Guía del usuario de Respuesta frente a incidencias de seguridad de AWS

Version December 1, 2024

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Guía del usuario de Respuesta frente a incidencias de seguridad de AWS:

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

¿Qué es Respuesta frente a incidencias de seguridad de AWS? 1
Configuraciones admitidas 1
Resumen de características 3
Supervisión e investigación 3
Optimización de la respuesta ante incidentes 3
Soluciones de seguridad de autoservicio 3
Panel de visibilidad 3
Posición de seguridad 3
Asistencia acelerada 3
Preparación y disposición 4
Conceptos y terminología 5
Introducción 8
Selección de una cuenta de membresía 8
Configuración de los detalles de la membresía 10
Asociación de cuentas con AWS Organizations 10
Configuración de flujos de trabajo de respuesta proactiva y clasificación de alertas 11
Tareas de usuario 12
Panel de control 12
Administración de mi equipo de respuesta ante incidentes 12
Asociación de una cuenta a AWS Organizations 13
Supervisión e investigación 3
Preparación 14
Detección y análisis 15
Contención 17
Erradicación 20
Recuperar 20
Informe posterior al incidente 21
Casos 22
Creación de un caso compatible con AWS 22
Creación de un caso autoadministrado 24
Respuesta a un caso generado por AWS 26
Administración de casos 26
Cambio del estado de un caso 27
Cambio de herramienta de solución 27
Elementos de acción 28

Edición de un caso ... 28
Comunicación ... 29
Permisos ... 29
Archivos adjuntos ... 30
Etiquetas ... 30
Actividades de un caso ... 31
Cierre de un caso ... 31
Uso de conjuntos de pilas de AWS CloudFormation ... 31
Cancelación de la membresía ... 38
Etiquetado de recursos de Respuesta frente a incidencias de seguridad de AWS ... 40
Uso de AWS CloudShell ... 41
Obtención de permisos de IAM para AWS CloudShell ... 41
Interacción con Respuesta ante incidentes de seguridad mediante AWS CloudShell ... 42
Registros de CloudTrail ... 43
Información de Respuesta ante incidentes de seguridad en CloudTrail ... 43
Descripción de las entradas de los archivos de registro de Respuesta ante incidentes de seguridad ... 45
Administración de cuentas con AWS Organizations ... 48
Recomendaciones y consideraciones ... 48
Acceso de confianza ... 49
Permisos necesarios para designar una cuenta de administrador delegado de Respuesta ante incidentes de seguridad ... 51
Designación de un administrador delegado para Respuesta frente a incidencias de seguridad de AWS ... 52
Cómo agregar miembros a Respuesta frente a incidencias de seguridad de AWS ... 54
Eliminación de miembros de Respuesta frente a incidencias de seguridad de AWS ... 55
... 56
Administración de eventos con Amazon EventBridge ... 56
Envío de eventos de Respuesta ante incidentes de seguridad ... 57
Referencia detallada de los eventos ... 58
Eventos de casos ... 60
Eventos de comentarios de casos ... 63
Eventos de membresías ... 66
Uso de eventos de Respuesta frente a incidencias de seguridad de AWS ... 69
Tutorial: envío de alertas de Amazon Simple Notification Service para eventos `Membership Updated` ... 70
Requisitos previos ... 70

Tutorial: creación de un tema de Amazon SNS y suscribirse a él ... 70
Tutorial: registro de una regla de eventos ... 71
Tutorial: prueba de la regla ... 73
Regla alternativa: actualizaciones de casos de Respuesta ante incidentes de seguridad ... 73
Solución de problemas ... 74
Problemas ... 74
Errores ... 74
Soporte ... 76
Seguridad ... 77
Protección de datos en Respuesta frente a incidencias de seguridad de AWS ... 77
Cifrado de datos ... 78
Privacidad del tráfico entre redes ... 79
Tráfico entre el servicio y las aplicaciones y clientes locales ... 79
Tráfico entre recursos de AWS en la misma región ... 80
Identity and Access Management ... 80
Autenticación con identidades ... 81
Funcionamiento de Respuesta frente a incidencias de seguridad de AWS con IAM ... 84
Solución de problemas de identidades y accesos en Respuesta frente a incidencias de seguridad de AWS ... 93
Uso de roles de servicio ... 95
Cómo utilizar roles vinculados a servicios ... 95
AWSServiceRoleForSecurityIncidentResponse ... 96
AWSServiceRoleForSecurityIncidentResponse_Triage ... 97
Regiones compatibles con SLR ... 98
Políticas administradas de AWS ... 99
política administrada: AWSSecurityIncidentResponseServiceRolePolicy ... 100
política administrada: AWSSecurityIncidentResponseAdmin ... 101
política administrada: AWSSecurityIncidentResponseReadOnlyAccess ... 102
política administrada: AWSSecurityIncidentResponseCaseFullAccess ... 102
política administrada: AWSSecurityIncidentResponseTriageServiceRolePolicy ... 103
Actualizaciones de SLR y políticas administradas ... 104
Respuesta a incidentes ... 106
Validación de conformidad ... 107
Registro y supervisión en Respuesta ante incidentes de seguridad de AWS ... 108
Resiliencia ... 108
Seguridad de la infraestructura ... 109
Configuración y análisis de vulnerabilidades ... 109

Prevención de la sustitución confusa entre servicios ... 110
Service Quotas ... 111
Respuesta frente a incidencias de seguridad de AWS ... 111
Guía técnica sobre Respuesta frente a incidencias de seguridad de AWS ... 113
Resumen ... 113
¿Tiene Well-Architected? ... 113
Introducción ... 114
Antes de empezar ... 115
Información general sobre la respuesta ante incidentes de AWS ... 115
Preparación ... 122
Personas ... 123
Proceso ... 127
Tecnología ... 135
Resumen de los elementos de preparación ... 143
Operaciones ... 148
Detección ... 149
Análisis ... 153
Contención ... 158
Erradicación ... 164
Recuperación ... 166
Conclusión ... 168
Actividad posterior al incidente ... 169
Establecimiento de un marco de trabajo para aprender de los incidentes ... 169
Establecimiento de métricas para el éxito ... 171
Uso de indicadores de riesgo ... 175
Educación y formación continuas ... 176
Conclusión ... 176
Colaboradores ... 177
Apéndice A: Definiciones de capacidades en la nube ... 177
Registro y eventos ... 177
Visibilidad y alertas ... 180
Automatización ... 182
Almacenamiento seguro ... 183
Capacidades de seguridad futuras y personalizadas ... 183
Apéndice B: recursos de respuesta ante incidentes de AWS ... 184
Recursos de manuales de estrategias ... 184
Recursos de análisis forense ... 184

Avisos 185
Historial de documentos 186

¿Qué es Respuesta frente a incidencias de seguridad de AWS?

Respuesta frente a incidencias de seguridad de AWS lo ayuda a prepararse, responder y recibir orientación rápidamente para recuperarse de los incidentes de seguridad. Esto incluye incidentes como la toma de control de cuentas, las filtraciones de datos y los ataques de ransomware.

Respuesta frente a incidencias de seguridad de AWS clasifica los resultados, escala los eventos de seguridad y administra los casos que requieren su atención inmediata. Además, tiene acceso al equipo de respuesta ante incidentes del cliente (CIRT) de AWS, 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 sus requisitos empresariales.

Respuesta frente a incidencias de seguridad de AWS funciona con otros servicios de detección y respuesta de AWS y lo guía durante todo el ciclo de vida del incidente, desde la detección hasta la recuperación.

Contenido

- Configuraciones admitidas
- Resumen de características

Configuraciones admitidas

Respuesta frente a incidencias de seguridad de AWS admite las siguientes configuraciones de idioma y región:

- Idioma: Respuesta frente a incidencias de seguridad de AWS ofrece asistencia dedicada en inglés. La asistencia en japonés se limita al horario laboral de Japón (hora estándar) y tiene restricciones específicas:

- > **Note**
  >
  > La asistencia en japonés se ofrece en la medida de lo posible durante el horario laboral (de 09:00 a 17:00 h, de lunes a viernes, excepto festivos)

- Regiones de AWS admitidas:

  Respuesta frente a incidencias de seguridad de AWS está disponible en un subconjunto de Regiones de AWS. En estas regiones admitidas, puede crear una membresía, crear y ver casos y acceder al panel.

  - Este de EE. UU. (Ohio)
  - Oeste de EE. UU. (Oregón)
  - EE.UU. Este (Virginia)
  - UE (Fráncfort)
  - UE (Irlanda)
  - UE (Londres)
  - UE (París)
  - UE (Estocolmo)
  - Asia-Pacífico (Bombay)
  - Asia-Pacífico (Seúl)
  - Asia-Pacífico (Singapur)
  - Asia-Pacífico (Sídney)
  - Asia-Pacífico (Tokio)
  - Canadá (centro)
  - América del Sur (São Paulo)

  Al habilitar la característica de supervisión e investigación, Respuesta frente a incidencias de seguridad de AWS supervisa los resultados de Amazon GuardDuty de todas las Regiones de AWS comerciales activas. Como práctica recomendada de seguridad, AWS recomienda habilitar GuardDuty en todas las regiones de AWS compatibles. Esta configuración permite a GuardDuty generar resultados sobre actividades no autorizadas o inusuales, incluso en Regiones de AWS en las que no se implementan recursos de forma activa. Al hacerlo, mejora su posición general de seguridad y mantiene una cobertura integral de detección de amenazas en todo su entorno de AWS.

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

Resumen de características

Supervisión e investigación

Respuesta frente a incidencias de seguridad de AWS revisa rápidamente las alertas de seguridad de Amazon GuardDuty y las integraciones de terceros con AWS Security Hub, lo que reduce el número de alertas que su equipo tiene que analizar. Configura reglas de supresión basadas en su entorno para reducir las alertas de baja prioridad que tiene que clasificar e investigar.

Optimización de la respuesta ante incidentes

Escale y ejecute la respuesta ante incidentes en cuestión de minutos con las partes interesadas pertinentes, servicios de terceros y herramientas.

Soluciones de seguridad de autoservicio

Respuesta frente a incidencias de seguridad de AWS proporciona API para integrar y permitirle crear sus propias soluciones de seguridad personalizadas.

Panel de visibilidad

Supervise y mida la preparación para responder ante incidentes.

Posición de seguridad

Acceda a las prácticas recomendadas de AWS y a las herramientas acreditadas para evaluar la seguridad e investigar rápidamente la respuesta ante incidentes.

Asistencia acelerada

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

Preparación y disposición

Para implementar un proceso optimizado de notificación, configure su equipo de respuesta ante incidentes de modo que desencadene 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 Respuesta frente a incidencias de seguridad de AWS y su funcionamiento.

Alcance: Respuesta frente a incidencias de seguridad de AWS se ajusta a la publicación 800-61 Computer Security Incident Handling Guide de National Institute of Standards and Technology (NIST), que proporciona un enfoque coherente para la administración de eventos de seguridad en relación con las prácticas recomendadas del sector.

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

Portal del servicio Respuesta frente a incidencias de seguridad de AWS: un portal de autoservicio para que pueda iniciar y administrar los casos de eventos de seguridad. La comunicación y la presentación de informes continuas se facilitan mediante el sistema de tickets, las notificaciones automatizadas y la interacción directa con el equipo del servicio.

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

Contención, erradicación y recuperación: la prevención de actividades no autorizadas adicionales (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: Respuesta frente a incidencias de seguridad de AWS incorpora los comentarios y las lecciones aprendidas de proyectos anteriores para mejorar sus capacidades de detección, sus procesos de investigación y las acciones de corrección. Respuesta frente a incidencias de seguridad de AWS también se mantiene al día con las amenazas de seguridad y las prácticas recomendadas más recientes para abordar los desafíos de seguridad en constante evolución.

Evento de ciberseguridad: una acción que utiliza un sistema o red de información para producir un efecto adverso en el sistema, la red o la información que contiene.

Incidente de ciberseguridad: infracción o amenaza inminente de infracción de las políticas de seguridad informática, las políticas de uso aceptable o las prácticas de seguridad estándar.

Equipo de respuesta ante incidentes: un grupo de personas que proporcionan asistencia durante los eventos de seguridad activos. Para los casos compatibles con AWS, se trata del equipo de respuesta ante incidentes del cliente (CIRT) de AWS.

Flujo de trabajo de respuesta ante incidentes: la secuencia definida de pasos y actividades que intervienen en la administración integral de un evento de seguridad, ajustada al estándar 800-61 de NIST.

Herramientas de investigación: herramientas de Respuesta frente a incidencias de seguridad de AWS y roles vinculados a servicios que se utilizan para revisar el estado operativo de su cuenta y sus recursos.

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

Supervisión e investigación: Respuesta frente a incidencias de seguridad de AWS revisa rápidamente las alertas de seguridad de Amazon GuardDuty y pone de relieve las alertas más importantes que su equipo tiene que 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 administrar con eficacia los eventos de seguridad, como el desarrollo de planes de respuesta ante incidentes y procedimientos de prueba.

Informes y comunicación: los procesos que se utilizan para mantenerlo informado durante todo el proceso de respuesta ante incidentes, incluidas las notificaciones automatizadas, los puentes de llamadas y la entrega de artefactos de investigación. Respuesta frente a incidencias de seguridad de AWS proporciona un panel único y centralizado en la AWS Management Console para administrar todos sus esfuerzos de Respuesta frente a incidencias de seguridad de AWS.

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

Experiencia en eventos de seguridad: los conocimientos y habilidades especializados necesarios para responder ante los eventos de seguridad y administrarlos con eficacia, especialmente en el contexto de la nube de AWS.

Modelo de responsabilidad compartida: la 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 de 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 ante ellas.

Sistema de tickets: una plataforma dedicada a la administración de casos que le permite incorporar y administrar los casos de eventos de seguridad, agregar archivos adjuntos y hacer un seguimiento del ciclo de vida de la respuesta ante 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: la secuencia definida de pasos y actividades que intervienen en la administración integral de un evento de seguridad.

Introducción

Contenido

- Selección de una cuenta de membresía
- Configuración de los detalles de la membresía
- Asociación de cuentas con AWS Organizations
- Configuración de flujos de trabajo de respuesta proactiva y clasificación de alertas

Selección de una cuenta de membresía

Una cuenta de membresía es la cuenta de AWS que se usa para configurar los detalles de la cuenta y agregar y eliminar detalles de su equipo de respuesta ante incidentes y es el lugar donde se pueden crear y administrar todos los eventos de seguridad activos e históricos. Se recomienda que ajuste su cuenta de membresía de Respuesta frente a incidencias de seguridad de AWS a la misma cuenta que ha habilitado para servicios como Amazon GuardDuty y AWS Security Hub.

Tiene dos opciones para seleccionar su cuenta de membresía de Respuesta ante incidentes de seguridad de AWS mediante AWS Organizations. Puede crear una membresía en la cuenta de administración de Organizations o en una cuenta de administrador delegado de Organizations.

Uso de la cuenta de administrador delegado: las tareas administrativas y la administración de casos de Respuesta ante incidentes de seguridad de AWS se encuentran en la cuenta de administrador delegado. Se recomienda usar el mismo administrador delegado que haya configurado para otros servicios de seguridad y cumplimiento de AWS. Proporcione el ID de la cuenta de administrador delegado de 12 dígitos y, a continuación, inicie sesión en esa cuenta para continuar.

> **Important**
>
> Cuando utiliza una cuenta de administrador delegado como parte de la configuración, Respuesta frente a incidencias de seguridad de AWS no puede crear automáticamente el rol vinculado al servicio de clasificación requerido en su cuenta de administración de AWS Organizations.
> Puede usar IAM para crear este rol en su cuenta de administración de AWS Organizations.
>
> Para crear un rol vinculado a un servicio (consola)
>
> 1. Inicie sesión en la cuenta de administración de AWS Organizations.

2. Acceda a la ventana de AWS CloudShell o a la cuenta mediante la CLI con el método que prefiera.
3. Utilice el comando de la CLI `aws iam create-service-linked-role --aws-service-name triage.security-ir.amazonaws.com`.
4. (Opcional) Para comprobar que el comando ha funcionado, puede ejecutar el comando `aws iam get-role --role-name AWSServiceRoleForSecurityIncidentResponse_Triage`.
5. Revise el rol y, a continuación, seleccione Crear rol.

Uso de la cuenta que tiene la sesión iniciada actualmente: al seleccionar esta cuenta, la cuenta actual se designará como cuenta de membresía central para su membresía de Respuesta frente a incidencias de seguridad de AWS. Las personas de su organización deberán acceder al servicio a través de esta cuenta para acceder a los casos activos y resueltos, crearlos y administrarlos.

Asegúrese de tener los permisos suficientes para administrar Respuesta frente a incidencias de seguridad de AWS.

Consulte en Adición y eliminación de permisos de identidad de IAM los pasos específicos para agregar permisos.

Consulte Respuesta frente a incidencias de seguridad de AWS managed policies.

Para verificar los permisos de IAM, puede seguir estos pasos:

- Comprobación de la política de IAM: revise la política de IAM adjunta a su usuario, grupo o rol para asegurarse de que concede los permisos necesarios. Para ello, vaya a https://console.aws.amazon.com/iam/, seleccione la opción `Users`, elija el usuario específico y, a continuación, en la página de resumen, vaya a la pestaña `Permissions` donde aparece una lista de todas las políticas adjuntas; puede expandir la fila de cada política para ver sus detalles.
- Prueba de los permisos: intente llevar a cabo la acción necesaria para verificar los permisos. Por ejemplo, si necesita acceder a un caso, pruebe `ListCases`. Si no tiene los permisos necesarios, recibirá un mensaje de error.
- Uso de la AWS CLI o el SDK: puede usar la AWS Command Line Interface o un AWS SDK en el lenguaje de programación que prefiera para probar los permisos. Por ejemplo, con la AWS Command Line Interface, puede ejecutar el comando `aws sts get-caller-identity` para verificar sus permisos de usuario actuales.

- Comprobación de los registros de AWS CloudTrail: revise los registros de CloudTrail para comprobar si se están registrando las acciones que intenta llevar a cabo. Esto puede ayudarlo a identificar cualquier problema con los permisos.
- Uso del simulador de política de IAM: el simulador de política de IAM es una herramienta que le permite probar las políticas de IAM y ver el efecto que tienen en sus permisos.

> **Note**
>
> Los pasos específicos pueden variar según el servicio de AWS y las acciones que intente llevar a cabo.

Configuración de los detalles de la membresía

- Seleccione una Región de AWS en la que se almacenarán su membresía y sus casos.

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

- Si lo desea, puede seleccionar un nombre para esta membresía.
- Se debe proporcionar un contacto principal y uno secundario como parte del flujo de trabajo de creación de membresías. Estos contactos se incluyen automáticamente como parte de su equipo de respuesta ante 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 ante incidentes.
- Defina etiquetas opcionales para su membresía. Las etiquetas lo ayudan a hacer un seguimiento de los costos de AWS y a buscar recursos.

Asociación de cuentas con AWS Organizations

Su membresía da derecho a cobertura en todas las Cuentas de AWS vinculadas en AWS Organizations. Las cuentas asociadas se actualizarán automáticamente a medida que se agreguen o eliminen cuentas de su organización.

Configuración de flujos de trabajo de respuesta proactiva y clasificación de alertas

El flujo de trabajo de respuesta proactiva y clasificación de alertas es una característica opcional que se puede habilitar en su organización para supervisar los servicios de seguridad habilitados. Seleccione el conmutador situado junto a la característica para habilitarla.

Si experimenta algún problema durante la incorporación, cree un caso de AWS Support para obtener más asistencia. Asegúrese de incluir detalles como el ID de la Cuenta de AWS y cualquier error que haya podido observar durante el proceso de configuración.

Respuesta proactiva y clasificación de alertas: Respuesta frente a incidencias de seguridad de AWS supervisa e investiga las alertas generadas a partir de las integraciones de Amazon GuardDuty y Security Hub. Para utilizar esta característica, Amazon GuardDuty debe estar habilitado. Respuesta frente a incidencias de seguridad de AWS clasifica las alertas de baja prioridad con la automatización del servicio para que su equipo pueda concentrarse en los problemas más críticos. Para obtener información adicional sobre cómo funciona Respuesta frente a incidencias de seguridad de AWS con Amazon GuardDuty y AWS Security Hub, consulte la sección Detección y análisis de la guía del usuario.

Esta característica permite a Respuesta frente a incidencias de seguridad de AWS supervisar e investigar los resultados en todas las cuentas y Regiones de AWS compatibles activas en su organización. Para facilitar esta funcionalidad, Respuesta frente a incidencias de seguridad de AWS crea automáticamente un rol vinculado a servicios en todas las cuentas de miembros de su organización de AWS Organizations. Sin embargo, para la cuenta de administración, debe crear manualmente el rol vinculado a servicios para habilitar la supervisión.

El servicio no puede crear el rol vinculado a servicios en la cuenta de administración. Debe crear este rol manualmente en la cuenta de administración usando conjuntos de pilas de AWS CloudFormation.

Contención: en caso de un incidente de seguridad, Respuesta frente a incidencias de seguridad de AWS puede ejecutar acciones de contención para mitigar rápidamente el impacto, como aislar los hosts comprometidos o rotar las credenciales. Respuesta ante 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. Para ello, se puede implementar un StackSet de AWS CloudFormation, que crea los roles necesarios.

Tareas de usuario

Contenido

- Panel de control
- Administración de mi equipo de respuesta ante incidentes
- Asociación de una cuenta a AWS Organizations
- Supervisión e investigación
- Casos
- Administración de casos
- Uso de conjuntos de pilas de AWS CloudFormation
- Cancelación de la membresía

Panel de control

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

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

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

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

Administración de mi equipo de respuesta ante incidentes

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

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

Algunos ejemplos de partes interesadas externas son los proveedores de software independientes (ISV) y proveedores de servicios administrados (MSP) que desee incluir en un proceso de respuesta ante incidentes.

> **Note**
>
> La configuración de su equipo de respuesta ante incidentes no otorga automáticamente a los compañeros de equipo acceso a los recursos del servicio, como la membresía y los casos. Puede usar políticas administradas por AWS para Respuesta frente a incidencias de seguridad de AWS para conceder acceso de lectura y escritura a los recursos. Haga clic aquí para obtener más información.

Sus compañeros del equipo de respuesta ante incidentes especificados en el nivel de una membresía se agregarán automáticamente a cualquier caso. Puede agregar o eliminar compañeros de equipo individuales en cualquier momento después de crear un caso.

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

- Caso (creación, eliminación, actualización)
- Comentario (creación, eliminación, actualización)
- Archivo adjunto (creación, eliminación, actualización)
- Membresía (creación, actualización, cancelación, reanudación)

Asociación de una cuenta a AWS Organizations

Al habilitar Respuesta frente a incidencias de seguridad de AWS, se creará la membresía y se alineará a su organización de AWS Organizations. Todas las cuentas de su organización están alineadas a su membresía de Respuesta frente a incidencias de seguridad de AWS.

Para obtener más información, consulte Administración de cuentas de Respuesta frente a incidencias de seguridad de AWS con AWS Organizations.

Supervisión e investigación

Respuesta frente a incidencias de seguridad de AWS revisa y clasifica las alertas de seguridad de Amazon GuardDuty y AWS Security Hub y, a continuación, configura las reglas de supresión en función de su entorno para evitar alertas innecesarias. El equipo de CIRT de AWS investiga los resultados no clasificados, los escala deprisa y guía a su equipo para contener rápidamente los posibles problemas. Si lo desea, puede conceder a Respuesta frente a incidencias de seguridad de AWS permiso para implementar acciones de contención en su nombre.

Respuesta frente a incidencias de seguridad de AWS se ajusta a la publicación 800-61r2 Computer Security event Handling Guide de NIST en relación con la respuesta ante incidentes de seguridad. Al ajustarse a este estándar del sector, Respuesta frente a incidencias de seguridad de AWS proporciona un enfoque coherente para la administración de eventos de seguridad y sigue las prácticas recomendadas de protección y respuesta ante los eventos de seguridad en su entorno de AWS.

Cuando el servicio Respuesta frente a incidencias de seguridad de AWS identifica una alerta de seguridad o se solicita asistencia de seguridad, el equipo de CIRT de AWS lo investiga. El equipo recopila los eventos de registro y los datos de servicio, como las alertas de GuardDuty, clasifica y analiza esos datos, lleva a cabo actividades de corrección y contención y proporciona informes posteriores al incidente.

Contenido

- Preparación
- Detección y análisis
- Contención
- Erradicación
- Recuperar
- Informe posterior al incidente

Preparación

El equipo de Respuesta frente a incidencias de seguridad de AWS investiga y colabora con usted durante todo el ciclo de vida de respuesta ante los eventos de seguridad. Se recomienda estructurar este equipo y asignar los permisos necesarios antes de que se produzca un evento de seguridad.

Detección y análisis

Respuesta frente a incidencias de seguridad de AWS supervisa, clasifica e investiga los resultados de seguridad de Amazon GuardDuty y las integraciones mediante AWS Security Hub. Entre las acciones adicionales que pueden mejorar considerablemente el alcance y la eficacia de las capacidades de supervisión e investigación de Respuesta frente a incidencias de seguridad de AWS se incluyen las siguientes:

Habilitación de orígenes de detección compatibles

> **Note**
>
> Los costos del servicio Respuesta frente a incidencias de seguridad de AWS no incluyen el uso ni otros costos y tarifas asociados con los orígenes de detección compatibles o el uso de otros servicios de AWS. Consulte las páginas de las características o los servicios individuales para obtener detalles sobre los costos.

Amazon GuardDuty

GuardDuty es un servicio de detección de amenazas que supervisa, analiza y procesa continuamente los orígenes de datos y los registros del entorno de AWS. No es necesario habilitar GuardDuty para usar Respuesta frente a incidencias de seguridad de AWS; sin embargo, para usar la característica de respuesta proactiva y clasificación de alertas, Amazon GuardDuty debe habilitarse.

Para habilitar GuardDuty en toda su organización, consulte la sección `Setting up GuardDuty` de la Guía del usuario de Amazon GuardDuty.

Se recomienda encarecidamente que habilite GuardDuty en todas las Regiones de AWS compatibles. Esto permite a GuardDuty generar resultados sobre la actividad no autorizada o inusual incluso en las regiones que no utiliza de forma activa. Para obtener más información, consulte Amazon GuardDuty Regions and endpoints

La habilitación de GuardDuty proporciona a Respuesta frente a incidencias de seguridad de AWS acceso a datos críticos de detección de amenazas, lo que mejora su capacidad de identificación y respuesta ante posibles problemas de seguridad en su entorno de AWS.

AWS Security Hub

Security Hub puede ingerir los resultados de seguridad de varios servicios de AWS y soluciones de seguridad de terceros que sean compatibles. Estas integraciones pueden ayudar a Respuesta frente a incidencias de seguridad de AWS a supervisar e investigar los resultados procedentes de otras herramientas de detección.

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

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

Respuesta frente a incidencias de seguridad de AWS puede supervisar e investigar los resultados de las siguientes herramientas cuando están integradas con AWS Security Hub:

- CrowdStrike – CrowdStrike Falcon
- Lacework – Lacework
- Trend Micro – Cloud One

Al habilitar estas integraciones, puede mejorar significativamente el alcance y la eficacia de las capacidades de supervisión e investigación de Respuesta frente a incidencias de seguridad de AWS.

Análisis de resultados

Las automatizaciones de Respuesta frente a incidencias de seguridad de AWS y el equipo del servicio de CIRT de AWS analizará todos los resultados de las herramientas compatibles. Para empezar a obtener información sobre su entorno, nos comunicaremos con usted mediante casos de AWS Support. Por ejemplo, cuando necesitemos saber si un resultado 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.

Notificación de un evento

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

Comunicación

Respuesta frente a incidencias de seguridad de AWS lo mantiene informado durante la investigación al interactuar con sus contactos de seguridad a lo largo de todo el proceso. Es posible que varios compañeros del equipo atiendan su evento y todos ellos podrán utilizar el ticket del evento para ver el contenido proporcionado por el cliente y las actualizaciones de AWS.

La comunicación puede incluir notificaciones automatizadas 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 archivos de registro) y la obtención de los resultados de las investigaciones durante el evento de seguridad.

El servicio creará casos de Respuesta frente a incidencias de seguridad de AWS para comunicarse con sus equipos. Crearemos casos en su cuenta de membresía. Este enfoque centraliza la comunicación de todas sus cuentas en un solo lugar. El prefijo “[Proactive case]” ayuda a identificar los casos iniciados por Respuesta frente a incidencias de seguridad de AWS.

Al participar de forma activa en estas comunicaciones y proporcionar respuestas puntuales, puede ayudar al servicio Respuesta frente a incidencias de seguridad de AWS a lo siguiente:

- Comprender mejor su entorno y los comportamientos esperados.
- Reducir los falsos positivos a lo largo del tiempo.
- Mejorar la precisión y la relevancia de las alertas.
- Garantizar una respuesta rápida ante los incidentes de seguridad auténticos.
- Recuerde que la eficacia del servicio Respuesta frente a incidencias de seguridad de AWS mejora con su colaboración, lo que se traduce en un entorno de AWS más seguro y supervisado de forma eficiente.

Contención

Respuesta frente a incidencias de seguridad de AWS colabora con usted para contener los eventos. Puede configurar un rol de servicio para Respuesta frente a incidencias de seguridad de AWS para que lleve a cabo acciones automatizadas y manuales en su cuenta en respuesta a las alertas. También puede llevar a cabo la contención usted mismo o en colaboración con sus relaciones con terceros mediante documentos de SSM.

Una parte esencial de la contención es la toma de decisiones, por ejemplo, si se debe apagar 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. Respuesta frente a incidencias de seguridad de AWS proporciona la estrategia de contención, lo informa sobre el posible impacto y lo guía para implementar la solución solo después de haber considerado y aceptado los riesgos involucrados.

Respuesta frente a incidencias de seguridad de AWS ejecuta acciones de contención admitidas en su nombre para acelerar la respuesta y reducir el tiempo del que dispone un agente de amenazas para causar posibles daños en su entorno. Esta capacidad permite mitigar las amenazas identificadas con mayor rapidez, minimizar el impacto potencial y mejorar su posición general de seguridad. Hay diferentes opciones de contención en función de los recursos que se analicen. Las acciones de contención admitidas son las siguientes:

- Contención de EC2: la automatización de la contención de `AWSSupport-ContainEC2Instance` lleva a cabo una contención reversible de red de una instancia de EC2 y deja la instancia intacta y en ejecución, pero la aísla de cualquier actividad de red nueva e impide que se comunique con los recursos dentro y fuera de su VPC.

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

- Contención de IAM: la automatización de la contención de `AWSSupport-ContainIAMPrincipal` lleva a cabo una contención reversible de red de un usuario o rol de IAM y deja al usuario o rol en IAM, pero lo aísla de la comunicación con los recursos de su cuenta.
- Contención de S3: la automatización de la contención de `AWSSupport-ContainS3Resource` lleva a cabo una contención reversible de un bucket de S3, deja los objetos en el bucket y aísla al bucket u objeto de Amazon S3 mediante la modificación de sus políticas de acceso.

