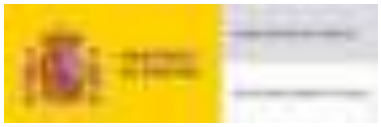
Guía de Seguridad de las TIC
CCN-STIC 887F

Guía de respuesta a incidentes de seguridad en AWS

Febrero 2022

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:



2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.02.14 19:19:08 +01'00'

Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2022
NIPO: 083-22-076-8

Fecha de Edición: febrero de 2022
Davinci Tecnologías de la Información, S.L ha participado en la realización y modificación del presente documento y sus anexos, que ha sido financiado por Amazon.

LIMITACIÓN DE RESPONSABILIDAD
El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL
Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN)

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Febrero de 2022

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. GUÍA DE RESPUESTA A INCIDENTES DE SEGURIDAD EN AWS 5
1.1. DESCRIPCIÓN DEL USO DE ESTA GUÍA 5
2. CONFIGURACIÓN SEGURA PARA LA RESPUESTA FRENTE A INCIDENTES EN AWS ... 5
2.1. MONITORIZACIÓN DEL SISTEMA 6
2.1.1. PREPARACIÓN 6
2.1.2. DETECCIÓN DE INTRUSIÓN 7
2.1.3. SISTEMA DE MÉTRICAS 12
1.1.1 RESPUESTA BASADA EN EVENTOS 16
1.1.2 POST-INCIDENTE 16
3. SERVICIOS DISPONIBLES PARA LA RESPUESTA A INCIDENTES 16
3.1. AMAZON GUARDDUTY 16
3.2. AMAZON DETECTIVE 18
3.3. AMAZON CLOUDWATCH 20
3.4. AWS SECURITY HUB 21
3.5. AWS SYSTEMS MANAGER 22
3.6. AWS CLOUDTRAIL 24
3.7. AWS WAF 25
3.8. AWS NETWORK FIREWALL 25
3.9. AWS PERSONAL HEALTH DASHBOARD 25

1. GUÍA DE RESPUESTA A INCIDENTES DE SEGURIDAD EN AWS

1.1. DESCRIPCIÓN DEL USO DE ESTA GUÍA

El propósito de esta Guía es ayudar al Sector Público al establecimiento de las capacidades de respuesta a ciberincidentes y su adecuado tratamiento, en entornos de nube pública de Amazon Web Services (AWS). Esta guía debe usarse en complemento con la Guía de Seguridad de **las TIC CCN-STIC 817** referente a la **Gestión de Ciberincidentes** en el Esquema Nacional de Seguridad

La guía esta especialmente dirigida a:

- Equipos de Respuesta a Ciberincidentes internos a las organizaciones.

- Responsables de Seguridad de la Información (de obligada nominación para los Operadores de Servicios Esenciales, de conformidad con lo previsto en el artículo 16.3 del Real Decreto-ley 12/2018, de 7 de septiembre) y responsables delegados.

- Responsables de Sistemas de Información (CIO Chief Information Officer) y, en general,
  - Gestores de programas de Ciberseguridad.
  - Administradores de Red y de Sistemas.
  - Administradores y responsables de Cloud.
  - Responsables de seguridad

2. CONFIGURACIÓN SEGURA PARA LA RESPUESTA FRENTE A INCIDENTES EN AWS

La nube de AWS cuenta con un modelo de responsabilidad compartida. AWS administra la seguridad de la nube. El usuario es responsable de la seguridad en la nube. Esto significa que mantiene el control de la seguridad que decida implementar. Dispone de acceso a cientos de herramientas y servicios que lo ayudarán a cumplir sus objetivos de seguridad. Estas prestaciones contribuyen a establecer una referencia de seguridad que satisface los objetivos para las aplicaciones que se ejecutan en la nube.

Es importante saber qué controles y prestaciones se pueden utilizar, revisar ejemplos temáticos para resolver posibles problemas e identificar métodos de reparación que se pueden utilizar para aprovechar la automatización y mejorar la velocidad de respuesta.

2.1. MONITORIZACIÓN DEL SISTEMA

2.1.1. Preparación

Definición de roles y responsabilidades

Debido a que no podemos predecir ni codificar todas las posibles direcciones que tomará un evento, se confía en la automatización para tareas simples y repetitivas, y se deja que las personas tomen las decisiones difíciles. La gestión de eventos de seguridad poco claros requiere de una buena definición de roles y de comunicación entre diferentes departamentos. Hay que tener en cuenta estos roles y responsabilidades, y si debe participar alguna tercera parte. La creación de un gráfico de responsables, aprobadores, consultados e informados (RACI) para un incidente puede parecer un trámite burocrático, permite una comunicación rápida y directa, y describe claramente el liderazgo en diferentes etapas del evento.

Definición de los mecanismos de respuesta

El mecanismo de respuesta depende del modelo de gobernanza, riesgos y conformidad (GRC). Idealmente, el modelo de GRC se crea antes de planificar la respuesta ante Incidentes. Se tendrá que identificar a las partes interesadas y los contactos relevantes, y asegurarse de que se dispone de un acceso adecuado para llevar a cabo la respuesta necesaria.

Preparación del acceso a las cuentas de AWS

Durante un incidente los diferentes equipos que se encarguen de responder, deberán tener accesos adecuados a su función para realizar las diferentes tareas que se requieran.

Será necesario identificar y debatir la estrategia de cuentas de AWS y la estrategia de identidades en la nube con los arquitectos de la nube de la organización para comprender qué métodos de autenticación y autorización están configurados, por ejemplo:

- Federación: un usuario asume un rol de IAM en una cuenta de AWS de un proveedor de identidades.
- Acceso entre cuentas: un usuario asume un rol de IAM en varias cuentas de AWS.
- Autenticación: un usuario se autentica como un usuario de AWS IAM creado dentro de una sola cuenta de AWS.

Preparación de procesos

Árboles de decisión

Desde AWS se recomienda el uso de árboles de decisión con el equipo y partes interesadas. Esta herramienta ayudará a la hora de respaldar la toma de decisiones lo que facilitará a determinar las acciones que se realizarán.

Visualización o copia de datos importantes
El equipo de respuesta deberá tener acceso a registros y otras pruebas para poder investigar los datos. Dentro de AWS en el servicio IAM se pueden encontrar políticas predefinidas que ayuden con estos temas. Entre ellas se pueden encontrar SecurityAudit o ViewOnlyAccess.

