debe comprobar que los pasos y los flujos de trabajo de sus manuales incluyen sus tecnologías y procesos.

Realice simulaciones periódicas

Las organizaciones crecen y evolucionan con el tiempo, al igual que el panorama de amenazas. Por eso, es importante revisar continuamente sus capacidades de respuesta a incidentes. Las simulaciones son un método que se puede utilizar para realizar esta evaluación. Las simulaciones utilizan escenarios de eventos de seguridad del mundo real diseñados para imitar las tácticas, técnicas y procedimientos de un actor de amenazas (TTPs) y permiten a una organización ejercitar y evaluar sus capacidades de respuesta a incidentes respondiendo a estos simulacros de cibereventos tal como podrían ocurrir en la realidad.

Las simulaciones ofrecen diversas ventajas, entre las que se incluyen las siguientes:

- 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.

Tipos de simulaciones

Hay tres tipos principales de simulaciones:

- Ejercicios de sobremesa: el enfoque de las simulaciones de mesa consiste estrictamente en una sesión basada en el debate en la que participan las distintas partes interesadas en la respuesta a los incidentes para que practiquen sus funciones y responsabilidades y utilicen las herramientas de comunicación y los manuales de estrategias establecidos. Por lo general, la facilitación del ejercicio se puede realizar en un día completo en un lugar virtual, físico o en una combinación de ambos. Debido a su naturaleza basada en el debate, el ejercicio de mesa se centra en los procesos, las personas y la colaboración. La tecnología es una parte integral del debate; sin embargo, el uso real de las herramientas o guiones de respuesta a incidentes generalmente no forma parte del ejercicio de mesa.
- Ejercicios del equipo morado: los ejercicios del equipo morado aumentan el nivel de colaboración entre el personal de respuesta a los incidentes (equipo azul) y los actores de amenazas simuladas (equipo rojo). El equipo azul suele estar compuesto por miembros del Centro de Operaciones de Seguridad (SOC), pero también puede incluir a otras partes interesadas que podrían participar durante un ciberevento real. Por lo general, el Equipo Rojo está compuesto por un equipo de pruebas de penetración o por partes interesadas clave que están capacitadas en seguridad ofensiva. El equipo rojo trabaja en colaboración con los facilitadores del ejercicio a la hora de diseñar un escenario para que sea preciso y factible. Durante los ejercicios del Purple Team, la atención se centra principalmente en los mecanismos de detección, las herramientas y los procedimientos operativos estándar (SOPs) que respaldan las iniciativas de respuesta a los incidentes.
- Ejercicios del equipo rojo: durante un ejercicio del equipo rojo, el infractor (equipo rojo) lleva a cabo una simulación para lograr un objetivo determinado o un conjunto de objetivos con un alcance predeterminado. Los defensores (equipo azul) no conocerán necesariamente el alcance y la duración del ejercicio, lo que proporciona una evaluación más realista de cómo responderían ante

un incidente real. Como los ejercicios del Equipo Rojo pueden ser pruebas invasivas, debes tener cuidado e implementar controles para verificar que el ejercicio no cause daños reales a tu entorno.

> **Note**
>
> AWS exige que los clientes revisen la política de pruebas de penetración disponible en el sitio web de pruebas de penetración antes de realizar los ejercicios de Purple Team o Red Team.

En la tabla 1 se resumen algunas de las principales diferencias entre estos tipos de simulaciones. Es importante tener en cuenta que, por lo general, las definiciones se consideran definiciones vagas y se pueden personalizar para adaptarlas a las necesidades de la organización.

Tabla 1: Tipos de simulaciones

	Ejercicio de mesa	Ejercicio Purple Team	Ejercicio Red Team
Resumen	Ejercicios en papel que se centran en un escenario de incidente de seguridad específico. Estos pueden ser de alto nivel o técnicos, y están impulsados por una serie de inyecciones de papel.	Una oferta más realista en comparación con los ejercicios de mesa. Durante los ejercicios de Purple Team, los facilitadores trabajan en colaboración con los participantes para aumentar su participación en el ejercicio y ofrecen capacitación cuando es necesario.	Por lo general, se trata de una oferta de simulación más avanzada. Por lo general, hay un alto nivel de ocultación, por lo que es posible que los participantes no conozcan todos los detalles del ejercicio.
Recursos necesarios	Se requieren recursos técnicos limitados	Se requieren diversas partes interesadas y un alto nivel de recursos técnicos	Se necesitan diversas partes interesadas y un alto nivel de recursos técnicos
Complejidad	Bajo	Medio	Alto

Considere la posibilidad de llevar a cabo simulaciones de ataques cibernéticos con regularidad. Cada tipo de ejercicio puede ofrecer ventajas únicas a los participantes y a la organización en su conjunto, por lo que puede optar por empezar con tipos de simulación menos complejos (como los ejercicios de mesa) y pasar a tipos de simulación más complejos (ejercicios del 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 no elijan realizar los ejercicios de Red Team debido a su complejidad y coste.

Ciclo vital del ejercicio

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

1. Defina los elementos básicos del ejercicio: defina el escenario de simulación y los objetivos de la simulación. Ambos deben contar con la aceptación de los directivos.
2. Identifique a las partes interesadas clave: como mínimo, un ejercicio necesita facilitadores y participantes del ejercicio. En función 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 sea necesario redefinir el escenario a medida que se va creando si elementos específicos no son factibles. Se espera que, al final de esta etapa, haya un escenario definitivo.
4. Facilitar la simulación: el tipo de simulación determina la facilitación utilizada (escenario basado en papel en comparación con un escenario simulado altamente 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 salieron bien, las que podrían mejorarse y las posibles brechas. AARDeberían medir la eficacia de la simulación, así como la respuesta del equipo al evento simulado, de modo que se pueda hacer un seguimiento del progreso a lo largo del tiempo con futuras simulaciones.

Tecnología

Si desarrolla e implementa las tecnologías adecuadas antes de un incidente de seguridad, su personal de respuesta a incidentes podrá investigar, comprender el alcance y tomar medidas de manera oportuna.

Desarrolle AWS una estructura contable

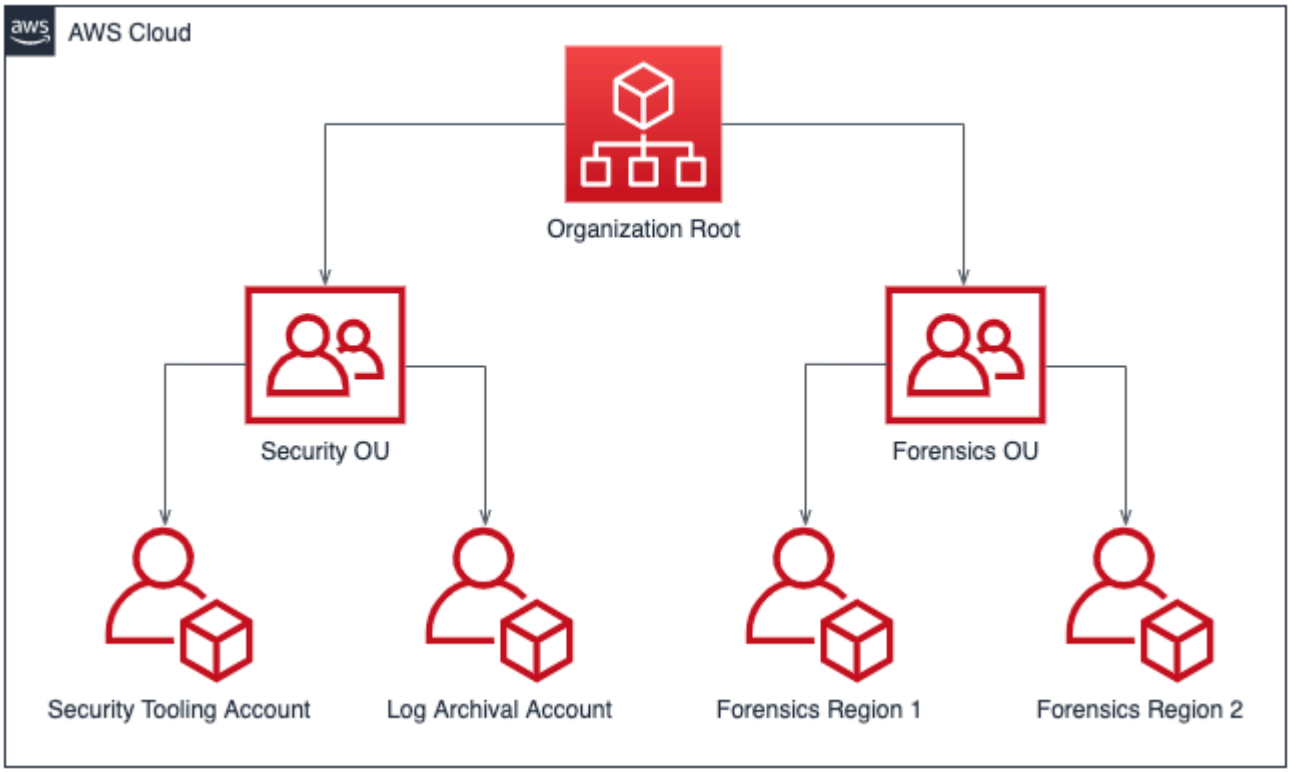
AWS Organizationsayuda a administrar y gobernar un AWS entorno de forma centralizada a medida que crece y escala AWS los recursos. Una AWS organización consolida sus AWS cuentas para que pueda administrarlas como una sola unidad. Puedes usar las unidades organizativas (OUs) para agrupar las cuentas y administrarlas como una sola unidad.

Para la respuesta a incidentes, resulta útil contar con una estructura AWS contable que respalde las funciones de respuesta a incidentes, que incluya una unidad organizativa de seguridad y una unidad organizativa forense. Dentro de la unidad organizativa de seguridad, debe tener cuentas para:

- Archivo de registros: agregue los registros en una cuenta de archivo de registros. AWS
- Herramientas de seguridad: centralice los servicios de seguridad en una cuenta de herramientas de seguridad. AWS 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. Como ejemplo de un enfoque de cuentas por región, si solo opera en EE. UU. Este (Virginia del Norte) (us-east-1) y EE. UU. oeste (Oregón) (us-west-2), tendrá dos cuentas en la OU forense: una para us-east-1 y otra para us-west-2. 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 contable por región para la respuesta a incidentes

Desarrollo e implementación de una estrategia de etiquetado

Puede resultar difícil obtener información contextual sobre el caso de uso empresarial y las partes interesadas internas relevantes relacionadas con un AWS recurso. Una forma de hacerlo es mediante etiquetas, que asignan metadatos a los AWS recursos y constan 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.

Tener una estrategia de etiquetado coherente puede acelerar los tiempos de respuesta, ya que permite identificar y discernir rápidamente la información contextual sobre un recurso. AWS Las etiquetas también pueden servir como un mecanismo para iniciar automatizaciones de respuesta. Para obtener más información sobre qué etiquetar, consulte la documentación sobre el etiquetado AWS de recursos. Primero tendrá que definir las etiquetas que desea implementar en toda la organización. Después, implementará y hará cumplir la estrategia de etiquetado. Los detalles sobre la implementación y el cumplimiento se encuentran en el AWS blog Implemente una estrategia de etiquetado de AWS recursos utilizando las políticas de AWS etiquetado y las políticas de control de servicios () SCPs.

Actualice la información AWS de contacto de la cuenta

Para cada una de tus AWS cuentas, es importante contar up-to-date con información de contacto precisa para que las partes interesadas correctas reciban notificaciones importantes AWS sobre temas como la seguridad, la facturación y las operaciones. Para cada AWS cuenta, tienes un contacto principal y contactos alternativos para la seguridad, la facturación y las operaciones. Las diferencias entre estos contactos se encuentran en la Guía de referencia de administración de AWS cuentas.

Para obtener más información sobre la administración de contactos alternativos, consulta la AWS documentación sobre cómo agregar, cambiar o eliminar contactos alternativos. Se recomienda utilizar una lista de distribución de correo electrónico si tu equipo gestiona la facturación, las operaciones y los problemas relacionados con la seguridad. Una lista de distribución de correo electrónico elimina las dependencias de una persona, lo que puede provocar bloqueos si se encuentra fuera de la oficina o deja la empresa. También debes comprobar que el correo electrónico y la información de contacto de la cuenta, incluido el número de teléfono, estén bien protegidos para evitar que se restablezcan las contraseñas de las cuentas raíz y los restablecimientos de la autenticación multifactorial (). MFA

Para los clientes que AWS Organizations lo utilicen, los administradores de la organización pueden gestionar de forma centralizada los contactos alternativos de las cuentas de los miembros mediante la cuenta de administración o una cuenta de administrador delegado sin necesidad de credenciales para cada cuenta. AWS También tendrás que comprobar que las cuentas recién creadas tengan información de contacto precisa. Consulta la sección Actualizar automáticamente contactos alternativos para ver la entrada de Cuentas de AWS blog recién creada.

Prepara el acceso a Cuentas de AWS

Durante un incidente, sus equipos de respuesta a incidentes deben tener acceso a los entornos y recursos involucrados en el incidente. Asegúrese de que sus equipos tengan el acceso adecuado para desempeñar sus funciones antes de que se produzca un suceso. Para ello, debes saber qué nivel de acceso necesitan los miembros de tu equipo (por ejemplo, qué tipo de medidas es probable que tomen) y debes proporcionar de antemano el acceso con privilegios mínimos.

Para implementar y aprovisionar este acceso, debe identificar y analizar la estrategia de AWS cuentas y la estrategia de identidad en la nube con los arquitectos de nube de su organización para comprender qué métodos de autenticación y autorización están configurados. Debido a la naturaleza privilegiada de estas credenciales, debería considerar la posibilidad de utilizar flujos de aprobación o recuperar las credenciales de un almacén o caja fuerte como parte de su implementación. Tras la

implementación, debes documentar y probar el acceso de los miembros del equipo mucho antes de que se produzca un evento para asegurarte de que pueden responder sin demoras.

Por último, los usuarios que se crean específicamente para responder a un incidente de seguridad suelen tener privilegios para proporcionar un acceso suficiente. Por lo tanto, el uso de estas credenciales debe restringirse, supervisarse y no utilizarse para las actividades diarias.