> **Important**
>
> Respuesta frente a incidencias de seguridad de AWS no habilita las capacidades de contención de forma predeterminada; para ejecutar estas acciones de contención, primero debe conceder los permisos necesarios al servicio mediante roles. Puede crear estos roles individualmente por cuenta o en toda la organización usando conjuntos de pilas de AWS CloudFormation, que crean los roles necesarios.

Respuesta frente a incidencias de seguridad de AWS le anima a considerar estrategias de contención para cada tipo de evento importante que se ajusten a su tolerancia al riesgo. Documente criterios claros que lo ayuden a tomar decisiones durante un evento. Entre los criterios que se deben considerar se incluyen los siguientes:

- Posibles daños a los recursos
- Preservación de pruebas y requisitos normativos
- Falta de disponibilidad del servicio (por ejemplo, conectividad de red, servicios prestados a terceros)
- Tiempo y recursos necesarios para implementar la estrategia
- Eficacia 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, solución permanente). Aplique controles de seguridad que puedan reducir el riesgo y permitan disponer de tiempo para definir e implementar una estrategia de contención más eficaz.

Respuesta frente a incidencias de seguridad de AWS recomienda un enfoque gradual para lograr una contención eficiente y eficaz, que incluya estrategias a corto y largo plazo basadas en el tipo de recurso.

- Estrategia de contención
  - ¿Puede Respuesta frente a incidencias de seguridad de AWS identificar el alcance del evento de seguridad?
    - En caso afirmativo, identifique todos los recursos (usuarios, sistemas, recursos).
    - En caso contrario, investigue en paralelo mientras ejecuta el siguiente paso en los recursos identificados.
  - ¿Se puede aislar el recurso?
    - En caso afirmativo, proceda a aislar los recursos afectados.
    - En caso contrario, colabore con los propietarios y administradores del sistema para determinar las medidas adicionales necesarias para contener el problema.
  - ¿Están todos los recursos afectados aislados de los no afectados?
    - En caso afirmativo, continúe con el siguiente paso.
    - En caso contrario, continúe aislando los recursos afectados para completar la contención a corto plazo y evitar que el evento se escale aún más.

- Copia de seguridad del sistema
  - ¿Se crearon copias de seguridad de los sistemas afectados para su posterior análisis?
  - ¿Están las copias forenses cifradas y almacenadas en una ubicación segura?
    - En caso afirmativo, continúe con el siguiente paso.
    - En caso contrario, cifre las imágenes forenses y almacénelas en una ubicación segura para evitar el uso accidental, los daños y las manipulaciones.

Erradicación

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 corrección uniforme en todo el entorno.

Es una práctica recomendada utilizar un enfoque gradual para la erradicación y la recuperación, y priorizar los pasos de corrección. El objetivo de las primeras fases es aumentar la seguridad general rápidamente (en 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 el equipo de CIRT de AWS trabajará con usted para evaluar las acciones necesarias.

Considere lo siguiente:

- ¿Puede volver a crear la imagen del sistema y reforzarla con revisiones 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 línea de base limpia y, al mismo tiempo, terminar el elemento infectado?
- ¿Ha eliminado todo el malware y otros artefactos que el uso no autorizado ha dejado atrás y ha reforzado los sistemas afectados contra nuevos ataques?
- ¿Es necesario hacer análisis forenses de los recursos afectados?

Recuperar

Respuesta frente a incidencias de seguridad de AWS le proporciona orientación para ayudar a restaurar los sistemas a su funcionamiento normal, confirmar que funcionan correctamente y corregir cualquier vulnerabilidad para evitar eventos similares en el futuro. Respuesta frente a incidencias

de seguridad de AWS no ayuda directamente a la recuperación de los sistemas. Las principales consideraciones incluyen las siguientes:

- ¿Cuentan los sistemas afectados con las revisiones necesarias y están protegidos contra el ataque reciente?
- ¿Cuál es el plazo factible para restablecer los sistemas a producción?
- ¿Qué herramientas utilizará para probar, supervisar y verificar los sistemas restaurados?

Informe posterior al incidente

Respuesta frente a incidencias de seguridad de AWS proporciona un resumen del evento tras la conclusión de las actividades de seguridad entre su equipo y el nuestro.

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

Métricas de casos

- Casos creados
  - Nombre de la dimensión: tipo
  - Valores de la dimensión: compatibles con AWS, soporte propio
  - Unidad: recuento
  - Descripción: número de casos creados.
- Casos cerrados
  - Nombre de la dimensión: tipo
  - Valores de la dimensión: compatibles con AWS, autoadministrados
  - Unidad: recuento
  - Descripción: medida del número total de casos cerrados.
- Casos abiertos
  - Nombre de la dimensión: tipo
  - Valores de la dimensión: compatibles con AWS, soporte propio
  - Unidad: recuento
  - Descripción: número de casos abiertos.

Métricas de clasificación

- Resultados recibidos
  - Unidad: recuento
  - Descripción: número de resultados enviados para su clasificación.
- Resultados archivados
  - Unidad: recuento
  - Descripción: número de resultados archivados tras procesarse sin investigación manual.
- Resultados investigados manualmente
  - Unidad: recuento
  - Descripción: número de resultados con investigación manual llevada a cabo.
- Investigaciones archivadas
  - Unidad: recuento
  - Descripción: número de investigaciones manuales que dieron lugar a un falso positivo y se enviaron para su archivado.
- Investigaciones escaladas
  - Unidad: recuento
  - Descripción: número de investigaciones manuales que dieron lugar a un incidente de seguridad.

Casos

Respuesta frente a incidencias de seguridad de AWS permite crear dos tipos de casos: casos compatibles con AWS o casos autoadministrados.

Creación de un caso compatible con AWS

Puede crear un caso compatible con AWS para Respuesta frente a incidencias de seguridad de AWS mediante la consola, la API o la AWS Command Line Interface. Los casos compatibles con AWS le permiten recibir asistencia del equipo de respuesta ante incidentes del cliente (CIRT) de AWS.

> **Note**
>
> El equipo de CIRT de AWS responderá a su caso en un plazo de 15 minutos. El tiempo de respuesta se aplica a una primera respuesta del equipo de CIRT de AWS. Haremos todo

lo posible por responder a la solicitud inicial en este plazo. Este tiempo de respuesta no se aplica a las respuestas posteriores.

En el siguiente ejemplo se abarca el uso de la consola.

1. Inicie sesión en la AWS Management Console. Abra la consola de Respuesta ante incidentes de seguridad en https://console.aws.amazon.com/security-ir/.
2. Elija Crear caso.
3. Elija Resolver el caso con AWS.
4. Seleccione el tipo de solicitud:
   a. Incidente de seguridad activo: este tipo es para asistencia y servicios de respuesta ante incidentes urgentes.
   b. Investigaciones: las investigaciones le permiten obtener asistencia para incidentes de seguridad percibidos en los que el equipo de CIRT de AWS puede ayudar en el análisis de registros y la confirmación secundaria de la investigación de respuesta ante incidentes.
5. Establezca la fecha estimada de inicio como la fecha del primer indicador del incidente. Por ejemplo, cuando experimentó un comportamiento anómalo 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 ante incidentes a resolver el caso:
   a. ¿Qué ha pasado?
   b. ¿Quién descubrió y notificó 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 ID de Cuenta de AWS que estén dentro del alcance del caso.
8. Agregue detalles opcionales del caso:
   a. Seleccione los servicios principales que se ven afectados en la lista desplegable.
   b. Seleccione las regiones principales que se ven afectadas en la lista desplegable.
   c. Agregue una o varias direcciones IP de agente de amenazas que haya identificado como parte de este caso.

9. Agregue al caso personal adicional y opcional de respuesta ante incidentes que recibirá las notificaciones. Para agregar a una persona, haga lo siguiente:
   a. Agregue una dirección de correo electrónico.
   b. Agregue un nombre y apellidos opcionales.
   c. Elija Agregar nuevo para agregar a otra persona.
   d. Para eliminar a una persona, elija la opción Eliminar para una persona.
   e. Elija Agregar para agregar al caso a todas las personas indicadas.
      i. Puede seleccionar varias personas y elegir Eliminar para eliminarlas de la lista.
10. Agregue etiquetas opcionales al caso.
   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 compatible con AWS, se notifica inmediatamente al equipo de CIRT de AWS y a su equipo de respuesta ante incidentes.

Creación de un caso autoadministrado

Puede crear un formulario autoadministrado para Respuesta frente a incidencias de seguridad de AWS mediante la consola, la API o la AWS Command Line Interface. Este tipo de caso NO involucra al equipo de CIRT de AWS. En el siguiente ejemplo se abarca el uso de la consola.

1. Inicie sesión en la AWS Management Console. Abra la consola de Respuesta ante incidentes de seguridad en https://console.aws.amazon.com/security-ir/.
2. Elija Create Case (Crear caso).
3. Elija Resolve case with my own incident response team.
4. Establezca la fecha estimada de inicio como la fecha del primer indicador del incidente. Por ejemplo, cuando experimentó un comportamiento anómalo 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 como se sugiere al seleccionar la opción Generar título.

6. Ingrese los ID de Cuenta de AWS que forman parte del caso. Para agregar un ID de cuenta, haga lo siguiente:
   a. Ingrese el ID de 12 dígitos de la cuenta y elija Agregar cuenta.
   b. Para eliminar una cuenta, elija Eliminar junto a la cuenta que quiera eliminar del caso.
7. Proporcione una descripción detallada del caso.
   a. Tenga en cuenta los siguientes aspectos que pueden ayudar al personal de respuesta ante incidentes a resolver el caso:
      i. ¿Qué ha pasado?
      ii. ¿Quién descubrió y notificó el incidente?
      iii. ¿A quién afecta el caso?
      iv. ¿Cuál es el impacto conocido?
      v. ¿Cuál es la urgencia de este caso?
8. Agregue detalles opcionales del caso:
   a. Seleccione los servicios principales que se ven afectados en la lista desplegable.
   b. Seleccione las regiones principales que se ven afectadas en la lista desplegable.
   c. Agregue una o varias direcciones IP de agente de amenazas que haya identificado como parte de este caso.
9. Agregue al caso personal adicional y opcional de respuesta ante incidentes que recibirá las notificaciones. Para agregar a una persona, haga lo siguiente:
   a. Agregue una dirección de correo electrónico.
   b. Agregue un nombre y apellidos opcionales.
   c. Elija Agregar nuevo para agregar a otra persona.
   d. Para eliminar a una persona, elija la opción Eliminar para una persona.
   e. Elija Agregar para agregar al caso a todas las personas indicadas. Puede seleccionar varias personas y elegir Eliminar para eliminarlas de la lista.
10. Agregue etiquetas opcionales al caso. 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 ante incidentes recibirá una notificación por correo electrónico una vez creado el caso.

Respuesta a un caso generado por AWS

Respuesta frente a incidencias de seguridad de AWS puede crear una notificación o un caso saliente cuando necesite tomar medidas o tener conocimiento de algo que pueda afectar a su cuenta o sus recursos. Esto solo ocurrirá si ha habilitado los flujos de trabajo de respuesta proactiva y clasificación de alertas como parte de su suscripción.

Estas notificaciones aparecerán como casos de Respuesta ante incidentes de seguridad con el prefijo “[Proactive case]” en la consola de Respuesta frente a incidencias de seguridad de AWS. Para ver y administrar estos casos:

- Abra la consola de Respuesta ante incidentes de seguridad en https://console.aws.amazon.com/security-ir/.
- Haga clic en “Casos” en el menú.
- Debería poder ver todos los casos, incluidos los que tienen el prefijo “[Proactive case]”.

Estos casos le permiten actualizarlos, resolverlos y reabrirlos según sea necesario. Puede comunicarse directamente con el equipo de Respuesta frente a incidencias de seguridad de AWS mediante estos casos, lo que garantiza una gestión eficiente de los posibles problemas de seguridad.

Administración de casos

Contenido

- Cambio del estado de un caso
- Cambio de herramienta de solución
- Elementos de acción
- Edición de un caso
- Comunicación
- Permisos
- Archivos adjuntos
- Etiquetas
- Actividades de un caso

- Cierre de un caso

Cambio del estado de un caso

Un caso se encontrará en uno de los siguientes estados:

- Enviado: este es el estado inicial de un caso. Un solicitante ha enviado los casos que tienen este estado, pero aún no se está trabajando en ellos.
- Detection and Analysis: este estado indica que el equipo de respuesta ante 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.
- Containment, Eradication and Recovery: en este estado, el personal de respuesta ante incidentes ha identificado una actividad sospechosa que requiere un esfuerzo adicional para eliminarla. El personal de respuesta ante incidentes le proporcionará recomendaciones para el análisis de riesgos empresariales y medidas adicionales. Si ha habilitado las características opcionales del servicio, un miembro del equipo de respuesta ante incidentes de AWS solicitará su consentimiento para llevar a cabo acciones de contención con los documentos de SSM en las cuentas afectadas.
- Actividades posteriores al incidente: en este estado, se ha contenido el evento de seguridad principal. El objetivo ahora es recuperar las operaciones comerciales y volver a la normalidad. Se proporciona un resumen y un análisis de la causa raíz si el personal de respuesta del caso es compatible con AWS.
- 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 reabrir, así que debe asegurarse de que todas las acciones se hayan completado antes de pasar a este estado.

Elija Acción/Actualizar estado para cambiar el estado del caso en los casos autoadministrados. Para los casos compatibles con AWS, el estado lo establece el personal de respuesta del equipo de CIRT de AWS.

Cambio de herramienta de solución

Para los casos autoadministrados, su equipo de respuesta ante incidentes puede solicitar ayuda a AWS. Elija Obtenga ayuda de AWS para cambiar la herramienta de solución de este caso a AWS. Una vez que el caso se haya actualizado a compatible con AWS, el estado cambiará a Enviado. El historial de casos existente estará disponible para el equipo de CIRT de AWS. Una vez que haya solicitado ayuda de AWS, no podrá volver a cambiarlo a autoadministrado.

Elementos de acción

Un miembro del equipo de repuesta de CIRT de AWS que esté trabajando en el caso puede solicitar acciones a su equipo interno.

Entre los elementos de acción que aparecen después de crear un caso se incluyen los siguientes:

- Solicitud para conceder permisos a un miembro del equipo de respuesta ante 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 tomar medidas en función de un nuevo comentario para continuar con el caso.

Elementos de acción cuando un caso está listo para cerrarse:

- Solicitud para revisar el informe del caso.
- Solicitud para cerrar el caso.

Edición de un caso

Elija Editar para cambiar los detalles de un caso.

Para casos compatibles con AWS y autoadministrados:

Puede cambiar los siguientes detalles del caso después de crearlo:

- Título
- Descripción

Solo para casos compatibles con AWS:

Puede cambiar los campos adicionales:

- Tipo de solicitud:
  - Incidente de seguridad activo: este tipo es para asistencia y servicios de respuesta ante incidentes urgentes.

  - Investigaciones: las investigaciones le permiten obtener asistencia para incidentes de seguridad percibidos en los que el equipo de CIRT de AWS puede ayudar en el análisis de registros y la confirmación secundaria del evento de seguridad.
- 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 detectado recientemente en el campo de descripción o agregar un comentario en la pestaña de comunicaciones.

Comunicación

El equipo de CIRT de AWS puede agregar comentarios para documentar sus actividades cuando trabaja en un caso. Diferentes miembros del equipo de CIRT de AWS pueden trabajar en un caso al mismo tiempo. Se representan como AWS Responder en el registro de comunicaciones.

Permisos

En la pestaña de permisos se muestra una lista de todas las personas a las que se les notificará cualquier cambio en el caso. Puede agregar 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 de nivel de caso a estas partes interesadas.

Concesión de acceso a un caso en la consola

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

Cómo agregar la política de IAM a un usuario o rol:

1. Copie la política de permisos de IAM.
2. Abra IAM en https://console.aws.amazon.com/iam/.
3. En el panel de navegación, elija Usuario o Roles.
4. Seleccione un usuario o un rol para abrir la página de detalles.

5. En la pestaña de permisos, elija Agregar permisos.
6. Elija Asociar política.
7. Seleccione la política administrada por Respuesta frente a incidencias de seguridad de AWS adecuada.
8. Elija Add Policy (Agregar política).

Archivos adjuntos

Los miembros del equipo de respuesta ante incidentes pueden agregar archivos adjuntos a un caso para ayudar a otros miembros en su investigación de casos autoadministrados.

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

Elija Cargar para seleccionar un archivo de su equipo y agregarlo al caso.

> **Note**
>
> Todos los archivos adjuntos cargados se eliminan cuando el caso lleva siete días en estado `Closed`.

Etiquetas

Una etiqueta es una marca opcional que puede asignar a sus casos para almacenar metadatos sobre ese recurso. Cada etiqueta es una marca que consta de una clave y un valor opcional. Puede utilizar etiquetas 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 de un 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.

Cierre de un caso

Para los casos compatibles con AWS, seleccione Cerrar caso en la página de detalles del caso para cerrarlo permanentemente en cualquier estado. Un caso normalmente alcanza el estado Listo para cerrar antes de cerrarse permanentemente. Si cierra un caso de forma prematura en un estado que no sea Listo para cerrar, está solicitando que el equipo de CIRT de AWS deje de trabajar en este caso compatible con AWS.

Si su equipo de respuesta ante incidentes es el encargado de responder, seleccione 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 reabrir después de haberse 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 el caso.

Uso de conjuntos de pilas de AWS CloudFormation

> **Important**
>
> Respuesta frente a incidencias de seguridad de AWS no habilita las capacidades de contención de forma predeterminada; para ejecutar estas acciones de contención, primero debe conceder los permisos necesarios al servicio mediante roles. Puede crear estos roles de forma individual por cuenta o en toda la organización mediante la implementación de conjuntos de pilas de AWS CloudFormation, que crean los roles necesarios.

Puede consultar instrucciones específicas sobre cómo crear un conjunto de pilas con permisos administrados por servicios.

A continuación se muestran plantillas de conjuntos de pilas para crear los roles AWSSecurityIncidentResponseContainment y AWSSecurityIncidentResponseContainmentExecution.

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'Template for Respuesta frente a incidencias de seguridad de AWS
 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': '*',
            },
        ],
    }
```

Cancelación de la membresía

Un rol que tenga el permiso CancelMembership para Respuesta frente a incidencias de seguridad de AWS puede cancelar la membresía desde la consola, la API o la AWS Command Line Interface.

Important

Una vez cancelada una membresía, no podrá ver los datos históricos de los casos. Si cancela la membresía durante el mes, estará disponible hasta el final del mes. Cualquier recurso o investigación cuyo estado sea `Active` o `ready to close` se terminará tras la cancelación definitiva de la membresía al final del ciclo de facturación.

Important

Respuesta frente a incidencias de seguridad de AWS no sigue el ciclo de facturación de aniversario estándar que ocurre todos los meses. La facturación del servicio se produce mes a mes. Presentamos algunos ejemplos:

- Del 29 de diciembre al 29 de enero
- Del 29 de enero al 26 de febrero (año no bisiesto)
- Del 26 de febrero al 29 de marzo

> **Important**
>
> Si vuelve a suscribirse al servicio, se creará una nueva membresía y solo podrá acceder a los recursos de casos que estaban en la membresía anterior si los descargó antes de la cancelación.

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

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

Etiquetado de recursos de Respuesta frente a incidencias de seguridad de AWS

Una etiqueta es un elemento de metadatos que usted o AWS asigna a un recurso de AWS. 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:

- Identificar y organizar sus recursos de AWS. 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.
- Realizar un seguimiento de los costos de AWS. Estas etiquetas se activan en el panel de AWS Billing. AWS usa las etiquetas para clasificar los costos y enviar un informe mensual de asignación de costos. Para obtener más información, consulte Use cost allocation tags en la Guía del usuario de facturación de AWS.
- Controle el acceso a los recursos de AWS. Para obtener más información, consulte Control del acceso mediante etiquetas en la Guía del usuario de IAM.

Consulte la referencia de la API de Respuesta frente a incidencias de seguridad de AWS para el etiquetado.

Uso de AWS CloudShell para trabajar con Respuesta ante incidentes de seguridad de AWS

AWS CloudShell es un intérprete de comandos previamente autenticado y basado en navegador que se puede lanzar directamente desde la AWS Management Console. Puede ejecutar comandos de AWS CLI en servicios de AWS (tales como Respuesta ante incidentes de seguridad de AWS) mediante su intérprete de comandos preferido (Bash, PowerShell o Z shell). Y puede hacerlo sin necesidad de descargar o instalar herramientas de línea de comandos.

Inicia AWS CloudShell desde la AWS Management Console y las credenciales de AWS que usó para iniciar sesión en la consola están automáticamente disponibles en una nueva sesión de intérprete de comandos. Esta autenticación previa de usuarios de AWS CloudShell le permite omitir la configuración de las credenciales cuando interactúa con servicios de AWS, como Respuesta ante incidentes de seguridad, mediante la versión 2 de la AWS CLI (preinstalada en el entorno de computación del intérprete de comandos).

Contenido

- Obtención de permisos de IAM para AWS CloudShell
- Interacción con Respuesta ante incidentes de seguridad mediante AWS CloudShell

Obtención de permisos de IAM para AWS CloudShell

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

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

- `AWSCloudShellFullAccess`: concede permiso para usar AWS CloudShell con acceso completo a todas las características.

Si desea limitar el alcance de las acciones que un usuario de IAM puede realizar con AWS CloudShell, puede crear una política personalizada que utilice la política administrada de

`AWSCloudShellFullAccess` como plantilla. Para obtener más información sobre cómo limitar las acciones disponibles para los usuarios en CloudShell, consulte Administrar el acceso y el uso de AWS CloudShell con políticas de IAM en la Guía del usuario de AWS CloudShell.

> **Note**
>
> Su identidad de IAM también requiere una política que conceda permiso para hacer llamadas a Respuesta ante incidentes de seguridad.

Interacción con Respuesta ante incidentes de seguridad mediante AWS CloudShell

Tras lanzar AWS CloudShell desde la AWS Management Console, podrá empezar a interactuar inmediatamente con Respuesta ante incidentes de seguridad mediante la interfaz de la línea de comandos.

> **Note**
>
> Al usar AWS CLI en AWS CloudShell, no necesita descargar o instalar recursos adicionales. Además, dado que ya está autenticado en el intérprete de comandos, no tiene que configurar las credenciales antes de realizar llamadas.

Uso de AWS CloudShell y Respuesta ante incidentes de seguridad

- Desde la AWS Management Console, puede seleccionar las siguientes opciones disponibles en la barra de navegación para iniciar CloudShell:
  - Elija el icono de CloudShell.
  - Escriba “cloudshell” en el cuadro de búsqueda y, a continuación, elija la opción CloudShell.

Registro de llamadas a la API de Respuesta ante incidentes de seguridad de AWS mediante AWS CloudTrail

Respuesta a incidentes de seguridad de AWS se integra con AWS CloudTrail, un servicio que proporciona un registro de las acciones que lleva a cabo un usuario, un rol o un servicio de AWS en Respuesta ante incidentes de seguridad. CloudTrail captura todas las llamadas a la API de Respuesta ante incidentes de seguridad como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de Respuesta a incidentes de seguridad y las llamadas desde el código a las operaciones de la API de Respuesta ante incidentes de seguridad. Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail en un bucket de Amazon S3, incluidos los eventos de Respuesta ante incidentes de seguridad. Si no configura un registro de seguimiento, puede ver los eventos más recientes en la consola de CloudTrail en el Historial de eventos. Mediante la información que recopila CloudTrail, puede determinar la solicitud que se hizo a Respuesta ante incidentes de seguridad, la dirección IP desde la que se hizo dicha solicitud, quién la hizo y cuándo, además de información adicional.

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

Información de Respuesta ante incidentes de seguridad en CloudTrail

CloudTrail se habilita en su Cuenta de AWS cuando se crea la cuenta. Cuando se produce una actividad en Respuesta ante incidentes de seguridad, dicha actividad se registra en un evento de CloudTrail junto con eventos de otros servicios de AWS en Historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para más información, consulte Visualización de eventos con el historial de eventos de CloudTrail.

Para mantener un registro permanente de los eventos en su Cuenta de AWS más allá de los 90 días, cree un registro de seguimiento o un almacén de datos de eventos de CloudTrail Lake.

Registros de seguimiento de CloudTrail

> Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. Todos los registros de seguimiento que cree con la AWS Management Console son multirregionales. Puede crear un registro de seguimiento de una sola región o multirregionales mediante la AWS CLI. Se recomienda crear un registro de seguimiento multirregional, ya que registra actividad en todas las Regiones de AWS de su 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 crear un registro de seguimiento para enviar una copia de los eventos de administración en curso en su bucket de Amazon S3 sin costo alguno desde CloudTrail; sin embargo, hay cargos por almacenamiento en Amazon S3. Para obtener más información sobre los precios de CloudTrail, consulte Precios de AWS CloudTrail. Para obtener información acerca de los precios de Amazon S3, consulte Precios de Amazon S3.

Almacenes de datos de eventos de CloudTrail Lake

CloudTrail Lake le permite ejecutar consultas basadas en SQL sobre los eventos. CloudTrail Lake convierte los eventos existentes en formato JSON basado en filas al formato ORC de Apache. ORC es un formato de almacenamiento en columnas optimizado para una recuperación rápida 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 Trabajar con AWS CloudTrail Lake en la Guía del usuario de AWS CloudTrail.

Los almacenes de datos de eventos de CloudTrail Lake y las consultas generan costos adicionales. 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 período de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información sobre los precios de CloudTrail, consulte Precios de AWS CloudTrail.

Todas las acciones de Respuesta ante incidentes de seguridad las registra CloudTrail y se documentan en la referencia de la API de Respuesta ante incidentes de seguridad de AWS. Por ejemplo, las llamadas a las acciones `CreateMembership`, `CreateCase` y `UpdateCase` generan entradas en los archivos de registros de CloudTrail.

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

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

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

Para obtener más información, consulte Elemento userIdentity de CloudTrail.

Descripción de las entradas de los archivos de registro de Respuesta ante incidentes de seguridad

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros en un bucket de Amazon S3 que especifique. Los archivos de registro de CloudTrail pueden contener una o varias entradas de registro. Un evento representa una solicitud específica realizada desde un origen cualquiera, y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

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