Es posible que los equipos de respuesta deseen hacer una copia puntual de los datos, como los registros de AWS CloudTrail, de un bucket de Amazon S3 de una cuenta a un bucket de Amazon S3 de otra cuenta. Los permisos proporcionados por la política administrada ReadOnlyAccess, por ejemplo, permiten al personal de emergencia llevar a cabo estas acciones.

Compartir las instantáneas de Amazon EBS

Para realizar una investigación de un volumen de Amazon EBS en una cuenta separada y aislada, se deberán modificar los permisos de la instantánea para compartirla con las otras cuentas de AWS especificadas. Los usuarios que se hayan autorizado pueden utilizar las instantáneas que comparta como base para crear sus propios volúmenes de EBS, mientras que la instantánea original no se verá afectada.

Para realizar este procedimiento, se puede consultar la siguiente web del fabricante: https://docs.aws.amazon.com/es_es/AmazonCloudWatch/latest/logs/CrossAccountSubscriptions.html

Si la instantánea está cifrada, también se debrá compartir la clave administrada por el cliente (CMK) personalizada de AWS Key Management Service (AWS KMS) que se utilizó para cifrar la instantánea. Se pueden aplicar permisos entre cuentas a una CMK personalizada en el momento de crearla o posteriormente. Las instantáneas están restringidas a la región en la que se crean, pero se puede compartir una instantánea con otra región copiándola a esa región.

Compartir los logs de Amazon CloudWatch
Los registros que se crean en Amazon CloudWatch Logs, como los registros de flujo de Amazon VPC, se pueden compartir con otra a través de una suscripción a CloudWatch Logs.

2.1.2. Detección de Intrusión

Esta medida es exigida por igual en las categorías MEDIA y ALTA del Esquema Nacional de Seguridad, quedando exentos los entornos de categoría BAJA, la cual indica que se dispondrán de herramientas de detección o de prevención de intrusión.

Para estas tareas se recomienda el uso de los siguientes servicios expuestos los cuales permiten la detección de amenazas, su denegación, su interrupción y la respuesta una vez se han identificado o producido.

Clasificación de los incidentes

Los incidentes que ocurren dentro de los servicios de AWS deberán estar clasificados según el tipo de incidencia o evento y su peligrosidad.

La peligrosidad de un incidente dado se asignará a uno de una escala de cuatro valores. Esta escala, de menor a mayor peligrosidad, se muestra en la siguiente tabla:

Nivel	Peligrosidad
1	BAJO
2	MEDIO
3	ALTO
4	CRÍTICO

Tabla 1 Clasificación de peligrosidad en AWS

Detección de la Intrusión

El objetivo del control de detección en la fase de reconocimiento de la intrusión es descubrir o discernir la existencia, la presencia o el hecho de una intrusión en los sistemas de información.

Para ello se disponen de los siguientes servicios de AWS que nos permiten detectar la intrusión:

Servicio	Descripción
Amazon GuardDuty	Este control detecta actividad de reconocimiento, como la actividad inusual de la API, el escaneo de puertos intra-VPC, patrones inusuales de solicitudes de inicio de sesión fallidas o el sondeo de puertos no bloqueados desde una dirección IP conocida.
AWS WAF	Los atacantes escanean y examinan las aplicaciones web orientadas a Internet en busca de vulnerabilidades. Envían una serie de peticiones que generan códigos de error HTTP 4xx y esta generación de errores se puede usar para ayudar a identificar y bloquear las direcciones IP de origen malicioso. Si bien la solución AWS WAF puede prevenir los ataques es posible definirla para generar eventos de seguridad.
Amazon CloudWatch, AWS CloudTrail	Estos servicios ayudan a monitorizar, detectar, visualizar, generar notificaciones y responder a cambios en sus recursos de AWS.

AWS Security Hub	Este servicio ofrece una visión completa de las alertas de seguridad de alta prioridad y del estado de conformidad en todas las cuentas de AWS.
Amazon Detective	Amazon Detective complementa la detección facilitando el análisis, la investigación y la rápida identificación de la causa raíz de posibles problemas de seguridad o actividades sospechosas. Amazon Detective recopila automáticamente los datos de los logs de los recursos de AWS y utiliza el aprendizaje automático, el análisis estadístico y la teoría de gráficos para crear un conjunto de datos vinculados que permita realizar fácilmente investigaciones de seguridad más rápidas y eficaces.
AWS Network Firewall	Este control detecta la actividad de reconocimiento utilizando detección basada en firmas.

Denegación

El objetivo del control de denegación es impedir que el atacante acceda y utilice información, sistemas y servicios críticos.

Servicio	Descripción
Amazon VPC	Amazon VPC puede ayudar a evitar que los atacantes escaneen los recursos de la red durante reconocimiento. Rutas de agujeros negros de Amazon VPC (como una lista blanca o negra de activos alcanzables en la red antes de los grupos de seguridad o las NACL).
AWS IAM	En este contexto, los atacantes no pueden ejecutar las llamadas a la API sin tener permisos.
AWS Certificate Manager	La protección de los datos en tránsito niega a los atacantes la capacidad de capturar datos en tránsito durante la fase de reconocimiento, a menos que sean capaces de hacerse pasar por un punto final legítimo.
AWS WAF	Este servicio es una solución que permite configurar de forma rápida y fácil las reglas de AWS WAF que ayudan a bloquear Scanners y Probes Orígenes de atacantes conocidos, y Bots y Scrapers.
Amazon Cognito	Este servicio proporciona credenciales de AWS temporales y con privilegios limitados de AWS para permitir el acceso a otros servicios de AWS.

Interrupción

El objetivo del control de interrupción es romper o interrumpir el flujo de información.

Servicio	Descripción
Amazon GuardDuty + AWS Lambda	Estos servicios en conjunto detectan las actividades de reconocimiento y modifican las configuraciones de seguridad para bloquear el tráfico asociado a un ataque.
AWS Network Firewall	El servicio detecta la actividad de reconocimiento bloqueando los escaneos y sondeos de la red utilizando prevención de intrusiones basada en firmas.