Comprenda el panorama de amenazas

Desarrolle modelos de amenazas

Al desarrollar modelos de amenazas, las organizaciones pueden identificar las amenazas y las mitigaciones antes que un usuario no autorizado. Existen varias estrategias y enfoques para el modelado de amenazas; consulte la entrada del blog Cómo abordar el modelado de amenazas. Para la respuesta a los incidentes, un modelo de amenazas puede ayudar a identificar los vectores de ataque que un actor de amenazas podría haber utilizado durante un incidente. Comprender de qué se está defendiendo será crucial para poder responder de manera oportuna. También puede utilizar una AWS Partner para modelar las amenazas. Para buscar un AWS socio, usa el AWS Partner Network.

Integre y utilice la inteligencia sobre ciberamenazas

La inteligencia sobre ciberamenazas son los datos y el análisis de la intención, la oportunidad y la capacidad de un actor de amenazas. Obtener y utilizar la inteligencia sobre amenazas es útil para detectar un incidente de forma temprana y comprender mejor el comportamiento de los actores de amenazas. La inteligencia sobre ciberamenazas incluye indicadores estáticos, como las direcciones IP o los hashes de archivos de malware. También incluye información de alto nivel, como patrones de comportamiento e intenciones. Puede recopilar información sobre amenazas de varios proveedores de ciberseguridad y de repositorios de código abierto.

Para integrar y maximizar la inteligencia de amenazas para su AWS entorno, puede utilizar algunas out-of-the-box capacidades e integrar sus propias listas de inteligencia de amenazas. Amazon GuardDuty utiliza fuentes de inteligencia de amenazas AWS internas y de terceros. Otros AWS servicios, como el DNS firewall y AWS WAF las reglas, también reciben información de un «grupo avanzado de inteligencia sobre amenazas AWS». Algunos de GuardDuty los hallazgos están relacionados con el Marco MITRE ATT &CK, que proporciona información sobre las observaciones del mundo real sobre las tácticas y técnicas de los adversarios.

Selección y configuración de registros de análisis y alertas

Durante una investigación de seguridad, necesitará poder revisar los registros correspondientes para registrar y comprender todo el alcance y la cronología del incidente. También necesita los registros para generar alertas que indican que se han producido determinadas acciones de interés. Es fundamental seleccionar, habilitar, almacenar y configurar mecanismos de consulta y recuperación, así como de alerta. En esta sección se analiza cada una de estas acciones. Para obtener más información, consulte la entrada del AWS blog sobre el registro de estrategias para la respuesta a incidentes de seguridad.

Seleccione y habilite las fuentes de registro

Antes de iniciar una investigación de seguridad, debes capturar los registros relevantes para reconstruir retroactivamente la actividad de una AWS cuenta. Seleccione y habilite las fuentes de registro relevantes para las cargas de trabajo de sus AWS cuentas.

AWS CloudTrail es un servicio de registro que rastrea las API llamadas realizadas en comparación con la actividad del AWS servicio de captura de AWS cuentas. Está habilitado de forma predeterminada y permite retener durante 90 días los eventos de administración, que se pueden recuperar a través CloudTrail del historial de eventos utilizando AWS Management Console AWS CLI, el o un AWS SDK. Para prolongar la retención y la visibilidad de los eventos de datos, debe crear una CloudTrail ruta y asociarla a un bucket de Amazon S3 y, opcionalmente, a un grupo de CloudWatch registros. Como alternativa, puede crear un CloudTrail lago, que retenga CloudTrail los registros durante un máximo de siete años y proporcione un servicio de consultas SQL basado en ellos.

AWS recomienda a los clientes que utilicen una red de VPC activación del tráfico y DNS los registros mediante registros de consultas de resolución de VPCFlow Logs y Amazon Route 53, respectivamente, y que los transmitan a un bucket de Amazon S3 o a un CloudWatch grupo de registros. Puede crear un registro de VPC flujo para una interfazVPC, una subred o una interfaz de red. En el caso de los registros de VPC flujo, puede seleccionar cómo y dónde habilitar los registros de flujo para reducir los costos.

AWS CloudTrail Los registros, los registros de VPC flujo y los registros de consultas de resolución de Route 53 son el conjunto básico de registros para respaldar las investigaciones de seguridad. AWS

AWS los servicios pueden generar registros no capturados por la trifecta de registros básica, como los registros, registros de AWS Config grabadores de Elastic Load Balancing, GuardDuty hallazgos de Amazon, registros de auditoría de Amazon Elastic Kubernetes Service EKS (Amazon) y registros

de aplicaciones EC2 y sistemas operativos de instancias de Amazon. AWS WAF Consulte la lista completa the section called “Apéndice A: Definiciones de capacidad en la nube” de opciones de registro y monitoreo.

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 y el costo. Cuando habilites los registros de AWS servicio, proporciona una instalación de almacenamiento; normalmente, un bucket o grupo de CloudWatch registros de Amazon S3.

Un bucket de Amazon S3 proporciona un almacenamiento duradero y rentable con una política de ciclo de vida opcional. Los registros almacenados en los buckets de Amazon S3 se pueden consultar de forma nativa mediante servicios como Amazon Athena. Un grupo de CloudWatch registros proporciona un almacenamiento duradero y una función de consulta integrada a través de Logs Insights. CloudWatch

Identifique la retención de registros adecuada

Cuando utilice un depósito o un grupo de CloudWatch registros de S3 para almacenar registros, debe establecer ciclos de vida adecuados para cada fuente de registros a fin de optimizar los costes de almacenamiento y recuperación. Por lo general, los clientes disponen de registros de entre 3 y 12 meses disponibles para consultarlos, con una 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.

Seleccione e implemente mecanismos de consulta de registros

En AWS, los principales servicios que puede utilizar para consultar CloudWatch registros son Logs Insights para los datos almacenados en grupos de CloudWatch registros, y Amazon Athena y Amazon OpenSearch Service para los datos almacenados en Amazon S3. También puede utilizar herramientas de consulta de terceros, como la gestión 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 con los requisitos operativos, empresariales y de seguridad, y que sea accesible y fácil de mantener 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 que los clientes dispongan

de varias herramientas de consulta debido a limitaciones técnicas o de coste. Por ejemplo, los clientes pueden utilizar SIEM a un tercero para realizar consultas de los últimos 90 días de datos y utilizar Athena para realizar consultas más allá de los 90 días debido al coste de ingesta de registros que supone un. SIEM Independientemente de la implementación, compruebe que su enfoque minimice la cantidad de herramientas necesarias para maximizar la eficiencia operativa, especialmente durante la investigación de un incidente de seguridad.

Utilice registros para emitir alertas

AWS proporciona alertas de forma nativa a través de servicios de seguridad, como Amazon GuardDuty AWS Security Hub, y. AWS Config También puede utilizar motores de generación de alertas personalizados para las alertas de seguridad que no estén cubiertas por estos servicios o para alertas específicas relevantes para su entorno. La creación de estas alertas y detecciones se describe en la sección denominada the section called “Detección” en este documento.

Desarrolle capacidades forenses

Antes de que se produzca un incidente de seguridad, considere la posibilidad de desarrollar capacidades forenses que lo ayuden a investigar los eventos de seguridad. La Guía para integrar las técnicas forenses en la respuesta a incidentes NIST proporciona dicha orientación.

Análisis forense sobre AWS

Los conceptos de la ciencia forense local tradicional se aplican a. AWS Las estrategias del entorno de investigación forense de la entrada del Nube de AWS blog proporcionan información clave para empezar a migrar sus conocimientos forenses. AWS

Una vez que haya configurado su entorno y su estructura AWS contable para la ciencia forense, querrá definir las tecnologías necesarias para aplicar de forma eficaz metodologías sólidas desde el punto de vista forense en las cuatro fases:

- Recopilación: recopile AWS los registros relevantes AWS CloudTrail, AWS Config como los registros de VPC flujo y los registros a nivel de host. Recopile instantáneas, copias de seguridad y archivos de memoria de los recursos afectados. AWS
- Examen: examine los datos recopilados extrayendo y evaluando la información relevante.
- Análisis: analice los datos recopilados para comprender el incidente y sacar conclusiones a partir de él.
- Informes: presente la información resultante de la fase de análisis.

Captura de copias de seguridad e instantáneas

Crear copias de seguridad de los principales sistemas y bases de datos es fundamental para poder recuperarse de un incidente de seguridad y para fines forenses. Con las copias de seguridad, puede restaurar los sistemas a su estado seguro anterior. Sí AWS, puede tomar instantáneas de varios recursos. Las instantáneas le proporcionan point-in-time copias de seguridad de esos recursos. Hay muchos servicios de AWS que pueden ayudarle con la copia de seguridad y la recuperación. Consulte la Guía prescriptiva de respaldo y recuperación para obtener detalles sobre estos servicios y enfoques de respaldo y recuperación. Para obtener más información, consulte la entrada del blog sobre cómo usar copias de seguridad para recuperarse de incidentes de seguridad.

Es esencial que las copias de seguridad estén bien protegidas, especialmente en ciertas situaciones, como el ransomware. Consulte las 10 mejores prácticas de seguridad para proteger las copias de seguridad en la entrada del AWS blog para obtener orientación sobre cómo proteger las copias de seguridad. Además de proteger las copias de seguridad, debe probar periódicamente los procesos de copia de seguridad y restauración para comprobar que la tecnología y los procesos que tiene implementados funcionan según lo previsto.

Automatización de la ciencia forense en AWS

Durante un incidente de seguridad, su equipo de respuesta a incidentes debe poder recopilar y analizar pruebas rápidamente y, al mismo tiempo, mantener la precisión durante el período de tiempo que rodeó el evento. Para el equipo de respuesta a incidentes, recopilar manualmente las pruebas pertinentes en un entorno de nube supone un desafío y lleva mucho tiempo, especialmente en un gran número de instancias y cuentas. Además, la recopilación manual puede ser más propensa a errores humanos. Por estas razones, los clientes deben desarrollar e implementar la automatización para el análisis forense.

AWS ofrece una serie de recursos de automatización para la ciencia forense, que se resumen en el apéndice siguiente. the section called “Recursos forenses” 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.

Resumen de los elementos de preparación

La preparación minuciosa para responder a los eventos de seguridad es fundamental para una respuesta oportuna y eficaz a los incidentes. La preparación de la respuesta a los incidentes implica a las personas, los procesos y la tecnología. Estos tres dominios son igualmente importantes para

la preparación. Debe preparar y desarrollar su programa de respuesta a incidentes en los tres dominios.

En la tabla 2 se resumen los elementos de preparación detallados en esta sección.

Tabla 2: Elementos de preparación para la respuesta a incidentes

Dominio	Elemento de preparación	Elementos de acción
Personas	Defina las funciones y responsabilidades.	• Identifique a las partes interesadas relevantes en la respuesta a incidentes. • Desarrolle un gráfico responsable, responsab le, informado y consultado (RACI) para un incidente.
¿Personas	Capacite al personal de respuesta a incidentes AWS.	• Capacite a las partes interesadas en la respuesta a incidentes sobre AWS las bases. • Capacite a las partes interesadas en la respuesta a incidentes sobre los servicios de AWS seguridad y monitoreo. • Capacite a las partes interesadas en la respuesta a incidentes sobre su AWS entorno y su arquitectura.
Personas	Comprenda las opciones de AWS soporte.	• Comprenda las diferenci as entre el AWS soporte, el equipo de respuesta a incidentes del cliente (CIRT), el equipo de DDoS respuesta (DRT) yAMS.

Dominio	Elemento de preparación	Elementos de acción
		• Comprenda la ruta de clasificación y escalamie nto para comunicarse CIRT durante un evento de seguridad activa, si es necesario.
Proceso	Desarrolle un plan de respuesta a incidentes.	• Cree un documento de alto nivel que defina su programa y estrategia de respuesta a incidentes. • Incluya un plan de comunicaciónRACI, definiciones de incidentes y fases de la respuesta a los incidentes en el plan de respuesta a incidentes.
Proceso	Documente y centralice los diagramas de arquitectura.	• Documente los detalles sobre cómo está configura do su AWS entorno en función de la estructura de la cuenta, los usos de los servicios, IAM los patrones y otras funciones principales de su AWS configuración. • Desarrolle diagramas de arquitectura de sus arquitect uras de nube.

Dominio	Elemento de preparación	Elementos de acción
Proceso	Desarrolle manuales de respuesta a incidentes.	• Cree una plantilla para la estructura de sus manuales de estrategias. • Cree manuales de estrategias para los eventos de seguridad esperados. • Cree manuales para las alertas de seguridad conocidas, como GuardDuty los hallazgos.
Proceso	Ejecute simulaciones periódicas.	• Desarrolle una cadencia regular para ejecutar simulaciones de incidentes. • Utilice los resultados y las lecciones aprendidas para repetir su programa de respuesta a incidentes.
Tecnología	Desarrolle una estructura AWS contable.	• Planifique una estructura contable para separar las cargas de trabajo por AWS cuentas. • Cree una unidad organizativa de seguridad con una cuenta de almacenamiento de registros y herramientas de seguridad. • Cree una unidad organizativa forense con cuentas forenses para cada región en la que opere.

Dominio	Elemento de preparación	Elementos de acción
Tecnología	Desarrolle e implemente una estrategia de etiquetado que ayude a los socorristas a identificar la propiedad y el contexto de los hallazgos.	• Planifique una estrategi a de etiquetado y qué etiquetas quiere asociar a sus recursos. AWS • Implemente y aplique la estrategia de etiquetado.
Tecnología	Actualice la información de contacto de la AWS cuenta.	• Comprueba que AWS las cuentas incluyan la información de contacto en la lista. • Cree listas de distribución de correo electrónico para la información de contacto a fin de eliminar los puntos únicos de error. • Proteja las cuentas de correo electrónico asociadas a la información de la AWS cuenta.
Tecnología	Prepare el acceso a AWS las cuentas.	• Defina qué acceso necesitarán los servicios de respuesta a incidentes para responder a un incidente. • Implemente, pruebe y supervise el acceso.
Tecnología	Comprenda el panorama de amenazas.	• Desarrolle modelos de amenazas para su entorno y sus aplicaciones. • Integre y utilice la inteligen cia sobre ciberamenazas.

Dominio	Elemento de preparación	Elementos de acción
Tecnología	Seleccione y configure los registros.	• Identifique y habilite los registros para las investiga ciones. • Seleccione el almacenam iento de registros. • Identifique e implemente la retención de registros. • Desarrolle un mecanismo para recuperar y consultar registros y artefactos. • Utilice los registros para emitir alertas.
Tecnología	Desarrolle capacidades forenses.	• Identifique los artefactos necesarios para la recolecci ón forense. • Capture y proteja las copias de seguridad de los sistemas clave. • Defina los mecanismos para el análisis de los registros y artefactos identificados. • Implemente la automatiz ación para el análisis forense.