```
{
    "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"
}
```

Administración de cuentas de Respuesta frente a incidencias de seguridad de AWS con AWS Organizations

Respuesta frente a incidencias de seguridad de AWS está integrado en AWS Organizations. La cuenta de administración de AWS Organizations de la organización puede designar una cuenta como administrador delegado de Respuesta frente a incidencias de seguridad de AWS. Esta acción habilita a Respuesta frente a incidencias de seguridad de AWS como servicio de confianza en AWS Organizations. Para obtener información sobre cómo se conceden estos permisos, consulte Using AWS Organizations with other AWS services.

En las siguientes secciones se explican varias tareas que puede llevar a cabo como cuenta de administrador delegado de Respuesta ante incidentes de seguridad.

Contenido

- Consideraciones y recomendaciones para utilizar Respuesta frente a incidencias de seguridad de AWS con AWS Organizations
- Habilitación del acceso de confianza para AWS Account Management
- Permisos necesarios para designar una cuenta de administrador delegado de Respuesta ante incidentes de seguridad
- Designación de un administrador delegado para Respuesta frente a incidencias de seguridad de AWS
- Cómo agregar miembros a Respuesta frente a incidencias de seguridad de AWS
- Eliminación de miembros de Respuesta frente a incidencias de seguridad de AWS

Consideraciones y recomendaciones para utilizar Respuesta frente a incidencias de seguridad de AWS con AWS Organizations

Las siguientes consideraciones y recomendaciones pueden resultar útiles para comprender el funcionamiento de una cuenta de administrador delegado de Respuesta ante incidentes de seguridad en Respuesta frente a incidencias de seguridad de AWS:

Una cuenta de administrador delegado de Respuesta ante incidentes de seguridad es regional.

> La cuenta de administrador delegado de Respuesta ante incidentes de seguridad y las cuentas de miembros deben agregarse mediante AWS Organizations.

Cuenta de administrador delegado de Respuesta frente a incidencias de seguridad de AWS.

Puede designar una cuenta de miembro como cuenta de administrador delegado de Respuesta ante incidentes de seguridad. Por ejemplo, si designa una cuenta de miembro *111122223333* en *Europa (Irlanda)*, no podrá designar otra cuenta de miembro *555555555555* en *Canadá (Central)*. Se requiere que use la misma cuenta como administrador delegado de Respuesta ante incidentes de seguridad en todas las demás regiones.

No se recomienda configurar la cuenta de administración de la organización como administrador delegado de Respuesta ante incidentes de seguridad.

La cuenta de administración de la organización puede ser la cuenta de administrador delegado de Respuesta ante incidentes de seguridad. 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 delegado de Respuesta ante incidentes de seguridad de una suscripción activa, se cancela la suscripción inmediatamente.

Si elimina una cuenta de administrador delegado de Respuesta ante incidentes de seguridad, Respuesta frente a incidencias de seguridad de AWS elimina todas las cuentas de miembros asociadas a esta cuenta de administrador delegado de Respuesta ante incidentes de seguridad. El servicio Respuesta frente a incidencias de seguridad de AWS ya no estará habilitado para todas estas cuentas de miembros.

Habilitación del acceso de confianza para AWS Account Management

Cuando habilita el acceso de confianza para Respuesta frente a incidencias de seguridad de AWS, el administrador delegado de la cuenta de administración puede modificar la información y los metadatos (por ejemplo, los detalles del contacto principal o los alternativos) específicos de cada cuenta de miembro en AWS Organizations.

Utilice el siguiente procedimiento para habilitar el acceso de confianza para Respuesta frente a incidencias de seguridad de AWS 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

Habilitación del acceso de confianza para Respuesta frente a incidencias de seguridad de AWS

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; 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. En la lista de servicios, elija Respuesta frente a incidencias de seguridad de AWS.
4. Elija Habilitar acceso de confianza.
5. En el cuadro de diálogo Habilitar el acceso de confianza para Respuesta frente a incidencias de seguridad de AWS, escriba habilitar para confirmar y, a continuación, elija Habilitar el acceso de confianza.

API/CLI

Habilitación del acceso de confianza para AWS Account Management

Luego de ejecutar este comando, puede usar las credenciales de la cuenta de administración de la organización para llamar a las operaciones de la API de Account Management que utilizan el parámetro `--accountId` para hacer referencia a las cuentas de miembro en una organización.

- AWS CLI: enable-aws-service-access

  En el siguiente ejemplo se permite el acceso de confianza para Respuesta frente a incidencias de seguridad de AWS en la organización de la cuenta que hace 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 delegado de Respuesta ante incidentes de seguridad

Puede optar por configurar su membresía de Respuesta frente a incidencias de seguridad de AWS mediante el administrador delegado para AWS Organizations. Para obtener información sobre cómo se conceden estos permisos, consulte Utilizar AWS Organizations con otros servicios de AWS.

> **Note**
>
> Respuesta frente a incidencias de seguridad de AWS habilita automáticamente la relación de confianza de AWS Organizations al utilizar la consola para la configuración y la administración. Si usa la CLI o el SDK, debe habilitarla manualmente mediante la API de EnableAWSServiceAccess para confiar en `security-ir.amazonaws.com`.

Como administrador de AWS Organizations, antes de designar la cuenta de administrador delegado de Respuesta ante incidentes de seguridad de la organización, verifique que pueda llevar a cabo las siguientes acciones de Respuesta frente a incidencias de seguridad de AWS: `security-ir:CreateMembership` y `security-ir:UpdateMembership`. Estas acciones le permiten designar la cuenta de administrador delegado de Respuesta ante incidentes de seguridad para su organización mediante Respuesta frente a incidencias de seguridad de AWS. Además, debe asegurarse de que está autorizado a realizar las acciones AWS Organizations que le ayuden a recuperar información sobre la organización.

Para conceder estos permisos, incluya la siguiente instrucción en la política (de IAM) AWS Identity and Access Management de su 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 la cuenta de administración de AWS Organizations como cuenta de administrador delegado de Respuesta ante incidentes de seguridad, su cuenta también necesitará la acción de IAM: `CreateServiceLinkedRole`. Revise Consideraciones y recomendaciones para utilizar Respuesta frente a incidencias de seguridad de AWS con AWS Organizations antes de proceder a agregar los permisos.

Para continuar con la designación de su cuenta de administración de AWS Organizations como cuenta de administrador delegado de Respuesta ante incidentes de seguridad, agregue la siguiente instrucción a la política de IAM y reemplace *111122223333* por el ID de Cuenta de AWS de la cuenta de administración de AWS Organizations:

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

Designación de un administrador delegado para Respuesta frente a incidencias de seguridad de AWS

En esta sección se indican los pasos para designar un administrador delegado en la organización de Respuesta frente a incidencias de seguridad de AWS.

Como administrador de la organización de AWS, asegúrese de leer las Recomendaciones y consideraciones sobre cómo funciona una cuenta de administrador delegado de Respuesta ante incidentes de seguridad. Antes de continuar, asegúrese de contar con Permisos necesarios para designar una cuenta de administrador delegado de Respuesta ante incidentes de seguridad.

Elija un método de acceso preferente para designar una cuenta de administrador delegado de Respuesta ante incidentes de seguridad para la organización. Solo una cuenta de administración puede llevar a cabo este paso.

Console

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

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

API/CLI

- Ejecute CreateMembership con las credenciales de la Cuenta de AWS de administración de la organización.
  - También puede utilizar la AWS Command Line Interface para hacerlo. El siguiente comando de la AWS CLI designa una cuenta de administrador delegado de Respuesta ante incidentes de seguridad. A continuación se muestran 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 el servicio Respuesta frente a incidencias de seguridad de AWS no está habilitado en su cuenta de administrador delegado de Respuesta ante incidentes de seguridad, no podrá llevar a cabo ninguna acción. Si aún no lo ha hecho, asegúrese de habilitar Respuesta frente a incidencias de seguridad de AWS para la cuenta de administrador delegado de Respuesta ante incidentes de seguridad recién designada.

Cómo agregar miembros a Respuesta frente a incidencias de seguridad de AWS

Existe una relación de uno a uno entre AWS Organizations y su membresía de Respuesta frente a incidencias de seguridad de AWS. A medida que se agreguen (o eliminen) cuentas de Organizations,

esto se reflejará en las cuentas cubiertas de su membresía de Respuesta frente a incidencias de seguridad de AWS.

Para agregar una cuenta a su membresía, siga una de las opciones de administración de cuentas en una organización con AWS Organizations.

Eliminación de miembros de Respuesta frente a incidencias de seguridad de AWS

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

Amazon EventBridge

Con Amazon EventBridge, puede reaccionar ante los eventos asociados a los casos y las membresías de Respuesta frente a incidencias de seguridad de AWS, así como supervisarlos y orquestarlos. Puede redirigir estos eventos a través de reglas (para escenarios de distribución ramificada a uno o más destinos) o a través de canalizaciones (para integraciones punto a punto con capacidades mejoradas de filtrado, enriquecimiento y transformación).

Puede crear integraciones entre Respuesta ante incidentes de seguridad y herramientas de terceros o agregar datos para analizarlos mediante la IA generativa y otras herramientas de AWS. Por ejemplo, cuando Respuesta ante incidentes de seguridad crea un caso de forma proactiva, puede usar las automatizaciones de EventBridge para desencadenar los sistemas y notificar a las partes interesadas. Además, si administra varios entornos de AWS, puede utilizar la integración de Amazon EventBridge para supervisar las membresías de Respuesta frente a incidencias de seguridad de AWS y garantizar que todos los entornos mantengan una postura de seguridad sólida.

Para obtener más información, puede consultar What is Amazon EventBridge?

Contenido

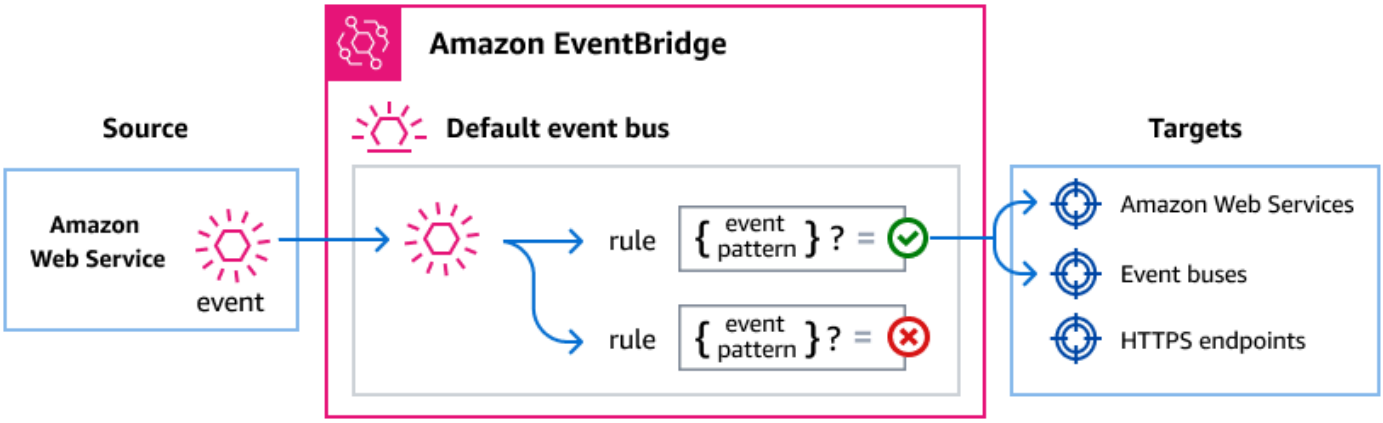
- Administración de eventos de Respuesta ante incidentes de seguridad mediante Amazon EventBridge
- Uso de eventos de Respuesta frente a incidencias de seguridad de AWS
- Tutorial: envío de alertas de Amazon Simple Notification Service para eventos Membership Updated

Administración de eventos de Respuesta ante incidentes de seguridad mediante Amazon EventBridge

Amazon EventBridge es un servicio sin servidor que utiliza eventos para conectar los componentes de la aplicación entre sí, lo que facilita la creación de aplicaciones escalables basadas en eventos. La arquitectura basada en eventos es un estilo de creación de sistemas de software de acoplamiento flexible que funcionan juntos emitiendo eventos y respondiendo a ellos. Los eventos representan un cambio en un recurso o entorno.

Así es como funciona:

Como ocurre con muchos servicios de AWS, Respuesta ante incidentes de seguridad genera y envía eventos al bus de eventos predeterminado de EventBridge. (El bus de eventos predeterminado se aprovisiona de manera automática en su cuenta de AWS). Un bus de eventos es un enrutador que recibe eventos y los envía a cero o más destinos u objetivos. Las reglas que se especifican al bus de eventos evalúan los eventos a medida que llegan. Cada regla comprueba si un evento coincide con el patrón de evento de la regla. Si el evento coincide, el bus de eventos envía el evento a los destinos especificados.



Entrega de eventos de Respuesta ante incidentes de seguridad mediante reglas de EventBridge

Para que el bus de eventos predeterminado de EventBridge envíe los eventos de Respuesta ante incidentes de seguridad a un destino, debe crear una regla. Cada regla contiene un patrón de eventos, que EventBridge compara con cada evento recibido en el bus de eventos. Si los datos del evento coinciden con el patrón de evento especificado, EventBridge entrega ese evento al o a los destinos de la regla.

Para obtener instrucciones detalladas sobre cómo crear reglas de bus de eventos, consulte Creating rules that react to events en la Guía del usuario de Amazon EventBridge.

Creación de patrones de eventos que coincidan con los eventos de Respuesta ante incidentes de seguridad

Cada patrón de eventos es un objeto JSON que contiene:

- Un atributo `source` que identifica el servicio que envía el evento. En el caso de los eventos de Respuesta ante incidentes de seguridad, el origen es `"aws.security-ir"`.

- (Opcional): un atributo `detail-type` que contiene una matriz de los tipos de eventos que deben coincidir.
- (Opcional): un atributo `detail` que contiene cualquier otro dato de evento con el que coincidir.

Por ejemplo, el siguiente patrón de eventos coincide con todos los eventos de `Case Updated by Respuesta frente a incidencias de seguridad de AWS Service` de una Cuenta de AWS especificada:

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T03:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "security-ir.amazonaws.com"
  }
}
```

Para obtener más información sobre la escritura de los patrones de eventos, consulte Patrones de eventos en la Guía del usuario de EventBridge.

Referencia de detalles de los eventos de Respuesta ante incidentes de seguridad

Todos los eventos de los servicios de AWS tienen un conjunto común de campos que contienen metadatos sobre el evento, como el servicio de AWS que es el origen del evento, la hora en que se generó el evento, la cuenta y la región en las que tuvo lugar el evento, etc. Para ver las definiciones de estos campos generales, consulte Event structure reference en la Guía del usuario de Amazon EventBridge.

Además, cada evento tiene un campo `detail` que contiene datos específicos de ese evento en particular. En la siguiente referencia se definen los campos de detalle para los distintos eventos de Respuesta ante incidentes de seguridad.

Al usar EventBridge para seleccionar y administrar eventos de Respuesta ante incidentes de seguridad, es útil tener en cuenta lo siguiente:

- El campo `source` de todos los eventos de Respuesta ante incidentes de seguridad está establecido en `"aws.security-ir"`.
- El campo `detail-type` especifica el tipo de evento.

  Por ejemplo, `"Case Updated"`.
- El campo `detail` contiene los datos específicos de ese evento en particular.

Para obtener más información sobre cómo crear patrones de eventos que permitan que las reglas coincidan con los eventos de Respuesta ante incidentes de seguridad, consulte Event patterns en la Guía del usuario de Amazon EventBridge.

Para obtener más información sobre los eventos y cómo EventBridge los procesa, consulte Eventos de EventBridge en la Guía del usuario de Amazon EventBridge.

Campos comunes: todos los eventos de Respuesta frente a incidencias de seguridad de AWS incluyen estos campos estándar de Amazon EventBridge:

- version: versión del formato de evento de EventBridge.
- id: identificador único del evento.
- detail-type: descripción inteligible del tipo de evento.
- source: siempre “aws.security-ir” para los eventos de Respuesta ante incidentes de seguridad.
- account: ID de la cuenta de AWS en la que se produjo el error.
- time: marca temporal ISO 8601 de cuando se produjo el evento.
- region: Región de AWS en la que está el recurso.
- resources: matriz que contiene el ARN del recurso afectado.

Campos de detalle: el objeto `detail` contiene información específica de Respuesta ante incidentes de seguridad:

- caseId: identificador único del caso (solo para eventos de casos).

- membershipId: identificador único de la membresía (solo para eventos de membresías).
- updatedBy: persona que llevó a cabo la actualización (solo para eventos de actualización de casos y comentarios).
- createdBy: persona que creó la entidad (solo para eventos de creación de casos y comentarios).

Valores del agente: los campos `updatedBy` y `createdBy` pueden contener:

- AWS Responder: acción que lleva a cabo un miembro del equipo de seguridad de AWS.
- *`security-ir.amazonaws.com`*: acción que el servicio lleva a cabo automáticamente.
- ID de cuenta: acción que lleva a cabo el cliente (por ejemplo, “111122223333”).

Valores de ARN de recursos: los recursos de Respuesta frente a incidencias de seguridad de AWS utilizan estos formatos de ARN:

- Casos: `arn:aws:security-ir:{region}:{account-id}:case/{case-id}`.
- Membresías: `arn:aws:security-ir:{region}:{account-id}:membership/{membership-id}`.

Eventos de casos

Caso creado por un miembro del equipo de respuesta de AWS

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T00:00:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "AWS Responder"
  }
}
```

Caso creado por un servicio

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T00:00:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "security-ir.amazonaws.com"
  }
}
```

Caso creado por un cliente

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T00:00:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "111122223333"
  }
}
```

Caso actualizado por un miembro del equipo de respuesta de AWS

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T01:30:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "AWS Responder"
  }
}
```

Caso actualizado por un cliente de AWS

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:15:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "111122223333"
  }
}
```

Caso actualizado por un servicio de Respuesta frente a incidencias de seguridad de AWS

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T03:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "security-ir.amazonaws.com"
  }
}
```

Caso cerrado

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Closed",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-15T14:22:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890"
  }
}
```

Eventos de comentarios de casos

Comentario del caso creado por un miembro del equipo de respuesta de AWS

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T04:30:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "AWS Responder"
  }
}
```

Comentario del caso creado por un cliente

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:15:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "111122223333"
  }
}
```

Comentario del caso creado por un servicio de Respuesta frente a incidencias de seguridad de AWS

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:15:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "security-ir.amazonaws.com"
  }
}
```

Comentario del caso actualizado por un cliente

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "111122223333"
  }
}
```

Comentario del caso actualizado por un servicio de Respuesta frente a incidencias de seguridad de AWS

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "security-ir.amazonaws.com"
  }
}
```

Comentario del caso creado por un miembro del equipo de respuesta de AWS

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "AWS Responder"
  }
}
```

Eventos de membresías

Membresía creada

```
            {
              "version": "0",
              "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
              "detail-type": "Membership Created",
              "source": "aws.security-ir",
              "account": "111122223333",
              "time": "2023-04-01T10:00:00Z",
              "region": "us-west-2",
              "resources": [
                "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
              ],
              "detail": {
                "membershipId": "m-1234567890abcdef0"
              }
            }
```

Membresía actualizada

```
            {
              "version": "0",
              "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
              "detail-type": "Membership Updated",
              "source": "aws.security-ir",
              "account": "111122223333",
              "time": "2023-04-15T16:30:00Z",
              "region": "us-west-2",
              "resources": [
                "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
              ],
              "detail": {
                "membershipId": "m-1234567890abcdef0"
              }
            }
```

Membresía cancelada

```
            {
              "version": "0",
              "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
              "detail-type": "Membership Closed",
              "source": "aws.security-ir",
              "account": "111122223333",
              "time": "2023-06-30T23:59:59Z",
              "region": "us-west-2",
              "resources": [
                "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
              ],
              "detail": {
                "membershipId": "m-1234567890abcdef0"
              }
            }
```

Membresía terminada

```
            {
              "version": "0",
              "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
              "detail-type": "Membership Terminated",
              "source": "aws.security-ir",
              "account": "111122223333",
              "time": "2023-07-01T00:00:00Z",
              "region": "us-west-2",
              "resources": [
                "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
              ],
              "detail": {
                "membershipId": "m-1234567890abcdef0"
              }
            }
```

Uso de eventos de Respuesta frente a incidencias de seguridad de AWS

Puede crear reglas de EventBridge para que coincidan con estos eventos y desencadenen acciones automatizadas. A continuación se muestran algunos ejemplos de casos de uso:

Coincidir con todos los eventos de Respuesta frente a incidencias de seguridad de AWS:

```
{
  "source": ["aws.security-ir"]
}
```

Coincidir solo con los eventos de casos:

```
{
  "source": ["aws.security-ir"],
  "detail-type": [
    "Case Created",
    "Case Updated",
    "Case Closed",
    "Case Comment Created",
    "Case Comment Updated"
  ]
}
```

Coincidir con los casos actualizados por miembros del equipo de respuesta de AWS:

```
{
  "source": ["aws.security-ir"],
  "detail-type": ["Case Updated"],
  "detail": {
    "updatedBy": ["AWS Responder"]
  }
}
```

Coincidir los eventos de un caso específico:

```
{
  "source": ["aws.security-ir"],
  "detail": {
    "caseId": ["1234567890"]
  }
}
```

Tutorial: envío de alertas de Amazon Simple Notification Service para eventos **`Membership Updated`**

En este tutorial, configura una regla de evento de Amazon EventBridge que solo captura eventos en los que la suscripción pasa al estado `Membership Updated`.

Requisitos previos

En este tutorial se presupone que tiene una suscripción activa y cuentas de AWS activas en su membresía.

Temas

- Tutorial: creación de un tema de Amazon SNS y suscribirse a él
- Tutorial: registro de una regla de eventos
- Tutorial: prueba de la regla
- Regla alternativa: actualizaciones de casos de Respuesta ante incidentes de seguridad

Tutorial: creación de un tema de Amazon SNS y suscribirse a él

Para este tutorial, se configura un tema de Amazon SNS para utilizarse como destino de eventos para la nueva regla de eventos.

Para crear un tema de Amazon SNS

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. Seleccione Topics (Temas), Create topic (Creación de tema).
3. En Tipo, seleccione Estándar.

4. Para Nombre, escriba **`MembershipUpdated`** y, a continuación, elija Creación de tema.
5. En la pantalla MembershipUpdated, elija Crear una suscripción.
6. En Protocolo, seleccione Correo electrónico.
7. En Endpoint (Punto de conexión), ingrese una dirección de email a la que actualmente tenga acceso y elija Create subscription (Creación de suscripción).
8. Consulte su cuenta de correo electrónico y espere para recibir un mensaje de correo electrónico de confirmación de la suscripción. Cuando lo reciba, seleccione Confirmar suscripción.

Tutorial: registro de una regla de eventos

A continuación, registre una regla de eventos que solo capture los eventos `Membership Updated`.

Para registrar su regla de EventBridge

1. Abra la consola de Amazon EventBridge en https://console.aws.amazon.com/events/.
2. En el panel de navegación, seleccione Reglas.
3. Elija Creación de regla.
4. Escriba un nombre y una descripción para la regla.

> **Note**
>
> Una regla no puede tener el mismo nombre que otra regla de la misma región y del mismo bus de eventos.

5. En Bus de eventos, seleccione el bus de eventos que desea asociar a esta regla. Si desea que esta regla coincida con eventos procedentes de su cuenta, seleccione Bus de eventos predeterminado de AWS. Cuando un servicio de AWS en su cuenta emite un evento, siempre va al bus de eventos predeterminado de su cuenta.

> **Note**
>
> Esto debe configurarse en su cuenta de AWS Organizations o de administrador delegado en la que creó la membresía de Respuesta frente a incidencias de seguridad de AWS.

6. En Tipo de regla, elija Regla con un patrón de evento.
7. Seleccione Siguiente.

8. En Origen del evento, seleccione Otro.
9. En Patrón de eventos, seleccione Patrones personalizados (editor de JSON).
10. Pegue el siguiente patrón de eventos en el área de texto.

```
{
  "source": ["aws.security-ir"],
  "detail-type": ["Membership Updated"]
}
```

Este código define una regla de EventBridge que coincide con cualquier evento en el que se actualice o modifique la membresía del servicio. Para obtener más información sobre los patrones de eventos, consulte Eventos y patrones de eventos en la Guía del usuario de Amazon EventBridge.

11. Elija Siguiente.
12. En Tipos de destino, seleccione Servicio de AWS.
13. En Seleccione un destino, elija Tema de SNS y, en Tema, elija MembershipUpdated.
14. (Opcional) En Configuración adicional, haga lo siguiente:

    a. En Antigüedad máxima del evento, indique un valor entre un minuto (00:01) y 24 horas (24:00).

    b. En Cantidad de reintentos, indique un número entre 0 y 185.

    c. En Cola de mensajes falidos, seleccione si desea utilizar una cola de Amazon SQS estándar como cola de mensajes fallidos. EventBridge envía eventos que coincidan con esta regla a la cola de mensajes fallidos si no se entregan correctamente al destino. Realice una de las siguientes acciones:

    - Seleccione Ninguna para no usar una cola de mensajes fallidos.
    - Elija Seleccionar una cola de Amazon SQS en la cuenta de AWS actual para usarla como cola de mensajes fallidos y luego seleccione de la lista desplegable la cola que quiera usar.
    - Elija Seleccionar una cola de Amazon SQS en otra cuenta de AWS como cola de mensajes fallidos y luego ingrese el ARN de la cola que quiera usar. Debe asociar una política basada en recursos a la cola que conceda permiso a EventBridge para enviarle mensajes. Para obtener más información, consulte Concesión de permisos a la cola de mensajes fallidos en la Guía del usuario de Amazon EventBridge.

15. Elija Siguiente.
16. (Opcional) Introduzca una o varias etiquetas para la regla. Para obtener más información, consulte Etiquetas de Amazon EventBridge en la Guía del usuario de Amazon EventBridge.
17. Elija Siguiente.
18. Revise los detalles de la regla y seleccione Creación de regla.

Tutorial: prueba de la regla

Para probar la regla, envíe una actualización de su membresía de Respuesta frente a incidencias de seguridad de AWS. Si su regla está configurada correctamente, debería recibir un mensaje de correo electrónico en unos minutos con el texto del evento.

Regla alternativa: actualizaciones de casos de Respuesta ante incidentes de seguridad

Para crear una regla de eventos que supervise todas las actualizaciones de casos, repita estos tutoriales con las siguientes modificaciones:

1. En Tutorial: creación de un tema de Amazon SNS y suscribirse a él, utilice *CaseUpdates* como nombre del tema.
2. En Tutorial: registro de una regla de eventos, utilice el siguiente patrón en el editor JSON:

```
{
  "source": ["aws.security-ir"],
  "detail-type": [
    "Case Created",
    "Case Updated",
    "Case Closed",
    "Case Comment Created",
    "Case Comment Updated"
  ]
}
```

Solución de problemas

Si tiene problemas relacionados con una acción específica de Respuesta frente a incidencias de seguridad de AWS, consulte los temas de esta sección.

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

Contenido

- Problemas
- Errores
- Soporte

Problemas

Las solicitudes no se envían desde el contexto correcto

Todas las llamadas a las API de Respuesta frente a incidencias de seguridad de AWS deben provenir de una entidad principal de IAM de la cuenta de administrador delegado o de membresía del servicio. Asegúrese de que esté operando desde la entidad principal de IAM correcta de la Cuenta de AWS que sea la cuenta de administrador delegado o de membresía de Respuesta frente a incidencias de seguridad de AWS de la organización.

Errores

AccessDeniedException

No tiene acceso suficiente para realizar esta acción.

Trabaje con su administrador de AWS para asegurarse de que tiene permiso para asumir un rol de IAM en su cuenta de administrador delegado o de membresía de Respuesta frente a incidencias de seguridad de AWS. Compruebe también que el rol tenga una política de IAM que permita la acción solicitada. Para obtener más información, consulte Respuesta frente a incidencias de seguridad de AWS IAM.

ConflictException

La solicitud provoca un estado incoherente.

Compruebe que los nombres de los archivos adjuntos al caso o los miembros predeterminados del equipo de respuesta que haya especificado sean únicos. Compruebe también que su membresía del servicio Respuesta frente a incidencias de seguridad de AWS aún no esté configurada. Abra la consola de Respuesta ante incidentes de seguridad en https://console.aws.amazon.com/security-ir/ y acceda a `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, abra un caso con Soporte.

ResourceNotFoundException

La solicitud hace referencia a un recurso que no existe.

Uno o varios de los recursos especificados en la solicitud no existen. Compruebe que todos los ARN o ID de los recursos proporcionados sean correctos. Esto se aplica a los ID de AWS Organizations, ID de cuentas, roles de IAM, membresías, casos, miembros del equipo de respuesta, casos, personal de respuesta a casos, archivos adjuntos de casos y comentarios de casos.

ThrottlingException

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

Su entidad principal de IAM ha hecho demasiadas solicitudes a esa función de la API en un periodo especificado. Espere un minuto e inténtelo de nuevo. Si el problema persiste, considere la posibilidad de implementar un algoritmo de retroceso exponencial y reintento.

ValidationException

La entrada no satisface las limitaciones que especifica un Servicio de AWS.

Uno o varios de los campos de datos de su solicitud no cumplían con los requisitos de validación o combinación lógica. Compruebe que todos los ARN de los recursos se completen y que los valores de texto cumplan con las restricciones de tamaño y formato de la Guía de referencia de la API de Respuesta frente a incidencias de seguridad de AWS. Compruebe también que se permitan las actualizaciones de valores. Por ejemplo, no es posible cambiar un caso compatible con AWS para que sea un caso autoadministrado.

Soporte

Si necesita más ayuda, póngase en contacto con el centro de Soporte para solucionar problemas. Tenga la siguiente información disponible:

- La Región de AWS que usó.
- El ID de Cuenta de AWS 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 Respuesta frente a incidencias de seguridad de AWS
- Privacidad del tráfico entre redes
- Identity and Access Management
- Solución de problemas de identidades y accesos en Respuesta frente a incidencias de seguridad de AWS
- Uso de roles de servicio
- Cómo utilizar roles vinculados a servicios
- Políticas administradas de AWS
- Respuesta a incidentes
- Validación de conformidad
- Registro y supervisión en Respuesta ante incidentes de seguridad de AWS
- Resiliencia
- Seguridad de la infraestructura
- Configuración y análisis de vulnerabilidades
- Prevención de la sustitución confusa entre servicios

Protección de datos en Respuesta frente a incidencias de seguridad de AWS

Contenido

- Cifrado de datos

El Modelo de responsabilidad compartida de AWS se aplica a la protección de datos para el servicio Respuesta ante incidentes de seguridad de AWS. Tal como se describe en este modelo, AWS es responsable de proteger la infraestructura que ejecuta los servicios que se ofrecen en la nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También es responsable de la configuración de seguridad y de las tareas de administración para los servicios de AWS que utiliza. Para obtener más información sobre la privacidad de datos, consulte Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de

datos en Europa, consulte la publicación del blog AWSModelo de responsabilidad compartida de y RGPDAWS en el blog de seguridad de .

A efectos de protección de datos, en las prácticas recomendadas de seguridad de AWS se establece que debe proteger las credenciales de las cuentas de AWS y configurar los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Utiliza SSL/TLS para comunicarse con los recursos de AWS. Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure el registro de la actividad del usuario y la API con AWS CloudTrail.
- Utilice las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de AWS.
- Actualmente, el servicio no admite FIPS 140-3.

No debe ingresar nunca información confidencial, como sus direcciones de correo electrónico, en etiquetas o campos de texto de formato libre, como el campo Nombre. Esto incluye cuando trabaje con AWS Support u otros servicios de AWS mediante la consola, la API, la AWS CLI o los AWS SDK. Cualquier dato que ingrese en etiquetas o campos de texto de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Cifrado de datos

Contenido

- Cifrado en reposo
- Cifrado en tránsito
- Administración de claves

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

Respuesta frente a incidencias de seguridad de AWS recopila y accede a los datos exclusivamente a través de un canal protegido por seguridad de la capa de transporte (TLS).

Administración de claves

Respuesta frente a incidencias de seguridad de AWS implementa integraciones con AWS KMS para proporcionar cifrado en reposo para los datos de casos y archivos adjuntos.

Respuesta frente a incidencias de seguridad de AWS no admite las claves administradas por el cliente.

Privacidad del tráfico entre redes

Tráfico entre el servicio y las aplicaciones y clientes locales

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

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

El acceso a Respuesta frente a incidencias de seguridad de AWS a través de la red se realiza mediante las API publicadas por AWS. Los clientes deben admitir el protocolo de seguridad de la capa de transporte (TLS) 1.2. Nosotros recomendamos TLS 1.3. Los clientes también deben admitir conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Diffie-Hellman Ephemeral (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 a la hora de firmar solicitudes.

Tráfico entre recursos de AWS en la misma región

Un punto de conexión de Amazon Virtual Private Cloud (Amazon VPC) para Respuesta frente a incidencias de seguridad de AWS es una entidad lógica dentro de una VPC que permite conectividad solo a Respuesta frente a incidencias de seguridad de AWS. La VPC de Amazon dirige las solicitudes a Respuesta frente a incidencias de seguridad de AWS y vuelve a dirigir las respuestas a la VPC. Para obtener más información, consulte Puntos de enlace de la VPC en la Guía del usuario de Amazon VPC. Para consultar ejemplos de políticas que puede usar para controlar el acceso desde los puntos de conexión de VPC, consulte Uso de políticas de IAM para controlar el acceso a DynamoDB.

> **Note**
>
> No se puede acceder a los puntos de conexión de VPC 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 servicio de AWS que ayuda a los administradores a controlar el acceso a los recursos de AWS. Los administradores de IAM controlan las entidades principales autenticadas (han iniciado sesión) y autorizadas (tienen permisos) para utilizar recursos de Respuesta frente a incidencias de seguridad de AWS. IAM es un servicio de AWS que puede utilizar sin cargo adicional.

Contenido

- Autenticación con identidades
- Funcionamiento de Respuesta frente a incidencias de seguridad de AWS con IAM

Público

La forma en que utilice AWS Identity and Access Management (IAM) difiere en función del trabajo que realice en Respuesta frente a incidencias de seguridad de AWS.

Administradores de seguridad

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

Observadores de casos

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

Miembros del equipo de respuesta ante incidentes

A los miembros del equipo se les puede otorgar tanto acceso completo a la membresía como a los casos. Se recomienda que no todas las personas tengan capacidad de decisión sobre la membresía del servicio, pero que tengan acceso a todos y cada uno de los casos que se creen y administren a través del servicio. Para obtener más información, consulte Respuesta frente a incidencias de seguridad de AWS managed policies.

Autenticación con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales de identidad. Debe estar autenticado (haber iniciado sesión en AWS) como usuario raíz de la cuenta de AWS, como un usuario de IAM o asumiendo un rol de IAM.

Puede iniciar sesión en AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS Los usuarios de IAM Identity Center (IAM 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 una identidad federada, su gestionador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accede a AWS mediante la federación, está asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en la Consola de administración de AWS o en el portal de acceso de AWS. Para obtener más información sobre el inicio de sesión en AWS, consulte How to sign in to your AWS account en la Guía del usuario de Inicio de sesión en AWS.

Si accede a AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de la línea de comandos (CLI) para firmar criptográficamente las solicitudes mediante el uso de las credenciales. Si no usa las herramientas de AWS, debe firmar las solicitudes. Para obtener más información sobre la firma de solicitudes, consulte Firma de solicitudes API de AWS en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, AWS le recomienda el uso de la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte

Multi-factor authentication en la Guía del usuario de AWS IAM Identity Center y Autenticación multifactor de AWS en IAM en la Guía del usuario de IAM.

usuario raíz de la cuenta de AWS

Cuando se crea una cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todos los servicios y recursos de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la cuenta de AWS y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizó para crear la cuenta. No utilice nunca el usuario raíz para las tareas diarias y tome medidas para proteger las credenciales de su usuario raíz. Utilícelo únicamente para llevar a cabo las tareas que solo puede efectuar el usuario raíz. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulta Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

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

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web, AWS Directory Service, el directorio de Identity Center o cualquier usuario que acceda a los servicios de AWS con credenciales proporcionadas a través de un origen de identidades. Cuando identidades federadas acceden a AWS, asumen roles y los roles proporcionan credenciales temporales.

Para una administración de acceso centralizada, 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 propio origen de identidades para usarlos en todas sus cuentas y aplicaciones de AWS. Para obtener más información sobre IAM Identity Center, consulte What is IAM Identity Center? en la Guía del usuario de AWS IAM Identity Center.

Usuarios y grupos de IAM

Un usuario de IAM es una identidad de la cuenta de AWS que dispone de permisos específicos para una sola persona o aplicación. Recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. Si tiene un caso de uso específico que requiera credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para 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 grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puedes iniciar sesión como grupo. Puedes usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

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 permanentes a largo plazo y los roles proporcionan credenciales temporales. Para obtener más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad de la cuenta de AWS que dispone de permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente un rol de IAM en la Consola de administración de AWS si cambia de roles. Puede asumir un rol realizando una llamada a una operación de AWS CLI o de la API de AWS, o bien utilizando una URL personalizada. Para más información sobre 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, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener más información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidad externo en la Guía del usuario de IAM. Si utiliza IAM Identity Center, configura un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué puede acceder las identidades después de autenticarse. Para obtener más información sobre los conjuntos de permisos, consulte Permission sets en la Guía del usuario de AWS IAM Identity Center.
- Permisos de usuario de IAM temporales: un usuario o rol de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan llevar a cabo una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunos servicios de AWS, puede asociar

una política directamente a un recurso (en lugar de utilizar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulta Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

- Acceso entre servicios: algunos servicios de AWS utilizan características de otros servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común 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.
  - Rol de servicio: un rol de servicio es un rol de IAM que asume un servicio para llevar a cabo 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.
  - Rol vinculado a un servicio: un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un servicio de 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.
- Aplicaciones que se ejecutan en Amazon EC2: puede utilizar un rol de IAM para administrar credenciales temporales para las aplicaciones que se ejecutan en una instancia de EC2 y envían solicitudes a la AWS CLI o a la API de AWS. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar un rol de AWS a una instancia de EC2 y ponerla a disposición de sus aplicaciones, cree 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 de EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre cuándo usar los roles o usuarios de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Funcionamiento de Respuesta frente a incidencias de seguridad de AWS con IAM

AWS Identity and Access Management (IAM) es un servicio de AWS que ayuda a los administradores a controlar de forma segura el acceso a los recursos de AWS. Los administradores

de IAM controlan quién puede estar autenticado (iniciar sesión) y autorizado (tener permisos) para utilizar los recursos de Respuesta ante incidentes de seguridad de AWS. IAM es un servicio de AWS que puede utilizar sin cargo adicional.

Características de IAM que puede utilizar con Respuesta ante incidentes de seguridad de AWS	
Característica de IAM	Alineación de servicios
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condiciones de políticas	Sí (global)
ACL	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	No
Roles vinculados al servicio	Sí

Contenido

- Políticas de Respuesta frente a incidencias de seguridad de AWS basadas en identidades
- Claves de condición de políticas para Respuesta ante incidentes de seguridad de AWS
- Listas de control de acceso (ACL) en Respuesta frente a incidencias de seguridad de AWS

Políticas de Respuesta frente a incidencias de seguridad de AWS basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, 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 y los recursos permitidos o denegados, así como 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 los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Contenido

- Ejemplos de políticas basadas en identidades
- Prácticas recomendadas sobre las políticas
- Mediante la consola de Respuesta frente a incidencias de seguridad de AWS
- Cómo permitir a los usuarios consultar sus propios permisos
- Políticas basadas en recursos
- Acciones de política

Ejemplos de políticas basadas en identidades

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de Respuesta frente a incidencias de seguridad de AWS. Tampoco pueden llevar a cabo tareas mediante la Consola de administración de AWS, la Interfaz de la línea de comandos de AWS (AWS CLI) ni la API de AWS. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para llevar a cabo acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Para obtener más información sobre acciones y tipos de recursos definidos por Respuesta ante incidentes de seguridad de AWS, incluido el formato de los ARN para cada tipo de recurso, consulte Actions, resources, and condition keys for Respuesta frente a incidencias de seguridad de AWS en la Referencia de autorizaciones de servicio.

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar los recursos de Respuesta frente a incidencias de seguridad de AWS de la cuenta. Estas acciones pueden generar costos adicionales para su cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

Comienza con las políticas administradas por AWSy continúa con los permisos de privilegio mínimo: a fin de comenzar a conceder permisos a los usuarios y las cargas de tarea, utiliza las políticas administradas por AWS, que conceden permisos para muchos casos de uso comunes. Están disponibles en su cuenta de AWS. Se recomienda definir políticas gestionadas por el cliente de AWS específicas para sus casos de uso a fin de reducir aún más los permisos. Con el fin de obtener más información, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea 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 pueden 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, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.

Utilice 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 políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puede usar condiciones para conceder acceso a acciones de servicios si se emplean a través de un servicio determinado de AWS como, por ejemplo, AWS CloudFormation. Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para

más información, consulte Política de validación de Analizador de acceso de IAM en la Guía de usuario de IAM.

Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesita un usuario raíz o usuarios de IAM en su cuenta de AWS, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

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

Mediante la consola de Respuesta frente a incidencias de seguridad de AWS

Para acceder a https://console.aws.amazon.com/security-ir/, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle registrar y consultar los detalles sobre los recursos de Respuesta frente a incidencias de seguridad de AWS en su cuenta de AWS. 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 conceda permisos mínimos para la consola a los usuarios que solo realizan llamadas a AWS CLI o a la API de AWS. En su lugar, permite el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Adjunte la política administrada por AWS Access o ReadOnly de Respuesta frente a incidencias de seguridad de AWS para asegurarse de que los usuarios y roles puedan utilizar la consola del 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 gestionadas 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 con AWS CLI o la API de AWS.