Respuesta

Servicio	Descripción
AWS WAF, WAF Managed Rules + Automatización	Los atacantes escanean y prueban las aplicaciones web en busca de vulnerabilidades. Envían una serie de serie de peticiones que generan códigos de error HTTP 4xx de error HTTP 4xx. Se pueden utilizar estos registros para ayudar a identificar y bloquear direcciones IP de origen malicioso.
Amazon GuardDuty + AWS Lambda	Estos servicios en conjunto detectan las actividades de reconocimiento y modifican las configuraciones de seguridad para bloquear el tráfico asociado a un ataque.
Amazon CloudWatch Events & Alarms + Amazon SNS	Estos servicios supervisan, detectan, visualizan, reciben notificaciones sobre ataques y responden a cambios en los recursos de AWS.

Amazon GuardDuty

Para la detección de intrusiones se recomienda el uso de Amazon GuardDuty, el cual es un servicio de detección de amenazas que monitoriza continuamente para identificar actividades maliciosas y comportamientos no autorizados con el fin de proteger datos, cargas de trabajo y cuentas de AWS almacenados en Amazon S3.
El servicio utiliza aprendizaje automático, detección de anomalías e inteligencia contra amenazas integrada para identificar y priorizar las posibles amenazas. Amazon GuardDuty analiza miles de millones de eventos a través de varios orígenes de datos de AWS, como los registros de eventos de AWS CloudTrail, los registros de flujo de Amazon VPC y los registros de DNS. Mediante la integración con Amazon CloudWatch Events, las alertas de Amazon GuardDuty son procesables, fáciles de agregar a diferentes cuentas y fáciles de insertar en los sistemas existentes de flujos de trabajo y administración de eventos. Amazon GuardDuty utiliza fuentes de información de

amenazas, como listas de direcciones IP y dominios maliciosos, y aprendizaje automático para identificar la actividad anómala y potencialmente no permitida, así como la actividad malintencionada en su entorno de AWS.

Se deberán aplicar los procesos adecuados para la correcta explotación de las herramientas de detección de intrusión.

- En ausencia de otras herramientas de terceros la entidad usuaria deberá habilitar Amazon Guarduty para la detección de amenazas e intrusiones.

Amazon GuardDuty aprovecha entre otras fuentes los logs de flujos de red a nivel de VPC y los logs de actividad de gestión. Para poder aprovechar estas fuentes los correspondientes servicios han de estar activados.

- Activar el servicio de eventos de gestión AWS CloudTrail para todas las regiones.
- Activar el servicio de VPC Flowlogs para poder recopilar información de tráfico de red.

Para más información sobre GuardDuty y su activación puede consultar la guía del fabricante:
https://docs.aws.amazon.com/es_es/guardduty/latest/ug/what-is-guardduty.html

AWS WAF

Se pueden configurar tres comportamientos distintos:

- **Permitir todas las solicitudes excepto las que se especifiquen**: esto es útil si se quiere que Amazon CloudFront, Amazon API Gateway, Application Load Balancer o AWS AppSync distribuyan contenido para un sitio web público y si, además, se quiere bloquear las solicitudes de atacantes.
- **Bloquear todas las solicitudes excepto las que se especifiquen**: esto es útil si se quiere distribuir contenido a un sitio web restringido cuyos usuarios se puedan identificar fácilmente por medio de las propiedades de las peticiones web, como una dirección IP.
- **Contar las solicitudes que coincidan con las propiedades especificadas**: si se desea permitir o bloquear solicitudes en función de nuevas propiedades de las peticiones web, primero se puede configurar AWS WAF para que cuente las solicitudes que coincidan con esas propiedades, sin permitirlas ni bloquearlas. Esto permite confirmar que no se configuró AWS WAF accidentalmente para que bloquease todo el tráfico a su sitio web. Se puede cambiar el comportamiento para permitir o bloquear solicitudes.

Beneficios del uso de AWS WAF:

- Protección adicional frente a ataques web gracias al uso de condiciones especificadas.

- Reglas permiten, bloquear o contar peticiones web que cumplen las condiciones previamente configuradas. Las reglas pueden bloquear o contar peticiones web que no solo cumplan las condiciones especificadas, sino que también superen un número determinado de peticiones en un periodo de cinco minutos.
- Permite tener métricas en tiempo real.

Amazon Detective

Detective extrae automáticamente eventos basados en el tiempo, como intentos de inicio de sesión, llamadas API y tráfico de red de AWS CloudTrail Registros de flujo de Amazon VPC. También ingiere los hallazgos detectados por GuardDuty.

A partir de esos eventos, Detective utiliza el aprendizaje automático y la visualización para crear una vista unificada e interactiva de los comportamientos de los recursos y las interacciones entre ellos a lo largo del tiempo. Este gráfico de comportamiento permite examinar acciones dispares, como intentos de inicio de sesión fallidos o llamadas a API sospechosas. También se puede ver cómo afectan estas acciones a recursos como cuentas AWS e instancias Amazon EC2. Detective permite:

- Investigar rápidamente cualquier actividad que esté fuera de la norma.
- Identificar patrones que pueden indicar un problema de seguridad.
- Comprender todos los recursos afectados por un hallazgo.

Para usar Amazon Detective se debe habilitar primero Amazon GuardDuty.

2.1.3. Sistema de métricas y registros

Esta medida es exigida de diferentes formas para las categorías BAJA, MEDIA y ALTA del Esquema Nacional de Seguridad, exige que se recopilarán los datos necesarios.

Amazon CloudTrail

AWS basa la mayor parte de las funcionalidades de monitorización en los servicios de AWS CloudTrail y Amazon CloudWatch. CloudTrail es un servicio de AWS que ayuda a habilitar la gestión, el cumplimiento, el funcionamiento y el análisis de operaciones y riesgo de una cuenta de AWS. Las medidas que adopta un usuario, la función o un servicio de AWS se registran como eventos en CloudTrail.