Se recomienda un enfoque iterativo para la preparación de la respuesta a los incidentes. Todos estos elementos de preparación no se pueden realizar de la noche a la mañana; debe crear un plan para empezar poco a poco y mejorar continuamente sus capacidades de respuesta a los incidentes a lo largo del tiempo.

Operaciones

Las operaciones son el núcleo de la respuesta ante los incidentes. Aquí es donde se llevan a cabo las acciones de respuesta y reparación de los incidentes de seguridad. Las operaciones incluyen las cinco fases siguientes: detección, análisis, contención, erradicación y recuperación. Las descripciones de estas fases y los objetivos se encuentran en la tabla 3.

Tabla 3: Fases de operaciones

Fase	Objetivo
Detección	Identifique un posible evento de seguridad.
Análisis	Determine si un incidente de seguridad es un incidente y evalúe el alcance del incidente.
Contención	Minimice y limite el alcance del evento de seguridad.
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 verificar 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.

Detección

Una alerta es el componente principal de la fase de detección. Genera una notificación para iniciar el proceso de respuesta al incidente en función de la actividad de la AWS cuenta que sea de interés.

La precisión de las alertas es un desafío; no siempre es posible determinar con total certeza si se ha producido un incidente, si está en curso o si ocurrirá en el futuro. Estas son algunas de las razones:

- Los mecanismos de detección se basan en la desviación de la línea base, los patrones conocidos y la notificación de entidades internas o externas.
- Debido a la naturaleza impredecible de la tecnología y las personas, que son los medios y los actores de los incidentes de seguridad, respectivamente, las bases de referencia cambian con el tiempo. Los patrones deshonestos surgen a través de tácticas, técnicas y procedimientos novedosos o modificados por los actores de amenazas (). TTPs
- Los cambios en las personas, la tecnología y los procesos no se incorporan inmediatamente al proceso de respuesta a los incidentes. Algunos se descubren durante el progreso de una investigación.

Fuentes de alerta

Debería considerar la posibilidad de utilizar las siguientes fuentes para definir las alertas:

- Hallazgos: AWS servicios como Amazon GuardDuty AWS Security Hub, Amazon Macie, Amazon Inspector AWS Config, IAMAccess Analyzer y Network Access Analyzer generan hallazgos que se pueden utilizar para elaborar alertas.
- Registros: los registros de AWS servicios, infraestructuras y aplicaciones almacenados en depósitos y grupos de registros de Amazon S3 se pueden analizar y CloudWatch correlacionar para generar alertas.
- Actividad de facturación: un cambio repentino en la actividad de facturación puede indicar un problema de seguridad. Sigue la documentación sobre Cómo crear una alarma de facturación para controlar tus AWS cargos estimados y así poder comprobarlo.
- Inteligencia sobre ciberamenazas: si te suscribes a una fuente de inteligencia sobre ciberamenazas de terceros, puedes correlacionar esa información con otras herramientas de registro y supervisión para identificar posibles indicadores de eventos.
- Herramientas para socios: Partners in the AWS Partner Network (APN) ofrece productos de primer nivel que pueden ayudarlo a cumplir sus objetivos de seguridad. Para responder a incidentes, asocie productos con la detección y respuesta de puntos finales (EDR) o SIEM puede ayudarlo a cumplir sus objetivos de respuesta a incidentes. Para obtener más información, consulte Security Partner Solutions y Security Solutions en la AWS Marketplace.
- AWS confianza y seguridad: podemos contactar Support con los clientes si identificamos una actividad abusiva o malintencionada.

- Contacto único: dado que pueden ser sus clientes, desarrolladores u otros miembros del personal de su organización los que adviertan algo inusual, es importante contar con un método conocido y bien publicitado para contactar con su equipo de seguridad. Entre las opciones más populares se incluyen los sistemas de venta de entradas, las direcciones de correo electrónico de contacto y los formularios web. Si su organización trabaja con el público en general, es posible que también necesite un mecanismo de contacto de seguridad orientado al público.

Para obtener más información sobre las capacidades de la nube que puede utilizar durante sus investigaciones, consulte este documento. the section called “Apéndice A: Definiciones de capacidad en la nube”

La detección como parte de la ingeniería de control de seguridad

Los mecanismos de detección son una parte integral del desarrollo del control de seguridad. A medida que se definan los controles directivos y preventivos, se deben construir controles de detección y de respuesta relacionados. Por ejemplo, una organización establece un control directivo relacionado con el usuario raíz de una AWS cuenta, que solo debe usarse para actividades específicas y muy bien definidas. Lo asocian con un control preventivo implementado mediante la política de control de servicios de una AWS organización ()SCP. Si la actividad del usuario root supera la línea de base esperada, un control de detección implementado con una EventBridge regla y un SNS tema alertará al centro de operaciones de seguridad (SOC). El control responsivo implica SOC seleccionar el manual de estrategias adecuado, realizar un análisis y trabajar hasta que se resuelva el incidente.

La mejor forma de definir los controles de seguridad es modelar las amenazas de las cargas de trabajo que se estén ejecutando. AWS La importancia de los controles de detección se determinará examinando el análisis del impacto empresarial (BIA) de cada carga de trabajo concreta. Las alertas generadas por los controles de detección no se gestionan a medida que llegan, sino que se basan en su criticidad inicial, para ajustarlas durante el análisis. El conjunto inicial de criticidad es una ayuda para establecer prioridades; el contexto en el que se produjo la alerta determinará su verdadera criticidad. Por ejemplo, una organización usa Amazon GuardDuty como un componente del control de detectives que se usa para EC2 las instancias que forman parte de una carga de trabajo. `Impact:EC2/SuspiciousDomainRequest.Reputation`Se genera el hallazgo y te informa de que la EC2 instancia de Amazon incluida en tu carga de trabajo está consultando un nombre de dominio sospechoso de ser malicioso. Esta alerta está configurada de forma predeterminada como de gravedad baja y, a medida que avanzaba la fase de análisis, se determinó que un actor no autorizado había desplegado varios cientos de EC2 instancias de este tipo`p4d.24xlarge`, lo que aumentaba considerablemente los costes operativos de la organización. En este punto, el equipo de

respuesta a incidentes toma la decisión de ajustar la gravedad de esta alerta a un nivel alto, lo que aumenta la sensación de urgencia y agiliza las acciones futuras. Tenga en cuenta que la gravedad de la GuardDuty detección no se puede cambiar.

Implementaciones de control de Detectives

Es importante entender cómo se implementan los controles de detección porque ayudan a determinar cómo se utilizará la alerta para un evento en particular. Hay dos implementaciones principales de los controles de detección técnica:

- La detección del comportamiento se basa en modelos matemáticos comúnmente denominados aprendizaje automático (ML) o inteligencia artificial (IA). La detección se realiza por inferencia; por lo tanto, es posible que la alerta no refleje necesariamente un evento real.
- La detección basada en reglas es determinista; los clientes pueden establecer los parámetros exactos de la actividad sobre la que van a recibir alertas, y eso es seguro.

Las implementaciones modernas de los sistemas de detección, como un sistema de detección de intrusos (IDS), suelen incluir ambos mecanismos. Los siguientes son algunos ejemplos de detecciones conductuales y basadas en reglas con. GuardDuty

- Cuando se genera el hallazgo, `Exfiltration:IAMUser/AnomalousBehavior` se le informa de que «se ha observado una API solicitud anómala en su cuenta». Al profundizar en la documentación, se indica que «el modelo de aprendizaje automático evalúa todas las API solicitudes de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios», lo que indica que este hallazgo se debe a un comportamiento.
- Para el hallazgo`Impact:S3/MaliciousIPCaller`, GuardDuty se analizan API las llamadas del servicio Amazon S3 en CloudTrail, comparando el elemento de `SourceIPAddress` registro con una tabla de direcciones IP públicas que incluye fuentes de inteligencia de amenazas. Una vez que encuentra una coincidencia directa con una entrada, genera el hallazgo.

Recomendamos implementar una combinación de alertas conductuales y basadas en reglas, ya que no siempre es posible implementar alertas basadas en reglas para todas las actividades incluidas en su modelo de amenazas.

Detección basada en personas

Hasta este punto, hemos hablado de la detección basada en la tecnología. La otra fuente importante de detección proviene de personas dentro o fuera de la organización del cliente. Las personas con

información privilegiada se pueden definir como empleados o contratistas, y las personas ajenas son entidades como los investigadores de seguridad, las fuerzas del orden, las noticias y las redes sociales.

Si bien la detección basada en la tecnología se puede configurar de forma sistemática, la detección basada en personas se presenta de diversas formas, como correos electrónicos, entradas, correos electrónicos, publicaciones de noticias, llamadas telefónicas e interacciones en persona. Cabe esperar que las notificaciones de detección basadas en la tecnología se envíen prácticamente en tiempo real, pero no se prevé un cronograma para la detección basada en personas. Es imperativo que la cultura de seguridad incorpore, facilite y potencie los mecanismos de detección basados en las personas para adoptar un enfoque de seguridad exhaustivo y defensivo.

Resumen

En el caso de la detección, es importante contar con una combinación de alertas basadas en reglas y basadas en el comportamiento. Además, debes contar con mecanismos para que las personas, tanto internas como externas, envíen una denuncia sobre un problema de seguridad. Las personas pueden ser una de las fuentes más valiosas de los eventos de seguridad, por lo que es importante contar con procesos para que las personas puedan plantear sus problemas. Debe utilizar los modelos de amenazas de su entorno para empezar a crear detecciones. Los modelos de amenazas le ayudarán a crear alertas basadas en las amenazas más relevantes para su entorno. Por último, puede utilizar marcos como MITRE ATT &CK para comprender las tácticas, las técnicas y los procedimientos de los actores de amenazas (TTPs). Puede resultar útil utilizar el marco MITRE ATT &CK como lenguaje común en los distintos mecanismos de detección.

Análisis

Los registros, las funciones de consulta y la inteligencia sobre amenazas son algunos de los componentes de apoyo necesarios en la fase de análisis. Muchos de los mismos registros que se utilizan para la detección también se utilizan para el análisis y requerirán la incorporación y configuración de las herramientas de consulta.

Valide, determine el alcance y evalúe el impacto de la alerta

Durante la fase de análisis, se realiza un análisis exhaustivo del registro con el objetivo de validar las alertas, definir el alcance y evaluar el impacto de la posible interrupción.

- La validación de la alerta es el punto de partida de la fase de análisis. Los encargados de responder a las incidencias buscarán entradas de registro procedentes de diversas fuentes y se pondrán en contacto directamente con los responsables de la carga de trabajo afectada.

- El siguiente paso es determinar el alcance, cuando se inventarian todos los recursos involucrados y se ajusta la criticidad de las alertas una vez que las partes interesadas están de acuerdo en que es poco probable que se trate de un falso positivo.
- Por último, el análisis de impacto detalla la verdadera disrupción empresarial.

Una vez identificados los componentes de la carga de trabajo afectados, los resultados del análisis se pueden correlacionar con el objetivo de punto de recuperación (RPO) y el objetivo de tiempo de recuperación () de la carga de trabajo correspondiente, ajustándose a la criticidad de la alerta, lo que iniciará la asignación de recursos y todas las actividades que se llevarán a cabo a continuación. RTO No todos los incidentes interrumpirán directamente las operaciones de una carga de trabajo que respalde un proceso empresarial. Es posible que incidentes como la divulgación de datos confidenciales, el robo de propiedad intelectual o el secuestro de recursos (como en el caso de la minería de criptomonedas) no detengan ni debiliten un proceso empresarial de forma inmediata, pero pueden tener consecuencias en el futuro.

Mejore los registros y hallazgos de seguridad

Enriquecimiento con inteligencia sobre amenazas y contexto organizacional

Durante el transcurso del análisis, es necesario enriquecer los observables de interés para mejorar la contextualización de la alerta. Como se indica en la sección de preparación, integrar y aprovechar la inteligencia sobre ciberamenazas puede resultar útil para comprender mejor un hallazgo de seguridad. Los servicios de inteligencia sobre amenazas se utilizan para asignar reputación y atribuir la propiedad a las direcciones IP públicas, los nombres de dominio y los hashes de archivos. Estas herramientas están disponibles como servicios de pago y gratuitos.

Los clientes que adoptan Amazon Athena como herramienta de consulta de registros obtienen la ventaja de los trabajos de AWS Glue para cargar la información de inteligencia de amenazas en forma de tablas. Las tablas de inteligencia de amenazas se pueden utilizar en las SQL consultas para correlacionar elementos del registro, como las direcciones IP y los nombres de dominio, lo que proporciona una visión enriquecida de los datos que se van a analizar.

AWS no proporciona inteligencia de amenazas directamente a los clientes, pero servicios como Amazon utilizan GuardDuty la inteligencia de amenazas para enriquecer y generar hallazgos. También puede cargar listas de amenazas personalizadas en GuardDuty función de su propia información sobre amenazas.

Enriquecimiento con automatización

La automatización es una parte integral de la Nube de AWS gobernanza. Se puede utilizar en las distintas fases del ciclo de vida de la respuesta a los incidentes.

Para la fase de detección, la automatización basada en reglas compara los patrones de interés del modelo de amenazas en los registros y toma las medidas adecuadas, como el envío de notificaciones. La fase de análisis permite aprovechar el mecanismo de detección y reenviar el cuerpo de la alerta a un motor capaz de consultar los registros y enriquecer los elementos observables para contextualizar el evento.

El cuerpo de alerta, en su forma fundamental, está compuesto por un recurso y una identidad. Por ejemplo, podrías implementar una automatización CloudTrail para consultar la AWS API actividad realizada por la identidad o el recurso del organismo de la alerta en torno al momento de la alerta, lo que proporcionaría información adicional`eventSource`, como`eventName`,`SourceIPAddress`, y sobre `userAgent` la API actividad identificada. Al realizar estas consultas de forma automática, los respondedores pueden ahorrar tiempo durante la clasificación y obtener un contexto adicional que les ayude a tomar decisiones mejor fundamentadas.

Consulte la entrada del blog Cómo enriquecer los hallazgos de AWS Security Hub con metadatos de cuentas para ver un ejemplo sobre cómo utilizar la automatización para enriquecer los hallazgos de seguridad y simplificar el análisis.