```
{
"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

Políticas basadas en recursos en Respuesta ante incidentes de seguridad de AWS

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores 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 Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones de política

Acciones de política para Respuesta frente a incidencias de seguridad de AWS

Compatibilidad con acciones de política: sí

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

El elemento Action de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API de AWS asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. 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 frente a incidencias de seguridad de AWS, consulte Actions defined by Respuesta frente a incidencias de seguridad de AWS en la Referencia de autorizaciones de servicio.

Las acciones de políticas de Respuesta frente a incidencias de seguridad de AWS utilizan el siguiente prefijo antes de la acción:

Respuesta frente a incidencias de seguridad de AWS -identity

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

"Action": ["Respuesta frente a incidencias de seguridad de AWS -identity:action1", "Respuesta frente a incidencias de seguridad de AWS -identity:action2"]

Recursos de políticas para Respuesta ante incidentes de seguridad de Amazon AWS

Compatibilidad con recursos de políticas: sí. Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento Resource de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben incluir un elemento Recurso o un elemento No recurso. Como práctica

recomendada, especifique un recurso utilizando el 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 políticas para Respuesta ante incidentes de seguridad de AWS

Compatibilidad con claves de condición de políticas específicas del servicio: no

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

El elemento Condition (o bloque Condition) permite especificar condiciones en las que entra en vigor una instrucción. 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 Condition en una instrucción o varias claves en un único elemento Condition, AWS las evalúa mediante una operación lógica AND. Si especifica varios valores para una única clave de condición, AWS evalúa la condición con una operación lógica OR. 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, puedes conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulta 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 globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.

Listas de control de acceso (ACL) en Respuesta frente a incidencias de seguridad de AWS

Compatibilidad con ACL: no

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Control de acceso basado en atributos (ABAC) con Respuesta ante incidentes de seguridad de AWS

Compatibilidad con ABAC (etiquetas en políticas): sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puedes adjuntar etiquetas a entidades de IAM (usuarios o roles) y a muchos recursos de AWS. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, diseña las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder. ABAC es útil en entornos que crecen rápidamente y ayuda en situaciones en las que la administración de políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política mediante las claves de condición AWS:ResourceTag/key-name, AWS:RequestTag/key-name o 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 sobre ABAC, consulte What is ABAC? en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Credenciales temporales con Respuesta ante incidentes de seguridad de Amazon AWS

Compatibilidad con credenciales temporales: sí

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

Puede crear credenciales temporales de forma manual mediante la AWS CLI o la API de AWS. A continuación, puedes usar esas credenciales temporales para acceder a AWS. AWS recomienda

generar credenciales temporales de forma dinámica en lugar de usar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Sesiones de acceso directo para Respuesta ante incidentes de seguridad de Amazon AWS

Admite sesiones de acceso directo (FAS): sí

Cuando utiliza un usuario o un rol de IAM para llevar a cabo acciones en AWS, se le considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos de la entidad principal para llamar a un servicio deAWS, combinados con el servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros servicios o recursos de AWS para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Solución de problemas de identidades y accesos en Respuesta frente a incidencias de seguridad de AWS

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con Respuesta ante incidentes de seguridad de AWS y IAM.

Temas

- No tengo autorización para realizar una acción
- No tengo autorización para realizar la operación iam:PassRole
- Deseo permitir que personas ajenas a mi cuenta de AWS puedan acceder a mis recursos de Respuesta frente a incidencias de seguridad de AWS

No tengo autorización para llevar a cabo una 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.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM mateojackson intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio my-example-widget, pero no tiene los permisos ficticios de :GetWidget de Respuesta ante incidentes de seguridad de AWS.

User: arn:AWS:iam::123456789012:user/mateojackson is not authorized to perform: Respuesta frente a incidencias de seguridad de AWS :GetWidget on resource: my-example-widget

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

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

No tengo autorización para llevar a cabo iam:PassRole Si recibe un error que indica que no tiene autorización para llevar a cabo la acción iam:PassRole, sus políticas deben actualizarse para permitirle pasar un rol a Respuesta frente a incidencias de seguridad de AWS.

Algunos servicios de AWS le permiten transferir un rol existente a dicho servicio en lugar de crear un nuevo rol de servicio o uno vinculado al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM llamado marymajor intenta utilizar la consola para llevar a cabo una acción en Respuesta ante incidentes de seguridad de AWS. 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.

User: arn:AWS:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole

En este caso, las políticas de Mary se deben actualizar para permitirle llevar a cabo la acción iam:PassRole. Si necesita ayuda, póngase en contacto con su gestionador de AWS. El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

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

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

Para obtener más información, consulte lo siguiente:

- Para obtener información sobre si Respuesta frente a incidencias de seguridad de AWS de Amazon es compatible con estas características, consulte How AWS Security Incident Response works with IAM.

- Para obtener información acerca de cómo proporcionar acceso a los recursos de las cuentas de AWS de su propiedad, consulte Proporcionar acceso a un usuario de IAM a otra cuenta de AWS de la que es propietario en la Guía del usuario de IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos a cuentas de AWS de terceros, consulte Proporcionar acceso a cuentas de AWS que son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulta Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Uso de roles de servicio

Compatible con roles 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 puedes 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.

Cómo utilizar roles vinculados a servicios

Roles vinculados a servicios de Respuesta frente a incidencias de seguridad de AWS

Contenido

- SLR de AWS: AWSServiceRoleForSecurityIncidentResponse
- SLR de AWS: AWSServiceRoleForSecurityIncidentResponse_Triage
- Regiones admitidas para los roles vinculados a un servicio de Respuesta frente a incidencias de seguridad de AWS

Admite roles vinculados a servicios: sí

Una función vinculada a un servicio es un tipo de función del servicio que está vinculado a un servicio de 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.

Con un rol vinculado a servicios, resulta más sencillo configurar Respuesta frente a incidencias de seguridad de AWS, porque no es preciso agregar los permisos necesarios manualmente. Respuesta frente a incidencias de seguridad de AWS define los permisos de los roles vinculados con su propio servicio y, a menos que esté definido de otra manera, solo Respuesta frente a incidencias de seguridad de AWS puede asumir sus roles. 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 roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestren Sí en la columna Roles vinculados a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

SLR de AWS: AWSServiceRoleForSecurityIncidentResponse

Respuesta frente a incidencias de seguridad de AWS utiliza el rol vinculado a servicios (SLR) denominado AWSServiceRoleForSecurityIncidentResponse y la política de Respuesta frente a incidencias de seguridad de AWS para identificar las cuentas suscritas, crear casos y etiquetar los recursos relacionados.

Permisos

El rol vinculado a servicios AWSServiceRoleForSecurityIncidentResponse confía en el siguiente servicio para asumir el rol:

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

La política administrada por AWS denominada AWSSecurityIncidentResponseServiceRolePolicy está adjunta a este rol. El servicio usa el rol para llevar a cabo acciones en los siguientes recursos:

- AWS Organizations: permite que el servicio busque cuentas de membresía para usarlas con el servicio.
- CreateCase: permite al servicio crear casos de servicio en nombre de las cuentas de membresía.
- TagResource: permite al servicio etiquetar recursos configurados como parte del servicio.

Administración del rol

No necesita crear manualmente un rol vinculado a servicios. Cuando se incorpora a Respuesta frente a incidencias de seguridad de AWS en la AWS Management Console, la AWS CLI o la API de AWS, el servicio se encarga de crear el rol vinculado a servicios.

> **Note**
>
> Si creó una membresía con una cuenta de administrador delegado, los roles vinculados a servicios deberán crearse manualmente en las cuentas de administración de 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. Al incorporarse al servicio, este se encarga nuevamente de crear el rol vinculado a servicios.

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

SLR de AWS: AWSServiceRoleForSecurityIncidentResponse_Triage

Respuesta frente a incidencias de seguridad de AWS utiliza el rol vinculado a servicios (SLR) denominado AWSServiceRoleForSecurityIncidentResponse_Triage y la política de Respuesta frente a incidencias de seguridad de AWS para supervisar continuamente su entorno en busca de amenazas de seguridad, ajustar los servicios de seguridad para reducir el ruido de las alertas y recopilar información para investigar posibles incidentes.

Permisos

El rol vinculado a servicios AWSServiceRoleForSecurityIncidentResponse_Triage confía en que los siguientes servicios asuman el rol:

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

La política administrada por AWS AWSSecurityIncidentResponseTriageServiceRolePolicy está adjunta a este rol. El servicio usa el rol para llevar a cabo acciones en los siguientes recursos:

- Eventos: permite al servicio crear una regla administrada de Amazon EventBridge. Esta regla es la infraestructura necesaria en su cuenta de AWS para enviar eventos desde su cuenta al servicio. Esta acción se lleva a cabo en cualquier recurso de AWS administrado 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 lleva a cabo en cualquier recurso de AWS.
- 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 lleva a cabo en cualquier recurso de AWS.

Administración del rol

No necesita crear manualmente un rol vinculado a servicios. Cuando se incorpora a Respuesta frente a incidencias de seguridad de AWS en la AWS Management Console, la AWS CLI o la API de AWS, el servicio se encarga de crear el rol vinculado a servicios.

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. Al incorporarse al servicio, este se encarga nuevamente de crear el rol vinculado a servicios.

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a un servicio de Respuesta frente a incidencias de seguridad de AWS

Respuesta frente a incidencias de seguridad de AWS admite el uso de roles vinculados a servicios 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 (París)
- UE (Estocolmo)
- Asia-Pacífico (Bombay)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Tokio)
- Canadá (centro)
- América del Sur (São Paulo)

Políticas administradas de AWS

Una política administrada de AWS es una política independiente que AWS crea y administra. Las políticas administradas de AWS se diseñan para ofrecer permisos para muchos casos de uso comunes, por lo que puede empezar a asignar permisos a los usuarios, grupos y roles.

Para agregar permisos a usuarios, grupos y roles, es más fácil utilizar las políticas administradas de AWS que escribirlas uno mismo. Se necesita tiempo y experiencia para crear políticas administradas por el cliente de IAM que le brinden a su equipo solo los permisos necesarios. Para comenzar a hacerlo con rapidez, puede utilizar nuestras políticas administradas de AWS. Estas políticas cubren casos de uso comunes y están disponibles en su cuenta de AWS. Para obtener más información sobre las políticas administradas de AWS, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

Los servicios de AWS mantienen y actualizan las políticas administradas por AWS asociadas. No puede cambiar los permisos en las políticas gestionadas de AWS. 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 AWScuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no quitan los permisos de una política administrada de AWS, por lo tanto, las actualizaciones de las políticas no deteriorarán los permisos existentes.

Además, AWS admite políticas administradas para funciones de trabajo que abarcan varios servicios. Por ejemplo, la política administrada de AWS ReadOnlyAccess proporciona acceso de solo lectura a todos los servicios y los recursos de AWS. Cuando un servicio lanza una nueva característica, AWS

agrega permisos de solo lectura para las operaciones y los recursos nuevos. Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte Políticas administradas de AWS para funciones de trabajo en la Guía del usuario de IAM.

Contenido

- Política administrada por AWS: AWSSecurityIncidentResponseServiceRolePolicy
- Política administrada por AWS: AWSSecurityIncidentResponseFullAccess
- Política administrada por AWS: AWSSecurityIncidentResponseReadOnlyAccess
- Política administrada por AWS: AWSSecurityIncidentResponseCaseFullAccess
- Política administrada por AWS: AWSSecurityIncidentResponseTriageServiceRolePolicy
- Actualizaciones de Respuesta frente a incidencias de seguridad de AWS en SLR y políticas administradas

Política administrada por AWS: AWSSecurityIncidentResponseServiceRolePolicy

Respuesta frente a incidencias de seguridad de AWS utiliza la política administrada por AWS AWSSecurityIncidentResponseServiceRolePolicy. Esta política administrada por AWS está adjunta al rol vinculado a servicios AWSServiceRoleForSecurityIncidentResponse. La política proporciona acceso para que Respuesta frente a incidencias de seguridad de AWS identifique las cuentas suscritas, cree casos y etiquete los recursos relacionados.

> **Important**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Respuesta frente a incidencias de seguridad de AWS usa etiquetas para proporcionarle servicios administrativos. Las etiquetas no se han diseñado para usarse con información privada o confidencial.

Detalles de los permisos

El servicio usa esta política para llevar a cabo acciones en los siguientes recursos:

- AWS Organizations: permite que el servicio busque cuentas de membresía para usarlas con el servicio.

- CreateCase: permite al servicio crear casos de servicio en nombre de las cuentas de membresía.
- TagResource: permite al servicio etiquetar recursos configurados como parte del servicio.

Puede ver los permisos asociados a esta política en políticas administradas por AWS para AWSSecurityIncidentResponseServiceRolePolicy.

Política administrada por AWS: AWSSecurityIncidentResponseFullAccess

Respuesta frente a incidencias de seguridad de AWS usa la política administrada por AWS AWSSecurityIncidentResponseAdmin. Esta política concede acceso completo a los recursos del servicio y acceso a los Servicios de AWS relacionados. Puede utilizar esta política con sus entidades principales de IAM para agregar permisos rápidamente para Respuesta frente a incidencias de seguridad de AWS.

> **Important**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Respuesta frente a incidencias de seguridad de AWS usa etiquetas para proporcionarle servicios administrativos. Las etiquetas no se han diseñado para usarse con información privada o confidencial.

Detalles de los permisos

El servicio usa esta política para llevar a cabo acciones en los siguientes recursos:

- Acceso de solo lectura de entidades principales de IAM: otorga a un usuario del servicio la capacidad de llevar a cabo acciones de solo lectura en los recursos existentes de Respuesta frente a incidencias de seguridad de AWS.
- Acceso de escritura de entidades principales de IAM: otorga a un usuario del servicio la capacidad de actualizar, modificar, eliminar y crear recursos de Respuesta frente a incidencias de seguridad de AWS.

Puede ver los permisos asociados a esta política en políticas administradas por AWS para AWSSecurityIncidentResponseFullAccess.

Política administrada por AWS: AWSSecurityIncidentResponseReadOnlyAccess

Respuesta frente a incidencias de seguridad de AWS utiliza la política administrada por AWS AWSSecurityIncidentResponseReadOnlyAccess. La política concede acceso de solo lectura a los recursos de casos del servicio. Puede utilizar esta política con sus entidades principales de IAM para agregar permisos rápidamente para Respuesta frente a incidencias de seguridad de AWS.

> **Important**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Respuesta frente a incidencias de seguridad de AWS usa etiquetas para proporcionarle servicios administrativos. Las etiquetas no se han diseñado para usarse con información privada o confidencial.

Detalles de los permisos

El servicio usa esta política para llevar a cabo acciones en los siguientes recursos:

- Acceso de solo lectura de entidades principales de IAM: otorga a un usuario del servicio la capacidad de llevar a cabo acciones de solo lectura en los recursos existentes de Respuesta frente a incidencias de seguridad de AWS.

Puede ver los permisos asociados a esta política en políticas administradas por AWS para AWSSecurityIncidentResponseReadOnlyAccess.

Política administrada por AWS: AWSSecurityIncidentResponseCaseFullAccess

Respuesta frente a incidencias de seguridad de AWS utiliza la política administrada por AWS AWSSecurityIncidentResponseCaseFullAccess. La política concede acceso completo a los recursos de casos del servicio. Puede utilizar esta política con sus entidades principales de IAM para agregar permisos rápidamente para Respuesta frente a incidencias de seguridad de AWS.

> **Important**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Respuesta frente a incidencias de seguridad de AWS usa etiquetas para

proporcionarle servicios administrativos. Las etiquetas no se han diseñado para usarse con información privada o confidencial.

Detalles de los permisos

El servicio usa esta política para llevar a cabo acciones en los siguientes recursos:

- Acceso de solo lectura a casos de entidades principales de IAM: otorga a un usuario del servicio la capacidad de llevar a cabo acciones de solo lectura en casos de Respuesta frente a incidencias de seguridad de AWS existentes.
- Acceso de escritura a casos de entidades principales de IAM: otorga a un usuario del servicio la capacidad de actualizar, modificar, eliminar y crear casos de Respuesta frente a incidencias de seguridad de AWS.

Puede ver los permisos asociados a esta política en políticas administradas por AWS para AWSSecurityIncidentResponseCaseFullAccess.

Política administrada por AWS: AWSSecurityIncidentResponseTriageServiceRolePolicy

Respuesta frente a incidencias de seguridad de AWS utiliza la política administrada por AWS AWSSecurityIncidentResponseTriageServiceRolePolicy. Esta política administrada por AWS está adjunta al rol vinculado a servicios AWSServiceRoleForSecurityIncidentResponse_Triage.

La política proporciona acceso a Respuesta frente a incidencias de seguridad de AWS para supervisar continuamente su entorno en busca de amenazas de 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 otra información confidencial en las etiquetas. Respuesta frente a incidencias de seguridad de AWS usa etiquetas para proporcionarle servicios administrativos. Las etiquetas no se han diseñado para usarse con información privada o confidencial.

Detalles de los permisos

El servicio usa esta política para llevar a cabo acciones en los siguientes recursos:

- Eventos: permite al servicio crear una regla administrada de Amazon EventBridge. Esta regla es la infraestructura necesaria en su cuenta de AWS para enviar eventos desde su cuenta al servicio. Esta acción se lleva a cabo en cualquier recurso de AWS administrado 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 lleva a cabo en cualquier recurso de AWS.
- 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 lleva a cabo en cualquier recurso de AWS.

Puede ver los permisos asociados a esta política en políticas administradas por AWS para AWSSecurityIncidentResponseTriageServiceRolePolicy.

Actualizaciones de Respuesta frente a incidencias de seguridad de AWS en SLR y políticas administradas

Es posible consultar detalles sobre las actualizaciones de los SLR y las políticas administradas de Respuesta frente a incidencias de seguridad de AWS debido a que este servicio comenzó a hacer el seguimiento de estos cambios.

Cambio	Descripción	Fecha
Actualizaciones del SLR y adición de permisos para admitir los derechos del servicio.	AWSSecurityIncidentResponseTriageServiceRolePolicy se actualizó para agregar los permisos security-ir:GetMembership, security-ir:ListMemberships, security-ir:UpdateCase, guardduty:ListFilters, guarduty:UpdateFilter, guardduty:DeleteFilter y guardduty:GetAdministratorAccount. guardduty:GetAdministratorAccount se agregó para facilitar la administración de los filtros de archivado automático de GuardDuty en cuentas delegadas.	2 de junio de 2025
Nuevo SLR: AWSServiceRoleForS	Nuevo rol vinculado a servicios y nueva política adjunta que permiten al servicio acceder a sus cuentas de AWS Organizations para identificar la membresía.	1 de diciembre de 2024

Cambio	Descripción	Fecha
ecurityIn cidentResponse Nueva política administrada: AWSSecuri tyInciden tResponse ServiceRo lePolicy.		
Nuevo SLR: AWSServic eRoleForS ecurityIn cidentRes ponse_Triage Nueva política administrada: AWSSecuri tyInciden tResponse TriageSer viceRolePolicy	Nuevo rol vinculado a servicios y nueva política adjunta que permiten al servicio acceder a sus cuentas de AWS Organizations para clasificar los eventos de seguridad.	1 de diciembre de 2024
Nueva política administrada: AWSSecuri tyInciden tResponse FullAccess	Respuesta frente a incidencias de seguridad de AWS agrega un nuevo SLR para adjuntarlo a las entidades principales de IAM para acciones de lectura y escritura del servicio.	1 de diciembre de 2024

Cambio	Descripción	Fecha
Nuevo rol de política administrada: AWSSecurityIncidentResponseReadOnlyAccess	Respuesta frente a incidencias de seguridad de AWS agrega un nuevo SLR para adjuntarlo a las entidades principales de IAM para acciones de lectura.	1 de diciembre de 2024
Nueva política administrada: AWSSecurityIncidentResponseCaseFullAccess	Respuesta frente a incidencias de seguridad de AWS agrega un nuevo SLR para adjuntarlo a las entidades principales de IAM para acciones de lectura y escritura de los casos del servicio.	1 de diciembre de 2024
Comenzó el seguimiento de los cambios	Comenzó el seguimiento de los cambios de los SLR y las políticas administradas de Respuesta frente a incidencias de seguridad de AWS.	1 de diciembre de 2024

Respuesta a incidentes

Los asuntos relacionados con la seguridad y la conformidad son una responsabilidad compartida entre 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 host y la capa de virtualización hasta la seguridad física de las instalaciones en las que operan los servicios. Por otra parte, el cliente asume la responsabilidad y la administración del sistema operativo invitado (incluidas las actualizaciones y los parches de seguridad), de otros softwares de aplicaciones asociadas y de la configuración del firewall del grupo de seguridad que ofrece AWS. Para obtener más información, consulte el Modelo de responsabilidad compartida de AWS.

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 ante los incidentes de seguridad puede ser un tema complejo, le recomendamos que consulte los siguientes recursos para comprender mejor el impacto que la respuesta ante incidentes y sus elecciones tienen en sus objetivos corporativos: el documento técnico AWS Security Best Practices y el documento técnico Security Perspective of the AWS Cloud Adoption Framework (CAF).

Validación de conformidad

Los auditores externos evalúan la seguridad y la conformidad de los servicios de AWS en distintos programas de conformidad de AWS. Estos incluyen SOC, PCI, FedRAMP, HIPAA y otros.

No se ha evaluado el cumplimiento de Respuesta frente a incidencias de seguridad de AWS con los programas antes mencionados.

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

Puede descargar los informes de auditoría de terceros mediante AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact.

Su responsabilidad de cumplimiento al utilizar servicios de AWS está determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y regulaciones aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido de seguridad y cumplimiento: en estas guías de implementación se tratan consideraciones sobre arquitectura y se ofrecen pasos para implementar los entornos de referencia centrados en la seguridad y el cumplimiento en AWS.
- Documento técnico sobre arquitectura para seguridad y cumplimiento de HIPAA: en este documento técnico se describe cómo las empresas pueden utilizar AWS para crear aplicaciones conformes con HIPAA.
- Recursos de conformidad de AWS: un conjunto de manuales y guías que podría aplicarse a su sector o ubicación.
- Evaluating resources with AWS Config Rules en la Guía para desarrolladores de AWS Config: AWS Config evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub: este producto de AWS proporciona una visión completa de su estado de seguridad en AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: este servicio de AWS detecta posibles amenazas para sus cuentas, cargas de trabajo, contenedores y datos de AWS mediante el monitoreo de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a satisfacer varios requisitos

de conformidad, como PCI DSS, cumpliendo los requisitos de detección de intrusos que exigen determinados marcos de conformidad.

- AWS Audit Manager: este servicio de AWS le ayuda a auditar de manera continua su uso de AWS para simplificar la forma en que administra el riesgo y la conformidad con las regulaciones y los estándares del sector.

Registro y supervisión en Respuesta ante incidentes de seguridad de AWS

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Respuesta frente a incidencias de seguridad de AWS y las demás soluciones de AWS. Respuesta frente a incidencias de seguridad de AWS admite actualmente los dos servicios de AWS siguientes para supervisar su organización y la actividad que tiene lugar dentro de ella.

AWS CloudTrail: con CloudTrail, puede capturar llamadas a la API desde la consola de Respuesta ante incidentes de seguridad de AWS. Por ejemplo, cuando un usuario se autentica, CloudTrail puede registrar detalles como la dirección IP en la solicitud, quién realizó la solicitud y cuándo se realizó.

Métricas de Amazon CloudWatch: con las métricas de CloudWatch, puede monitorear, informar y emprender acciones automáticas en caso de que se produzca un evento casi en tiempo real. Por ejemplo, puede crear paneles de CloudWatch en las métricas proporcionadas para supervisar el uso de Respuesta frente a incidencias de seguridad de AWS o puede crear alarmas de CloudWatch en las métricas proporcionadas para notificarle en caso de incumplimiento de un umbral establecido.

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

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

Resiliencia

La infraestructura global de AWS está conformada por regiones y zonas de disponibilidad de AWS. 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 latencia. 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 centros de datos únicos o múltiples.

Para obtener más información sobre las zonas de disponibilidad y las regiones de AWS, consulta Infraestructura global de AWS.