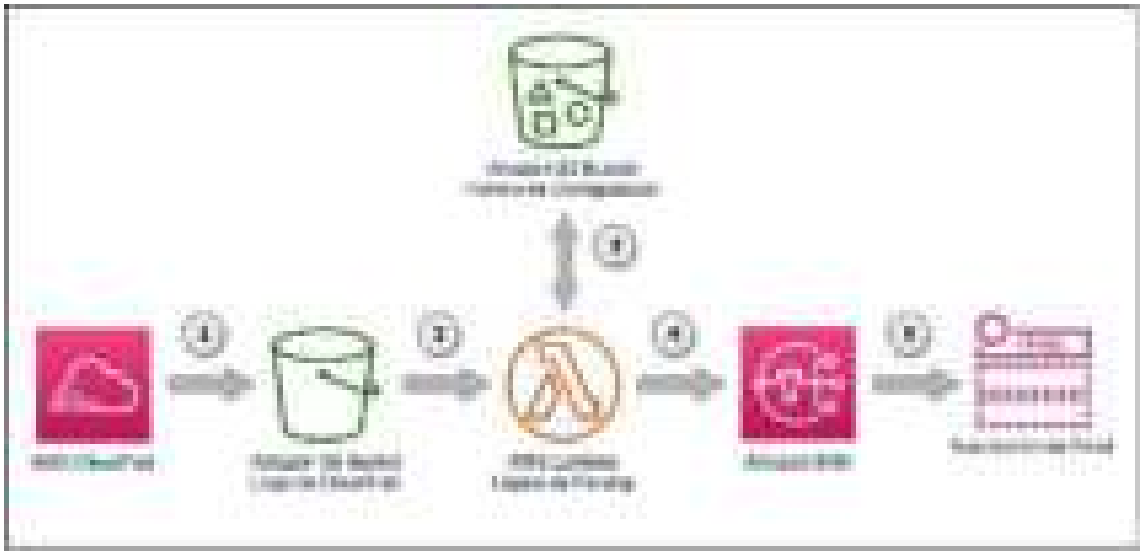


Ilustración 1 Ejemplo de gestión de eventos de acceso con diferentes servicios de AWS.

- Se recomienda crear un registro de seguimiento.

Para obtener un registro continuo de los eventos de la cuenta de AWS, se debe crear un registro de seguimiento. Aunque CloudTrail proporciona 90 días de información del historial de eventos de gestión en la consola de CloudTrail sin crear un rastro, no es un registro permanente, y no proporciona información sobre todos los tipos de eventos posibles. Para un registro permanente, y para un registro que contenga todos los tipos de eventos que se especifiquen, se deberá crear un rastro, que entregará los archivos de registro a un bucket de Amazon S3 que se especifique.

Para la creación de este registro de seguimiento, se puede consultar la siguiente guía del fabricante:
https://docs.aws.amazon.com/es_es/awscloudtrail/latest/userguide/cloudtrail-create-a-trail-using-the-console-first-time.html#creating-a-trail-in-the-console

- Se deberá establecer un filtro de métricas y una alarma para detectar cambios en las configuraciones de CloudTrail. La supervisión de los cambios en la configuración de CloudTrail ayudará a garantizar una visibilidad sostenida de las actividades realizadas en la cuenta de AWS.

Para poder garantizar la seguridad de un servicio se deberá monitorizar el correcto uso de las llamadas a la API. Esto se puede lograr dirigiendo los registros de AWS CloudTrail a los registros de AWS CloudWatch y estableciendo los filtros y alarmas métricas correspondientes.

Para la creación de los filtros, se puede consultar la siguiente guía del fabricante:

https://docs.aws.amazon.com/es_es/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

- Se deberá aplicar el registro de seguimiento en todas las regiones de AWS.

Para obtener un registro completo de los eventos, se deberá configurar cada registro para registrar los eventos en todas las regiones de AWS, de esta manera se registrarán todos los eventos que se producen en la cuenta de AWS.

- Se deberá activar la integridad de los archivos de registro de CloudTrail.

Los archivos de registro validados son especialmente valiosos en las investigaciones de seguridad y forenses. Por ejemplo, un archivo de registro validado permite afirmar positivamente que el propio archivo de registro no ha cambiado, o que determinadas credenciales de usuario realizaron una actividad específica de la API. El proceso de validación de la integridad de los archivos de registro de CloudTrail también permite saber si un archivo de registro ha sido eliminado o modificado, o afirmar positivamente que no se entregaron archivos de registro en la cuenta durante un período de tiempo determinado. La validación de la integridad de los archivos de registro de CloudTrail utiliza algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. Esto hace que sea computacionalmente inviable modificar, borrar o falsificar los archivos de registro de CloudTrail sin ser detectado.

Para activar la integridad de los archivos de registro, se puede seguir la siguiente guía del fabricante:
https://docs.aws.amazon.com/es_es/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html#cloudtrail-log-file-validation-intro-enabling-and-using

Amazon CloudWatch

Amazon CloudWatch es un repositorio de métricas. Un servicio de AWS, como Amazon EC2, pone las métricas en el repositorio del que es posible obtener estadísticas en función de dichas métricas. Con métricas personalizadas en el repositorio es posible recuperar estadísticas sobre estas métricas también.