Recopile y analice pruebas forenses

La ciencia forense, como se menciona en la the section called “Preparación” sección de este documento, es el proceso de recopilar y analizar artefactos durante la respuesta a un incidente. Además AWS, se aplica a los recursos del dominio de infraestructura, como las capturas de paquetes de tráfico de red o el volcado de memoria del sistema operativo, y a los recursos del dominio de servicios, como los registros. AWS CloudTrail

El proceso forense tiene las siguientes características fundamentales:

- Coherente: sigue los pasos exactos documentados, sin desviaciones.
- Repetible: produce exactamente los mismos resultados cuando se repite contra el mismo artefacto.
- Consuetudinario: está documentado públicamente y se ha adoptado ampliamente.

Es importante mantener una cadena de custodia para los artefactos recolectados durante la respuesta a un incidente. El uso de la automatización y la generación automática de la documentación de esta colección pueden ayudar, además de almacenar los artefactos en

repositorios de solo lectura. El análisis solo debe realizarse en réplicas exactas de los artefactos recolectados para mantener la integridad.

Recopila los artefactos relevantes

Teniendo en cuenta estas características, y en función de las alertas pertinentes y de la evaluación del impacto y el alcance, tendrás que recopilar los datos que sean pertinentes para seguir investigando y analizando. Varios tipos y fuentes de datos que pueden ser relevantes para la investigación, incluidos los registros del plano de servicio/control (CloudTraileventos de datos de Amazon S3, registros de VPC flujo), datos (metadatos y objetos de Amazon S3) y recursos (bases de datos, EC2 instancias de Amazon).

Los registros del plano de servicio/control se pueden recopilar para su análisis local o, idealmente, se pueden consultar directamente mediante AWS servicios nativos (cuando proceda). Los datos (incluidos los metadatos) se pueden consultar directamente para obtener información relevante o adquirir los objetos de origen; por ejemplo, utilícelos AWS CLI para adquirir metadatos de objetos y buckets de Amazon S3 y adquirir directamente los objetos de origen. Los recursos deben recopilarse de manera coherente con el tipo de recurso y el método de análisis previsto. Por ejemplo, las bases de datos se pueden recopilar creando una base copy/snapshot of the system running the database, creating a copy/snapshot de datos completa o consultando y extrayendo ciertos datos y registros de la base de datos relevantes para la investigación.

Para EC2 las instancias de Amazon, hay un conjunto específico de datos que deben recopilarse y un orden específico de recopilación que debe realizarse para adquirir y conservar la mayor cantidad de datos para su análisis e investigación.

En concreto, el orden de respuesta para adquirir y conservar la mayor cantidad de datos de una EC2 instancia de Amazon es el siguiente:

1. Adquiera metadatos de la instancia: adquiera los metadatos de la instancia relevantes para la investigación y las consultas de datos (ID de instancia, tipo, dirección IP, ID de VPC /subnet, región, ID de Amazon Machine Image (AMI), grupos de seguridad adjuntos, hora de lanzamiento).
2. Habilite las protecciones y etiquetas de las instancias: habilite las protecciones de las instancias, como la protección de terminación, configure el comportamiento de apagado para que se detenga (si está configurado para terminar), deshabilite los atributos Delete on Termination para los EBS volúmenes adjuntos y aplique las etiquetas adecuadas tanto para la denotación visual como para su uso en posibles automatizaciones de respuesta (por ejemplo, al aplicar una etiqueta con el nombre `Status` y el valor de`Quarantine`, realizar una adquisición forense de datos y aislar la instancia).

3. Adquirir el disco (EBSinstantáneas): adquiera una EBS instantánea de los volúmenes adjuntos. EBS Cada instantánea contiene la información necesaria para restaurar los datos (desde el momento en que se tomó la instantánea) en un EBS volumen nuevo. Consulta el paso para recopilar artefactos o respuestas en tiempo real si utilizas volúmenes de almacenes de instancias.
4. Adquirir memoria: dado que las EBS instantáneas solo capturan los datos que se han escrito en su EBS volumen de Amazon, lo que podría excluir los datos que sus aplicaciones o el sistema operativo almacenan o almacenan en caché en la memoria, es imprescindible adquirir una imagen de la memoria del sistema mediante una herramienta comercial o de código abierto de terceros adecuada para adquirir los datos disponibles del sistema.
5. (Opcional) Realice una recopilación de artefactos o respuestas en vivo: realice una recopilación de datos específica (disk/memory/logs) mediante una respuesta en vivo en el sistema solo si no se puede adquirir el disco o la memoria de otra manera, o si existe un motivo comercial u operativo válido. De este modo, se modificarán datos y artefactos valiosos del sistema.
6. Retirar la instancia: separe la instancia de los grupos de Auto Scaling, anule el registro de la instancia de los balanceadores de carga y ajuste o aplique un perfil de instancia prediseñado con permisos minimizados o sin permisos.
7. Aísle o contenga la instancia: compruebe que la instancia esté aislada de manera efectiva de otros sistemas y recursos del entorno. Para ello, finalice e impida las conexiones actuales y futuras hacia y desde la instancia. Consulte la the section called “Contención” sección de este documento para obtener más información.
8. Elección del personal de respuesta: en función de la situación y los objetivos, seleccione una de las siguientes opciones:
   - Retirar y apagar el sistema (recomendado).

     Cierre el sistema una vez que se hayan adquirido las pruebas disponibles para verificar la mitigación más efectiva contra un posible futuro impacto en el medio ambiente por parte de la instancia.
   - Continúe ejecutando la instancia en un entorno aislado equipado para la supervisión.

     Aunque no se recomienda como enfoque estándar, si una situación requiere una observación continua de la instancia (por ejemplo, cuando se necesitan datos o indicadores adicionales para realizar una investigación y un análisis exhaustivos de la instancia), podría considerar cerrar la instancia, crear una AMI de la instancia y volver a lanzar la instancia en su cuenta forense dedicada dentro de un entorno aislado que esté completamente aislado y configurado con instrumentación que facilite la supervisión casi continua de la instancia (por ejemplo, registros de VPC flujo o duplicación de VPC tráfico).

> **Note**
>
> Es esencial capturar la memoria antes de las actividades de respuesta en tiempo real o de aislar o apagar el sistema para capturar los datos volátiles (y valiosos) disponibles.

Desarrolle narrativas

Durante el análisis y la investigación, documente las medidas adoptadas, los análisis realizados y la información identificada para utilizarla en las fases posteriores y, en última instancia, en un informe final. Estas narraciones deben ser sucintas y precisas y confirmar que se incluye la información relevante para verificar la comprensión efectiva del incidente y mantener un cronograma preciso. También son útiles cuando interactúas con personas ajenas al equipo principal de respuesta a incidentes. A continuación se muestra un ejemplo:

> El departamento de marketing y ventas recibió una nota de rescate el 15 de marzo de 2022 exigiendo el pago en criptomonedas para evitar la publicación de posibles datos confidenciales. SOCDeterminaron que la RDS base de datos de Amazon perteneciente a marketing y ventas era de acceso público el 20 de febrero de 2022. Tras SOC consultar los registros de RDS acceso, determinaron que la dirección IP 198.51.100.23 se utilizó el 20 de febrero de 2022 con las credenciales *`mm03434`* de Major Mary, una de las desarrolladoras web. SOCConsultaron los registros de VPC flujo y determinaron que aproximadamente 256 MB de datos habían ingresado a la misma dirección IP y en la misma fecha (fecha y hora 2022-02-20T 15:50 +00Z). Gracias a la inteligencia sobre amenazas de código abierto, SOC determinaron que las credenciales están disponibles actualmente en texto plano en el repositorio público. *`https[:]//example[.]com/majormary/rds-utils`*

Contención

Una definición de contención, en lo que respecta a la respuesta a incidentes, es el proceso o la implementación de una estrategia durante la gestión de un evento de seguridad que actúa para minimizar el alcance del evento de seguridad y contener los efectos del uso no autorizado en el entorno.

Una estrategia de contención depende de una miríada de factores y puede variar de una organización a otra en cuanto a la aplicación de las tácticas de contención, el tiempo y el propósito.

La guía de gestión de incidentes de seguridad informática NIST SP 800-61 describe varios criterios para determinar la estrategia de contención adecuada, entre los que se incluyen:

- Posibles daños y robos de recursos
- Necesidad de preservar las pruebas
- Disponibilidad del servicio (conectividad de red, servicios prestados a terceros)
- Tiempo y recursos necesarios para implementar la estrategia
- Efectividad de la estrategia (contención parcial o total)
- Duración de la solución (solución de emergencia que se eliminará en cuatro horas, solución temporal en dos semanas, solución permanente)

Sin embargo AWS, en lo que respecta a los servicios, los pasos fundamentales de contención se pueden resumir en tres categorías:

- Contención de la fuente: utilice el filtrado y el enrutamiento para evitar el acceso desde una fuente determinada.
- Técnica y contención del acceso: elimine el acceso para evitar el acceso no autorizado a los recursos afectados.
- Contención del destino: utilice el filtrado y el enrutamiento para impedir el acceso a un recurso de destino.

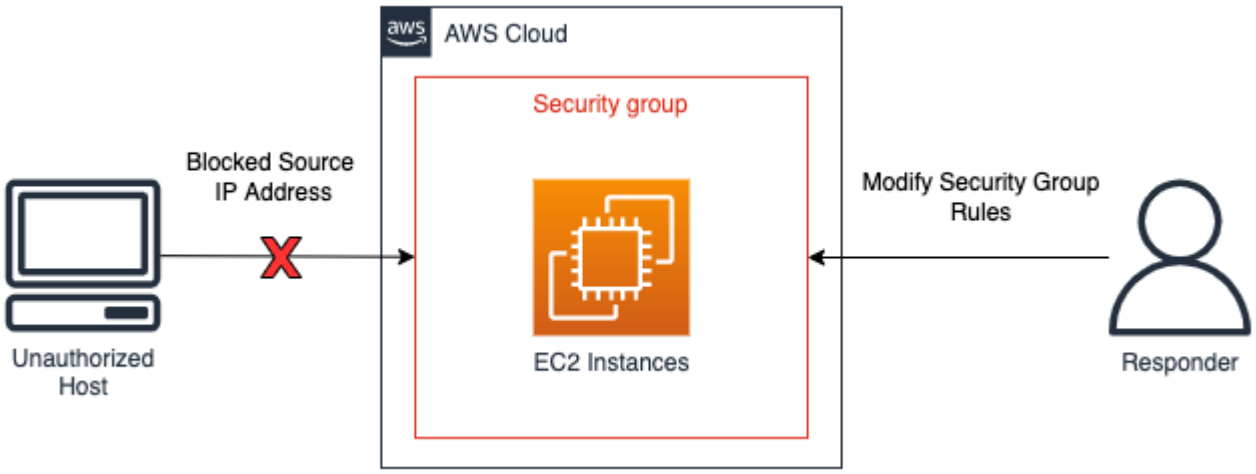
Contención de fuentes

La contención de la fuente es el uso y la aplicación del filtrado o el enrutamiento dentro de un entorno para impedir el acceso a los recursos desde una dirección IP de origen o un rango de redes específicos. A continuación, se destacan algunos ejemplos de contención de fuentes mediante AWS servicios:

- Grupos de seguridad: crear y aplicar grupos de seguridad de aislamiento a las EC2 instancias de Amazon o eliminar reglas de un grupo de seguridad existente puede ayudar a contener el tráfico no autorizado a una EC2 instancia o AWS recurso de Amazon. Es importante tener en cuenta que las conexiones rastreadas existentes no se cerrarán como resultado del cambio de grupo de seguridad, sino que el nuevo grupo de seguridad solo bloqueará eficazmente el tráfico futuro (consulte este manual de estrategias de respuesta a incidentes y seguimiento de conexiones de grupos de seguridad para obtener información adicional sobre las conexiones rastreadas y no rastreadas).

- Políticas: las políticas de bucket de Amazon S3 se pueden configurar para bloquear o permitir el tráfico desde una dirección IP, un rango de redes o un VPC punto final. Las políticas permiten bloquear las direcciones sospechosas y el acceso al bucket de Amazon S3. Puede encontrar información adicional sobre las políticas de bucket en Añadir una política de bucket mediante la consola Amazon S3.
- AWS WAF — Las listas de control de acceso a la web (webACLs) se pueden configurar AWS WAF para proporcionar un control detallado de las solicitudes web a las que responden los recursos. Puede añadir una dirección IP o un rango de redes a un conjunto de IP configurado y aplicar condiciones de coincidencia, como el bloqueo, al conjunto de IP. AWS WAF Esto bloqueará las solicitudes web a un recurso si la dirección IP o la red que van desde el tráfico de origen coinciden con los configurados en las reglas del conjunto de IP.

En el siguiente diagrama, se puede ver un ejemplo de contención de fuentes, en el que un analista de respuesta a incidentes modifica un grupo de seguridad de una EC2 instancia de Amazon para restringir las nuevas conexiones solo a determinadas direcciones IP. Como se indica en el bullet de los grupos de seguridad, las conexiones rastreadas existentes no se cerrarán como resultado de un cambio de grupo de seguridad.