Seguridad de la infraestructura

La seguridad de la red global de AWS protege a Respuesta frente a incidencias de seguridad de AWS. Para obtener información sobre los servicios de seguridad de AWS y sobre cómo AWS protege la infraestructura, consulte Seguridad en la nube de AWS. Para diseñar su entorno de AWS con las prácticas recomendadas de seguridad de infraestructura, consulte Protección de la infraestructura en Portal de seguridad de AWS Well-Architected Framework.

Puede utilizar llamadas a la API publicadas en AWS para obtener acceso a Respuesta frente a incidencias de seguridad de AWS a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o 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. También puede utilizar el AWS Security Token Service (AWS STS) con el objeto de generar credenciales de seguridad temporales para firmar solicitudes.

Configuración y análisis de vulnerabilidades

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

AWS se encarga de las tareas de seguridad básicas, tales como la aplicación de revisiones en la base de datos y el sistema operativo (SO) invitado, 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 AWS, la suplantación entre servicios puede dar lugar al problema de la sustitución confusa. La suplantación entre servicios puedes 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 lo ayudan a proteger sus datos para todos los servicios con entidades principales de servicio a las que se les ha dado acceso a los recursos de su cuenta.

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

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

Para ver un ejemplo de una política de asunción de roles que muestra cómo se puede evitar un problema de suplente confuso, consulte Confused deputy prevention policy.

Service Quotas

Respuesta frente a incidencias de seguridad de AWS

En las siguientes tablas se indican las cuotas para los recursos de Respuesta frente a incidencias de seguridad de AWS de su Cuenta de AWS. Algunas cuotas pueden aumentarse por encima de las indicadas 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 compatibles con AWS activos	10	Sí (hasta 50)	Número de casos activos que solicitan la asistencia del equipo de CIRT de AWS.
2	Casos autoadministrados activos	50	Sí (hasta 100)	Número de casos activos que utilizan la plataforma sin la asistencia del equipo de CIRT de AWS.
3	Casos compatibles con el servicio creados en 24 horas	10	No	Número de casos creados que solicitan la asistencia del equipo de CIRT de AWS en un periodo continuo de 24 horas.

	Nombre	Valor predeterminado	Ajustable	Comentarios
4	Número máximo de entidades en el equipo de respuesta ante incidentes predeterminado	10	No	Número máximo de entidades del equipo de respuesta ante incidentes predeterminado.
5	Número máximo de miembros adicionales en un caso	30	No	Número máximo de entidades asociadas a un caso. Inicialmente, se rellenará con las entidades de su equipo de respuesta ante incidentes predeterminado.
6	Número máximo de archivos adjuntos del caso	50	Sí (hasta 100)	Número máximo de archivos que pueden adjuntarse a un caso.
7	Tamaño máximo de los comentarios del caso	1 000	No	Número máximo de caracteres en el comentario del caso.
8	Tamaño máximo del nombre del archivo adjunto del caso	255	No	Número máximo de caracteres en un nombre de archivo.

Guía técnica sobre Respuesta frente a incidencias de seguridad de AWS

Contenido

- Resumen
- ¿Usa Well-Architected?
- Introducción
- Preparación
- Operaciones
- Actividad posterior al incidente
- Conclusión
- Colaboradores
- Apéndice A: Definiciones de capacidades en la nube
- Apéndice B: recursos de respuesta ante incidentes de AWS
- Avisos

Resumen

En esta guía se presenta información general sobre los aspectos fundamentales de la respuesta ante incidentes de seguridad en el entorno en la nube de Amazon Web Services (AWS). 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 roles técnicos y se presupone que se ha familiarizado con los principios generales de la seguridad de la información, que tiene conocimientos básicos sobre la respuesta ante incidentes de seguridad en los entornos en las instalaciones actuales y que se ha familiarizado 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. Mediante AWS Well-Architected Tool, disponible sin costo alguno en la Consola de AWS Well-Architected Tool, puede comparar las 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 máxima prioridad en AWS. Los clientes de AWS se beneficiarán de una arquitectura de red y de centros de datos diseñados para satisfacer las necesidades de seguridad de las organizaciones más exigentes en materia de 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 lo ayudarán a cumplir sus objetivos de seguridad. Estas capacidades lo ayudan a establecer una línea de base de seguridad para las aplicaciones que se ejecutan en la Nube de AWS.

Si se produce una desviación de la línea de base (por ejemplo, debido a un error de configuración o a un cambio de factores externos), tendrá que responder a ella e investigarla. Para hacerlo correctamente, debe comprender los conceptos básicos de la respuesta ante incidentes de seguridad en su entorno de AWS y los requisitos para preparar, formar y capacitar a los equipos de trabajo en la nube antes de que se produzcan problemas de seguridad. Es importante saber qué controles y capacidades puede utilizar, revisar ejemplos temáticos para resolver posibles problemas e identificar métodos de remediación que utilicen la automatización a fin de 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 ante incidentes de seguridad que cumpla con esos requisitos.

La respuesta ante 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 de estrategias para crear una biblioteca inicial de mecanismos de respuesta ante incidentes sobre los que pueda iterar y mejorar.

Antes de empezar

Antes de empezar a aprender sobre la respuesta ante incidentes de seguridad en AWS, familiarícese con los estándares y marcos pertinentes de seguridad y respuesta ante incidentes de AWS. Estos aspectos fundamentales lo ayudarán a comprender los conceptos y las prácticas recomendadas que se presentan en esta guía.

Estándares y marcos de seguridad de AWS

Para empezar, le recomendamos que consulte Prácticas recomendadas para la seguridad, la identidad y el cumplimiento, pilar de seguridad: AWS Well-Architected Framework y el documento técnico Perspectiva de seguridad de “Información general sobre AWS Cloud Adoption Framework (AWS CAF)”.

AWS CAF proporciona una guía que apoya la coordinación entre las diferentes partes de las organizaciones que migran a la nube. La guía de AWS CAF se divide en varias áreas de enfoque (denominadas perspectivas) que son importantes para la creación de 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 ante incidentes. Este documento es el resultado de nuestra experiencia trabajando con clientes para ayudarlos a crear programas y capacidades de respuesta ante incidentes de seguridad eficaces y eficientes.

Estándares y marcos de respuesta ante incidentes del sector

Este documento técnico sigue los estándares de respuesta ante incidentes y las prácticas recomendadas de la guía Computer Security Incident Handling Guide SP 800-61 r2, creada por el Instituto Nacional de Estándares y Tecnología (NIST). Leer y comprender los conceptos introducidos por el NIST es un requisito previo útil. Los conceptos y las prácticas recomendadas de esta guía del NIST se aplicarán a las tecnologías de AWS en este documento. Sin embargo, los escenarios de incidentes en las instalaciones están fuera del alcance de esta guía.

Información general sobre la respuesta ante incidentes de AWS

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

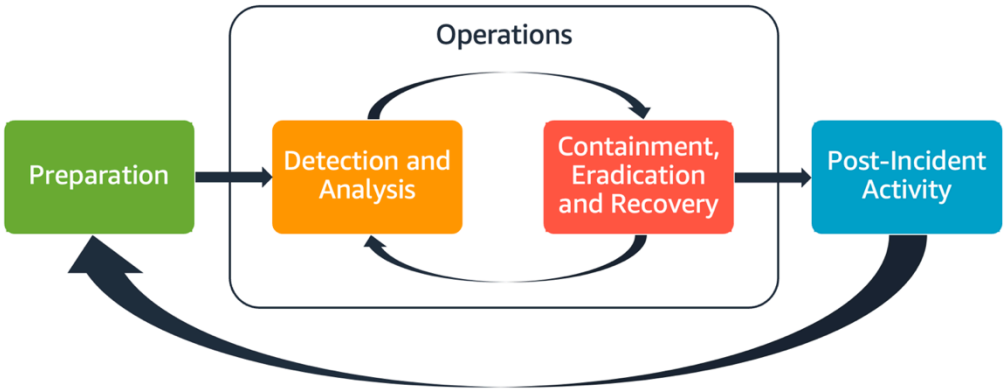
Aspectos de la respuesta ante incidentes de AWS

Todos los usuarios de AWS de una organización deben tener un conocimiento básico de los procesos de respuesta ante incidentes de seguridad; de igual manera, el personal de seguridad debe entender cómo responder a los problemas de seguridad. La educación, la capacitación y la experiencia son fundamentales para el éxito de un programa de respuesta ante incidentes en la nube y, en un escenario ideal, deben implementarse mucho antes de tener que gestionar un posible incidente de seguridad. La base de un programa de respuesta antes incidentes exitoso en la nube es la preparación, las operaciones y la actividad posterior al incidente.

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

- Preparación: prepare a su equipo de respuesta ante incidentes para que detecte y responda a los incidentes internos de AWS mediante la habilitación de controles de detección y la comprobación de que tengan el acceso adecuado a las herramientas y los servicios en la nube necesarios. Asimismo, prepare las guías de estrategias necesarias, tanto manuales como automatizadas, para comprobar respuestas fiables y coherentes.
- Operaciones: opere en caso de eventos de seguridad y posibles incidentes según las fases de respuesta ante incidentes del NIST (detección, análisis, contención, erradicación y recuperación).
- Actividad posterior al incidente: repita el resultado de sus eventos y simulaciones de seguridad para mejorar la eficacia de su respuesta, aumentar el valor derivado de la respuesta y la investigación y reducir aún más el riesgo. Hay que aprender de los incidentes y ser plenamente responsable de las actividades de mejora.

En esta guía se explora y se detalla cada uno de estos aspectos. En el siguiente diagrama se muestra el flujo de estos aspectos y se alinea con el ciclo de vida de respuesta ante incidentes del NIST mencionado anteriormente, pero con operaciones que abarcan detección y análisis con contención, erradicación y recuperación.



Principios de respuesta ante incidentes y objetivos de diseño de AWS

Si bien los procesos y mecanismos generales de respuesta ante incidentes, como los definidos en la guía SP 800-61 Computer Security Incident Handling Guide del NIST, siguen siendo válidos, le recomendamos que valore también estos objetivos de diseño específicos que son pertinentes para responder a los incidentes de seguridad en un entorno de nube:

- Establecimiento de objetivos de repuesta: trabaje con las partes interesadas, el consejo legal y el equipo directivo de la organización para determinar el objetivo de respuesta ante un incidente. Algunos objetivos habituales incluyen la contención y mitigación del problema, la recuperación de los recursos afectados, la conservación de los datos para el análisis forense, el retorno a las operaciones seguras conocidas y, en última instancia, el aprendizaje de los incidentes.
- Respuesta a través de la nube: implemente los patrones de respuesta en la nube, donde tiene lugar el evento y se generan los datos.
- Conocimientos sobre lo que tiene y lo que necesita: preserve los registros, los recursos, las instantáneas y otras pruebas. Cópielos y almacénelos en una cuenta en la nube centralizada dedicada a la respuesta. Utilice etiquetas, metadatos y mecanismos que cumplan las políticas de retención. Deberá comprender qué servicios utiliza y, a continuación, identificar los requisitos para la investigación de dichos servicios. Para ayudarlo a comprender mejor su entorno, también puede utilizar el etiquetado, que se trata más adelante en este documento en la sección the section called “Desarrollo e implementación de una estrategia de etiquetado”.
- Uso de mecanismos de repetición de la implementación: si se puede atribuir una anomalía de seguridad a una configuración errónea, la solución podría ser tan sencilla como eliminar la varianza mediante la repetición de la implementación de los recursos con la configuración adecuada. En caso de que se identificara un posible compromiso, compruebe que la repetición de la implementación incluya una mitigación correcta y verificada de las causas raíz.
- Automatización siempre que sea posible: a medida que surjan problemas o se repitan los incidentes, cree mecanismos para clasificar y responder a eventos habituales mediante programación. Utilice respuestas humanas para incidentes únicos, complejos o delicados en los que las automatizaciones sean insuficientes.
- Uso de soluciones escalables: esfuércese por igualar la escalabilidad del enfoque de su organización con respecto a la computación en la nube. Implemente mecanismos de detección y respuesta que se escalen en todos sus entornos para reducir eficazmente el tiempo entre la detección y la respuesta.

- Mejora y aprendizaje del proceso: sea proactivo a la hora de identificar las carencias en sus procesos, herramientas o personas e implemente un plan para solucionarlas. Las simulaciones son métodos seguros para detectar carencias y mejorar los procesos. Consulte la sección the section called “Actividad posterior al incidente” de este documento para obtener información detallada sobre cómo iterar en 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 y lo ideal es que sea con una metodología de respuesta sólida desde el punto de vista forense. En algunos casos, esto significa que podría tener varias organizaciones, cuentas y herramientas configuradas específicamente para estas tareas de respuesta. Estas herramientas y funciones deben ponerse a disposición del personal de respuesta ante incidentes mediante una canalización de implementación. No deben ser estáticas porque pueden causar un riesgo mayor.

Dominios de incidentes de seguridad en la nube

Para prepararse y responder eficazmente a los eventos de seguridad en su entorno de AWS, 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 su Cuenta de AWS, a los permisos de AWS Identity and Access Management (IAM), a los metadatos de los recursos, a la facturación o a otras áreas. Un evento del dominio de servicio es aquel al que responde exclusivamente con mecanismos de API de AWS, 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 al servicio.
- Dominio de infraestructura: los incidentes en el dominio de infraestructura son actividades relacionadas con la red o los datos, como los procesos y los datos de sus instancias de Amazon Elastic Compute Cloud (Amazon EC2), el tráfico a sus instancias de Amazon EC2 dentro de la nube privada virtual (VPC) y otras áreas, como contenedores u otros servicios futuros. Su respuesta a los eventos del dominio de infraestructura suele implicar la adquisición de datos relacionados con los incidentes para su análisis forense. Es probable que implique la interacción con el sistema operativo de una instancia y, en varios casos, también pueda implicar mecanismos de API de AWS. En el dominio de infraestructura, puede utilizar una combinación

de API y herramientas de análisis forense digital o respuesta a incidentes (DFIR) de AWS en un sistema operativo huésped, como una instancia de Amazon EC2 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 (Amazon EBS) o memoria volátil adquirida de una instancia.

- Dominio de aplicación: los incidentes en el dominio de 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 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 la implementación automatizadas.

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

Principales diferencias de la respuesta ante incidentes en AWS

La respuesta ante 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 privilegio mínimo 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. Varios patrones de respuesta ante incidentes que respaldan estos principios de seguridad siguen la misma línea, como la retención de registros, la selección de alertas derivadas del modelado de amenazas, el desarrollo de manuales de estrategias y la integración de la administración de información y eventos de seguridad (SIEM). Las diferencias comienzan cuando los clientes empiezan a diseñar e implementar estos patrones en la nube. Las siguientes son las principales diferencias de la respuesta ante incidentes en AWS.

Diferencia n.º 1: la seguridad como responsabilidad compartida

Los asuntos relacionados con la seguridad y el cumplimiento son una responsabilidad compartida entre AWS y sus clientes. Este modelo de responsabilidad compartida alivia la carga operativa del cliente, ya que AWS opera, administra y controla los componentes del sistema operativo host y la capa de virtualización con el fin de ofrecer seguridad física en las instalaciones en las que operan los servicios. 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 ante incidentes. Planificar y comprender estas diferencias y adaptarlas a sus necesidades de gobernanza es un paso crucial en la respuesta ante incidentes.

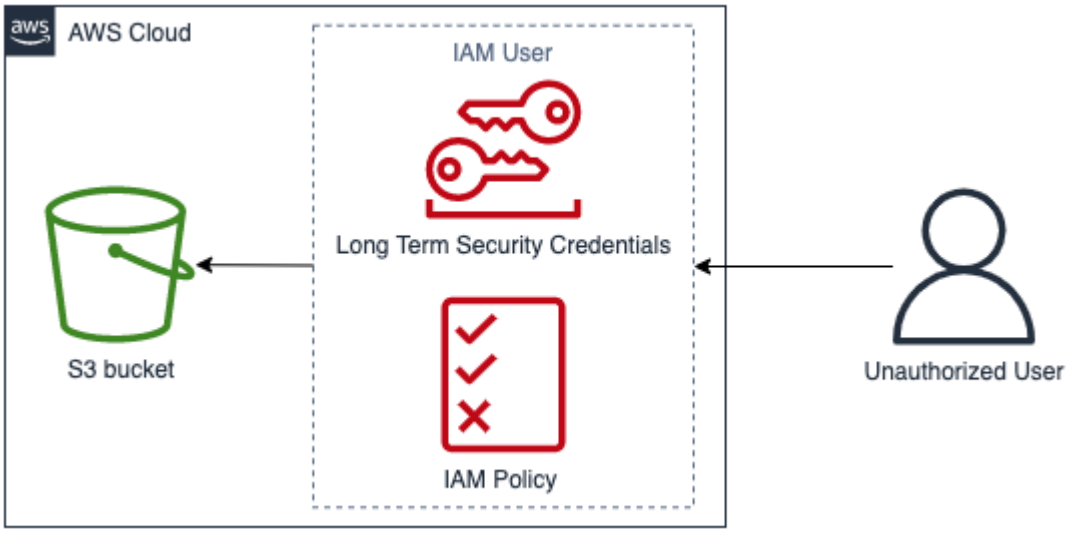
Además de la relación directa que tiene con AWS, es posible que haya otras entidades que tengan responsabilidades en su modelo de responsabilidad particular. Por ejemplo, es posible que tenga unidades organizativas internas que asuman la responsabilidad de algunos aspectos de sus operaciones. Es posible que también tenga relaciones con otras partes que desarrollen, administren u operen parte de su tecnología en la nube.

Es de suma importancia crear y probar un plan de respuesta ante incidentes y los manuales adecuados que se adapten a su modelo operativo.

Diferencia n.º 2: dominio de servicio en la nube

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

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



Ejemplo de dominio de servicio

Diferencia n.º 3: API para el aprovisionamiento de la infraestructura

Otra diferencia proviene de la característica de la nube del autoservicio bajo demanda. Los clientes de las instalaciones principales interactúan con la Nube de AWS mediante una API RESTful a través de puntos de conexión públicos y privados disponibles en muchas ubicaciones geográficas de todo el mundo. Los clientes pueden acceder a estas API con credenciales de AWS. A diferencia del control de acceso en las instalaciones, estas credenciales no están necesariamente vinculadas a una red o a un dominio de Microsoft Active Directory. En cambio, las credenciales se asocian a una entidad principal de IAM dentro de una cuenta de AWS. Se puede acceder a estos puntos de conexión de la API desde fuera de la red corporativa, lo cual será importante a la hora de responder a un incidente en el que las credenciales se utilicen fuera de la red o la zona geográfica esperadas.

Debido a la naturaleza basada en API de AWS, AWS CloudTrail es un origen de registro importante para responder a los eventos de seguridad. Permite hacer un seguimiento de las llamadas a la API de administración que se realizan en sus cuentas de AWS y puede encontrar información sobre la ubicación de origen de las llamadas a la API.

Diferencia n.º 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 los recursos de AWS y saber cómo realizar un seguimiento de la creación y

eliminación de los recursos de AWS. Puede utilizar AWS Config para realizar un seguimiento del historial de configuración de sus recursos de AWS.

Diferencia n.º 5: acceso a los datos

El acceso a los datos también es diferente en la nube. No puede conectarse a un servidor para recopilar los datos que necesita para una investigación de seguridad. Los datos se recopilan a través de la red y mediante llamadas a la API. Deberá practicar y comprender cómo realizar la recopilación de datos a través de las API a fin de prepararse para este cambio y verificar el almacenamiento adecuado para una recopilación y un acceso eficaces.

Diferencia n.º 6: importancia de la automatización

Para que los clientes se beneficien plenamente de la adopción de la nube, su estrategia operativa debe tener en cuenta la automatización. La infraestructura como código (IaC) es un patrón de entornos automatizados altamente eficientes en el que los servicios de AWS se implementan, configuran, reconfiguran y destruyen mediante código facilitado por servicios de IaC nativos, como AWS CloudFormation o soluciones de terceros. Esto exige que la implementación de la respuesta ante incidentes sea altamente automatizada, lo que es deseable para evitar errores humanos, especialmente al gestionar evidencias. Si bien la automatización se usa en las instalaciones, es esencial y más sencilla en la Nube de AWS.

Gestión de estas diferencias

Para gestionar estas diferencias, siga los pasos que se describen en la siguiente sección y compruebe que su programa de respuesta ante incidentes, tanto en lo que respecta a las personas como a 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:

- Personal: la preparación del personal para un incidente de seguridad implica identificar a las partes interesadas pertinentes para la respuesta a los incidentes y capacitarlas en materia de respuesta ante incidentes y tecnologías en la nube.
- Procesos: la preparación de los procesos para un incidente de seguridad implica documentar las arquitecturas, desarrollar planes exhaustivos de respuesta ante los incidentes y crear guías de estrategias para responder de manera coherente a los eventos de seguridad.

- Tecnología: la preparación de la tecnología para un incidente de seguridad implica configurar el acceso, agregar y 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, debe identificar a las partes interesadas que apoyarían la respuesta a dicho evento. Además, para una respuesta eficaz, es fundamental formarlas en las tecnologías de AWS y su entorno de AWS.

Definición de roles y responsabilidades

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

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

Por último, en la investigación o la respuesta pueden participar partes relacionadas de confianza, ya que pueden proporcionar conocimiento experto adicional y un control muy valioso. Si no dispone de

estas habilidades en su propio equipo, tal vez sea conveniente contratar a una persona externa para que le ayude.

Formación del personal de respuesta ante incidentes

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

Información sobre las tecnologías de Nube de AWS

Para reducir las dependencias y disminuir 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 oportunidades de práctica directa con el entorno en la nube específico que utiliza su organización. Para que el personal de respuesta ante incidentes sea eficaz, es importante entender los fundamentos de AWS, IAM, AWS Organizations, los servicios de registro y monitoreo de AWS y los servicios de seguridad de AWS.

AWS ofrece talleres de seguridad en línea (consulte AWS Security Workshops) en los que puede adquirir experiencias prácticas con los servicios de seguridad y monitoreo de AWS. 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 formación de AWS y las certificaciones. Para obtener más información, consulte Capacitación y certificación de AWS.

AWS ofrece formaciones gratuitas y por suscripción que apoya a varias personas y áreas de interés. Visite AWS Skill Builder para obtener más información.

Información sobre el entorno de AWS

Además de entender los servicios de AWS, sus casos de uso y cómo se integran entre sí, es igual de importante entender cómo se diseña realmente el entorno de AWS 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 dominio, 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 y comprender el conocimiento interno del entorno de AWS, así como tener acceso a él. 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 ante incidentes incluye la documentación y la centralización de los diagramas de arquitectura, que se incluyen más adelante en este documento técnico (the section called “Documentación y centralización de los diagramas de arquitectura”). 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 de AWS y comprenderlos.

Información sobre los equipos de asistencia y respuesta de AWS

Soporte

Soporte ofrece una serie de planes que proporcionan acceso a herramientas y conocimientos que contribuyen al éxito y la salud operativa de sus soluciones de AWS. Si necesita asistencia técnica y más recursos para planificar, implementar y optimizar su entorno de AWS, puede seleccionar el plan de asistencia que mejor se adapte a su caso de uso de AWS.

Piense en el Centro de soporte de la AWS Management Console (es necesario iniciar sesión) como punto de contacto central para obtener asistencia en caso de problemas que afecten a sus recursos de AWS. El acceso a Soporte está controlado por IAM. Para obtener más información sobre el acceso a las características de AWS Support, consulte Introducción a Soporte.

Además, si tiene que denunciar un abuso, póngase en contacto con el equipo del Centro de confianza y seguridad de AWS.

Equipo de respuesta ante incidentes de clientes (CIRT) de AWS

El equipo de respuesta ante incidentes de clientes (CIRT) de AWS es un equipo global de AWS especializado que está siempre disponible y ofrece asistencia a los clientes durante eventos de seguridad activos en el lado del cliente del Modelo de responsabilidad compartida de AWS.

Cuando el CIRT de AWS le ofrezca asistencia, usted recibirá ayuda en la clasificación y la recuperación de un evento de seguridad activo en AWS. Lo ayudarán a analizar la causa raíz mediante el uso de registros de servicio de AWS y ofrecerle recomendaciones para la recuperación.

También le proporcionará recomendaciones de seguridad y prácticas recomendadas para ayudarlo a evitar eventos de seguridad en el futuro.

Los clientes de AWS pueden interactuar con el CIRT de AWS a través de un caso de soporte de AWS.

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

- Clientes con planes Developer de Soporte:
  1. Cuenta y facturación
  2. Servicio: cuenta
  3. Categoría: seguridad
  4. Gravedad: pregunta importante

- Clientes con planes Business de Soporte:
  1. Cuenta y facturación
  2. Servicio: cuenta
  3. Categoría: seguridad
  4. Gravedad: pregunta urgente que afecta a la empresa

- Clientes con planes Enterprise de Soporte:
  1. Cuenta y facturación
  2. Servicio: cuenta
  3. Categoría: seguridad
  4. Gravedad: pregunta crítica sobre el riesgo para la empresa

- Clientes con suscripciones de Respuesta frente a incidencias de seguridad de AWS: abra la consola de respuesta ante incidentes de seguridad en https://console.aws.amazon.com/security-ir/

Asistencia en respuestas a DDoS

AWS ofrece AWS Shield, que proporciona un servicio administrado de protección contra ataques de denegación de servicio distribuida (DDoS) que protege las aplicaciones web que se ejecutan en AWS. AWS Shield proporciona detección continua y mitigaciones automáticas en línea que pueden minimizar el tiempo de inactividad y la latencia de las aplicaciones, por lo que no es necesario contratar Soporte para beneficiarse de la protección contra ataques DDoS. Hay dos niveles de AWS Shield: Shield Standard y Shield Advanced. Para conocer las diferencias entre estos dos niveles, consulte la documentación de características de Shield.

AWS Managed Services (AMS)

AWS Managed Services (AMS) proporciona una administración continua de su infraestructura de AWS para que pueda centrarse en sus aplicaciones. Mediante la implementación de prácticas recomendadas para mantener su infraestructura, AMS le ayuda a reducir la carga y el riesgo operativos. AMS automatiza actividades comunes, como solicitudes de cambios, supervisión, administración de parches, seguridad y servicios de copia de seguridad, y ofrece servicios de ciclo de vida completo para aprovisionar, ejecutar y brindar soporte a su infraestructura.

AMS asume la responsabilidad de implementar un conjunto de controles de detección de seguridad y cada día proporciona una primera línea de respuesta a las alertas. Cuando se inicia una alerta, AMS sigue un conjunto estándar de guías automáticas y manuales para verificar una respuesta coherente. Estas guías de estrategias se comparten con los clientes de AMS durante la incorporación para que puedan desarrollar y coordinar una respuesta con AMS.

Proceso

Desarrollar procesos de respuesta ante incidentes exhaustivos y claramente definidos es clave para que el programa de respuesta ante incidentes sea satisfactorio y escalable. Cuando se produce un evento de seguridad, tener unos pasos y flujos de trabajo claros puede lo ayudará a responder a tiempo. Es posible que ya tenga un proceso de respuesta ante incidentes. Independientemente de su estado actual, es importante actualizar, iterar y probar sus procesos de respuesta a incidentes con regularidad.

Desarrollo y prueba de un plan de respuesta ante incidentes

El primer documento que se desarrolla para la respuesta ante incidentes es el plan de respuesta ante 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 ante incidentes es un documento de alto nivel que normalmente incluye estas secciones:

- Descripción general del equipo de respuesta ante incidentes: describe los objetivos y las funciones del equipo de respuesta ante incidentes.
- Roles y responsabilidades: enumera las partes interesadas de la respuesta ante incidentes y detalla sus roles cuando se produce un incidente.
- Un plan de comunicación: detalla la información de contacto y cómo se comunicará durante un incidente.

  Se recomienda tener un método de comunicación auxiliar fuera de banda para informar de los incidentes. Un ejemplo de una aplicación que proporciona un canal de comunicaciones fuera de banda seguro es AWS Wickr.
- Fases de la respuesta ante incidentes y medidas que tomar: se enumeran las fases de la respuesta ante incidentes (por ejemplo, detección, análisis, erradicación, contención y recuperación), incluidas las medidas de alto nivel que se deben tomar en esas fases.
- Definiciones de gravedad y priorización del incidente: detalla cómo clasificar la gravedad de un incidente, cómo priorizar el incidente y, a continuación, cómo las definiciones de gravedad afectan a los procedimientos de escalamiento.

Aunque estas secciones son comunes en empresas de diferentes tamaños y de diferentes sectores, el plan de respuesta a incidentes de cada organización es único. Deberá elaborar un plan de respuesta ante incidentes que mejor se adapte a su organización.

Documentación y centralización de los diagramas de arquitectura

Para responder de forma rápida y precisa ante un incidente de seguridad, debe comprender la arquitectura de sus sistemas y redes. Comprender estos patrones internos no solo es importante para responder ante incidentes, sino también para verificar la coherencia entre las aplicaciones con las que se diseñan los patrones, de acuerdo con las prácticas recomendadas. 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:

- Estructura de cuentas de AWS: necesita saber:
  - ¿Cuántas cuentas de AWS tiene?
  - ¿Cómo están organizadas esas cuentas de AWS?
  - ¿Quiénes son los propietarios de la empresa de las cuentas de AWS?

  - ¿Utiliza políticas de control de servicio (SCP)? Si es así, ¿qué barreras de protección organizativas se implementan mediante las SCP?
  - ¿Limita las regiones y los servicios que se pueden usar?
  - ¿Qué diferencias hay entre las unidades de negocio y los entornos (desarrollo/pruebas/producción)?
- Patrones de servicio de AWS
  - ¿Qué servicios de AWS utiliza?
  - ¿Cuáles son los servicios de AWS más utilizados?
- Patrones de arquitectura
  - ¿Qué arquitecturas en la nube utiliza?
- Patrones de autenticación de AWS
  - ¿Cómo se suelen autenticar los desarrolladores en AWS?
  - ¿Utiliza roles o usuarios de IAM (o ambos)? ¿Su autenticación en AWS está conectada a un proveedor de identidades (IdP)?
  - ¿Cómo asigna un rol o un usuario de IAM a un empleado o un sistema?
  - ¿Cómo se revoca el acceso cuando alguien ya no está autorizado?
- Patrones de autorización de AWS
  - ¿Qué políticas de IAM utilizan sus desarrolladores?
  - ¿Utiliza políticas basadas en recursos?
- Registro y monitoreo
  - ¿Qué orígenes de registro utiliza y dónde se almacenan?
  - ¿Agrega los registros de AWS CloudTrail? Si es así, ¿dónde se almacenan?
  - ¿Cómo consulta los registros de CloudTrail?
  - ¿Ha activado Amazon GuardDuty?
  - ¿Cómo accede a los resultados de GuardDuty (por ejemplo, consola, sistema de tickets, SIEM)?
  - ¿Los resultados o eventos se agregan en un SIEM?
  - ¿Los tickets se crean automáticamente?
  - ¿Qué herramientas se utilizan para analizar los registros en una investigación?
- Topología de red
  - ¿Cómo se organizan física o lógicamente los dispositivos, los puntos de conexión y las conexiones de su red?