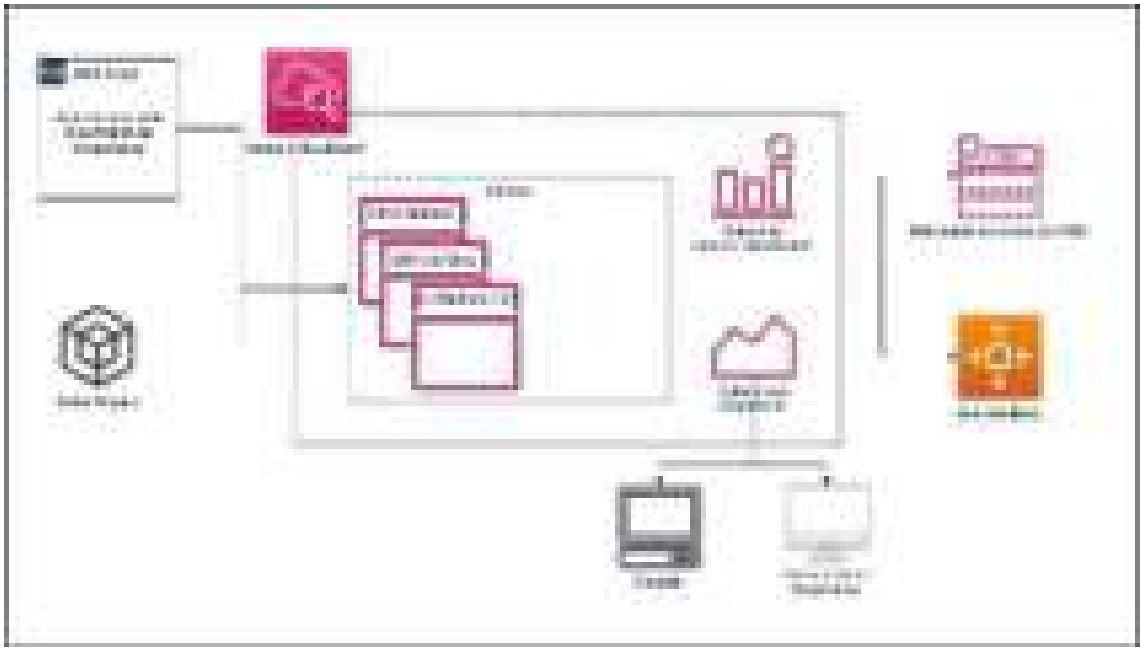


Ilustración 2 Descripción de una arquitectura CloudWatch.

Puede consultarse más información sobre el servicio de CloudWatch en el siguiente enlace:

https://docs.aws.amazon.com/es_es/AmazonCloudWatch/latest/monitoring/cloudwatch_architecture.html

Es importante entender en el ámbito de la monitorización el servicio de **VPC Flowlogs.** Se trata de un servicio que permite capturar información acerca del tráfico IP que entra y sale de los interfaces de red en la VPC, red o instancia. Los datos del registro de estos flujos de red pueden publicarse en Amazon CloudWatch Logs o Amazon S3. Una vez creado un log de flujo, es posible recuperarlo y ver los datos en el destino elegido.

Los logs de flujo son útiles en una serie de tareas, tales como:

- Diagnosticar reglas de grupo de seguridad muy restrictivas.
- Monitorizar el tráfico que llega a una instancia.
- Determinar la dirección del tráfico hacia y desde las interfaces de red.

Los datos de registro de flujo se recopilan fuera de la ruta del tráfico de red y, por lo tanto, no afectan al rendimiento ni a la latencia de la red. Se pueden crear o eliminar registros de flujo sin ningún riesgo de impacto en el rendimiento de la red.

1.1.1 Respuesta basada en eventos

Con un sistema de respuesta que se base en eventos se puede conseguir una automatización para corregir el incidente de forma rápida y eficaz. Se pueden usar respuestas rápidas basadas en eventos para reducir el tiempo. Para ello se puede usar el servicio de AWS Lambda que nos permitirá automatizar las respuestas.

Por ejemplo, en caso de tener una cuenta AWS con AWS CloudTrail habilitado y en algún momento alguien decide desactivarlo, se podría habilitar de manera automática a través de una función Lambda con una llamada a la API de AWS.

1.1.2 Post-incidente

1.1.2.1 Automatización de la respuesta ante incidentes

Servicio AWS	Descripción
AWS Lambda	Nos permite preparar una respuesta automatizada a través de los disparadores.
AWS Step Functions	AWS Step Functions es un que los desarrolladores usan para crear aplicaciones distribuidas, automatizar procesos de TI.
Corrección automática con reglas de AWS Config	Conjunto de reglas de AWS Config y correcciones automáticas que evalúan el entorno y lo devuelven a la especificación aprobada.

3. SERVICIOS DISPONIBLES PARA LA RESPUESTA A INCIDENTES

AWS ofrece múltiples herramientas para abordar los diferentes escenarios y necesidades a la hora de responder a una incidencia en AWS. A continuación, se describen los servicios más ligados a las tareas de respuesta a incidentes.

Además AWS ofrece otros canales de comunicación para ponerse en contacto con el equipo técnico o estar siempre informado de las últimas mejoras con los boletines de seguridad de AWS.

3.1. Amazon GuardDuty

Amazon GuardDuty es un servicio de detección de amenazas inteligente que ofrece una manera más precisa y sencilla de monitorear y proteger continuamente las cuentas de AWS, cargas de trabajo y datos almacenados en Amazon S3.

Ilustración 3 Funcionamiento de Amazon GuardDuty

GuardDuty se encarga de analizar los eventos en las cuentas de AWS a partir de eventos de administración de AWS CloudTrail, eventos de datos de S3 de AWS CloudTrail, registros de flujo de Amazon VPC (datos del tráfico de red) y registros de DNS.

Para la implementación de Amazon GuardDuty dentro de la organización, se puede consultar la siguiente guía del fabricante:
https://docs.aws.amazon.com/es_es/guardduty/latest/ug/guardduty_settingup.html

Detección de amenazas

Amazon GuardDuty ofrece detección de amenazas precisa de cuentas vulnerables realizando una monitorización continua de los factores en casi tiempo real. GuardDuty puede detectar señales de cuentas vulnerables, como el acceso a recursos de AWS a partir de una ubicación geográfica inusual en un momento atípico del día. Amazon GuardDuty controla las llamadas a la API inusuales, como los intentos de ocultar actividad en cuentas mediante la desactivación del registro de CloudTrail o la captura de instantáneas de una base de datos a partir de una dirección IP malintencionada.

Las principales categorías de detección incluyen:

- Reconocimiento: Algunos ejemplos son una actividad de API inusual, el escaneo de puertos en el interior de una VPC, patrones inusuales de solicitudes de inicio de sesión incorrectas o el sondeo de puertos no bloqueados a partir de una IP maliciosa conocida.
- Vulnerabilidad de instancias: Algunos ejemplos son una actividad que indica la vulnerabilidad de una instancia, como la minería de criptomonedas, actividad de comando y control (C&C) de puerta trasera, malware que utiliza algoritmos de generación de dominios (DGA), actividad de salida de denegación de servicios, volúmenes altos inusuales del tráfico de red, protocolos de red inusuales, comunicación de salida de instancias con una IP malintencionada

conocida, credenciales temporales de Amazon EC2 utilizadas por una dirección IP externa y exfiltración de datos con DNS.