Ejemplo de contención de fuentes

Técnica y contención de accesos

Evite el uso no autorizado de un recurso limitando las funciones y IAM los directores con acceso al recurso. Esto incluye restringir los permisos de los IAM directores que tienen acceso al recurso; también incluye la revocación temporal de las credenciales de seguridad. A continuación, se destacan algunos ejemplos de técnicas y de contención del acceso mediante AWS servicios:

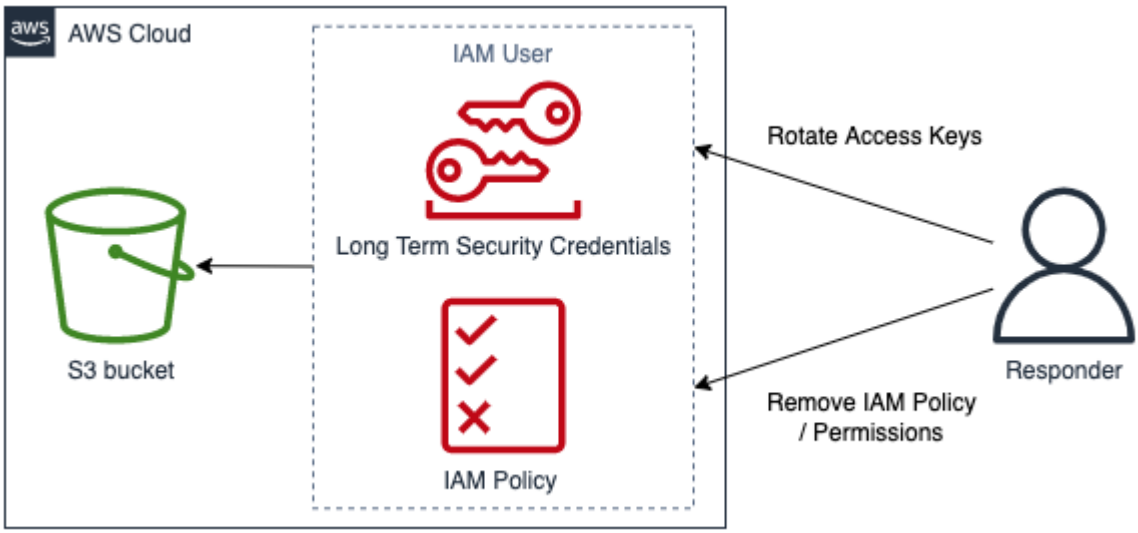
- Restringir los permisos: los permisos asignados a un IAM director deben seguir el principio del mínimo privilegio. Sin embargo, durante un evento de seguridad activo, es posible que deba restringir aún más el acceso a un recurso específico por parte de un IAM director específico. En este caso, es posible limitar el acceso a un recurso quitando los permisos del IAM principal que se va a contener. Esto se hace con el IAM servicio y se puede aplicar mediante el AWS Management Console AWS CLI, el o un AWS SDK.
- Revocar claves: los IAM directores utilizan las claves de IAM acceso para acceder a los recursos o administrarlos. Se trata de credenciales estáticas de larga duración para firmar solicitudes programáticas dirigidas al AWS CLI quirófano AWS API y comienzan por el prefijo AKIA(para obtener más información, consulte la sección Cómo entender los prefijos de identificación únicos de los identificadores). IAM Para restringir el acceso de un IAM director cuando una clave de IAM acceso se ha visto comprometida, la clave de acceso se puede desactivar o eliminar. Es importante tener en cuenta lo siguiente:
  - Una clave de acceso se puede reactivar después de haberla desactivado.
  - Una clave de acceso no se puede recuperar una vez eliminada.
  - Un IAM director puede tener hasta dos claves de acceso en un momento dado.
  - Los usuarios o las aplicaciones que usen la clave de acceso perderán el acceso una vez que la clave se desactive o se elimine.
- Revocar las credenciales de seguridad temporales: una organización puede utilizar las credenciales de seguridad temporales para controlar el acceso a AWS los recursos y empezar por el prefijo ASIA(para obtener más información, consulte la sección Descripción de los prefijos de identificación únicos en los identificadores). IAM Los IAM roles suelen utilizar las credenciales temporales y no es necesario rotarlas ni revocarlas de forma explícita porque tienen una duración limitada. En los casos en que se produzca un incidente de seguridad relacionado con una credencial de seguridad temporal antes de que caduque, es posible que tenga que modificar los permisos efectivos de las credenciales de seguridad temporales existentes. Esto se puede realizar mediante el IAM servicio incluido. AWS Management Console También se pueden emitir credenciales de seguridad temporales a IAM los usuarios (a diferencia de las IAM funciones); sin embargo, en el momento de escribir este artículo, no existe la opción de revocar las credenciales de seguridad temporales de un IAM usuario del AWS Management Console. En el caso de eventos de seguridad en los que la clave de IAM acceso de un usuario se vea comprometida por un usuario no autorizado que creó credenciales de seguridad temporales, las credenciales de seguridad temporales se pueden revocar mediante dos métodos:
  - Adjunte al IAM usuario una política interna que impida el acceso en función del momento en que se haya emitido el token de seguridad (consulte la sección Denegar el acceso a credenciales

de seguridad temporales emitidas antes de una hora específica de la sección Inhabilitar los permisos de credenciales de seguridad temporales para obtener más información).

- Elimine al IAM usuario propietario de las claves de acceso comprometidas. Vuelva a crear el usuario si es necesario.

- AWS WAF- Algunas técnicas empleadas por usuarios no autorizados incluyen patrones de tráfico maliciosos comunes, como las solicitudes que contienen SQL inyecciones y secuencias de comandos entre sitios (). XSS AWS WAF se puede configurar para igualar y denegar el tráfico mediante estas técnicas utilizando las instrucciones de reglas AWS WAF integradas.

En el siguiente diagrama se muestra un ejemplo de técnica y contención del acceso, en el que un respondedor de incidentes rota las claves de acceso o elimina una IAM política para impedir que un IAM usuario acceda a un bucket de Amazon S3.



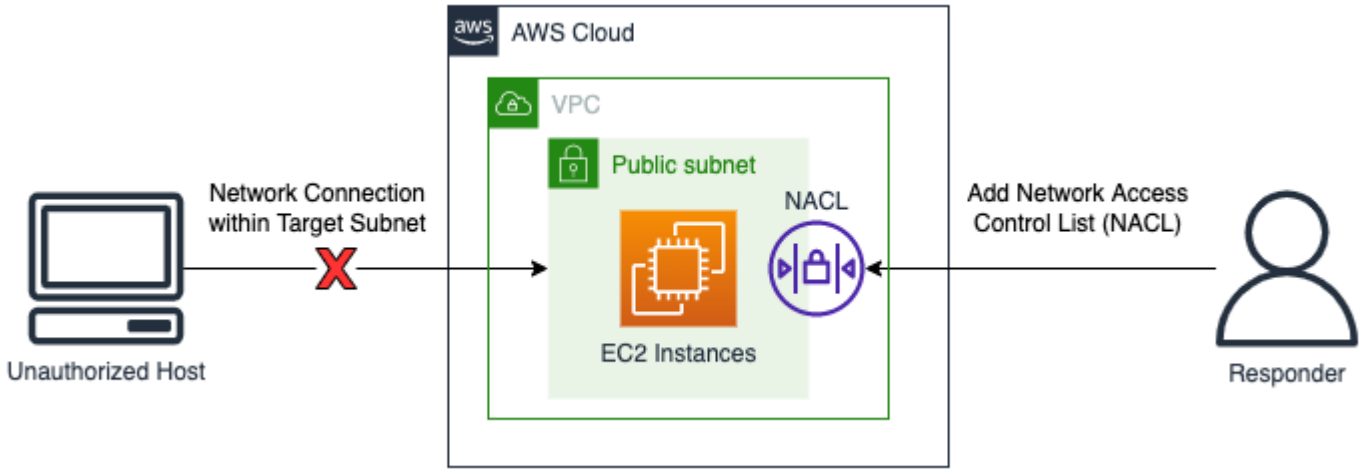
Ejemplo de técnica y contención de acceso

Contención de destino

La contención de destinos es la aplicación de filtrado o enrutamiento dentro de un entorno para impedir el acceso a un host o recurso de destino. En algunos casos, la contención del destino también implica una forma de resiliencia para verificar que los recursos legítimos se replican en función de su disponibilidad; los recursos deben separarse de estas formas de resiliencia para aislarlos y contenerlos. Algunos ejemplos de servicios de contención de destinos son los siguientes: AWS

- Red ACLs: a las redes ACLs (redesACLs) configuradas en subredes que contienen AWS recursos se les pueden agregar reglas de denegación. Estas reglas de denegación se pueden aplicar para impedir el acceso a un AWS recurso en particular; sin embargo, la aplicación de una lista de control de acceso a la red (redACL) afectará a todos los recursos de la subred, no solo a los recursos a los que se accede sin autorización. Las reglas enumeradas en una red ACL se procesan en orden descendente, por lo que la primera regla de una red existente ACL debe configurarse para denegar el tráfico no autorizado al recurso y la subred de destino. Como alternativa, se ACL puede crear una red completamente nueva con una sola regla de denegación para el tráfico entrante y saliente y asociarla a la subred que contiene el recurso de destino para impedir el acceso a la subred a través de la nueva red. ACL
- Apagar: cerrar un recurso por completo puede ser eficaz para contener los efectos del uso no autorizado. El cierre de un recurso también impedirá el acceso legítimo para satisfacer las necesidades empresariales y evitará que se obtengan datos forenses volátiles, por lo que esta decisión debe tomarse con un propósito determinado y debe juzgarse en función de las políticas de seguridad de la organización.
- Aislamiento VPCs: el aislamiento se VPCs puede utilizar para contener los recursos de forma eficaz y, al mismo tiempo, permitir el acceso al tráfico legítimo (como los antivirus (AV) o EDR las soluciones que requieren acceso a Internet o a una consola de administración externa). El aislamiento se VPCs puede preconfigurar antes de un evento de seguridad para permitir direcciones IP y puertos válidos, y los recursos de destino se pueden mover inmediatamente a este aislamiento VPC durante un evento de seguridad activo para contener el recurso y, al mismo tiempo, permitir que el recurso de destino envíe y reciba tráfico legítimo durante las fases posteriores de la respuesta al incidente. Un aspecto importante del uso de un aislamiento VPC es que los recursos, como EC2 las instancias, deben apagarse y volver a lanzarse en el nuevo aislamiento VPC antes de usarlos. EC2Las instancias existentes no se pueden mover a otra VPC u otra zona de disponibilidad. Para ello, sigue los pasos que se describen en ¿Cómo muevo mi EC2 instancia de Amazon a otra subred, zona de disponibilidad o VPC?
- Grupos de Auto Scaling y balanceadores de carga: AWS los recursos adjuntos a los grupos y balanceadores de carga de Auto Scaling deben separarse y darse de baja como parte de los procedimientos de contención de destino. La separación y anulación del registro de los AWS recursos se puede realizar mediante las teclas, y. AWS Management Console AWS CLI AWS SDK

En el siguiente diagrama, se muestra un ejemplo de contención de destinos, en el que un analista de respuesta a incidentes agrega una red ACL a una subred para bloquear una solicitud de conexión de red procedente de un host no autorizado.



Ejemplo de contención de destinos

Resumen

La contención es un paso del proceso de respuesta a un incidente y puede ser manual o automática. La estrategia general de contención debe ajustarse a las políticas de seguridad y las necesidades empresariales de la organización, y verificar que los efectos negativos se mitiguen de la manera más eficiente posible antes de proceder a la erradicación y la recuperación.

Erradicación

La erradicación, en relación con la respuesta a los incidentes de seguridad, consiste en eliminar recursos sospechosos o no autorizados para devolver la cuenta a un estado seguro conocido. La estrategia de erradicación depende de varios factores, que dependen de los requisitos empresariales de la organización.

La guía de gestión de incidentes de seguridad informática NIST SP 800-61 proporciona varios pasos para su erradicación:

1. Identifique y mitigue todas las vulnerabilidades que se explotaron.
2. Elimine el malware, los materiales inapropiados y otros componentes.
3. Si se descubren más hosts afectados (por ejemplo, nuevas infecciones de malware), repita los pasos de detección y análisis para identificar a todos los demás hosts afectados y, a continuación, contenga y erradique el incidente.

En cuanto a AWS los recursos, esto se puede refinar aún más mediante los eventos detectados y analizados a través de los registros disponibles o de herramientas automatizadas, como CloudWatch

Logs y Amazon GuardDuty. Esos eventos deberían ser la base para determinar qué medidas correctivas se deben realizar para restaurar adecuadamente el entorno a un estado seguro conocido.

El primer paso de la erradicación es determinar qué recursos de la AWS cuenta se han visto afectados. Esto se logra mediante el análisis de las fuentes de datos de registro, los recursos y las herramientas automatizadas disponibles.

- Identifique las acciones no autorizadas realizadas por las IAM identidades de su cuenta.
- Identifique los accesos no autorizados o los cambios en su cuenta.
- Identifique la creación de recursos o IAM usuarios no autorizados.
- Identifique los sistemas o recursos con cambios no autorizados.

Una vez identificada la lista de recursos, debe evaluar cada uno de ellos para determinar el impacto en el negocio si el recurso se elimina o se restaura. Por ejemplo, si un servidor web aloja su aplicación empresarial y eliminarla provocaría un tiempo de inactividad, debería considerar la posibilidad de recuperar el recurso a partir de copias de seguridad comprobadas y seguras o volver a iniciar el sistema desde un lugar limpio AMI antes de eliminar el servidor afectado.

Una vez finalizado el análisis del impacto empresarial, y utilizando los eventos del análisis de registro, debería ir a las cuentas y tomar las medidas correctivas adecuadas, como:

- Rotar o eliminar claves: este paso elimina la posibilidad del actor de seguir realizando actividades dentro de la cuenta.
- Rota las credenciales de IAM usuario potencialmente no autorizadas.
- Elimine los recursos no reconocidos o no autorizados.

> **Important**
>
> Si debe conservar los recursos para su investigación, considere la posibilidad de hacer copias de seguridad de esos recursos. Por ejemplo, si debes conservar una EC2 instancia de Amazon por motivos normativos, legales o de cumplimiento, crea una EBS instantánea de Amazon antes de eliminar la instancia.

- En el caso de las infecciones de malware, es posible que tengas que ponerte en contacto con uno AWS Partner u otro proveedor. AWS no ofrece herramientas nativas para el análisis o la eliminación del malware. Sin embargo, si utilizas el módulo GuardDuty Malware para AmazonEBS, es posible que haya recomendaciones disponibles sobre los resultados obtenidos.

Una vez que hayas erradicado los recursos afectados identificados, te AWS recomienda que realices una revisión de seguridad de tu cuenta. Esto se puede hacer mediante AWS Config reglas, utilizando soluciones de código abierto como Prowler o a través de otros ScoutSuite proveedores. También debería considerar la posibilidad de realizar escaneos de vulnerabilidades comparándolos con sus recursos públicos (Internet) para evaluar el riesgo residual.

La erradicación es un paso del proceso de respuesta a los incidentes y puede ser manual o automática, según el incidente y los recursos afectados. La estrategia general debe ajustarse a las políticas de seguridad y las necesidades empresariales de la organización, y comprobar que los efectos negativos se mitigan al eliminar recursos o configuraciones inadecuados.

Recuperación

La recuperación es el proceso que consiste en restaurar los sistemas a un estado seguro conocido, comprobar que las copias de seguridad son seguras o no se han visto afectadas por el incidente antes de la restauración, comprobar que los sistemas funcionan correctamente tras la restauración y abordar las vulnerabilidades asociadas a la incidencia de seguridad.

El orden de recuperación depende de los requisitos de la organización. Como parte del proceso de recuperación, debe realizar un análisis del impacto empresarial para determinar, como mínimo:

- Prioridades empresariales o de dependencia
- El plan de restauración
- Autenticación y autorización

La guía de gestión de incidentes de seguridad informática del NIST SP 800-61 proporciona varios pasos para recuperar los sistemas, entre los que se incluyen:

- Restauración de sistemas a partir de copias de seguridad limpias.
  - Compruebe que las copias de seguridad se evalúan antes de restaurarlas en los sistemas para asegurarse de que la infección no esté presente y evitar que reaparezca el problema de seguridad.