  - ¿Cómo se conecta su red con AWS?
  - ¿Cómo se filtra el tráfico de red entre entornos?
- Infraestructura externa
  - ¿Cómo se implementan las aplicaciones orientadas al exterior?
  - ¿Qué recursos de AWS son de acceso público?
  - ¿Qué cuentas de AWS contienen infraestructura orientada al exterior?
  - ¿Qué filtros de DDoS o externos existen?

La documentación de los procesos y diagramas técnicos internos facilita el trabajo del analista de respuesta ante incidentes y lo 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.

Desarrollo de sus manuales de estrategias de respuesta ante 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: deben crearse manuales de estrategias para los incidentes que anticipe. Esto puede incluir amenazas como la denegación de servicio (DoS), el ransomware y las amenazas de las credenciales.
- Alertas o resultados de seguridad conocidos: deben crearse manuales de estrategias para las alertas y los resultados de seguridad conocidos, como los resultados de GuardDuty. Podría recibir un resultado de GuardDuty y pensar: “¿Y ahora qué?”. Si desea evitar que un resultado de GuardDuty no se gestione del modo correcto, cree una manual de estrategias para cada posible resultado de GuardDuty. Puede encontrar información e instrucciones sobre los procesos de corrección en la documentación de GuardDuty. Conviene señalar que GuardDuty no está habilitado de forma predeterminada y que tiene un costo. Puede encontrar más detalles sobre

GuardDuty en el Apéndice A: Definiciones de capacidades en la nube: the section called "Visibilidad y alertas".

¿Qué incluir en los manuales de estrategias?

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 de estrategias: ¿qué escenario de riesgo o incidente se aborda en este manual de estrategias? ¿Cuál es el objetivo del manual de estrategias?
- Requisitos previos: ¿qué registros y mecanismos de detección se necesitan en el escenario de este 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?
- Medidas de respuesta: en las diferentes fases de respuesta ante un incidente, ¿qué medidas tácticas se deben tomar? ¿Qué consultas deben ejecutar los analistas? ¿Qué código debe ejecutarse para lograr el resultado deseado?
  - Detección: ¿cómo se va a detectar el incidente?
  - Análisis: ¿cómo se va a determinar el alcance del impacto?
  - Contención: ¿cómo se va a aislar el incidente para limitar el alcance?
  - Erradicación: ¿cómo se va a eliminar la amenaza del entorno?
  - Recuperación: ¿cómo se va a conseguir que el sistema o recurso afectado vuelva a ser productivo?
- Resultados esperados: después de ejecutar las consultas y el código, ¿cuál es el resultado esperado del manual de estrategias?

Para comprobar que la información de cada manual de estrategias sea 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 entre varios manuales de estrategias. Si ese es el caso, puede crear una documentación centralizada para esa información y hacer referencia a ella en el manual de estrategias 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 estos. Por último, es probable que sus manuales de estrategias evolucionen con el tiempo; una vez que haya confirmado que los pasos son coherentes, estos forman los requisitos para la automatización.

Manuales de estrategias de ejemplo

Puede encontrar varios manuales de estrategias de ejemplo en el Apéndice B en the section called "Recursos de manuales de estrategias". Los ejemplos que aparecen aquí se pueden usar como guía sobre qué manuales de estrategias crear y qué incluir en ellos. Sin embargo, es importante que elabore manuales de estrategias que incorporen los riesgos más pertinentes para su empresa. Debe verificar que los pasos y los flujos de trabajo de sus manuales de estrategias incluyan sus tecnologías y procesos.

Realización de simulaciones periódicas

Las organizaciones crecen y evolucionan con el tiempo, al igual que el panorama de amenazas. Por este motivo, es importante revisar continuamente sus capacidades de respuesta ante incidentes. Ejecutar simulaciones es un buen método para llevar a cabo esta evaluación. En las simulaciones, se utilizan escenarios de eventos de seguridad reales diseñados para imitar las tácticas, técnicas y procedimientos (TTP) del actor de una amenaza y permiten a la organización probar y evaluar sus capacidades de respuesta a los incidentes respondiendo a estos simulacros de ataques cibernéticos tal y como podría ocurrir en la realidad.

Las simulaciones tienen diversas ventajas, como, por ejemplo:

- 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 prácticos: el enfoque de los ejercicios prácticos consiste estrictamente en llevar a cabo una sesión de debate en la que participen las diversas partes interesadas en la respuesta a los

incidentes para practicar los roles y responsabilidades y utilizar las herramientas de comunicación y los manuales de estrategia establecidos. Por lo general, este ejercicio se puede hacer durante un día completo en un lugar virtual o físico, o bien en una combinación de ambos. Debido a su naturaleza de debate, el ejercicio de simulación se centra en los procesos, las personas y la colaboración. La tecnología forma parte integral del debate; sin embargo, en este tipo de ejercicio no se hace un uso real de las herramientas o los guiones de respuesta ante incidentes.

- Ejercicios del equipo morado: los ejercicios del equipo morado aumentan el nivel de colaboración entre las personas que se encargan de la respuesta a los incidentes (equipo azul) y los actores de las amenazas simuladas (equipo rojo). Por lo general, el equipo azul está compuesto por miembros del centro de operaciones de seguridad (SOC), pero también puede incluir a otras partes interesadas que participarían durante un ataque cibernético real. El equipo rojo suele estar compuesto por un equipo de pruebas de penetración o partes interesadas clave que cuentan con formación en seguridad ofensiva. El equipo rojo trabaja en colaboración con los facilitadores del ejercicio para diseñar un escenario que sea preciso y factible. Durante los ejercicios del equipo morado, la atención se centra en los mecanismos de detección, las herramientas y los procedimientos operativos estándar (SOP) que facilitan las iniciativas de respuesta a los incidentes.
- Ejercicios del equipo rojo: durante un ejercicio del equipo rojo, el atacante (equipo rojo) hace una simulación para lograr un determinado objetivo o conjunto de objetivos desde un ámbito predeterminado. Los defensores (equipo azul) no conocen necesariamente el ámbito y la duración del ejercicio; de esta manera, se consigue una evaluación más realista de cómo responderían ante un incidente real. Dado que los ejercicios del equipo rojo pueden ser pruebas invasivas, debe tener cuidado e implementar controles para verificar que el ejercicio no produzca un daño real en su entorno.

> **Note**
>
> AWS exige que los clientes revisen la política sobre pruebas de penetración, que está disponible en el sitio web de pruebas de penetración, antes de realizar los ejercicios de equipo morado y el equipo rojo.

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 práctico	Ejercicio del equipo morado	Ejercicio del equipo rojo
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 en papel.	Una oferta más realista en comparación con los ejercicios prácticos. Durante los ejercicios del equipo morado, los facilitadores trabajan en colaboración con los participantes para aumentar su participación en el ejercicio y ofrecen formación cuando es necesario.	Por lo general, se trata de una oferta de simulación más avanzada. Suele haber un alto nivel de encubrimiento, por lo que es posible que los participantes no conozcan todos los detalles del ejercicio.
Recursos necesarios	Recursos técnicos limitados requeridos	Se requieren diversas partes interesadas y un alto nivel de recursos técnicos	Se requieren 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 aportar ventajas únicas para los participantes y la organización en su conjunto, por lo que puede optar por empezar con tipos de simulaciones menos complejos (como los ejercicios prácticos) y pasar luego a los más complejos (ejercicios 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 opten por no llevar a cabo los ejercicios del equipo rojo por su complejidad y su costo.

Ciclo de vida del ejercicio

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

1. Definición de los elementos básicos del ejercicio: defina el escenario de simulación y los objetivos de la simulación. Ambos deben contar con la aceptación de los directivos.

2. Identificación de las principales partes interesadas: como mínimo, en un ejercicio debe haber facilitadores y participantes. En función del escenario, podrían participar otras partes interesadas, como los directivos del departamento legal, de comunicaciones o ejecutivo.
3. Creación y prueba del escenario: es posible que sea necesario redefinir el escenario a medida que se crea si algunos elementos específicos no son factibles. Se espera que, al final de esta etapa, haya un escenario definitivo.
4. Facilitación de la simulación: el tipo de simulación determina la forma de llevarla a cabo (un escenario en papel o un escenario simulado muy técnico). Los facilitadores deben adaptar sus tácticas de facilitación a los objetivos del ejercicio y, siempre que sea posible, involucrar a todos los participantes del ejercicio para obtener la mayor ventaja.
5. Desarrollo del informe posterior a la acción (AAR): identifique las áreas que funcionaron bien, las que pueden mejorar y las posibles carencias. El AAR debe medir la eficacia de la simulación, así como la respuesta del equipo al evento simulado, de modo que se pueda seguir su progreso a lo largo del tiempo con futuras simulaciones.

Tecnología

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

Desarrollo de la estructura de cuentas de AWS

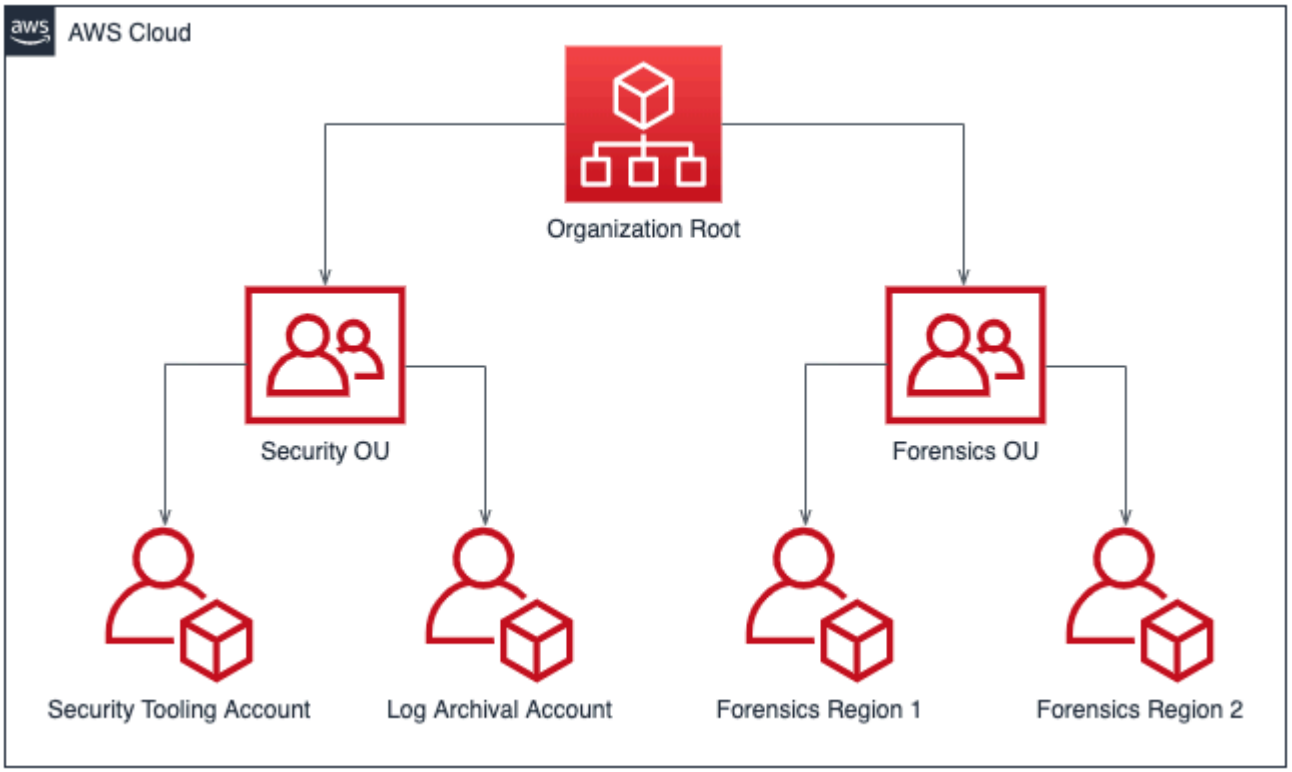
AWS Organizations permite administrar y gestionar un entorno de AWS de forma centralizada a medida que aumentan y se escalan los recursos de AWS. Una organización de AWS se encarga de agrupar las cuentas de AWS para que pueda administrarlas como una sola unidad. Puede utilizar unidades organizativas para agrupar las cuentas que desee administrar como una sola unidad.

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

- Archivo de registros: agregue los registros en una cuenta de AWS para el archivo de registros.
- Herramientas de seguridad: centralice los servicios de seguridad en una cuenta de AWS para las herramientas de seguridad. Esta cuenta funciona como un administrador delegado de los servicios de seguridad.

Dentro de la unidad organizativa forense, tiene la opción de implementar una o varias cuentas forenses diferentes para cada una de las regiones en las que opera, en función de lo que le venga mejor a su modelo empresarial y operativo. Como ejemplo de un enfoque de cuentas por región, si solo opera en Este de EE. UU. (Norte de Virginia) (us-east-1) y Oeste de EE. UU. (Oregón) (us-west-2), tendría dos cuentas en la unidad organizativa forense: una para us-east-1 y otra para us-west-2. Dado que aprovisionar nuevas cuentas lleva tiempo, es imperativo crear e instrumentar las cuentas forenses mucho antes de que se produzca un incidente para que los responsables puedan estar preparados y utilizarlas eficazmente en su respuesta.

En el siguiente diagrama, se muestra un ejemplo de una estructura de cuentas que incluye una unidad organizativa forense con cuentas forenses para cada región:



Estructura de cuentas por región para la respuesta ante 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 pertinentes en relación con un recurso de AWS. Una forma de hacerlo es mediante etiquetas, que asignan metadatos a los recursos de AWS y se componen de una clave y un valor definidos por el usuario. Puede crear etiquetas para clasificar los recursos en función de su propósito, propietario, entorno, tipo de datos procesados y otros criterios de su elección.

Una estrategia de etiquetado coherente puede acelerar los tiempos de respuesta al permitirle identificar y discernir rápidamente la información contextual sobre un recurso de AWS. Las etiquetas también pueden servir como un mecanismo para iniciar automatizaciones de respuesta. Para obtener más información sobre qué etiquetar, consulte la documentación sobre el etiquetado de recursos de AWS. Primero tendrá que definir las etiquetas que desea implementar en toda la organización. Después, implementará y hará cumplir la estrategia de etiquetado. Puede obtener más información sobre la implementación y el cumplimiento en la publicación en el blog de AWS Implement AWS resource tagging strategy using AWS Tag Policies and Service Control Policies (SCPs).

Actualización de la información de contacto de las cuentas de AWS

Para cada una de sus cuentas de AWS, es importante contar con información de contacto precisa y actualizada para que las partes interesadas correspondientes reciban notificaciones importantes de AWS sobre temas como la seguridad, la facturación y las operaciones. Para cada cuenta de AWS, tiene un contacto principal y contactos alternativos para la seguridad, la facturación y las operaciones. Las diferencias entre estos contactos se pueden encontrar en la guía de referencia sobre administración de cuentas de AWS.

Para obtener más información sobre la administración de contactos alternativos, consulte la documentación de AWS sobre cómo agregar, cambiar o eliminar contactos alternativos. Se recomienda utilizar una lista de distribución de correo electrónico si su equipo se encarga de administrar la facturación, las operaciones y los problemas relacionados con la seguridad. Las listas de distribución de correo electrónico eliminan las dependencias de una persona, lo que puede provocar bloqueos si se encuentra fuera de la oficina o deja la empresa. También debe comprobar que el correo electrónico y la información de contacto de la cuenta, incluido el número de teléfono, estén bien protegidos para evitar el restablecimiento de las contraseñas de las cuentas raíz y de la autenticación multifactor (MFA).

Para los clientes que utilicen AWS Organizations, los administradores de la organización pueden administrar 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 usar credenciales para cada cuenta de AWS. También tendrá que comprobar que las cuentas recién creadas tengan información de contacto precisa. Consulte la publicación en el blog Automatically update alternate contacts for newly created Cuentas de AWS.

Preparación del acceso a Cuentas de AWS

Durante un incidente, los equipos de respuesta ante incidentes deben tener acceso a los entornos y recursos involucrados en el incidente. Asegúrese de que los equipos tengan el acceso adecuado

para desempeñar sus funciones antes de que se produzca un evento. Para ello, debe saber qué nivel de acceso necesitan los miembros de su equipo (por ejemplo, qué tipo de acciones es probable que realicen) y debe proporcionar de antemano el acceso con privilegios mínimos.

Para implementar y aprovisionar este acceso, debe identificar y analizar la estrategia de cuentas de AWS y la estrategia de identidad en la nube con los arquitectos de nube de su organización para comprender qué métodos de autenticación y autorización se han configurado. Debido a la naturaleza privilegiada de estas credenciales, debería considerar utilizar flujos de aprobación o recuperar las credenciales de un almacén o caja fuerte como parte de su implementación. Tras la implementación, debe documentar y probar el acceso de los miembros del equipo mucho antes de que se produzca un evento para asegurarse de que pueden responder sin demoras.

Por último, los usuarios que se crean específicamente para responder ante 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.

Información sobre el panorama de amenazas

Desarrollo de 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 publicación en el blog How to approach threat modeling. Para la respuesta ante incidentes, un modelo de amenazas puede ayudar a identificar los vectores de ataque que un actor de amenazas podría haber utilizado durante un incidente. Entender contra qué se defiende será crucial para poder responder de manera oportuna. También puede utilizar una AWS Partner para el modelado de amenazas. Para buscar un socio de AWS, use la AWS Partner Network.

Integración y uso de la inteligencia de ciberamenazas

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

Para integrar y maximizar la inteligencia de amenazas para su entorno de AWS, puede utilizar algunas funciones listas para usar e integrar sus propias listas de inteligencia de amenazas. Amazon

GuardDuty utiliza orígenes de inteligencia de amenazas internas de AWS y de terceros. Otros servicios de AWS, como el firewall DNS y las reglas de AWS WAF, también reciben información del grupo de inteligencia de amenazas avanzada de AWS. Algunos resultados de GuardDuty están asignados al marco MITRE ATT&CK, que proporciona información sobre observaciones del mundo real sobre 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 en el blog de AWS Logging strategies for security incident response.

Selección y habilitación de los orígenes de registro

Antes de una investigación de seguridad, necesita obtener los registros pertinentes para reconstruir de forma retroactiva la actividad que se ha producido en una cuenta de AWS. Seleccione y habilite los orígenes de registro pertinentes para las cargas de trabajo de sus cuentas de AWS.

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

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

Los registros de AWS CloudTrail, los registros de flujo de VPC y los registros de consulta de Route 53 Resolver son los tres tipos de registros básicos que facilitan las investigaciones de seguridad en AWS.

Los servicios de AWS pueden generar registros que no capturan los tres tipos de registros básicos, como los registros de Elastic Load Balancing, los registros de AWS WAF, los registros del registrador de AWS Config, los resultados de Amazon GuardDuty, los registros de auditoría de Amazon Elastic Kubernetes Service (Amazon EKS) y los registros del sistema operativo y las aplicaciones de las instancias de Amazon EC2. Consulte la lista completa de opciones de registro y monitoreo en the section called “Apéndice A: Definiciones de capacidades en la nube”.

Selección del almacenamiento de registros

La elección del almacenamiento de registros suele estar relacionada con la herramienta de consulta que utilice, las capacidades de retención, la familiaridad y el costo. Cuando habilite los registros de servicio de AWS, debe proporcionar una instalación de almacenamiento; normalmente, un bucket de Amazon S3 o un grupo de registro de CloudWatch.

Un bucket de Amazon S3 es un almacenamiento rentable y duradero que tiene una política de ciclo de vida opcional. Los registros almacenados en los buckets de Amazon S3 pueden consultarse a través de servicios como Amazon Athena. Un grupo de registro de CloudWatch ofrece un almacenamiento duradero y una utilidad de consulta integrada a través de Información de registros de CloudWatch.

Identificación de la retención de registros adecuada

Cuando utilice un bucket de S3 o un grupo de registro de CloudWatch para almacenar registros, debe establecer ciclos de vida adecuados para cada origen de registros a fin de optimizar los costos de almacenamiento y recuperación. Por lo general, los clientes tienen entre tres y doce meses de registros disponibles para su consulta, con un periodo de retención de hasta siete años. La elección de la disponibilidad y el periodo de retención debe ajustarse a sus requisitos de seguridad y a una combinación de requisitos legales, reglamentarios y empresariales.

Selección e implementación de mecanismos de consulta para los registros

En AWS, los principales servicios que puede utilizar para consultar los registros son Información de registros de CloudWatch para los datos almacenados en los grupos de registro de CloudWatch, y Amazon Athena y Amazon OpenSearch Service para los datos almacenados en Amazon S3. También puede utilizar herramientas de consulta de terceros, como una herramienta de administración de eventos e información de seguridad (SIEM).

En el proceso de selección de una herramienta de consulta de registros, se deben tener en cuenta los aspectos relacionados con las personas, los procesos y la tecnología de sus operaciones de seguridad. Seleccione una herramienta que cumpla los requisitos operativos, empresariales y de seguridad, y que sea accesible y pueda mantenerse a largo plazo. Tenga en cuenta que las herramientas de consulta de registros funcionan de forma óptima cuando el número de registros a analizar se mantiene dentro de los límites de la herramienta. No es raro que los clientes dispongan de varias herramientas de consulta debido a limitaciones técnicas o de costos. Por ejemplo, los clientes podrían utilizar una herramienta SIEM de terceros para hacer consultas en los últimos 90 días de datos y utilizar Athena para efectuar consultas anteriores a esos 90 días debido al costo de la ingestión de registros de una herramienta SIEM. Independientemente de cuál sea la implementación, compruebe que su enfoque permite reducir al mínimo el número de herramientas necesarias para maximizar la eficiencia operativa, especialmente durante la investigación de un evento de seguridad.

Uso de los registros para las 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 alertas de seguridad que no cubran estos servicios o para alertas específicas pertinentes para su entorno. La creación de estas alertas y detecciones se describe en la sección denominada the section called “Detección” en este documento.

Desarrollo de 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. En la guía Guide to Integrating Forensic Techniques into Incident Response del NIST se proporciona esa orientación.

Análisis forenses en AWS

Los conceptos de la ciencia forense tradicional que se utiliza en el entorno en las instalaciones también son aplicables a AWS. Las publicación en el blog Forensic investigation environment strategies in the Nube de AWS le proporciona información clave para empezar a migrar su conocimiento experto forense a AWS.

Una vez que haya configurado la estructura del entorno y las cuentas de AWS para el análisis forense, deberá definir las tecnologías necesarias para ejecutar de forma eficaz unas metodologías sólidas desde el punto de vista forense en las cuatro fases:

- Recopilación: recopile registros de AWS pertinentes, como los registros de AWS CloudTrail, AWS Config, de flujo de VPC y de nivel de host. Recopile instantáneas, copias de seguridad y volcados de memoria de los recursos de AWS afectados.
- Examen: examine los datos recopilados mediante la extracción y la evaluación de la información importante.
- Análisis: analice los datos recopilados para comprender el incidente y sacar conclusiones.
- Informes: presente la información resultante de la fase de análisis.

Captura de copias de seguridad e instantáneas

Crear copias de seguridad de los principales sistemas y bases de datos es fundamental para poder recuperarse de un incidente de seguridad y para fines forenses. Con las copias de seguridad, puede restaurar los sistemas a su estado seguro anterior. En AWS, puede crear instantáneas de diversos recursos. Las instantáneas le proporcionan copias de seguridad puntuales de esos recursos. Hay muchos servicios de AWS que pueden ayudarle con la copia de seguridad y la recuperación. Consulte Backup and Recovery Prescriptive Guidance para obtener más detalles sobre estos servicios y enfoques de copia de seguridad y recuperación. Para obtener más información, consulte la entrada en el blog Use backups to recover from security incidents.

Es esencial que las copias de seguridad estén bien protegidas, especialmente en ciertas situaciones, como el ransomware. Para obtener información sobre cómo proteger las copias de seguridad, consulte Top 10 security best practices for securing backups in AWS. Además de proteger las copias de seguridad, debe probar periódicamente los procesos de copia de seguridad y restauración para comprobar que la tecnología y los procesos que tiene implementados funcionan según lo previsto.

Automatización de los análisis forenses en AWS

Durante un evento de seguridad, es necesario que el equipo de respuesta ante incidentes pueda recopilar y analizar las pruebas rápidamente y, al mismo tiempo, mantener la precisión durante todo el tiempo que rodee al evento. Para el equipo de respuesta ante incidentes, resulta difícil y lleva mucho tiempo recopilar manualmente las pruebas pertinentes en un entorno en la nube, especialmente en una gran cantidad 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 de los análisis forenses.

AWS ofrece una serie de recursos de automatización para los análisis forenses, que se consolidan en el apéndice de the section called “Recursos de análisis forense”. 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 exhaustiva para responder a los eventos de seguridad es fundamental para ofrecer una respuesta oportuna y eficaz ante los incidentes. La preparación de la respuesta ante 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 ante incidentes en los tres dominios.

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

Tabla 2: elementos de preparación para la respuesta ante incidentes

Dominio	Elemento de preparación	Elementos de acción
Personas	Defina los roles y las responsabilidades.	• Identifique a las partes interesadas pertinentes en la respuesta ante incidente s. • Desarrolle un diagrama RACI (responsable, aprobador, consultad o, informado) para un incidente.
Personas	Forme al personal de respuesta ante incidentes sobre AWS.	• Forme a las partes interesadas en la respuesta ante incidentes sobre los fundamentos de AWS. • Forme a las partes interesadas en la respuesta ante incidentes sobre los servicios de seguridad y monitoreo de AWS.

Dominio	Elemento de preparación	Elementos de acción
		• Forme a las partes interesadas en la respuesta ante incidentes sobre su entorno de AWS y su arquitectura.
Personas	Información sobre las opciones de soporte de AWS.	• Comprenda las diferencias entre el soporte de AWS, el equipo de respuesta ante incidentes de clientes (CIRT), el equipo de respuesta a ataques DDoS (DRT) y AMS. • Comprenda el proceso de clasificación y escalado para contactar con el CIRT durante un evento de seguridad activo, si es necesario.
Proceso	Desarrolle un plan de respuesta ante incidentes.	• Cree un documento de alto nivel que defina su programa y estrategia de respuesta ante incidentes. • En el plan de respuesta ante incidentes, incluya una matriz RACI, un plan de comunicación, definiciones de incidentes y fases de respuesta ante incidentes.

Dominio	Elemento de preparación	Elementos de acción
Proceso	Documente y centralice los diagramas de arquitectura.	• Documente los detalles sobre cómo está configura do el entorno de AWS en cuanto a la estructura de cuentas, el uso de servicios, los patrones de IAM y otras funcionalidades principal es de su configuración de AWS. • Desarrolle diagramas de arquitectura de sus arquitect uras en la nube.
Proceso	Desarrolle manuales de estrategias de respuesta ante incidentes.	• Cree una plantilla para la estructura de sus manuales de estrategias. • Cree manuales de estrategi as para los eventos de seguridad previstos. • Cree manuales de estrategi as para las alertas de seguridad conocidas, como los resultados de GuardDuty .
Proceso	Realice simulaciones con regularidad.	• Desarrolle una cadencia regular para realizar las simulaciones de incidentes. • Utilice los resultados y las lecciones aprendidas para repetir su programa de respuesta ante incidentes.

Dominio	Elemento de preparación	Elementos de acción
Tecnología	Desarrolle una estructura de cuentas de AWS.	• Planifique una estructura de cuentas para separar las cargas de trabajo por cuentas de AWS. • Cree una unidad organizativa de seguridad con una cuenta de almacenamiento de registros y herramientas de seguridad. • Cree una unidad organizativa de análisis forenses con cuentas forenses para cada región en la que opere.
Tecnología	Desarrolle e implemente una estrategia de etiquetado que ayude a los respondedores a identificar la propiedad y el contexto de los resultados.	• Planifique una estrategia de etiquetado y establezca qué etiquetas quiere asociar a sus recursos de AWS. • Implemente y aplique la estrategia de etiquetado.
Tecnología	Actualice la información de contacto de las cuentas de AWS.	• Compruebe que las cuentas de AWS 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 las cuentas de AWS.

Dominio	Elemento de preparación	Elementos de acción
Tecnología	Prepare el acceso a las cuentas de AWS.	• Defina qué acceso necesitarán los servicios de respuesta ante incidente s para responder a un incidente. • Implemente, pruebe y monitoree el acceso.
Tecnología	Comprenda el panorama de amenazas.	• Desarrolle modelos de amenazas para su entorno y sus aplicaciones. • Integre y use la inteligencia de ciberamenazas.
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 las alertas.

Dominio	Elemento de preparación	Elementos de acción
Tecnología	Desarrolle capacidades de análisis forenses.	• Identifique los artefactos necesarios para la recolección 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 automatización para el análisis forense.

Se recomienda un enfoque iterativo para la preparación de la respuesta ante 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 ante 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 las operaciones

Fase	Objetivo
Detección	Identifique un posible evento de seguridad.
Análisis	Determine si el evento de seguridad es un incidente y evalúe su alcance.

Fase	Objetivo
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 monitoree estos sistemas para comprobar que la amenaza no regrese.

Las fases deben servir de guía a la hora de responder y operar en los incidentes de seguridad con el fin de responder de manera eficaz y sólida. Las medidas reales que tome variarán según el incidente. Por ejemplo, un incidente relacionado con ransomware contará con un proceso de respuesta diferente al de un incidente que involucre a un bucket de Amazon S3 público. Además, no es necesario que estas fases se produzcan de forma secuencial. Tras la contención y la erradicación, es posible que tenga que volver al análisis para saber si sus acciones fueron eficaces.

Detección

La alerta es el componente principal de la fase de detección. Genera una notificación para iniciar el proceso de respuesta ante incidentes en función de la actividad de las cuentas de AWS que le interese.

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 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 líneas de base cambian con el tiempo. Los patrones maliciosos surgen a través de tácticas, técnicas y procedimientos (TTP) de los actores de amenazas novedosos o modificados.

- Los cambios en las personas, la tecnología y los procesos no se incorporan inmediatamente al proceso de respuesta ante incidentes. Algunos se descubren durante el progreso de una investigación.