- Vulnerabilidad de cuentas: Algunos ejemplos son llamadas a la API desde una ubicación geográfica inusual o un proxy anónimo, intentos de desactivar los registros de AWS CloudTrail, cambios que debilitan la política de contraseña de la cuenta, lanzamientos inusuales de infraestructuras o de instancias, implementaciones de infraestructura en una región inusual y llamadas a la API desde direcciones IP malintencionadas conocidas.
- Vulnerabilidad de buckets: Algunos ejemplos son una actividad que indique la vulnerabilidad de un bucket, como patrones de acceso a datos que muestren un mal uso de credenciales, actividad no usual de la API de S3 desde un host remoto, acceso a S3 no autorizado desde direcciones de IP confirmadas como maliciosas y llamadas a la API para recuperar datos en buckets de S3 de un usuario que no cuenta con un historial previo de acceso al bucket o invocadas desde una ubicación inusual. Amazon GuardDuty monitorea y analiza de manera continua eventos de datos de S3 de AWS CloudTrail para detectar actividad sospechosa en todos los buckets de Amazon S3.

Se puede consultar la lista entera de los tipos de hallazgos que localiza Amazon GuardDuty en el siguiente documento del fabricante: https://docs.aws.amazon.com/es_es/guardduty/latest/ug/guardduty_finding-types-active.html

Dentro del control de amenazas se dispone de tres niveles de gravedad (bajo, intermedio y alto), estos niveles de gravedad no tienen que ver con los niveles del ENS, para ayudar a priorizar la respuesta frente a posibles amenazas:

- Bajo: Indica una actividad sospechosa o malintencionada que se bloqueó antes de poner en peligro al recurso.
- Medio: Indica actividad sospechosa. Por ejemplo, actividad que no se ajusta al comportamiento observado normalmente.
- Alto: Indica que el recurso en cuestión está en peligro y que se está utilizando activamente para fines no autorizados.

Monitorización continua

Amazon GuardDuty se encarga de monitorizar y analizar continuamente datos de eventos de cargas de trabajo y cuentas de AWS que se encuentran en AWS CloudTrail, en el registro de flujo de VPC y registros de DNS. Amazon GuardDuty se enfoca en cómo responder rápidamente y cómo mantener la organización protegida.

3.2. Amazon Detective

Amazon Detective facilita el análisis, la investigación y la rápida identificación de la causa raíz de posibles problemas de seguridad o actividades sospechosas. Amazon Detective recopila datos de registro de manera automática a partir de los recursos de AWS y utiliza el aprendizaje automático, el análisis estadístico y la teoría

de gráficos para crear un conjunto de datos vinculados que permite llevar a cabo fácilmente investigaciones sobre la seguridad.

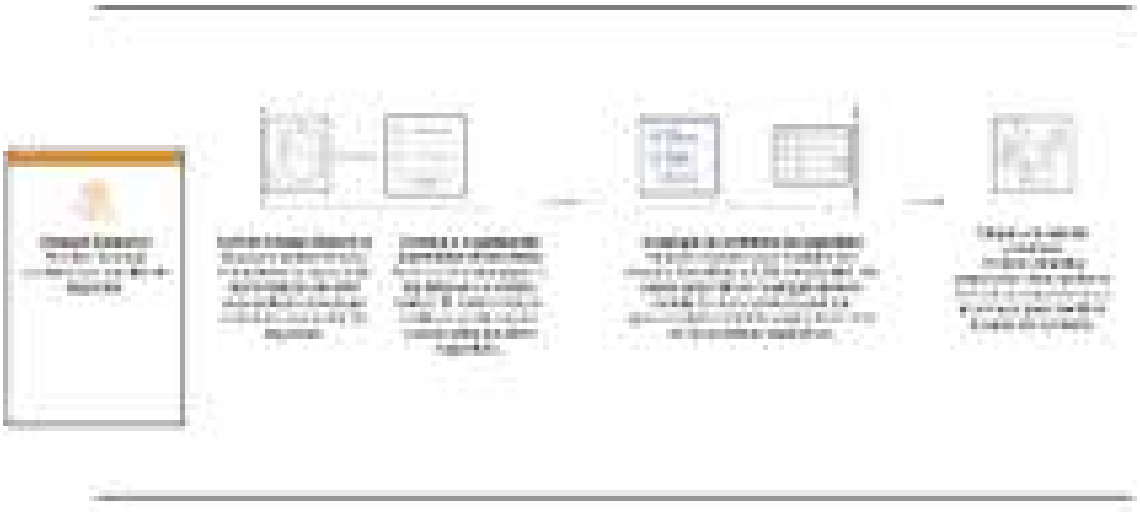


Ilustración 4 Funcionamiento de Amazon Detective

Amazon detective permite analizar eventos de varios orígenes de datos, como registros de flujos de Virtual Private Cloud (VPC), AWS CloudTrail y Amazon GuardDuty, además de crear de manera automática una visión unificada e interactiva de los recursos, los usuarios y las interacciones entre ellos a lo largo del tiempo. Gracias a esta visión unificada, se pueden visualizar todos los detalles y el contexto en un solo lugar a fin de identificar las razones subyacentes que explican los hallazgos, profundizar en actividades históricas relevantes y determinar con rapidez la causa raíz.

Recopilación automática de datos

Amazon Detective incorpora y procesa los datos relevantes de todas las cuentas habilitadas de manera automática. No SE tiene que configurar ni habilitar los orígenes de datos. Amazon Detective recopila y analiza eventos de orígenes de datos, como AWS CloudTrail, registros de flujo de VPC y hallazgos de Amazon GuardDuty, además de conservar hasta un año de datos agregados para su análisis.

Modelo de gráfico

Amazon Detective analiza eventos de diferentes orígenes de datos en relación con el tráfico de IP, las operaciones de administración de AWS y la actividad no autorizada o maliciosa para crear un modelo gráfico que separe los datos de registro con la ayuda del aprendizaje automático, el análisis estadístico y la teoría de gráficos. El modelo de gráfico está prediseñado con relaciones de seguridad y resume la información de contexto y de comportamiento.

3.3. Amazon CloudWatch

Amazon CloudWatch es un servicio de monitorización y administración que suministra datos e información procesable para aplicaciones y recursos de infraestructura locales, híbridos y de AWS. Con CloudWatch, se pueden recopilar y obtener acceso a todos los datos de rendimiento y operaciones en formato de registros y métricas a partir de una sola plataforma. Esto permite monitorear aplicaciones y sistemas individuales aislados (servidor, red, base de datos, etc.). CloudWatch permite monitorear una pila completa (aplicaciones, infraestructura y servicios) y utilizar alarmas, registros y datos de eventos para tomar acciones automatizadas y disminuir el tiempo de resolución.