    Las copias de seguridad deben evaluarse periódicamente como parte de las pruebas de recuperación ante desastres para comprobar que el mecanismo de copia de seguridad funciona correctamente y que la integridad de los datos cumple los objetivos del punto de recuperación.
  - Si es posible, utilice copias de seguridad anteriores a la fecha y hora del primer evento identificada como parte del análisis de la causa raíz.

- Reconstruir los sistemas desde cero, incluida la redistribución desde una fuente confiable mediante la automatización, en algún momento en una cuenta nueva. AWS
- Sustituir los archivos comprometidos por versiones limpias.

  Debe tener mucho cuidado al hacer esto. Debe estar absolutamente seguro de que el archivo que está recuperando es seguro y no se ha visto afectado por el incidente
- Instalación de parches.
- Cambiar las contraseñas.
  - Esto incluye las contraseñas de IAM los directores que podrían haber sido objeto de un uso indebido.
  - Si es posible, recomendamos utilizar funciones para IAM los directores y la federación como parte de una estrategia de privilegios mínimos.
- Reforzar la seguridad perimetral de la red (conjuntos de reglas de firewall, listas de control de acceso a los enrutadores limítrofes).

Una vez que se hayan recuperado los recursos, es importante aprovechar las lecciones aprendidas para actualizar las políticas, los procedimientos y las guías de respuesta a incidentes.

En resumen, es imprescindible implementar un proceso de recuperación que facilite el retorno a las operaciones seguras conocidas. La recuperación puede llevar mucho tiempo y requiere una estrecha relación con las estrategias de contención para equilibrar el impacto empresarial con el riesgo de reinfección. Los procedimientos de recuperación deben incluir medidas para restaurar los recursos y servicios, el IAM capital y realizar una revisión de seguridad de la cuenta para evaluar el riesgo residual.

Conclusión

Cada fase de las operaciones tiene objetivos, técnicas, metodologías y estrategias únicos. La tabla 4 resume estas fases y algunas de las técnicas y metodologías que se tratan en esta sección.

Tabla 4: Fases de las operaciones: objetivos, técnicas y metodologías

Fase	Objetivo	Técnicas y metodologías
Detección	Identifique un posible evento de seguridad.	• Controles de seguridad para la detección

Fase	Objetivo	Técnicas y metodologías
		• Detección basada en el comportamiento y las reglas • Detección basada en personas
Análisis	Determine si el evento de seguridad es un incidente y evalúe el alcance del incidente .	• Valide y alcance la alerta • Consulta de registros de • Inteligencia sobre amenazas • Automatización
Contención	Minimice y limite el impacto del evento de seguridad.	• Contención de fuentes • Técnica y contención de accesos • Contención de destino
Erradicación	Elimine los recursos o artefactos no autorizados relacionados con el evento de seguridad.	• Rotación o eliminación de credenciales compromet idas o no autorizadas • Eliminación no autorizada de recursos • Eliminación de malware • Análisis de seguridad
Recuperación	Restaure los sistemas a un estado de funcionalidad comprobada y supervise estos sistemas para garantizar que la amenaza no vuelva a aparecer.	• Restauración del sistema desde copias de seguridad • Sistemas reconstruidos desde cero • Los archivos compromet idos se sustituyeron por versiones limpias

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 iterar los resultados de sus incidentes y simulaciones a fin de mejorar sus capacidades para detectar, responder e investigar de manera efectiva los posibles incidentes de seguridad, reducir las posibles vulnerabilidades, el tiempo de respuesta y volver a las operaciones seguras. Los siguientes mecanismos pueden ayudarlo a comprobar que su organización está preparada con las capacidades y los conocimientos más recientes para responder de manera eficaz, sea cual sea la situación.

Establezca un marco para aprender de los incidentes

La implementación de un marco y una metodología sobre las lecciones aprendidas no solo ayudará a mejorar las capacidades de respuesta a los incidentes, sino que también ayudará a evitar que los incidentes se repitan. Al aprender de cada incidente, puede evitar que se repitan los mismos errores, riesgos o errores de configuración, lo que no solo mejora su postura de seguridad, sino que también minimiza el tiempo perdido en situaciones evitables.

Es importante implementar un marco de trabajo sobre las lecciones aprendidas que establezca y logre, al más alto nivel, los puntos siguientes:

- ¿Cuándo se imparte una lección aprendida?
- ¿Qué implica el proceso de lecciones aprendidas?
- ¿Cómo se lleva a cabo una lección aprendida?
- ¿Quién participa en el proceso y cómo?
- ¿Cómo se van a identificar las áreas de mejora?
- ¿Cómo se asegurará de que las mejoras se rastreen e implementen de manera efectiva?

Además de enumerar estos resultados de alto nivel, es importante asegurarse de hacer las preguntas correctas para obtener el máximo valor (información que conduce a mejoras prácticas) del proceso. Considere la posibilidad de usar estas preguntas para fomentar el debate sobre las lecciones aprendidas:

- ¿Cuál fue el incidente?
- ¿Cuándo se identificó por primera vez el incidente?
- ¿Cómo se identificó?

- ¿Qué sistemas alertaron sobre la actividad?
- ¿Qué sistemas, servicios y datos estaban involucrados?
- ¿Qué ocurrió exactamente?
- ¿Qué funcionó correctamente?
- ¿Qué no funcionó correctamente?
- ¿Qué procesos o procedimientos fallaron o no se lograron escalar para responder al incidente?
- ¿Qué se puede mejorar en las siguientes áreas?:
  - Personas
    - ¿Las personas a las que había que contactar estaban realmente disponibles y la lista de contactos estaba actualizada?
    - ¿A las personas les faltaba formación o capacidades necesarias para responder e investigar el incidente de manera eficaz?
    - ¿Los recursos adecuados estaban listos y disponibles?
  - Proceso
    - ¿Se siguieron los procesos y los procedimientos?
    - ¿Los procesos y procedimientos para este (tipo de) incidente estaban documentados y disponibles?
    - ¿Faltaba algún proceso y procedimiento necesario?
    - ¿Los encargados de responder al incidente pudieron acceder oportunamente a la información necesaria para responder al problema?
  - Tecnología
    - ¿Los sistemas de alerta existentes identificaron la actividad y alertaron sobre ella eficazmente?
    - ¿Es necesario mejorar las alertas existentes o crear nuevas alertas para este (tipo de) incidente?
    - ¿Permitieron las herramientas existentes una investigación efectiva (búsqueda/análisis) del incidente?
- ¿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?
- ¿Cuál es el plazo para implementar y monitoring/preventative controls/process probar la herramienta adicional?

Esta lista no es exhaustiva; su objetivo es servir como punto de partida para identificar cuáles son las necesidades de la organización y la empresa y cómo analizarlas a fin de aprender más eficazmente de los incidentes y mejorar continuamente su postura en materia 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.

Establezca métricas para lograr el éxito

Las métricas son necesarias para medir, evaluar y mejorar de manera efectiva sus capacidades de respuesta a incidentes. Sin métricas, no hay una referencia con la que medir con precisión o incluso identificar el rendimiento (o no) de su organización. Hay algunas métricas comunes a la respuesta a los incidentes que son un buen punto de partida para una organización que busca establecer expectativas y referencias para trabajar en pos de la excelencia operativa.

Tiempo medio de detección

El tiempo medio de detección es el tiempo medio que se tarda en descubrir un posible incidente de seguridad. En concreto, se trata del tiempo que transcurre entre la aparición del primer indicador de peligro y la identificación o alerta inicial.

Puede utilizar esta métrica para hacer un seguimiento del rendimiento de sus sistemas de detección y alerta. Los mecanismos eficaces de detección y alerta son fundamentales para verificar que los posibles incidentes de seguridad no persistan en sus entornos.

Cuanto mayor sea el tiempo medio de detección, mayor será la necesidad de crear alertas y mecanismos adicionales o más eficaces para identificar y descubrir posibles incidentes de seguridad. Cuanto menor sea el tiempo medio de detección, mejor funcionarán los mecanismos de detección y alerta.

Tiempo medio para reconocer

El tiempo medio de reconocimiento es el tiempo medio que se tarda en reconocer y priorizar un posible incidente de seguridad. En concreto, se trata del tiempo que transcurre entre la generación de una alerta y el momento en que un miembro de su SOC equipo de respuesta a incidentes identifica y prioriza la alerta para su procesamiento.

Puedes usar esta métrica para hacer un seguimiento del grado en que tu equipo procesa y prioriza las alertas. Si tu equipo no es capaz de identificar y priorizar las alertas de manera efectiva, las respuestas se retrasarán y serán ineficaces.

Cuanto mayor sea el tiempo medio de reconocimiento, mayor será la necesidad de comprobar que tu equipo cuenta con los recursos y la formación adecuados para reconocer rápidamente un posible incidente de seguridad y priorizarlo a la hora de responder. Cuanto menor sea el tiempo medio para reconocerlas, mejor responderá su equipo a las alertas de seguridad, lo que demostrará que está preparado de forma eficaz y que es capaz de priorizarlas correctamente.

Tiempo medio para responder

El tiempo medio de respuesta es el tiempo medio que se tarda en iniciar la respuesta inicial a un posible incidente de seguridad. Concretamente, es el tiempo que transcurre entre la alerta inicial o el descubrimiento de un posible incidente de seguridad y las primeras medidas adoptadas para responder. Es similar al tiempo medio que se tarda en reconocer, pero es la medida de las acciones de respuesta específicas (por ejemplo, adquirir datos del sistema, contener el sistema) en comparación con el simple reconocimiento o reconocimiento de la situación.

Puede utilizar esta métrica para realizar un seguimiento de su preparación para responder a los incidentes de seguridad. Como se ha mencionado, la preparación es clave para una respuesta eficaz. Consulte la the section called “Preparación” sección de este documento.

Cuanto mayor sea el tiempo medio de respuesta, mayor será la necesidad de verificar que su equipo esté debidamente capacitado sobre cómo responder, de modo que los procesos de respuesta se documenten y utilicen de manera efectiva. Cuanto menor sea el tiempo medio de respuesta, mejor podrá su equipo identificar la respuesta adecuada a las alertas identificadas y realizar las acciones de respuesta necesarias para comenzar el viaje de regreso a las operaciones seguras.

Tiempo medio para contener

El tiempo medio de contención es el tiempo medio que se tarda en contener un posible incidente de seguridad. En concreto, se trata del tiempo que transcurre entre la alerta inicial o el descubrimiento de un posible incidente de seguridad y la finalización de las acciones de respuesta necesarias para impedir de forma eficaz que el atacante o los sistemas comprometidos causen más daños.

Puedes usar esta métrica para hacer un seguimiento de la capacidad de tu equipo de mitigar o contener los posibles incidentes de seguridad. La incapacidad de contener de forma rápida y eficaz los posibles incidentes de seguridad aumenta el impacto, el alcance y la exposición a posibles riesgos adicionales.

Cuanto mayor sea el tiempo medio de contención, mayor será la necesidad de acumular conocimientos y capacidades para mitigar y contener de forma rápida y eficaz los incidentes de

seguridad que se estén produciendo. Cuanto menor sea el tiempo medio de contención, mejor podrá su equipo comprender y emplear las medidas necesarias para mitigar y contener las amenazas identificadas a fin de reducir el impacto, el alcance y el riesgo para la empresa.

Tiempo medio de recuperación

El tiempo medio de recuperación es el tiempo medio que se tarda en reanudar completamente las operaciones de forma segura tras un posible incidente de seguridad. En concreto, es el tiempo que transcurre entre la alerta inicial o el descubrimiento de un posible incidente de seguridad y el momento en que la empresa vuelve a funcionar con normalidad y seguridad sin verse afectada por el incidente.

Puede utilizar esta métrica para hacer un seguimiento de la eficacia de sus equipos a la hora de hacer que los sistemas, las cuentas y los entornos vuelvan a funcionar de forma segura tras un incidente de seguridad. La imposibilidad de volver a operar de forma segura de forma rápida o eficaz no solo puede tener un impacto en la seguridad, sino que también puede aumentar el impacto y los gastos para la empresa y sus operaciones.

Cuanto mayor sea el tiempo medio de recuperación, mayor será la necesidad de preparar a sus equipos y entornos para que dispongan de los mecanismos adecuados (por ejemplo, procesos de conmutación por error y canalizaciones de CI/CD para la redistribución segura de sistemas limpios) a fin de minimizar el impacto de los incidentes de seguridad en las operaciones y la empresa. Cuanto menor sea el tiempo medio de recuperación, más eficaces serán sus equipos a la hora de minimizar el impacto de los incidentes de seguridad en sus operaciones y su empresa.

Tiempo de permanencia del atacante

El tiempo de permanencia del atacante es el tiempo promedio que un usuario no autorizado tiene acceso a un sistema o entorno. Es similar al tiempo medio de contención, excepto que el período comienza con la primera vez que el atacante accedió al sistema o a los entornos, que puede ser anterior a la alerta o el descubrimiento iniciales.

Puede utilizar esta métrica para hacer un seguimiento del funcionamiento conjunto de muchos de sus sistemas y mecanismos a fin de reducir el tiempo, el acceso y las oportunidades de que un atacante o una amenaza afecten a su entorno. Reducir el tiempo de permanencia de los atacantes debe ser una de las principales prioridades de sus equipos y su empresa.

Cuanto mayor sea el tiempo de permanencia del atacante, mayor será la necesidad de identificar qué partes del proceso de respuesta a incidentes deben mejorarse para garantizar la capacidad de sus equipos de minimizar el impacto y el alcance de las amenazas o los ataques en sus entornos.

Cuanto menor sea el tiempo de permanencia del atacante, mejor podrán sus equipos minimizar el tiempo y las oportunidades que una amenaza o un atacante tienen en sus entornos y, en última instancia, reducir el riesgo y el impacto en sus operaciones y su negocio.

Resumen de métricas

El establecimiento y el seguimiento de las métricas de respuesta a los incidentes le permiten medir, evaluar y mejorar sus capacidades de respuesta a los incidentes de manera eficaz. Para lograrlo, hay una serie de métricas comunes de respuesta a incidentes que se destacaron en esta sección. En la tabla 5 se resumen estas métricas.