Orígenes de alertas

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

- Resultados: los servicios de AWS como Amazon GuardDuty, AWS Security Hub, Amazon Macie, Amazon Inspector, AWS Config, el Analizador de acceso de IAM y el Analizador de acceso a la red generan resultados que se pueden utilizar para elaborar alertas.
- Registros: los registros de servicios, infraestructura y aplicaciones de AWS almacenados en buckets de Amazon S3 y grupos de registro de CloudWatch se pueden analizar y correlacionar para generar alertas.
- Actividad de facturación: un cambio repentino en la actividad de facturación puede indicar un evento de seguridad. Siga la documentación de Crear una alarma de facturación para supervisar los cargos estimados de AWS para monitorearlo.
- Inteligencia de ciberamenazas: si se suscribe a un origen de inteligencia de ciberamenazas de terceros, puede correlacionar esa información con otras herramientas de registro y monitoreo para identificar posibles indicadores de eventos.
- Herramientas de socios: los socios de la AWS Partner Network (APN) ofrecen productos de primer nivel que pueden ayudarlo a cumplir sus objetivos de seguridad. Para la respuesta ante incidentes, los productos de socios con detección y respuesta de puntos de conexión (EDR) o SIEM pueden ayudarlo a cumplir sus objetivos de respuesta ante incidentes. Para obtener más información, consulte Soluciones de socios de seguridad y Soluciones de seguridad en AWS Marketplace.
- Confianza y seguridad de AWS: Soporte podría contactar a los clientes si identificamos actividad abusiva o malintencionada.
- Contacto único: dado que pueden ser sus clientes, desarrolladores u otros miembros del personal de su organización quienes adviertan algo inusual, es importante contar con un método conocido y bien publicitado para ponerse en contacto con su equipo de seguridad. Entre las opciones más populares se incluyen los sistemas de tickets, 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 en la nube que puede utilizar durante sus investigaciones, consulte the section called “Apéndice A: Definiciones de capacidades en la nube” en este documento.

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 definen los controles directivos y preventivos, se deben construir los controles de detección y respuesta relacionados. Por ejemplo, una organización establece un control directivo relacionado con el usuario raíz de una cuenta de AWS, que solo debe usarse para actividades específicas y muy bien definidas. Lo asocia a un control preventivo implementado mediante la política de control de servicio (SCP) de una organización de AWS. Si la actividad del usuario raíz supera la línea de base esperada, un control de detección implementado con una regla de EventBridge y un tema de SNS alertará al centro de operaciones de seguridad (SOC). El control de respuesta implica que el SOC seleccione el manual de estrategias adecuado, lleve a cabo el análisis y trabaje hasta que se resuelva el incidente.

La mejor forma de definir los controles de seguridad es mediante el modelado de amenazas de las cargas de trabajo que se ejecutan en AWS. El nivel de gravedad de los controles de detección se determinará analizando 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 se producen, sino que se basan en su nivel de gravedad inicial, que se ajustará durante el análisis. El nivel de gravedad inicial establecido ayuda a definir prioridades; el contexto en el que se haya producido la alerta determinará su verdadero nivel de gravedad. Por ejemplo, una organización utiliza Amazon GuardDuty como componente del control de detección que se utiliza para las instancias de EC2 que forman parte de una carga de trabajo. Se genera el resultado `Impact:EC2/SuspiciousDomainRequest.Reputation` y le informa de que la instancia de Amazon EC2 que aparece en la lista dentro de su carga de trabajo está consultando un nombre de dominio que se sospecha que es malicioso. Esta alerta se configuró de forma predeterminada como de gravedad baja y, a medida que avanzaba la fase de análisis, se determinó que un actor no autorizado había implementado varios cientos de instancias de EC2 del tipo `p4d.24xlarge`, lo que aumentó considerablemente los costos operativos de la organización. En este punto, el equipo de respuesta ante incidentes toma la decisión de ajustar el nivel de gravedad de esta alerta a alta, lo que aumenta la sensación de urgencia y agiliza las acciones futuras. Tenga en cuenta que la gravedad del resultado de GuardDuty no se puede cambiar.

Implementaciones de controles de detección

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 técnicos:

- La detección del comportamiento se basa en modelos matemáticos que se conocen comúnmente como machine learning (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 se generarán alertas, y eso es seguro.

Las implementaciones modernas de sistemas de detección, como un sistema de detección de intrusiones (IDS), suelen incluir ambos mecanismos. A continuación, se presentan algunos ejemplos de detecciones basadas en reglas y de comportamiento con GuardDuty.

- Cuando se genera el resultado `Exfiltration:IAMUser/AnomalousBehavior`, le informa de que “se ha observado una solicitud de API anómala en su cuenta”. A medida que profundiza en la documentación, se indica que “el modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios”, lo que indica que este resultado se refiere al comportamiento.
- Para el resultado `Impact:S3/MaliciousIPCaller`, GuardDuty analiza las llamadas a la API del servicio Amazon S3 en CloudTrail y compara el elemento de registro `SourceIPAddress` 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 resultado.

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

Detección basada en personas

Hasta este punto, hemos hablado de la detección basada en la tecnología. El otro origen importante de detección proviene de personas dentro o fuera de la organización del cliente. Las personas internas se pueden definir como empleados o contratistas, y las personas externas son entidades como investigadores de seguridad, fuerzas del orden, medios de comunicación y redes sociales.

Aunque 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, tickets, correo postal, publicaciones de noticias, llamadas telefónicas e interacciones en persona. Cabe esperar que las notificaciones de detección basadas en la tecnología se envíen en tiempo casi real, pero no hay expectativas de plazos para la detección basada en personas. Es imprescindible que la cultura de seguridad incorpore, facilite y potencie los mecanismos de detección basados en las personas para adoptar un enfoque de defensa en profundidad para la seguridad.

Resumen

En el caso de la detección, es importante contar con una combinación de alertas basadas en reglas y en el comportamiento. Además, debe contar con mecanismos para que las personas, tanto internas como externas, envíen tickets sobre los problemas de seguridad. Los seres humanos pueden ser uno de los orígenes más valiosos de eventos de seguridad, por lo que es importante contar con procesos para que las personas puedan derivar sus preocupaciones a los superiores. Debe utilizar los modelos de amenazas de su entorno para empezar a crear detecciones. Los modelos de amenazas lo ayudarán a crear alertas basadas en las amenazas más pertinentes para su entorno. Por último, puede utilizar marcos como MITRE ATT&CK para comprender las tácticas, técnicas y procedimientos (TTP) de los actores de amenazas. Utilizar el marco MITRE ATT&CK como lenguaje común puede resultar útil en sus diversos mecanismos de detección.

Análisis

Los registros, las capacidades de consulta y la inteligencia de 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.

Validación, determinación del alcance y evaluación del impacto de la alerta

Durante la fase de análisis, se realiza un análisis exhaustivo del registro con el objetivo de validar las alertas, definir su 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 los incidentes buscarán entradas de registro procedentes de diversos orígenes y se pondrán en contacto directamente con los responsables de la carga de trabajo afectada.
- El siguiente paso es determinar el alcance, cuando se haría un inventario de todos los recursos involucrados y se ajustaría el nivel de gravedad 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, en el análisis de impacto se detalla la verdadera interrupción para la empresa.

Una vez identificados los componentes de la carga de trabajo afectados, los resultados del análisis del alcance se pueden correlacionar con el objetivo de punto de recuperación (RPO) y el objetivo de tiempo de recuperación (RTO) de la carga de trabajo correspondiente, ajustándose al nivel de gravedad de la alerta, lo que iniciará la asignación de recursos y toda la actividad que tendrá lugar a continuación. No todos los incidentes interrumpirán directamente las operaciones de una carga de trabajo que respalda un proceso empresarial. Es posible que incidentes como la divulgación de información confidencial, 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.

Enriquecimiento de los registros y resultados de seguridad

Enriquecimiento con inteligencia de amenazas y contexto organizativo

Durante el transcurso del análisis, es necesario enriquecer los elementos observados de interés para mejorar la contextualización de la alerta. Como se indica en la sección de preparación, integrar y aprovechar la inteligencia de ciberamenazas puede resultar útil para comprender mejor un resultado de seguridad. Los servicios de inteligencia de amenazas se utilizan para asignar reputación y atribuir la propiedad a las direcciones IP públicas, los nombres de dominio y los hashes de archivo. 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 consultas SQL para correlacionar elementos del registro, como direcciones IP y 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 GuardDuty utilizan la inteligencia de amenazas para el enriquecimiento y la generación de resultados. También puede cargar listas de amenazas personalizadas en GuardDuty basadas en su propia inteligencia de amenazas.

Enriquecimiento con automatización

La automatización es una parte integral de la gobernanza en la Nube de AWS. Se puede utilizar en las distintas fases del ciclo de vida de la respuesta ante 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 observados para contextualizar el evento.

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

Consulte la publicación en el blog How to enrich AWS Security Hub findings with account metadata para ver un ejemplo sobre cómo utilizar la automatización para enriquecer los resultados de seguridad y simplificar el análisis.

Recopilación y análisis de las pruebas forenses

La ciencia forense, como se menciona en la sección the section called “Preparación” de este documento, es el proceso de recopilar y analizar artefactos durante la respuesta ante incidentes. En AWS, esto 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 servicio, como los registros de 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 en el mismo artefacto.
- Común: está documentado públicamente y se ha adoptado ampliamente.

Es importante mantener una cadena de custodia para los artefactos recolectados durante la respuesta ante incidentes. La automatización y la generación automática de la documentación de esta colección pueden ayudar, además del almacenamiento de los artefactos en repositorios de solo lectura. El análisis solo debe realizarse en réplicas exactas de los artefactos recopilados para mantener la integridad.

Recolección de artefactos pertinentes

Teniendo en cuenta estas características, y en función de las alertas pertinentes y de la evaluación del impacto y el alcance, tendrá que recopilar los datos que sean pertinentes para continuar la investigación y el análisis. Existen diversos tipos y orígenes de datos que pueden ser pertinentes para la investigación, como los registros del plano de control o de servicio (CloudTrail, eventos de datos de Amazon S3, registros de flujo de VPC), datos (metadatos y objetos de Amazon S3) y recursos (bases de datos o instancias de Amazon EC2).

Los registros del plano de control o de servicio se pueden recopilar para analizarlos localmente o, idealmente, se pueden consultar directamente mediante servicios nativos de AWS (cuando proceda). Los datos (incluidos los metadatos) se pueden consultar directamente para obtener información pertinente o para adquirir los objetos de origen; por ejemplo, utilice la 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 copia o instantánea del sistema que ejecuta la base de datos, creando una copia o instantánea de toda la base de datos en sí o consultando y extrayendo ciertos datos y registros de la base de datos pertinentes para la investigación.

En el caso de las instancias de Amazon EC2, hay un conjunto específico de datos que se deben recopilar y un orden específico de recopilación que se debe seguir 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 instancia de Amazon EC2 es el siguiente:

1. Adquirir metadatos de la instancia: adquiera los metadatos de la instancia pertinente para la investigación y las consultas de datos (ID de instancia, tipo, dirección IP, ID de VPC/subred, región, ID de imagen de máquina de Amazon (AMI), grupos de seguridad adjuntos, hora de lanzamiento).
2. Habilitar las protecciones y etiquetas de las instancias: habilite las protecciones de las instancias, como la protección contra terminación, configure el comportamiento de apagado para que se detenga (si está configurado para terminarse), deshabilite los atributos “Delete on Termination” de los volúmenes de EBS 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 `Quarantine`, realizar una adquisición forense de datos y aislar la instancia).

3. Adquirir el disco (instantáneas de EBS): adquiera una instantánea de EBS de los volúmenes de EBS adjuntos. Cada instantánea contiene información necesaria para restaurar los datos (del momento en que se tomó) en un volumen de EBS nuevo. Consulte el paso para realizar una recopilación de artefactos o respuestas en vivo si utiliza volúmenes de almacén de instancias.
4. Adquirir memoria: dado que las instantáneas de EBS solo capturan los datos que se han escrito en su volumen de Amazon EBS, lo que podría excluir los datos que las aplicaciones o el sistema operativo almacenan o guardan en caché en la memoria, es imprescindible adquirir una imagen de memoria del sistema mediante una herramienta comercial o de código abierto de terceros adecuada para obtener los datos disponibles del sistema.
5. (Opcional) Realizar una recopilación de artefactos o una respuesta en vivo: realice una recopilación de datos específica (disco/memoria/registros) mediante una respuesta en vivo en el sistema únicamente si no se puede adquirir el disco o la memoria de otra manera, o si existe un motivo empresarial u operativo válido. Con ello, se modificarán datos y artefactos valiosos del sistema.
6. Retirar la instancia: separe la instancia de los grupos de escalado automático, anule el registro de la instancia de los equilibradores 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 de entrada y salida de la instancia. Para obtener más información, consulte la sección the section called “Contención” de este documento.
8. Decisión del responsable: en función de la situación y los objetivos, seleccione una de las siguientes opciones:
   - Retirar y apagar el sistema (recomendado).

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

     Aunque no se recomienda como enfoque estándar, si una situación justifica una observación continua de la instancia (por ejemplo, cuando se necesitan datos o más indicadores 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 de análisis forenses dedicada dentro de un entorno de pruebas que esté preconfigurado para estar completamente aislado y configurado con instrumentación que facilite la supervisión casi continua de la instancia (por ejemplo, registros de flujo de VPC o duplicación de tráfico de VPC).

> **Note**
>
> Es esencial capturar la memoria antes de las actividades de respuesta en vivo o del aislamiento o apagado del sistema para capturar los datos volátiles (y valiosos) disponibles.

Desarrollo de narrativas

Durante el análisis y la investigación, documente las acciones tomadas, los análisis realizados y la información identificada, para utilizarlos en las fases posteriores y, en última instancia, en un informe final. Estas narrativas deben ser breves y precisas y debe asegurarse de que se incluya la información pertinente para verificar la comprensión efectiva del incidente y mantener una cronología precisa. También son útiles cuando interactúa con personas ajenas al equipo principal de respuesta ante incidentes. A continuación se muestra un ejemplo:

> El departamento de marketing y ventas recibió una nota de rescate el 15 de marzo de 2022 en la que se exigía el pago en criptomonedas para evitar la divulgación pública de posible información confidencial. El SOC determinó que la base de datos de Amazon RDS perteneciente a marketing y ventas fue de acceso público el 20 de febrero de 2022. El SOC consultó los registros de acceso de RDS y determinó que la dirección IP 198.51.100.23 se utilizó el 20 de febrero de 2022 con las credenciales *`mm03434`*, pertenecientes a Major Mary, una de las desarrolladoras web. El SOC consultó los registros de flujo de VPC y determinó que aproximadamente 256 MB de datos salieron hacia la misma dirección IP en la misma fecha (marca de tiempo 2022-02-20T15:50+00Z). El SOC determinó, mediante inteligencia de amenazas de código abierto, que las credenciales están disponibles actualmente en texto plano en el repositorio público *`https[:]//example[.]com/majormary/rds-utils`*.

Contención

Las contenciones, en lo que respecta a la respuesta ante incidentes, se definen como 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.

En la guía SP 800-61 Computer Security Incident Handling Guide del NIST se describen varios criterios para determinar la estrategia de contención adecuada, como, por ejemplo:

- 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 que se eliminará en dos semanas, solución permanente)

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

- Contención del origen: utilice el filtrado y el enrutamiento para evitar el acceso desde un origen determinado.
- Contención de técnicas y accesos: 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.

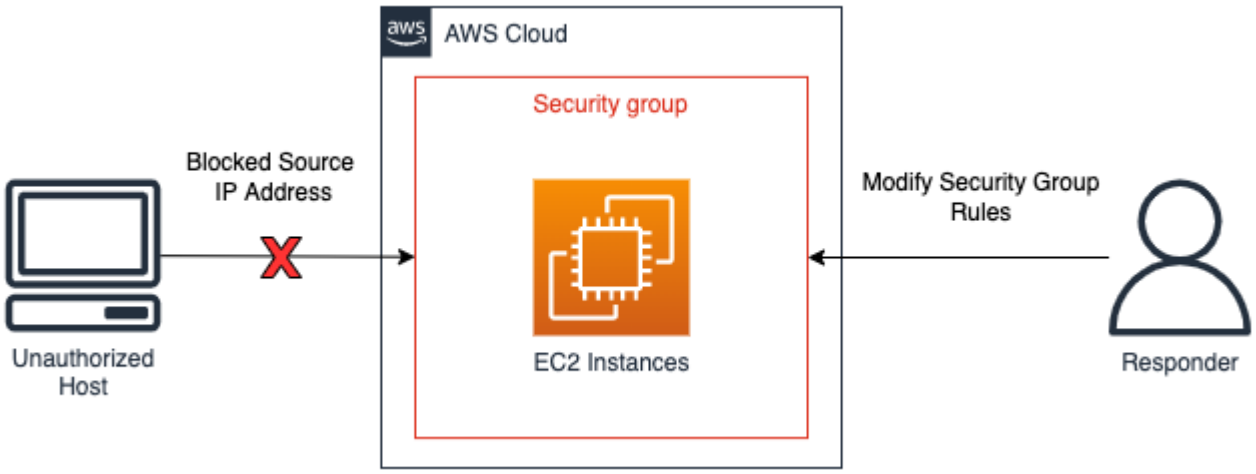
Contención del origen

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

- Grupos de seguridad: crear y aplicar grupos de seguridad de aislamiento a instancias de Amazon EC2 o eliminar reglas de un grupo de seguridad existente puede ayudar a contener el tráfico no autorizado a una instancia de Amazon EC2 o recurso de AWS. Es importante tener en cuenta que las conexiones rastreadas existentes no se cerrarán como resultado del cambio de grupos de seguridad; el nuevo grupo de seguridad solo bloqueará eficazmente el tráfico futuro (consulte este manual de estrategias de respuesta ante incidentes y Seguimiento de conexiones del grupo de seguridad para obtener más información 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 punto de conexión de VPC. Las políticas crean la capacidad de bloquear direcciones sospechosas y el acceso al bucket de Amazon S3. Puede encontrar más información sobre las políticas de bucket en Agregar una política de bucket mediante la consola de Amazon S3.
- AWS WAF: las listas de control de acceso web (ACL web) se pueden configurar en AWS WAF para proporcionar un control detallado sobre las solicitudes web a las que responden los recursos. Puede agregar una dirección IP o un rango de redes a un conjunto de IP configurado en AWS WAF y aplicar condiciones de coincidencia, como bloqueo, al conjunto de IP. Esto bloqueará las solicitudes web a un recurso si la dirección IP o los rangos de red del 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 origen en el que un analista de respuesta ante incidentes modifica un grupo de seguridad de una instancia de Amazon EC2 para restringir las nuevas conexiones solo a determinadas direcciones IP. Como se indica en el punto sobre los grupos de seguridad, como resultado del cambio de grupos de seguridad las conexiones rastreadas existentes no se cerrarán.



Ejemplo de contención del origen

> **Note**
>
> Los grupos de seguridad y las ACL de la red no filtran el tráfico a Amazon Route 53. Al contener una instancia de EC2, si quiere evitar que se comunique con hosts externos, asegúrese de bloquear también de forma explícita las comunicaciones DNS.

Contención de técnicas y acceso

Para evitar el uso no autorizado de un recurso, limite las funciones y las entidades principales de IAM con acceso al recurso. Para ello, restrinja los permisos de las entidades principales de IAM que tienen acceso al recurso; también puede revocar las credenciales de seguridad temporales. A continuación, se destacan algunos ejemplos de contención de técnicas y acceso mediante servicios de AWS:

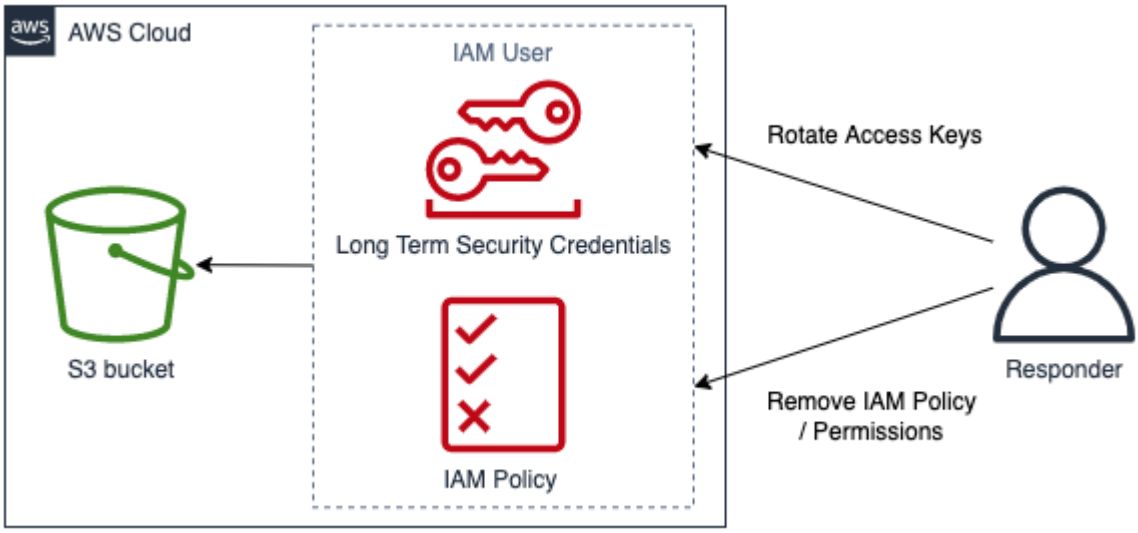
- Restringir los permisos: los permisos asignados a una entidad principal de IAM deben seguir el principio de privilegios mínimos. Sin embargo, durante un evento de seguridad activo, es posible que tenga que restringir aún más el acceso a un recurso específico desde una entidad principal de IAM concreta. En este caso, puede contener el acceso a un recurso quitando los permisos de la entidad principal de IAM que se va a contener. Esto se hace con el servicio de IAM y se puede aplicar mediante la AWS Management Console, la AWS CLI o un SDK de AWS.
- Revocar claves: las entidades principales de IAM utilizan las claves de acceso de IAM para acceder a los recursos o administrarlos. Se trata de credenciales estáticas de larga duración para firmar solicitudes mediante programación a la AWS CLI o la API de AWS y comienzan con el prefijo AKIA (para obtener más información, consulte la sección Descripción de los prefijos de ID único en Identificadores de IAM). Para contener el acceso de una entidad principal de IAM cuya clave de acceso de IAM se haya visto comprometida, puede desactivar o eliminar la clave de acceso. 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.
  - Una entidad principal de IAM puede tener hasta dos claves de acceso en un momento dado.
  - Los usuarios o las aplicaciones que utilicen 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 emplear las credenciales de seguridad temporales para controlar el acceso a los recursos de AWS. Estas credenciales comienzan con el prefijo ASIA (para obtener más información, consulte la sección Descripción de los prefijos de ID único en Identificadores de IAM). Los roles de IAM suelen utilizar credenciales temporales y no es necesario rotarlas ni revocarlas explícitamente porque tienen una duración limitada. En los casos en que se produzca un incidente de seguridad que implique una credencial de seguridad temporal antes de que esta caduque, es posible que tenga que modificar los permisos efectivos de las credenciales de seguridad temporales existentes. Esto se puede realizar mediante el servicio de IAM dentro de la AWS Management Console. También se pueden emitir credenciales de seguridad temporales a los usuarios de IAM (a diferencia de los

roles de IAM); sin embargo, en el momento de escribir este artículo, no existe la opción de revocar las credenciales de seguridad temporales de un usuario de IAM dentro de la AWS Management Console. En los casos de seguridad en los que la clave de acceso de IAM de un usuario se vea comprometida por un usuario no autorizado que creó credenciales de seguridad temporales, existen dos métodos para revocar las credenciales de seguridad temporales:

- Adjuntar al usuario de IAM una política insertada que impida el acceso en función del momento en que se haya emitido el token de seguridad (consulte la sección Denegar el acceso a sesiones de credenciales de seguridad temporales con claves de contexto de condiciones en Deshabilitar permisos para credenciales de seguridad temporales para obtener más información).
- Eliminar el usuario de IAM propietario de las claves de acceso comprometidas. Si es necesario, vuelva a crear el usuario.

- AWS WAF: algunas técnicas empleadas por usuarios no autorizados son los patrones de tráfico maliciosos comunes, como solicitudes que contienen inyección de código SQL y scripting entre sitios (XSS). AWS WAF se puede configurar para detectar y denegar el tráfico que emplea estas técnicas utilizando las declaraciones de reglas integradas de AWS WAF.

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



Ejemplo de contención de técnicas y acceso

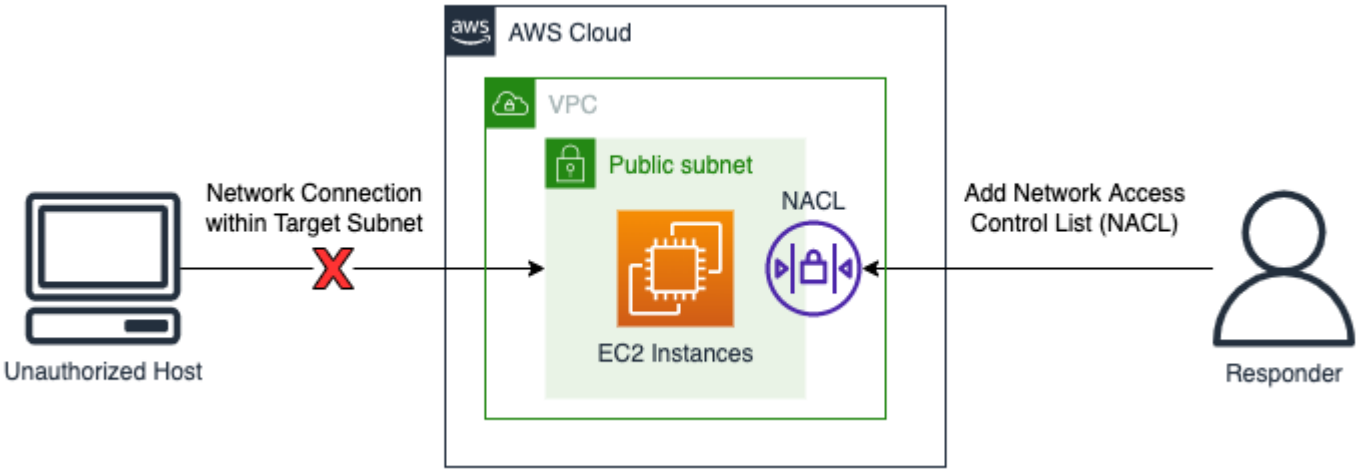
Contención del destino

La contención del destino 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 repliquen para garantizar su disponibilidad; los recursos deben separarse de estas formas de resiliencia para aislarlos y contenerlos. A continuación, se indican algunos ejemplos de contención del destino mediante los servicios de AWS:

- ACL de la red: a las ACL de la red que están configuradas en subredes que contienen recursos de AWS se les pueden agregar reglas de denegación. Estas reglas de denegación se pueden aplicar para impedir el acceso a un recurso de AWS en particular; sin embargo, la aplicación de una lista de control de acceso de la red (ACL de la red) afectará a todos los recursos de la subred, no solo a los recursos a los que se acceda sin autorización. Las reglas enumeradas en una ACL de la red se procesan en orden descendente, por lo que la primera regla de una ACL de la red existente debe configurarse para denegar el tráfico no autorizado al recurso y la subred de destino. Como alternativa, se puede crear una ACL de la 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 mediante la nueva ACL de la red.
- Apagado: apagar un recurso por completo puede ser eficaz para contener los efectos del uso no autorizado. El apagado 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.
- VPC de aislamiento: las VPC de aislamiento se pueden utilizar para contener los recursos de forma eficaz y, al mismo tiempo, permitir el acceso al tráfico legítimo (como las soluciones antivirus [AV] o EDR que requieren acceso a Internet o a una consola de administración externa). Las VPC de aislamiento se pueden preconfigurar antes de un evento de seguridad para permitir direcciones IP y puertos válidos. Los recursos de destino se pueden mover inmediatamente a esta VPC de aislamiento 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 ante el incidente. Un aspecto importante del uso de una VPC de aislamiento es que los recursos, como las instancias de EC2, deben apagarse y volver a lanzarse en la nueva VPC de aislamiento antes de utilizarlos. Las instancias de EC2 existentes no se pueden mover a otra VPC ni a otra zona de disponibilidad. Para ello, siga los pasos que se describen en ¿Cómo puedo mover mi instancia de Amazon EC2 a otra subred, zona de disponibilidad o VPC?

- Grupos de escalado automático y equilibradores de carga: como parte de los procedimientos de contención del destino, los recursos de AWS adjuntos a los grupos de escalado automático y equilibradores de carga deben desvincularse y se debe anular su registro. La desvinculación y anulación del registro de los recursos de AWS se pueden realizar mediante la AWS Management Console, la AWS CLI y el SDK de AWS.

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



Ejemplo de contención del destino

Resumen

La contención es un paso del proceso de respuesta ante incidentes 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 ante incidentes de seguridad, consiste en eliminar recursos sospechosos o no autorizados con el fin de devolver la cuenta a un estado seguro conocido. La estrategia de erradicación depende de varios factores que, a su vez, dependen de los requisitos empresariales de la organización.

En la guía SP 800-61 Computer Security Incident Handling Guide del NIST se proporcionan varios pasos para la 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 todos los demás hosts afectados y, a continuación, contenga y erradique el incidente en ellos.

En el caso de los recursos de AWS, esto se puede definir aún más mediante los eventos detectados y analizados a través de los registros disponibles o herramientas automatizadas, como Registros de CloudWatch y Amazon GuardDuty. Esos eventos deberían ser la base para determinar qué correcciones deben realizarse para restaurar adecuadamente el entorno a un estado seguro conocido.

El primer paso de la erradicación es determinar qué recursos se han visto afectados dentro de la cuenta de AWS. Para ello, se deben analizar los orígenes de datos de los registros, los recursos y las herramientas automatizadas disponibles.

- Identifique las acciones no autorizadas realizadas por las identidades de IAM en su cuenta.
- Identifique el acceso no autorizado o los cambios en su cuenta.
- Identifique la creación de recursos o usuarios de IAM 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 la empresa 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 de copias de seguridad seguras y verificadas o volver a iniciar el sistema desde una AMI limpia antes de eliminar el servidor afectado.

Una vez finalizado el análisis del impacto empresarial, y utilizando los eventos del análisis de registros, debería acceder a las cuentas y realizar las correcciones adecuadas, como, por ejemplo:

- Rotar o eliminar claves: este paso elimina la capacidad del actor de seguir realizando actividades dentro de la cuenta.
- Rotar las credenciales de los usuarios de IAM potencialmente no autorizados.
- 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 debe retener una instancia de Amazon EC2 por motivos normativos, de cumplimiento o legales, cree una instantánea de Amazon EBS antes de eliminar la instancia.

- En el caso de las infecciones de malware, es posible que tenga que ponerse en contacto con un socio de la AWS Partner u otro proveedor. AWS no ofrece herramientas nativas para el análisis o la eliminación del malware. Sin embargo, si utiliza el módulo de Protección contra malware de GuardDuty para Amazon EBS, es posible que haya recomendaciones disponibles sobre los resultados obtenidos.

Una vez que haya erradicado los recursos afectados identificados, AWS le recomienda que realice una revisión de seguridad de su cuenta. Para ello, use reglas de AWS Config, soluciones de código abierto como Prowler y ScoutSuite u otros proveedores. También debería considerar la posibilidad de realizar escaneos de vulnerabilidad comparándolos con sus recursos públicos (Internet) para evaluar el riesgo residual.