Ilustración 5 Funcionamiento de Amazon CloudWatch

Recopilación de datos

Amazon CloudWatch Logs permite recopilar y almacenar registros de recursos, aplicaciones y servicios casi en tiempo real. Existen tres categorías principales de registros

- Registros a la venta: Los servicios de AWS publican originalmente estos registros por parte del cliente. Actualmente, Amazon VPC Flow Logs y los registros de Amazon Route 53 son los dos tipos admitidos.
- Registros que publican los servicios de AWS: Actualmente, 30 servicios de AWS publican registros en CloudWatch. Estos servicios incluyen Amazon API Gateway, AWS Lambda, AWS CloudTrail y muchos otros.
- Registros personalizados: Estos son los registros de las aplicaciones propias de cada organización y recursos locales. Se puede usar AWS Systems Manager para instalar un agente de CloudWatch o recurrir a la acción de la API PutLogData para publicar registros fácilmente.

Monitoreo

Los paneles de Amazon CloudWatch permiten crear gráficos reutilizables y ver las aplicaciones y los recursos de la nube en una vista unificada. Se pueden visualizar en un gráfico los datos de registros y métricas lado a lado en un único panel para

obtener rápidamente el contexto y pasar de diagnosticar el problema a entender la causa raíz. También se puede correlacionar el patrón de registros de una métrica específica y definir alarmas para que avisen de manera proactiva acerca de problemas operativos y de rendimiento. Esto otorga una visibilidad completa del sistema sobre el estado de las operaciones y la capacidad para resolver errores rápidamente, lo que reduce el tiempo de resolución (MTTR).

Alarmas Compuestas

Las alarmas compuestas de Amazon CloudWatch permiten combinar varias alarmas y reducir el ruido de las alarmas. Si el problema de una aplicación afecta a varios recursos de la aplicación, se recibirá solo una única notificación de alarma que corresponde a toda la aplicación, en lugar de recibir una notificación por cada recurso, componente o servicio afectado. Se permite proporcionar un estado general de un grupo de recursos, como una aplicación, una región de AWS o una zona de disponibilidad.

Alarmas de alta resolución

Las alarmas de Amazon CloudWatch permiten definir un umbral de métricas y activar una acción. Se pueden crear alarmas de alta resolución, definir un percentil y, a continuación, especificar una acción u omisión, según corresponda.

Detección de anomalías

La detección de anomalías de Amazon CloudWatch aplica algoritmos de aprendizaje automático para analizar los datos de las métricas de manera permanente y detectar los comportamientos anormales. Permite crear alarmas que ajustan automáticamente los umbrales basándose en patrones de métricas naturales, como el momento del día, los días de la semana, las estaciones o las tendencias cambiantes. Esto permite monitorear, aislar y solucionar los cambios inesperados en las métricas.

3.4. AWS Security Hub

AWS Security Hub permite ver de manera integral las alertas de seguridad de alta prioridad y el estado de conformidad en todas las cuentas de AWS. Con Security Hub, se dispone de un único lugar donde se suman, organizan y priorizan las alertas de seguridad, o los resultados de múltiples servicios de AWS, por ejemplo, Amazon GuardDuty.

Ilustración 6 Funcionamiento de AWS Security Hub

Controles automatizados y continuos de las mejores prácticas de seguridad

Security Hub proporciona un conjunto de controles de seguridad automatizados denominado AWS Foundational Security Best. Se trata de un conjunto de prácticas recomendadas de seguridad que se ejecutan de forma continua cada vez que se producen cambios en los recursos asociados o en una programación periódica establecida. Cada control tiene una puntuación de gravedad específica para ayudar a priorizar.

Acciones automatizadas de respuesta, corrección y refuerzo

Se pueden crear flujos de trabajo personalizados de respuesta, corrección y enriquecimiento automatizados mediante la integración de Security Hub con Amazon EventBridge. Todos los hallazgos de Security Hub se envían automáticamente a EventBridge, y se pueden crear reglas de EventBridge que tengan como destino funciones de AWS Lambda, funciones de AWS Step Function o libros de ejecución de AWS Systems Manager Automation. Estas funciones o libros de ejecución pueden suministrar datos adicionales o tomar acciones de respuesta y corrección automatizadas sobre los hallazgos. Security Hub también admite el envío de hallazgos a EventBridge bajo demanda a través de acciones personalizadas.

3.5. AWS Systems Manager

AWS Systems Manager permite centralizar datos operacionales de diferentes servicios de AWS y automatizar tareas en recursos de AWS. Permite la creación de grupos lógicos de recursos, tales como aplicaciones, capas diferentes de una pila de aplicaciones o entornos de producción y de desarrollo. Con Systems Manager, se puede seleccionar un grupo de recursos y ver su actividad reciente, sus cambios en la configuración de recursos, sus notificaciones relacionadas, sus alertas operativas, su inventario de software y su estado de conformidad con parches. Systems Manager

proporciona un lugar centralizado para ver y administrar recursos de AWS. Esto permite tener un control y una visibilidad completos de las operaciones.

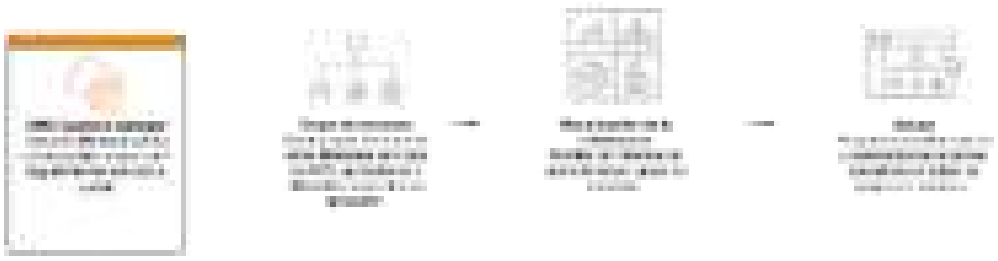


Ilustración 7 Funcionamiento de Systems Manager

State Manager

Es un servicio de administración de configuración seguro y escalable que automatiza el proceso de mantener la infraestructura híbrida y de Amazon Elastic Compute Cloud (Amazon EC2) en el estado que se defina.