Tabla 5: Métricas de respuesta a incidentes

Métrica	Descripción
Tiempo medio de detección	Tiempo medio que se tarda en descubrir un posible incidente de seguridad
Tiempo medio para reconocerlo	Tiempo medio que se tarda en reconocer (y priorizar) un posible incidente de seguridad
Tiempo medio de respuesta	Tiempo medio que se tarda en iniciar la respuesta inicial a un posible incidente de seguridad
Tiempo medio de contención	Tiempo medio que se tarda en contener un posible incidente de seguridad
Tiempo medio de recuperación	Tiempo medio que se tarda en volver por completo a las operaciones a salvo de un posible incidente de seguridad
Tiempo de permanencia del atacante	Tiempo promedio que un atacante tiene acceso a un sistema o entorno

Utilice indicadores de compromiso (IOCs)

Un indicador de peligro (IOC) es un artefacto observado en o sobre una red, un sistema o un entorno que puede (con un alto nivel de confianza) identificar una actividad maliciosa o un incidente de

seguridad. IOCspuede presentarse de diversas formas, como direcciones IP, dominios, artefactos a nivel de red, como TCP indicadores o cargas útiles, artefactos a nivel de sistema o de host, como archivos ejecutables, nombres de archivos y hashes, entradas de archivos de registro o entradas de registro, etc. También pueden ser una combinación de elementos o actividades, como la existencia de elementos o artefactos específicos en un sistema (un determinado archivo o conjunto de archivos y elementos de registro), acciones realizadas en un orden determinado (inicio de sesión en un sistema desde una IP determinada seguido de comandos anómalos específicos) o actividad de red (tráfico entrante o saliente anómalo hacia o desde ciertos dominios) que pueden indicar una metodología específica de amenaza, ataque o atacante.

A medida que trabaja para mejorar de forma iterativa su programa de respuesta a incidentes, debe implementar un marco para recopilar, administrar y utilizar IOCs como un mecanismo para crear y mejorar continuamente las detecciones y alertas y mejorar la velocidad y la eficacia de las investigaciones. Puede empezar por incorporar la recopilación y la gestión de las mismas IOCs en las fases de análisis e investigación de sus procesos de respuesta a incidentes. Al identificar, recopilar y almacenar de forma proactiva IOCs como parte estándar del proceso, puede crear un repositorio de datos (como parte de un programa de inteligencia de amenazas más completo) que, a su vez, se puede utilizar para mejorar las detecciones y alertas existentes, crear detecciones y alertas adicionales, identificar dónde y cuándo se vio un artefacto antes, crear y consultar documentación sobre cómo se realizaban anteriormente las investigaciones relacionadas con la coincidenciaIOCs, y más.

Educación y formación continuas

La educación y la formación son esfuerzos continuos y en evolución que deben proseguirse y mantenerse con determinación. Existen diversos mecanismos para comprobar que su equipo mantiene la conciencia, los conocimientos y las capacidades acordes con la evolución de la tecnología y el panorama de amenazas.

Un mecanismo consiste en utilizar la formación continua como parte estándar de los objetivos y las operaciones de sus equipos. Como se menciona en la sección de preparación, el personal de respuesta a incidentes y las partes interesadas deben estar debidamente capacitados para detectar, responder e investigar los incidentes internos AWS. Sin embargo, la educación no es un esfuerzo «único». La formación debe ser continua para comprobar que tu equipo está al tanto de los últimos avances tecnológicos, actualizaciones y mejoras que pueden aprovecharse para mejorar la eficacia y la eficiencia de la respuesta, así como de las adiciones o actualizaciones de los datos que pueden utilizarse para mejorar la investigación y el análisis.

Otro mecanismo consiste en verificar que las simulaciones se realicen de forma regular (por ejemplo, trimestralmente) y que se centren en resultados específicos para la empresa. Consulte la the section called “Ejecute simulaciones periódicas” sección de este documento.

Si bien realizar los primeros ejercicios de mesa es una forma excelente de generar una base de referencia inicial para la mejora, las pruebas continuas son fundamentales para lograr mejoras sostenidas up-to-date y mantener un reflejo preciso del estado actual de las operaciones. Al comparar las situaciones de seguridad más recientes y críticas y las capacidades de respuesta más importantes o más recientes, e incorporar las lecciones aprendidas en la educación, las operaciones y los procesos y procedimientos, comprobará que puede mejorar continuamente sus procesos de respuesta y su programa en su conjunto.

Conclusión

A medida que continúe su transición a la nube, es importante que tenga en cuenta los conceptos fundamentales de respuesta a los incidentes de seguridad para su AWS entorno. Puede combinar los controles disponibles, las capacidades de la nube y las opciones de reparación para mejorar la seguridad de su entorno de nube. También puede empezar poco a poco e ir cambiando a medida que vaya adoptando capacidades de automatización que mejoren su velocidad de respuesta, de modo que esté mejor preparado cuando se produzcan eventos de seguridad.

Colaboradores

Entre los colaboradores actuales y anteriores de este documento se incluyen:

- Anna McAbee, arquitecta sénior de soluciones de seguridad, Amazon Web Services
- Freddy Kasprzykowski, consultor sénior de seguridad, Amazon Web Services
- Jason Hurst, ingeniero de seguridad sénior de Amazon Web Services
- Jonathon Poling, consultor principal de seguridad, Amazon Web Services
- Josh Du Lac, director sénior de arquitectura de soluciones de seguridad, Amazon Web Services
- Paco Hope, ingeniero principal de seguridad de Amazon Web Services
- Ryan Tick, ingeniero de seguridad sénior de Amazon Web Services
- Steve de Vera, ingeniero de seguridad sénior de Amazon Web Services

Apéndice A: Definiciones de capacidades en la nube

AWS ofrece más de 200 servicios en la nube y miles de funciones. Muchas de ellas ofrecen capacidades nativas de detección, prevención y capacidad de respuesta, y otras se pueden utilizar para diseñar soluciones de seguridad personalizadas. Esta sección incluye un subconjunto de los servicios que son más relevantes para la respuesta a incidentes en la nube.

Temas

Registro y eventos

AWS CloudTrail— AWS CloudTrail servicio que permite la gobernanza, el cumplimiento, la auditoría operativa y la auditoría de riesgos de AWS las cuentas. Con CloudTrail él, puede registrar, monitorear continuamente y retener la actividad de la cuenta relacionada con las acciones en todos AWS los servicios. CloudTrail proporciona un historial de eventos de la actividad de su AWS cuenta, incluidas las acciones realizadas a través de las herramientas de línea de comandos y otros AWS servicios. AWS Management Console AWS SDKs Este historial de eventos simplifica el análisis de seguridad, el seguimiento de los cambios en los recursos y la solución de problemas. CloudTrail registra dos tipos diferentes de AWS API acciones:

- CloudTrail los eventos de administración (también conocidos como operaciones del plano de control) muestran las operaciones de administración que se llevan a cabo con los recursos de su AWS cuenta. Esto incluye acciones como la creación de un bucket de Amazon S3 y la configuración del registro.
- CloudTrail Los eventos de datos (también conocidos como operaciones del plano de datos) muestran las operaciones de recursos realizadas en un recurso de su AWS cuenta o dentro de él. Estas operaciones suelen ser actividades de gran volumen. Esto incluye acciones como la API actividad a nivel de objeto de Amazon S3 (por ejemplo `GetObject`, `DeleteObject`, y `PutObject` API las operaciones) y la actividad de invocación de funciones Lambda.

AWS Config— AWS Config es un servicio que permite a los clientes evaluar, auditar y evaluar las configuraciones de sus recursos. AWS AWS Config supervisa y registra continuamente las configuraciones de sus AWS recursos y le permite automatizar la evaluación de las configuraciones registradas comparándolas con las configuraciones deseadas. De este AWS Config modo, los clientes pueden revisar los cambios en las configuraciones y las relaciones entre AWS los recursos, de forma manual o automática, el historial detallado de configuraciones de los recursos y determinar el cumplimiento general de las configuraciones especificadas en las directrices del cliente. Esto permite simplificar la auditoría de conformidad, el análisis de seguridad, la gestión de cambios y la solución de problemas operativos.

Amazon EventBridge: Amazon EventBridge ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en AWS los recursos o el momento en que se publican las API llamadas AWS CloudTrail. Con reglas sencillas que puede configurar rápidamente, puede hacer coincidir los eventos y enrutarlos a una o más funciones o transmisiones objetivo. EventBridge se percata de los cambios operativos a medida que se producen. EventBridge puede responder a estos cambios operativos y tomar las medidas correctivas necesarias, enviando mensajes para responder al entorno, activando funciones, realizando cambios y recopilando información de estado. Algunos servicios de seguridad, como Amazon GuardDuty, producen sus resultados en forma de EventBridge eventos. Muchos servicios de seguridad también ofrecen la opción de enviar sus resultados a Amazon S3.

Registros de acceso a Amazon S3: si se almacena información confidencial en un bucket de Amazon S3, los clientes pueden habilitar los registros de acceso de Amazon S3 para registrar cada carga, descarga y modificación de esos datos. Este registro es independiente de los CloudTrail registros que registran los cambios en el propio depósito (por ejemplo, los cambios en las políticas de acceso y las políticas del ciclo de vida). Vale la pena señalar que los registros de acceso se entregan haciendo todo lo posible. En la mayoría de las solicitudes de registros para un bucket debidamente configurado se envían archivos de registro. No se garantiza que los registros de servidores estén completos ni que lleguen de manera puntual.

Amazon CloudWatch Logs: los clientes pueden usar Amazon CloudWatch Logs para monitorear, almacenar y acceder a los archivos de registro que se originan en sistemas operativos, aplicaciones y otras fuentes que se ejecutan en EC2 instancias de Amazon con un agente de CloudWatch Logs. CloudWatch Los registros pueden ser un destino para AWS CloudTrail DNS consultas de Route 53, registros de VPC flujo, funciones Lambda y otros. Luego, los clientes pueden recuperar los datos de registro asociados de los CloudWatch registros.

Amazon VPC Flow Logs: VPC Flow Logs permite a los clientes capturar información sobre el tráfico IP que entra y sale de las interfaces de red enVPCs. Tras habilitar los registros de flujo, se pueden

transmitir a Amazon CloudWatch Logs y Amazon S3. VPC Flow Logs ayuda a los clientes con una serie de tareas, como solucionar problemas por los que un tráfico específico no llega a una instancia, diagnosticar reglas de grupos de seguridad demasiado restrictivas y usarlo como una herramienta de seguridad para monitorear el tráfico a las EC2 instancias. Usa la versión más reciente del registro de VPC flujos para obtener los campos más robustos.

AWS WAF Registros: AWS WAF permite el registro completo de todas las solicitudes web inspeccionadas por el servicio. Los clientes pueden almacenarlos en Amazon S3 para cumplir con los requisitos de conformidad y auditoría, así como con los de depuración y análisis forense. Estos registros ayudan a los clientes a determinar la causa raíz de las reglas iniciadas y de las solicitudes web bloqueadas. Los registros se pueden integrar con herramientas de análisis de registros SIEM y de terceros.

Registros de consultas de Route 53 Resolver: los registros de consultas de Route 53 Resolver le permitirán registrar todas DNS las consultas realizadas por los recursos de Amazon Virtual Private Cloud (AmazonVPC). Tanto si se trata de una EC2 instancia de Amazon, una AWS Lambda función o un contenedor, si reside en tu Amazon VPC y hace una DNS consulta, esta función la registrará; de este modo, podrás explorar y comprender mejor cómo funcionan tus aplicaciones.

Otros AWS registros: publica AWS continuamente funciones y capacidades del servicio para los clientes con nuevas capacidades de registro y monitoreo. Para obtener información sobre las funciones disponibles para cada AWS servicio, consulte nuestra documentación pública.

Visibilidad y alertas

AWS Security Hub: AWS Security Hub proporciona a los clientes una visión completa de las alertas de seguridad y los estados de conformidad de alta prioridad en todas las cuentas. AWS Security Hub agrupa, organiza y prioriza los hallazgos de AWS servicios como Amazon, Amazon GuardDuty Inspector, Amazon Macie y soluciones. AWS Partner Los hallazgos se resumen visualmente en paneles de control integrados con gráficos y tablas procesables. También puede supervisar su entorno de forma continua mediante comprobaciones de conformidad automatizadas basadas en las AWS mejores prácticas y los estándares del sector que sigue su organización.

Amazon GuardDuty: Amazon GuardDuty es un servicio gestionado de detección de amenazas que monitorea continuamente el comportamiento malicioso o no autorizado para ayudar a los clientes a proteger AWS las cuentas y las cargas de trabajo. Supervisa la actividad, como las API llamadas inusuales o los despliegues potencialmente no autorizados, lo que indica la posibilidad de que las EC2 instancias de Amazon se vean comprometidas en la cuenta o los recursos, los buckets de Amazon S3 o el reconocimiento por parte de personas malintencionadas.

GuardDuty identifica a los posibles autores de delitos mediante fuentes integradas de inteligencia sobre amenazas que utilizan el aprendizaje automático para detectar anomalías en la actividad de las cuentas y la carga de trabajo. Cuando se detecta una amenaza potencial, el servicio envía una alerta de seguridad detallada a la GuardDuty consola y CloudWatch a Events. Esto hace que las alertas sean procesables y fáciles de integrar en los sistemas de flujo de trabajo y gestión de eventos existentes.

GuardDuty también ofrece dos complementos para monitorear las amenazas con servicios específicos: Amazon GuardDuty para la protección de Amazon S3 y Amazon GuardDuty para la EKS protección de Amazon. La protección de Amazon S3 permite monitorear API las operaciones GuardDuty a nivel de objeto para identificar posibles riesgos de seguridad para los datos dentro de los buckets de Amazon S3. La protección de Kubernetes permite GuardDuty detectar actividades sospechosas y posibles riesgos de los clústeres de Kubernetes en Amazon. EKS

Amazon Macie: Amazon Macie es un servicio de seguridad basado en inteligencia artificial que ayuda a evitar la pérdida de datos al descubrir, clasificar y proteger automáticamente los datos confidenciales almacenados en él. AWS Macie utiliza el aprendizaje automático (ML) para reconocer datos confidenciales, como la información de identificación personal (PII) o la propiedad intelectual, asignar un valor empresarial y proporcionar visibilidad sobre dónde se almacenan estos datos y cómo se utilizan en su organización. Amazon Macie monitorea continuamente la actividad de acceso a los datos para detectar anomalías y envía alertas cuando detecta un riesgo de acceso no autorizado o de fugas de datos inadvertidas.