La erradicación es un paso del proceso de respuesta ante 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 verificar que los efectos negativos se mitiguen a medida que se eliminen los recursos o configuraciones inapropiados.

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:

- Las prioridades empresariales o de dependencia
- El plan de restauración
- Autenticación y autorización

En la guía SP 800-61 Computer Security Incident Handling Guide del NIST se proporcionan varios pasos para recuperar sistemas, como, por ejemplo:

- La 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 marca de tiempo del primer evento identificada como parte del análisis de la causa raíz.
- Reconstruir los sistemas desde cero, incluida la redistribución desde un origen de confianza mediante la automatización, en algún momento en una nueva cuenta de 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 sea seguro y no se haya visto afectado por el incidente
- Instalar parches.
- Cambiar las contraseñas.
  - Esto incluye las contraseñas de las entidades principales de IAM que podrían haber sido objeto de un uso indebido.
  - Si es posible, recomendamos utilizar roles para las entidades principales de IAM y la federación como parte de una estrategia de privilegios mínimos.
- Reforzar la seguridad perimetral de la red (conjuntos de reglas del cortafuegos, listas de control de acceso de los enrutadores fronterizos).

Una vez que se hayan recuperado los recursos, es importante capturar las lecciones aprendidas para actualizar las políticas, los procedimientos y las guías de respuesta ante 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 frente al riesgo de reinfección. Los procedimientos de recuperación deben incluir pasos para restaurar los recursos y

servicios, las entidades principales de IAM 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. En la tabla 4 se resumen 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 • Detección basada en el comportamiento y en reglas • Detección basada en personas
Análisis	Determine si el evento de seguridad es un incidente y evalúe el alcance de este.	• Validación de la alerta y determinación de su alcance • Consulta de registros de • Inteligencia de amenazas • Automatización
Contención	Minimice y limite el impacto del evento de seguridad.	• Contención del origen • Contención de técnicas y acceso • Contención del 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 de recursos no autorizada

Fase	Objetivo	Técnicas y metodologías
		• Eliminación de malware • Análisis de seguridad
Recuperación	Restaure los sistemas a un estado seguro conocido y supervise estos sistemas para asegurarse de que la amenaza no regrese.	• Restauración del sistema desde copias de seguridad • Sistemas reconstruidos desde cero • Archivos comprometidos reemplazados 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 la iteración de los resultados de sus incidentes y simulaciones con el fin de mejorar sus capacidades para detectar e investigar de forma eficaz los posibles incidentes de seguridad y responder a ellos con el objetivo de reducir las posibles vulnerabilidades, el tiempo de respuesta y el retorno a operaciones seguras. Los siguientes mecanismos pueden ayudarlo a comprobar que su organización está preparada con las capacidades y los conocimientos más recientes para responder de manera eficaz, sea cual sea la situación.

Establecimiento de un marco de trabajo para aprender de los incidentes

La implementación de una metodología y un marco de trabajo sobre las lecciones aprendidas no solo ayudará a mejorar las capacidades de respuesta a los incidentes, sino también a evitar que el incidente se repita. Al aprender de cada incidente, puede ayudar a evitar que se repitan los mismos errores, exposiciones o configuraciones incorrectas, lo que no solo mejorará el nivel de seguridad, sino también minimizará el tiempo que se pierde en situaciones evitables.

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

- ¿Cuándo se imparte una lección aprendida?
- ¿Qué implica el proceso de lecciones aprendidas?

- ¿Cómo se lleva a cabo una lección aprendida?
- ¿Quién participa en el proceso y cómo?
- ¿Cómo se van a identificar las áreas de mejora?
- ¿Cómo se va a garantizar que las mejoras se supervisan e implementan de manera efectiva?

Además de estos resultados generales enumerados, es importante asegurarse de que se hagan las preguntas correctas para obtener el máximo valor del proceso (información que conduzca a mejoras viables). Considere la posibilidad de usar estas preguntas para fomentar el debate sobre las lecciones aprendidas:

- ¿Cuál fue el incidente?
- ¿Cuándo se identificó por primera vez el incidente?
- ¿Cómo se identificó?
- ¿Qué sistemas alertaron sobre la actividad?
- ¿Qué sistemas, servicios y datos estaban involucrados?
- ¿Qué ocurrió exactamente?
- ¿Qué funcionó correctamente?
- ¿Qué no funcionó correctamente?
- ¿Qué procesos o procedimientos fallaron o no se lograron escalar para responder al incidente?
- ¿Qué se puede mejorar en las siguientes áreas?:
  - 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?
    - ¿Las herramientas existentes permitían investigar (buscar o analizar) el incidente de forma eficaz?
- ¿Qué se puede hacer para poder identificar antes este (tipo de) incidente?
- ¿Qué se puede hacer para ayudar a evitar que este (tipo de) incidente vuelva a ocurrir?
- ¿Quién es el responsable del plan de mejora y cómo comprobará que se ha implementado?
- ¿Qué plazos hay para implementar y probar otros procesos y controles preventivos o de monitoreo?

En esta lista no se incluyen todas las posibilidades, pero pretende servir como punto de partida para identificar cuáles son las necesidades de la organización y la empresa, y cómo se pueden analizar para aprender lo mejor posible de los incidentes y aumentar continuamente el nivel de seguridad. Lo más importante es empezar incorporando las lecciones aprendidas como un componente estándar del proceso de respuesta a incidentes, la documentación y las expectativas de las partes interesadas.

Establecimiento de métricas para el éxito

Las métricas son necesarias para medir, evaluar y mejorar de manera efectiva sus capacidades de respuesta ante incidentes. Sin métricas, no hay una referencia con la que medir con precisión o incluso identificar el rendimiento (o la falta de rendimiento) de su organización. Hay algunas métricas comunes en la respuesta ante incidentes que son un buen punto de partida para una organización que busca establecer expectativas y referencias para trabajar hacia 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 usar esta métrica para realizar 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 de reconocimiento

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

Puede usar esta métrica para realizar un seguimiento de la forma en que su equipo procesa y prioriza las alertas. Si el 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 el 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 de reconocimiento, mejor responderá su equipo a las alertas de seguridad, lo que demuestra que está preparado de forma eficaz y es capaz de priorizarlas correctamente.

Tiempo medio de respuesta

El tiempo medio de respuesta es el tiempo medio que se tarda en iniciar la respuesta inicial ante 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. Esto es similar al tiempo medio de reconocimiento, pero es la medición de las acciones de respuesta específicas (por ejemplo, adquirir datos del sistema, contener el sistema) en comparación con el simple reconocimiento o confirmación de la situación.

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

Cuanto mayor sea el tiempo medio de respuesta, mayor será la necesidad de verificar que su equipo esté debidamente formado sobre cómo responder para que los procesos de respuesta se documenten y utilicen de manera eficaz. Cuanto menor sea el tiempo medio de respuesta, mejor será su equipo identificando una respuesta adecuada a las alertas detectadas y realizando las acciones de respuesta necesarias para comenzar el camino de vuelta a las operaciones seguras.

Tiempo medio de contención

El tiempo medio de contención es el tiempo promedio que se tarda en contener un posible incidente de seguridad. Específicamente, es el tiempo que transcurre entre la alerta inicial o el descubrimiento de un posible incidente de seguridad y la finalización de las acciones de respuesta que impiden de forma eficaz que el atacante o los sistemas comprometidos causen más daños.

Puede usar esta métrica para hacer un seguimiento de la capacidad de su equipo para 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 compromisos adicionales.

Cuanto mayor sea el tiempo medio de contención, mayor será la necesidad de desarrollar tanto conocimientos como 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 será el equipo a la hora de 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 volver completamente al funcionamiento seguro 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 devolver los sistemas, las cuentas y los entornos a un funcionamiento seguro tras un incidente de seguridad. La incapacidad de volver al funcionamiento seguro de manera 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 medio durante el que un usuario no autorizado tiene acceso a un sistema o entorno. Es similar al tiempo medio de contención, excepto que el periodo comienza con la primera vez que el atacante accedió al sistema o a los entornos, lo que puede ser anterior a la alerta o la detección 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 ante 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 empresa.

Resumen de las métricas

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

Tabla 5: métricas de respuesta ante incidentes

Métrica	Descripción
Tiempo medio de detección	Tiempo medio que se tarda en detectar un posible incidente de seguridad
Tiempo medio de reconocimiento	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

Métrica	Descripción
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 al funcionamiento seguro después de un posible incidente de seguridad
Tiempo de permanencia del atacante	Tiempo promedio que un atacante tiene acceso a un sistema o entorno

Uso de indicadores de riesgo (IOC)

Un indicador de riesgo (IOC) es un artefacto observado en una red, un sistema o un entorno que puede identificar (con alto nivel de confianza) una actividad malintencionada o un incidente de seguridad. Los IOC pueden tomar distintas formas: direcciones IP, dominios, artefactos a nivel de red como indicadores TCP o cargas útiles, artefactos a nivel de sistema o host como 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 ante incidentes, debe implementar un marco para recopilar, administrar y utilizar los IOC 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 administración de los IOC en las fases de análisis e investigación de sus procesos de respuesta ante incidentes. Al identificar, recopilar y almacenar los IOC de forma proactiva 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 actuales, crear más detecciones y alertas, identificar dónde y cuándo se vio un artefacto antes, crear y consultar la documentación sobre cómo se realizaban anteriormente las investigaciones relacionadas con los IOC coincidentes, y más.

Educación y formación continuas

La educación y la formación son esfuerzos en evolución y continuos que deben llevarse a cabo y mantenerse de forma intencionada. 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 emplear la formación continua como parte estándar de los objetivos y las operaciones de sus equipos. Como se mencionó en la sección de preparación, el personal de respuesta ante incidentes y las partes interesadas deben estar debidamente formados para detectar e investigar los incidentes dentro de AWS y para responder a ellos. Sin embargo, la educación no es un esfuerzo de una sola vez. La formación debe ser continua para comprobar que su 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 periódica (por ejemplo, trimestralmente) y se centren en resultados específicos para la empresa. Consulte la sección the section called “Realización de simulaciones periódicas” de este documento.

Aunque realizar los primeros ejercicios de simulación es una forma excelente de generar una línea de base inicial para la mejora, las pruebas continuas son fundamentales para lograr mejoras sostenidas y mantener un reflejo actualizado y preciso del estado actual de las operaciones. Probar 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 formación, las operaciones y los procesos y procedimientos, demostrará que es capaz de mejorar continuamente sus procesos de respuesta y su programa en su conjunto.

Conclusión

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

Colaboradores

Colaboradores actuales y anteriores de este documento:

- Anna McAbee, Senior Security Solutions Architect, Amazon Web Services
- Freddy Kasprzykowski, consultor sénior de seguridad, Amazon Web Services
- Jason Hurst, ingeniero sénior de seguridad, Amazon Web Services
- Jonathon Poling, consultor principal de seguridad, Amazon Web Services
- Josh Du Lac, director sénior, Security Solutions Architecture, Amazon Web Services
- Paco Hope, ingeniero principal de seguridad, Amazon Web Services
- Ryan Tick, ingeniero sénior de seguridad, Amazon Web Services
- Steve de Vera, ingeniero sénior de seguridad, Amazon Web Services

Apéndice A: Definiciones de capacidades en la nube

AWS tiene a su disposición más de 200 servicios en la nube y miles de características. Muchos de ellos ofrecen funcionalidades nativas de detección, prevención y respuesta, y se pueden utilizar otros servicios para diseñar soluciones de seguridad personalizadas. En esta sección se incluyen un subconjunto de los servicios que son más pertinentes para la respuesta ante incidentes en la nube.

Temas

- Registro y eventos
- Visibilidad y alertas
- Automation
- Almacenamiento seguro
- Capacidades de seguridad futuras y personalizadas

Registro y eventos

AWS CloudTrail: servicio de AWS CloudTrail que permite la gobernanza, el cumplimiento, la auditoría operativa y la auditoría de riesgos de las cuentas de AWS. Con CloudTrail, puede registrar, monitorear de forma continua y retener la actividad de las cuentas relacionada con las acciones en todos los servicios de AWS. CloudTrail proporciona un historial de eventos de la actividad de sus cuentas de AWS, como las acciones realizadas a través de la AWS Management Console, los

SDK de AWS, las herramientas de la línea de comandos y otros servicios de AWS. 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 acciones de las API de AWS:

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

AWS Config: AWS Config es un servicio que le permite evaluar, auditar y analizar las configuraciones de sus recursos de AWS. AWS Config monitorea y registra continuamente las configuraciones de recursos de AWS y le permite automatizar la comparación de las configuraciones registradas con las configuraciones deseadas. Con AWS Config, los clientes pueden revisar manual o automáticamente los cambios en las configuraciones y las relaciones entre los recursos de AWS, investigar los historiales detallados de configuración de recursos y determinar el cumplimiento general con respecto a las configuraciones especificadas en las pautas de los clientes. Esto puede simplificar las auditorías de cumplimiento, los análisis de seguridad, la administración de cambios y la resolución de problemas operativos.

Amazon EventBridge: Amazon EventBridge proporciona una transmisión de una secuencia de eventos de sistema casi en tiempo real que describen cambios en los recursos de AWS o cuando AWS CloudTrail publica llamadas a la API. Mediante reglas sencillas que puede configurar rápidamente, puede asignar los eventos y dirigirlos a uno o más flujos o funciones de destino. EventBridge toma conocimiento de los cambios operativos a medida que se producen. EventBridge puede responder a estos cambios operativos y tomar medidas de corrección según sea necesario, enviando mensajes para responder al entorno, activando funciones, realizando cambios y captando información de estado. Algunos servicios de seguridad, como Amazon GuardDuty, producen sus resultados en forma de eventos de EventBridge. Muchos servicios de seguridad también ofrecen la opción de enviar sus resultados a Amazon S3.

Registros de acceso de 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 y se suma a los registros de CloudTrail que registran los cambios en el propio bucket (como los cambios en las políticas de acceso y las políticas del ciclo de vida). Es importante tener en cuenta que las entradas de registro de acceso al servidor se envían según el “mejor esfuerzo”; es decir, en la medida que sea 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.

Registros de Amazon CloudWatch: los clientes pueden utilizar Registros de Amazon CloudWatch para monitorear y almacenar los archivos de registro procedentes de sistemas operativos, aplicaciones y otros orígenes que se ejecutan en instancias de Amazon EC2 con un agente de Registros de CloudWatch, así como acceder a ellos. Registros de CloudWatch puede ser un destino para AWS CloudTrail, consultas de DNS de Route 53, registros de flujo de VPC, funciones de Lambda y otros. Los clientes pueden recuperar los datos de registro asociados de Registros de CloudWatch.

Registros de flujo de Amazon VPC: los registros de flujo de VPC permiten que los clientes capturen información sobre el tráfico IP entrante y saliente de las interfaces de red de las VPC. Una vez habilitados los registros de flujo, se pueden transmitir a Registros de Amazon CloudWatch y Amazon S3. Los registros de flujo de VPC ayudan a los clientes a realizar 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 utilizarlos como herramienta de seguridad para supervisar el tráfico a las instancias de EC2. Utilice la versión más reciente del registro de flujos de VPC para obtener los campos más completos.

Registros de AWS WAF: AWS WAF admite 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 cumplimiento y auditoría, así como para la depuración y el 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 y SIEM de terceros.

Registros de consultas de Route 53 Resolver: los registros de consultas de Route 53 Resolver le permiten registrar todas las consultas de DNS realizadas por los recursos dentro de Amazon Virtual Private Cloud (Amazon VPC). Ya sea una instancia de Amazon EC2, una función de AWS Lambda o un contenedor, si reside en su Amazon VPC y realiza una consulta de DNS, esta característica la registrará; de este modo, podrá explorar y comprender mejor el funcionamiento de sus aplicaciones.

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

Visibilidad y alertas

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

Amazon GuardDuty: Amazon GuardDuty es un servicio administrado de detección de amenazas que monitorea de forma continua posibles comportamientos malintencionados o no autorizados para ayudar a los clientes a proteger sus cargas de trabajo y cuentas de AWS. Monitorea actividades como las llamadas inusuales a la API o las implementaciones potencialmente no autorizadas, lo que indica la posibilidad de que las cuentas o los recursos de las instancias de Amazon EC2 o buckets de Amazon S3 se vean comprometidos o el reconocimiento por parte de personas malintencionadas.

GuardDuty identifica a los presuntos actores maliciosos mediante fuentes de inteligencia de amenazas integradas que utilizan el machine learning para detectar anomalías en la actividad de la cuenta y la carga de trabajo. Cuando se detecta una amenaza potencial, el servicio envía una alerta de seguridad detallada a la consola de GuardDuty y a Eventos de CloudWatch. Esto hace que las alertas sean procesables y fáciles de integrar en los sistemas de administración de eventos y flujos de trabajo existentes.

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

Amazon Macie: Amazon Macie es un servicio de seguridad basado en inteligencia artificial que ayuda a prevenir la pérdida de datos al detectar, clasificar y proteger automáticamente la información confidencial almacenada en AWS. Macie utiliza machine learning (ML) para reconocer información

confidencial, como la información de identificación personal (PII) o la propiedad intelectual, asignar un valor empresarial y proporcionar visibilidad sobre dónde se almacenan esta información y cómo se utiliza 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 regla de AWS Config 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 las reglas de AWS Config, 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 lo ayuda a reducir los costos, aumentar el rendimiento y mejorar la seguridad mediante la optimización de su entorno de AWS. Trusted Advisor proporciona orientación en tiempo real para ayudarlo a aprovisionar sus recursos según las prácticas recomendadas de AWS. El conjunto completo de comprobaciones de Trusted Advisor, incluida la integración con Eventos de CloudWatch, está disponible para los clientes de los planes Business y Enterprise Support.

Amazon CloudWatch: Amazon CloudWatch es un servicio de monitoreo de recursos en Nube de AWS y aplicaciones que ejecuta en AWS. Puede utilizar CloudWatch para recopilar y realizar el seguimiento de métricas, recopilar y monitorear archivos de registro, establecer alarmas y reaccionar automáticamente a los cambios en sus recursos de AWS. CloudWatch puede monitorear recursos de AWS como, por ejemplo, instancias de Amazon EC2, tablas de Amazon DynamoDB e instancias de base de datos de Amazon RDS, así como métricas personalizadas generadas por las aplicaciones y los servicios, y los archivos de registro generados por las aplicaciones. Puede utilizar Amazon CloudWatch para obtener visibilidad de todo el sistema sobre la utilización de recursos, el rendimiento de las aplicaciones y el estado de funcionamiento. Puede usar esta información para iniciar y mantener la ejecución de la aplicación sin problemas según sea necesario.

Amazon Inspector: Amazon Inspector es un servicio automático de valoración de seguridad que ayuda a mejorar la seguridad y el cumplimiento de las aplicaciones implementadas en AWS. Amazon Inspector evalúa automáticamente las aplicaciones en busca de vulnerabilidades o desviaciones respecto a las prácticas recomendadas. Después de la evaluación, Amazon Inspector genera una lista detallada de resultados relacionados con la 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 o la API de Amazon Inspector.

Amazon Detective: Amazon Detective es un servicio de seguridad que recopila automáticamente los datos de registro de los recursos de AWS y utiliza el machine learning, el análisis estadístico y la teoría de gráficos para crear un conjunto de datos enlazados que le permita realizar investigaciones de seguridad más rápidas y eficientes. Detective puede analizar billones de eventos de varios orígenes de datos, como los registros de flujo de VPC, CloudTrail y 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 resultados, profundizar en las actividades históricas pertinentes y determinar rápidamente la causa raíz.

Automation

AWS Lambda: AWS Lambda es un servicio de computación sin servidor que ejecuta código como respuesta a eventos y administra automáticamente los recursos de computación subyacentes por usted. Puede utilizar Lambda para ampliar otros servicios de AWS con lógica personalizada o crear sus propios servicios de backend que operen con el nivel de seguridad, rendimiento y escala de AWS. Lambda ejecuta su código en una infraestructura de computación de alta disponibilidad y administra los recursos de computación por usted. Esto incluye el mantenimiento del servidor y del sistema operativo, el aprovisionamiento de capacidad y el escalado automático, la implementación de parches de código y seguridad y el monitoreo y el registro del código. Solo tiene que proporcionar el código.

AWS Step Functions: AWS Step Functions simplifica la coordinación de los componentes de aplicaciones y microservicios distribuidos con flujos de trabajo visuales. Step Functions proporciona una consola gráfica con la que puede organizar y visualizar los componentes de su aplicación en varios pasos. Esto facilita la creación y ejecución de aplicaciones de varios pasos. Step Functions inicia y monitorea cada paso de manera automática, y realiza reintentos cuando se producen errores, por lo que su aplicación se ejecuta en orden y según lo previsto.

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 agregar pasos sin necesidad de escribir código, de forma que pueda desarrollar e innovar su aplicación más rápido. AWS Step Functions forma parte de AWS sin servidor y facilita la orquestación de funciones de AWS Lambda para las aplicaciones sin servidor. También puede utilizar Step Functions para la orquestación de microservicios mediante recursos de computación como Amazon EC2 y Amazon ECS.

AWS Systems Manager: AWS Systems Manager le ofrece visibilidad y control de su infraestructura de AWS. Systems Manager proporciona una interfaz de usuario unificada para que pueda ver los datos operativos de varios servicios de AWS y le permite automatizar tareas operativas en todos sus

recursos de AWS. Con Systems Manager, puede agrupar los recursos por aplicación, ver los datos operativos para la supervisión y la resolución 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 del intérprete de comandos, 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 99,999999999 % 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 ayudarlo a cumplir sus requisitos normativos. Ofrece a los clientes flexibilidad en 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 ofrece una funcionalidad de consulta in situ que le permite ejecutar análisis potentes directamente sobre sus datos en reposo en Amazon S3. Amazon S3 es un servicio de almacenamiento en la nube altamente compatible que cuenta con la integración de una de las mayores comunidades de soluciones de terceros, socios integradores de sistemas y otros servicios de AWS.

Amazon S3 Glacier: Amazon S3 Glacier es un servicio de almacenamiento en la nube seguro, duradero y de bajo costo para archivo de datos y copias de seguridad a largo plazo. Está diseñado para ofrecer una durabilidad del 99,999999999 %, proporciona seguridad integral y está diseñado para ayudarlo a satisfacer sus requisitos normativos. S3 Glacier ofrece una funcionalidad de consulta in situ que le permite ejecutar análisis potentes directamente sobre sus datos en reposo archivados. Para mantener los costos 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 nuevas capacidades continuamente. Para obtener más información, le recomendamos que consulte las páginas Novedades de AWS y Seguridad en la nube de AWS. Además de los servicios de seguridad que AWS ofrece como servicios nativos en la nube, es posible que le interese desarrollar sus propias capacidades sobre los servicios de AWS.

Aunque recomendamos habilitar un conjunto básico de servicios de seguridad en sus cuentas, como AWS CloudTrail, Amazon GuardDuty y Amazon Macie, 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 de seguridad de la APN. También puede escribir sus propias consultas para buscar en sus registros. Con la amplia cantidad de servicios administrados que AWS ofrece, es más fácil que nunca. Existen muchos servicios de AWS adicionales que pueden ayudarlo en la investigación y que quedan 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 ante incidentes de AWS

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

Recursos de manuales de estrategias

- Marco para manuales de estrategias de respuesta ante incidentes: un marco de ejemplo para que los clientes creen, desarrollen e integren manuales de estrategias de seguridad en preparación para posibles escenarios de ataque al utilizar los servicios de AWS.
- Ejemplos de manuales de estrategias de respuesta ante incidentes: manuales de estrategias que cubren escenarios comunes a los que se enfrentan los clientes de AWS.
- AWS CIRT announces the release of five publicly available workshops.

Recursos de análisis forense

- Automated Incident Response and Forensics Framework: este marco y solución proporciona un proceso forense digital estándar, que consta de las siguientes fases: contención, adquisición, examen y análisis. Aprovecha las funciones de AWS Λ para activar el proceso de respuesta ante incidentes de forma automática y repetible. Proporciona división de cuentas para ejecutar los pasos de automatización, almacenar artefactos y crear entornos forenses.
- Automated Forensics Orchestrator for Amazon EC2: en esta guía de implementación se proporciona una solución de autoservicio para capturar y examinar datos de las instancias de EC2 y los volúmenes adjuntos para su análisis forense en caso de que se detecte un posible problema de seguridad. Hay una plantilla de AWS CloudFormation para implementar la solución.

- How to automate forensic disk collection in AWS: en esta publicación en el blog de AWS se 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 plantilla de AWS CloudFormation para implementar la solución.

Avisos

Es responsabilidad de los clientes realizar su propia evaluación independiente de la información que contiene este documento. El presente documento: (a) tiene sólo fines informativos, (b) representa las ofertas y prácticas actuales de los productos de AWS, que están sujetas a cambios sin previo aviso, y (c) no supone ningún compromiso ni garantía por parte de AWS y sus filiales, proveedores o licenciantes. Los productos o servicios de AWS se proporcionan “tal cual”, sin garantías, afirmaciones ni condiciones de ningún tipo, ya sean expresas o implícitas. Las responsabilidades y obligaciones de AWS con respecto a sus clientes se controlan mediante los acuerdos de AWS y este documento no forma parte ni modifica ningún acuerdo entre AWS y sus clientes.

© 2024 Amazon Web Services, Inc. o sus filiales. Todos los derechos reservados.

Historial del documento

Cambio	Descripción	Fecha
Adición de una página para la integración de Amazon EventBridge con Respuesta ante incidentes de seguridad de AWS.	Nueva sección de contenido para describir cómo Amazon EventBridge se integra en Respuesta ante incidentes de seguridad de AWS.	26 de junio de 2025
Actualizaciones del SLR y adición de permisos para admitir los derechos del servicio.	AWSSecurityIncidentResponseTriageServiceRolePolicy se actualizó para agregar los permisos security-ir:GetMembership, security-ir:ListMemberships, security-ir:UpdateCase, guardduty:ListFilters, guarduty:UpdateFilter, guardduty:DeleteFilter y guardduty:GetAdministratorAccount. guardduty:GetAdministratorAccount se agregó para facilitar la administración de los filtros de archivado automático de GuardDuty en cuentas delegadas.	2 de junio de 2025
Actualizaciones de recursos.	Se actualizó https://docs.aws.amazon.com/security-ir/latest/userguide/appendix-b-incident-response-resources.html#playbook-resources para reflejar los talleres activos disponibles para los clientes.	23 de mayo de 2025

Cambio	Descripción	Fecha
El servicio admite el japonés.	Se actualizaron las configuraciones admitidas para identificar la asistencia en japonés en la hora local de Japón. El inglés se admite globalmente.	13 de mayo de 2025
Actualizaciones de contenido y comentarios de los clientes.	Se agregó una nota en https://docs.aws.amazon.com/security-ir/latest/userguide/select-a-membership-account.html para reflejar una tarea adicional al usar una cuenta de administrador delegado como parte de la configuración. Se actualizó la experiencia del cliente al trabajar con un caso generado por el servicio y la detección y el análisis. Se actualizaron los detalles de cancelación de cuentas para proporcionar mayor claridad sobre las implicaciones de facturación al cancelar una membresía.	9 de mayo de 2025
Adición de tres nuevas regiones compatibles.	Se agregaron tres nuevas regiones en https://docs.aws.amazon.com/security-ir/latest/userguide/supported-configs.html: Mumbai, París y São Paulo.	7 de mayo de 2025

Cambio	Descripción	Fecha
Actualización: Actualizaciones a partir de los comentarios de los clientes sobre la documentación.	Se corrigieron errores ortográficos y gramaticales en varias páginas. Se actualizó https://docs.aws.amazon.com/en_us/security-ir/latest/userguide/organizations_permissions.html para reflejar con precisión security-ir como prefijo de servicio. Se agregó una nota en https://docs.aws.amazon.com/security-ir/latest/userguide/source-containment.html sobre Route53 y DNS.	7 de febrero de 2025

Cambio	Descripción	Fecha
Actualización: Actualizaciones a partir de los comentarios de los clientes sobre la documentación.	Se actualizó https://docs.aws.amazon.com/security-ir/latest/userguide/setup-monitoring-and-investigation-workflows.html a la plantilla de conjunto de pilas. Se corrigieron las entradas triage.security-ir.com con triage.security-ir.amazonaws.com. Se agregó una nota sobre las conexiones rastreadas para AWSSupport-ContainEC2Reversible en https://docs.aws.amazon.com/security-ir/latest/userguide/contain.html. Se corrigió el enlace que no funcionaba en https://docs.aws.amazon.com/security-ir/latest/userguide/managing-associated-accounts.html. 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 en https://docs.aws.amazon.com/en_us/security-	20 de diciembre de 2024

Cambio	Descripción	Fecha
	ir/latest/userguide/using-service-linked-roles.html para las cuentas de administración de AWS Organizations.	

Cambio	Descripción	Fecha
Actualización: Actualizaciones a partir de los comentarios de los clientes sobre la documentación.	Se eliminaron varios AWSAWS duplicados en el texto. Se corrigieron los enlaces que no funcionaban en https://docs.aws.amazon.com/security-ir/latest/userguide/sir_tagging.html y https://docs.aws.amazon.com/security-ir/latest/userguide/service-name-info-in-cloudtrail.html. Actualizaciones en https://docs.aws.amazon.com/security-ir/latest/userguide/contain.html. Se eliminó el símbolo > del primer párrafo. Se reemplazó AWSSupport-ContainEC2Reversible por AWSSupport-ContainEC2Instance. Se reemplazó AWSSupport-ContainIAMReversible por AWSSupport-ContainIAMPrincipal. Se reemplazó AWSSupport-ContainS3Reversible por AWSSupport-ContainS3Resource. Se actualizó el formato en https://docs.aws.amazon.com/en_us/security-ir/latest/userguide/issues.html.	10 de diciembre de 2024

Cambio	Descripción	Fecha
	Cuando se pide a los clientes que se pongan en contacto con el equipo de CIRT a través de un ticket de asistencia, en https://docs.aws.amazon.com/security-ir/latest/userguide/understand-response-teams-and-support.html ahora se ofrecen opciones que pueden seleccionar en los formularios de asistencia. Se eliminó Eventos de CloudWatch y se reemplazó por EventBridge en https://docs.aws.amazon.com/security-ir/latest/userguide/logging-and-events.html. Actualizaciones gramaticales en https://docs.aws.amazon.com/security-ir/latest/userguide/technique-access-containment.html. Se eliminó la fecha de publicación de https://docs.aws.amazon.com/security-ir/latest/userguide/security-incident-response-guide.html y se reemplazó por las actualizaciones de esta tabla.	
Actualización: Políticas administradas por AWS y roles vinculados a servicios.	Se actualizaron las políticas administradas y los roles vinculados a servicios.	1 de diciembre de 2024

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