State Manager ofrece las ventajas siguientes:

- Instancias de arranque con software específico en el inicio.
- Descargar y actualizar agentes, incluido el agente de SSM, utilizando una programación definida
- Unir instancias a un dominio de Windows.
- Parchear instancias con actualizaciones de software a lo largo de su ciclo de vida.
- Ejecutar scripts en Linux, macOS e instancias administradas de Windows a lo largo de su ciclo de vida.

Explorer

Explorer de AWS Systems Manager es un panel personalizable que incluye información y análisis clave acerca del rendimiento y estado operativo del entorno de AWS. Explorer combina datos operativos de diferentes cuentas y regiones de AWS para ayudar a priorizar e identificar dónde se debe actuar.

OpsCenter

OpsCenter ofrece una ubicación centralizada donde se pueden ver, investigar y resolver problemas operativos relacionados con cualquier recurso de AWS. OpsCenter incorpora y estandariza problemas operativos, denominados OpsItems, al mismo tiempo que provee información contextual relevante que ayuda a realizar un diagnóstico y lograr una resolución.

Incident Manager

AWS Systems Manager permite una resolución más rápida de problemas de disponibilidad y rendimiento de aplicaciones críticas. Ayuda a prepararse ante incidentes con planes de respuesta automatizados que unen a las personas correctas con la información adecuada. Con Incident Manager, se pueden tomar medidas de manera automática cuando una alarma de Amazon CloudWatch o un evento de Amazon EventBridge detecte un problema crítico. Incident Manager ejecuta planes de respuesta preconfigurados para interactuar con los servicios de emergencia a través de SMS y llamadas telefónicas, vincular canales de chat designados con AWS Chatbot y ejecutar runbooks de AWS Systems Manager Automation.

Application Manager

Application Manager de AWS Systems Manager ayuda a investigar y remediar los problemas con los recursos de AWS en el contexto de las aplicaciones. Con Application Manager, se puede detectar y/o definir los componentes de la aplicación, así como ver datos de las operaciones en el contexto de una aplicación. Además, puede realizar acciones de corrección, como la aplicación de parches y la ejecución de runbooks de automatización. Además, se puede utilizar Application Manager para ver los datos operativos y las alarmas de CloudWatch, así como para realizar acciones en los clústeres de contenedores existentes en entornos de Amazon EKS.

3.6. AWS CloudTrail

AWS CloudTrail es un servicio que permite realizar auditorías de gobernanza, de conformidad, operativas y de riesgo en las cuentas de AWS. Con CloudTrail, se pueden registrar, monitorear de manera continua y retener la actividad de la cuenta relacionada con acciones en toda la infraestructura de AWS. CloudTrail proporciona el historial de los eventos de actividad de la cuenta de AWS, incluidas las acciones efectuadas a través de la consola de administración de AWS, los SDK de AWS, las herramientas de línea de comandos y otros servicios de AWS. El historial de eventos simplifica el análisis de seguridad, el seguimiento de cambios de recursos y la resolución de problemas. Además, se puede usar CloudTrail para detectar actividad inusual en las cuentas de AWS. Estas funciones ayudan a simplificar los análisis operativos y la solución de problemas.

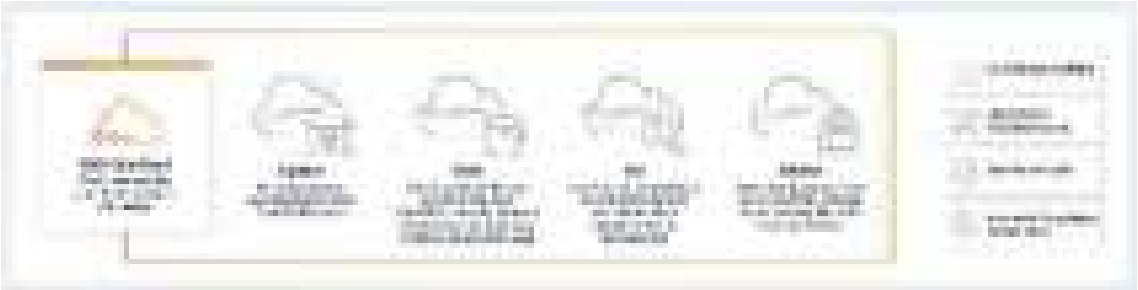


Ilustración 8 Funcionamiento de AWS CloudTrail (traducir)

3.7. AWS WAF

AWS WAF es un firewall de aplicaciones web que permite monitorizar las solicitudes HTTP y HTTPS que se reenvían a CloudFront y permite controlar quién accede al contenido. En función de las condiciones que se especifiquen, Amazon CloudFront, Amazon API Gateway, Application Load Balancer o AWS AppSync responde a las solicitudes con el contenido solicitado o con un código de estado HTTP 403 (Prohibido). También se puede configurar para devolver una página de error personalizada cuando se bloquea una solicitud.

3.8. AWS Network Firewall

AWS Network Firewall es un servicio administrado que facilita la implementación de protecciones de red básicas para todas sus Amazon Virtual Private Clouds (VPC). El motor de AWS Network Firewall permite definir reglas de firewall que brindan un control minucioso sobre el tráfico de la red. AWS Network Firewall trabaja junto a AWS Firewall Manager de modo que permite crear políticas basadas en reglas de AWS Network Firewall y luego aplicar de manera centralizada estas políticas en sus cuentas y VPC.

El sistema de prevención de intrusiones (IPS) de AWS Network Firewall proporciona una inspección activa del flujo de tráfico para que se pueda identificar y bloquear las vulnerabilidades mediante la detección basada en firmas. AWS Network Firewall también ofrece filtrado web que puede detener el tráfico a URL incorrectas conocidas y monitorear nombres de dominio completamente autorizados.

Se puede encontrar la implementación de esta tecnología en la siguiente guía del fabricante:
https://docs.aws.amazon.com/es_es/vpc/latest/userguide/network-firewall.html

3.9. AWS Personal Health Dashboard

AWS Personal Health Dashboard ofrece alertas y orientación sobre los eventos de AWS que pueden afectar al entorno. Mientras que Service Health Dashboard muestra el estado general de los servicios de AWS, Personal Health Dashboard proporciona notificaciones proactivas y transparentes sobre un entorno específico de AWS.