Reglas de AWS Config— Una AWS Config regla representa las configuraciones preferidas para un recurso y se evalúa en función de los cambios de configuración en los recursos pertinentes, según lo registrado por. AWS Config Puede ver los resultados de la evaluación de una regla con respecto a la configuración de un recurso en un panel de control. Con AWS Config las reglas, puede evaluar su estado general de cumplimiento y riesgo desde la perspectiva de la configuración, ver las tendencias de cumplimiento a lo largo del tiempo y determinar qué cambio de configuración provocó que un recurso no cumpliera con una regla.

AWS Trusted Advisor— AWS Trusted Advisor es un recurso en línea que le ayuda a reducir los costos, aumentar el rendimiento y mejorar la seguridad mediante la optimización de su AWS entorno. Trusted Advisor proporciona orientación en tiempo real para ayudarlo a aprovisionar sus recursos siguiendo las AWS mejores prácticas. El conjunto completo de Trusted Advisor comprobaciones, incluida la integración de CloudWatch eventos, está disponible para los clientes de los planes Business y Enterprise Support.

Amazon CloudWatch: Amazon CloudWatch es un servicio de supervisión de los Nube de AWS recursos y las aplicaciones en las que se ejecuta AWS. Puede usarlo CloudWatch para recopilar métricas y realizar un seguimiento, recopilar y monitorear archivos de registro, configurar alarmas y reaccionar automáticamente ante los cambios en sus AWS recursos. CloudWatch puede supervisar AWS los recursos, como las EC2 instancias de Amazon, las tablas de Amazon DynamoDB y las instancias de base de datos de RDS Amazon, así como las métricas personalizadas generadas por sus aplicaciones y servicios, y cualquier archivo de registro que generen sus aplicaciones. Puede usar Amazon CloudWatch para obtener visibilidad en todo el sistema sobre la utilización de los recursos, el rendimiento de las aplicaciones y el estado operativo. Puede utilizar estos conocimientos para reaccionar en consecuencia y mantener su aplicación funcionando sin problemas.

Amazon Inspector: Amazon Inspector es un servicio de evaluación de seguridad automatizado que ayuda a mejorar la seguridad y la conformidad de las aplicaciones desplegadas en ellas AWS. Amazon Inspector evalúa automáticamente las aplicaciones en busca de vulnerabilidades o desviaciones respecto a las prácticas recomendadas. Tras realizar una evaluación, Amazon Inspector elabora una lista detallada de los hallazgos de seguridad priorizados por nivel de gravedad. Estos resultados se pueden revisar directamente o como parte de informes de evaluación detallados que están disponibles a través de la consola de Amazon Inspector oAPI.

Amazon Detective: Amazon Detective es un servicio de seguridad que recopila automáticamente datos de registro de sus AWS recursos y utiliza el aprendizaje automático, el análisis estadístico y la teoría de grafos para crear un conjunto de datos enlazados que le permita llevar a cabo investigaciones de seguridad más rápidas y eficientes. Detective puede analizar billones de eventos de múltiples fuentes de datos, como registros de VPC flujo CloudTrail GuardDuty, y crea automáticamente una vista unificada e interactiva de sus recursos, usuarios y las interacciones entre ellos a lo largo del tiempo. Con esta vista unificada, puede visualizar todos los detalles y el contexto en un solo lugar para identificar las razones subyacentes de los hallazgos, profundizar en las actividades históricas relevantes y determinar rápidamente la causa raíz.

Automation

AWS Lambda— AWS Lambda es un servicio informático sin servidor que ejecuta el código en respuesta a eventos y gestiona automáticamente los recursos informáticos subyacentes. Puede usar Lambda para ampliar otros AWS servicios con una lógica personalizada o crear sus propios servicios de backend que funcionen a AWS escala, con rendimiento y seguridad. Lambda ejecuta el código en una infraestructura informática de alta disponibilidad y administra los recursos informáticos por usted. Esto incluye el mantenimiento del servidor y del sistema operativo, el aprovisionamiento

de capacidad y el escalado automático, el despliegue de códigos y parches de seguridad, y la supervisión y el registro del código. Todo lo que tiene que hacer es proporcionar el código.

AWS Step Functions— AWS Step Functions facilita la coordinación de los componentes de las aplicaciones distribuidas y los microservicios mediante flujos de trabajo visuales. Step Functions proporciona una consola gráfica para organizar y visualizar los componentes de la aplicación en una serie de pasos. Esto facilita la creación y ejecución de aplicaciones de varios pasos. Step Functions inicia y rastrea automáticamente cada paso, y lo vuelve a intentar cuando hay errores, para que la aplicación se ejecute en orden y según lo esperado.

Step Functions registra el estado de cada paso, de manera que, cuando algo sale mal, puede diagnosticar y depurar los problemas con rapidez. Puede cambiar y añadir pasos sin necesidad de escribir código, para que su aplicación evolucione e innove más rápido. AWS Step Functions forma parte de AWS Serverless y facilita la organización de AWS Lambda funciones para aplicaciones sin servidor. También puede usar Step Functions para la orquestación de microservicios mediante recursos de cómputo como Amazon y EC2 Amazon. ECS

AWS Systems Manager: AWS Systems Manager le brinda visibilidad y control de su infraestructura AWS. Systems Manager proporciona una interfaz de usuario unificada para que pueda ver los datos operativos de varios AWS servicios y le permite automatizar las tareas operativas en todos sus AWS recursos. Con Systems Manager, puede agrupar los recursos por aplicación, ver los datos operativos para la supervisión y la solución de problemas y actuar en función de sus grupos de recursos. Systems Manager puede mantener las instancias en el estado definido, realizar cambios bajo demanda, como actualizar aplicaciones o ejecutar scripts de shell, y realizar otras tareas de automatización y aplicación de parches.

Almacenamiento seguro

Amazon Simple Storage Service: Amazon S3 es un almacenamiento de objetos creado para almacenar y recuperar cualquier cantidad de datos desde cualquier lugar. Está diseñado para ofrecer una durabilidad del 99,19% y almacena datos para millones de aplicaciones utilizadas por los líderes del mercado en todos los sectores. Amazon S3 ofrece una seguridad integral y está diseñado para ayudarle a cumplir sus requisitos normativos. Ofrece a los clientes flexibilidad en cuanto a los métodos que utilizan para administrar los datos con el fin de optimizar los costos, controlar el acceso y cumplir con las normas. Amazon S3 proporciona una query-in-place funcionalidad que le permite ejecutar análisis potentes directamente en sus datos en reposo en Amazon S3. Amazon S3 es un servicio de almacenamiento en la nube altamente compatible, con la integración de una de las mayores comunidades de soluciones de terceros, socios integradores de sistemas y otros AWS servicios.

Amazon S3 Glacier: Amazon S3 Glacier es un servicio de almacenamiento en la nube seguro, duradero y de coste extremadamente bajo para archivar datos y realizar copias de seguridad a largo plazo. Está diseñado para ofrecer una durabilidad del 99,19%, proporciona una seguridad integral y está diseñado para ayudarle a cumplir sus requisitos normativos. S3 Glacier ofrece una query-in-place funcionalidad que le permite ejecutar análisis potentes directamente en los datos de archivo en reposo. Para mantener los costes bajos y, al mismo tiempo, adaptarse a las distintas necesidades de recuperación, S3 Glacier ofrece tres opciones de acceso a los archivos, desde unos minutos hasta varias horas.

Capacidades de seguridad futuras y personalizadas

Los servicios y características antes mencionados no son una lista exhaustiva. AWS agrega continuamente nuevas capacidades. Para obtener más información, le recomendamos que consulte las páginas Novedades en materia de arte AWS y Seguridad en AWS la nube. Además de los servicios de seguridad que se AWS ofrecen como servicios en la nube nativos, es posible que le interese desarrollar sus propias capacidades a partir de AWS los servicios.

Si bien le recomendamos habilitar un conjunto básico de servicios de seguridad en sus cuentas AWS CloudTrail, como Amazon y Amazon Macie GuardDuty, es posible que en algún momento desee ampliar estas capacidades para obtener un valor adicional de sus activos de registro. Hay varias herramientas de socios disponibles, como las que se enumeran en nuestro programa de competencias APN de seguridad. También es posible que desee escribir sus propias consultas para buscar en sus registros. Con la amplia cantidad de servicios gestionados que AWS ofrece, esto nunca ha sido tan fácil. Existen muchos AWS servicios adicionales que pueden ayudarle en la investigación y que están fuera del ámbito de este documento, como Amazon Athena, Amazon OpenSearch Service, Amazon QuickSight, Amazon Machine Learning y Amazon. EMR

Apéndice B: recursos de respuesta a AWS incidentes

AWS publica recursos para ayudar a los clientes a desarrollar capacidades de respuesta a incidentes. La mayoría de los ejemplos de códigos y procedimientos se encuentran en el repositorio GitHub público AWS externo. A continuación se presentan algunos recursos que proporcionan ejemplos de cómo responder a incidentes.

Recursos del manual

- Marco para los manuales de respuesta a incidentes: un marco de ejemplo para que los clientes creen, desarrollen e integren manuales de seguridad a fin de prepararse para posibles escenarios de ataque al utilizar los servicios. AWS

- Desarrolle sus propios manuales de respuesta a incidentes: este taller está diseñado para ayudarle a familiarizarse con el desarrollo de manuales de respuesta a incidentes. AWS
- Ejemplos de guías de respuesta a incidentes: guías que cubren los escenarios más comunes a los que se enfrentan los clientes. AWS
- Elaboración de un manual de respuesta a AWS incidentes con los manuales de Jupyter y CloudTrail Lake: este taller lo guiará a través de la creación de un manual de respuesta a incidentes para su AWS entorno utilizando los cuadernos de Jupyter y Lake. CloudTrail

Recursos forenses

- Marco forense y de respuesta automática a incidentes: este marco y solución proporcionan un proceso forense digital estándar, que consta de las siguientes fases: contención, adquisición, examen y análisis. Aprovecha las funciones AWS λ para activar el proceso de respuesta a los incidentes de forma automática y repetible. Proporciona la segregación de cuentas para ejecutar los pasos de automatización, almacenar artefactos y crear entornos forenses.
- Automated Forensics Orchestrator for Amazon EC2: esta guía de implementación proporciona una solución de autoservicio para capturar y examinar datos de EC2 instancias y volúmenes adjuntos para su análisis forense en caso de que se detecte un posible problema de seguridad. Existe una AWS CloudFormation plantilla para implementar la solución.
- Cómo automatizar la recopilación forense de discos en AWS: este AWS blog detalla cómo configurar un flujo de trabajo de automatización para recopilar las pruebas en disco y analizarlas a fin de determinar el alcance y el impacto de los posibles incidentes de seguridad. También se incluye una AWS CloudFormation plantilla para implementar la solución.

Avisos

Es responsabilidad de los clientes realizar su propia evaluación independiente de la información que contiene este documento. Este documento: (a) tiene únicamente fines informativos, (b) representa las ofertas y prácticas actuales de AWS productos, que están sujetas a cambios sin previo aviso, y (c) no implica ningún compromiso ni garantía por parte de AWS sus filiales, proveedores o licenciantes. AWS los productos o servicios se proporcionan «tal cual» sin garantías, representaciones o condiciones de ningún tipo, ya sean expresas o implícitas. Las responsabilidades y obligaciones de AWS sus clientes están reguladas por AWS acuerdos, y este documento no forma parte de ningún acuerdo entre sus clientes AWS y sus clientes ni lo modifica.

Historial del documento

Cambio	Descripción	Fecha
Actualizado: actualizaciones de los comentarios de los clientes en los documentos.	Actualizado https://docs.aws.amazon.com/security-ir/latest/userguide/setup: monitoring-and-investigation-workflows .html a la plantilla de Stackset. Se corrigieron las entradas triage.security-ir.com a triage.security-ir.amazonaws.com Se agregó una nota sobre las conexiones rastreadas para -Contain on .html. AWSSupport EC2Reversible https://docs.aws.amazon.com/security-ir/ latest/userguide/contain Se ha corregido un enlace roto en -associated-accounts.html. https://docs.aws.amazon.com/security-ir/ latest/userguide/managing Se agregó una definición de cuenta de membresía en https://docs.aws.amazon.com/security-ir/ latest/userguide/select - a-membership-account .html. Se agregó una nota aclaratoria a https://docs.aws.a	20 de diciembre de 2024

Cambio	Descripción	Fecha
	mazon.com/en_us/ security-ir/latest/userguide/using - service-linked-roles .html para las cuentas AWS Organizat ions de administración.	

Cambio	Descripción	Fecha
Actualizado: actualizaciones de los comentarios de los clientes sobre los documento s.	Se han eliminado varios duplicados AWS AWS en el texto. Se corrigieron los enlaces rotos en https://docs.aws.amazon.com/security-ir/ latest/ userguide/sir_tagging.html and https://docs.aws.amazon.com/security-ir/latest/userguide/ service - name-info-in-cloud trail .html. Actualizaciones a https:// docs.aws.amazon.com/ security-ir/ latest/userguide/contain .html. Se ha eliminado el símbolo > del primer párrafo. Se reemplazó AWSSupport -Contain por EC2Reversible AWSSupport -ContainEC2Instance. Se reemplazó AWSSupport -C por -C. ontainIAMReversible AWSSupport ontainIAM Principal Se reemplazó AWSSupport -contiene 3 reversibles por -contiene 3 recursos. AWSSupport Se actualizó el formato https:// docs.aws.amazon.com/en_us/ de seguridad: .html ir/latest/ userguide/issues	10 de diciembre de 2024

Cambio	Descripción	Fecha
	Al pedir a los clientes que CIRT contacten a través de un ticket de soporte, https://docs.aws.amazon.com/security-ir/ latest/userguide/understand - response-teams-and-support .html ahora ofrece opciones para seleccionar en los formularios de soporte. Se eliminaron CloudWatch los eventos y se reemplazaron por EventBridge el https://docs.aws.amazon.com/security-ir/ latest/userguide/logging archivo -and-events.html. Actualizaciones gramaticales en https://docs.aws.amazon.com/security-ir/ latest/userguide/technique -access-containment.html. Se quitó la fecha de publicación de https://docs.aws.amazon.com/security-ir/ latest/userguide/security incident-response-guide -.html y se sustituyó por las actualizaciones de esta tabla.	
Actualizado: políticas AWS gestionadas y funciones vinculadas al servicio.	Actualizaciones de las políticas gestionadas y las funciones vinculadas a los servicios.	1 de diciembre de 2024

Cambio	Descripción	Fecha
Lanzamiento del servicio	Documentación de servicio inicial para el lanzamiento del servicio en re:Invent 2024	1 de diciembre de 2024

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.