Guía técnica de AWS

Guía de respuestas ante incidentes de seguridad de AWS

Guía de respuestas ante incidentes de seguridad de AWS: Guía técnica de AWS

Table of Contents

Guía de respuestas ante incidentes de seguridad de AWS

Fecha de publicación: 23 de noviembre de 2020 (Revisiones del documento)

Esta guía proporciona información general sobre los aspectos fundamentales de la respuesta a incidentes de seguridad en el entorno de la nube de AWS de un cliente. Se centra en ofrecer información general sobre los conceptos de seguridad en la nube y respuesta ante incidentes e identifica las capacidades, los servicios y los mecanismos de la nube disponibles para los clientes que responden a problemas de seguridad.

Este documento está destinado a personas que desempeñan funciones técnicas y presupone que están familiarizadas con los principios generales de seguridad de la información, tienen una comprensión básica de la respuesta ante incidentes en sus entornos locales actuales y tienen ciertos conocimientos sobre los servicios en la nube.

Introducción

La seguridad es la mayor prioridad de AWS. Como cliente de AWS, se beneficiará de una arquitectura de red y un centro de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes. La nube de AWS cuenta con un modelo de responsabilidad compartida. AWS administra la seguridad de la nube. Usted es responsable de la seguridad en la nube. Esto significa que retiene el control de la seguridad que decida implementar. Dispone de acceso a cientos de herramientas y servicios que lo ayudarán a satisfacer sus objetivos de seguridad. Estas capacidades le permiten establecer una base de referencia de seguridad que cumple los objetivos para las aplicaciones que se ejecutan en la nube.

Cuando se produce alguna desviación respecto a esa base de referencia (por ejemplo, por una configuración incorrecta), es posible que tenga que responder e investigar. Para hacerlo correctamente, debe comprender los conceptos básicos de la respuesta ante incidentes de seguridad en su entorno de AWS, así como los problemas que debe tener en cuenta para preparar, educar y entrenar a sus equipos de la nube antes de que se produzcan problemas de seguridad. Es importante saber qué controles y capacidades se pueden usar, revisar ejemplos actuales para resolver posibles problemas e identificar métodos de reparación que se pueden utilizar para aprovechar la automatización y mejorar la velocidad de respuesta.

Dado que la respuesta ante incidentes de seguridad puede ser un tema complejo, se recomienda comenzar poco a poco, desarrollar runbooks, sacar partido de las capacidades básicas y crear una biblioteca inicial de mecanismos de respuesta ante incidentes que permita la iteración y la introducción de mejoras. Este trabajo inicial debe incluir tanto al departamento jurídico como a equipos que no están implicados en la seguridad, de forma que pueda comprender mejor el impacto de la respuesta ante incidentes (RI) y de las decisiones que ha tomado en sus objetivos corporativos.

Temas

Antes de comenzar

Además de este documento, recomendamos leer el documento de Prácticas recomendadas en materia de seguridad, identidad y cumplimiento y el documento técnico sobre perspectivas de

seguridad de AWS Cloud Adoption Framework (CAF). El marco de adopción de la nube (CAF) de AWS proporciona orientación para la coordinación entre las distintas partes de las organizaciones que se están trasladando a la nube. La orientación del CAF se divide en varias áreas de interés que son relevantes para la implementación de sistemas de TI basados en la nube, a las que nos referimos como perspectivas. La perspectiva de seguridad describe cómo implementar un programa de seguridad en varios flujos de trabajo, uno de los cuales se centra en la respuesta ante incidentes. En este documento se detallan algunas de nuestras experiencias para ayudar a los clientes a evaluar e implementar mecanismos adecuados en ese flujo de trabajo.

Perspectiva de seguridad del CAF de AWS

La perspectiva de seguridad incluye cuatro componentes:

- Controles directivos: establecen los modelos de gobernanza, riesgos y cumplimiento con los que opera el entorno.
- Controles preventivos: protegen sus cargas de trabajo y mitigan las amenazas y las vulnerabilidades.
- Controles de detección: proporcionan visibilidad y transparencia completas sobre el funcionamiento de las implementaciones en AWS.
- Controles de respuesta: son controles diseñados para remediar las posibles desviaciones del marco de referencia de seguridad.

Aunque la respuesta ante incidentes (RI) se suele considerar parte del componente de controles de respuesta, ambos dependen del resto de componentes y están influidos por ellos. Por ejemplo, los controles de seguridad directivos y preventivos ayudan a establecer un marco de referencia para poder monitorear e investigar cualquier desviación de la referencia base. Este enfoque no solo elimina el ruido, sino que también contribuye a un diseño de seguridad de tipo defensivo.

Base de la respuesta ante incidentes

Todos los usuarios de AWS de una organización deben tener conocimientos básicos de los procesos de respuesta ante incidentes de seguridad y el personal de seguridad debe comprender perfectamente cómo reaccionar ante los problemas de seguridad. La experiencia y la formación son esenciales para un programa de respuesta ante incidentes en la nube, antes de gestionar un evento de seguridad. La base de un programa de respuesta a incidentes satisfactorio en la nube es instruir, preparar, simular e iterar.

Para entender cada uno de estos aspectos, tenga en cuenta las descripciones siguientes:

- Instruya a su personal de operaciones de seguridad y respuesta a incidentes en relación con las tecnologías en la nube y la forma en que su organización pretende utilizarlas.
- Prepare a su equipo de respuesta ante incidentes para detectar los incidentes en la nube y responder a ellos al habilitar las capacidades de detección y garantizar el acceso adecuado a las herramientas y los servicios en la nube necesarios. Además, prepare los runbooks requeridos, tanto manuales como automatizados, para garantizar respuestas fiables y coherentes. Trabaje con otros equipos para establecer las operaciones de base de referencia esperadas y use estos conocimientos para identificar las desviaciones respecto a las operaciones normales.
- Simule eventos de seguridad esperados e inesperados dentro del entorno de nube para comprender la eficacia de su preparación.
- Itere el resultado de la simulación para mejorar el alcance de su posición de respuesta, disminuir el tiempo hasta obtener resultados y reducir el riesgo aún más.

Instrucción

Temas

Responsabilidad compartida

AWS y usted comparten la responsabilidad con respecto a la seguridad y el cumplimiento. Este modelo compartido alivia parte de su carga operativa, ya que AWS opera, administra y controla tanto los componentes del sistema operativo host y la capa de virtualización como la seguridad física de las instalaciones en las que funciona el servicio.

Usted es responsable de administrar los sistemas operativos invitados (incluidas las actualizaciones y las revisiones de seguridad) y el software de aplicaciones, así como de configurar los controles de seguridad proporcionados por AWS, tales como los grupos de seguridad, las listas de control de acceso a la red y la administración de identidades y accesos. Debe considerar detenidamente los servicios que va a utilizar, ya que sus responsabilidades variarán en función de los servicios que elija, la integración de estos en su entorno de TI y las leyes y normativas aplicables. La ilustración 2 muestra una representación típica del modelo de responsabilidad compartida aplicado a los servicios de infraestructura, como Amazon Elastic Compute Cloud (Amazon EC2). Este divide la mayoría de las responsabilidades en dos categorías: seguridad de la nube (administrada por AWS) y seguridad en la nube (administrada por el cliente). Las responsabilidades pueden cambiar en función de los servicios que utilice. En el caso de los servicios abstractos, como Amazon S3 y Amazon DynamoDB, AWS opera la capa de infraestructura, el sistema operativo y las plataformas, mientras que los clientes acceden a los puntos de conexión para almacenar y recuperar los datos. Los clientes son responsables de administrar sus datos (incluidas las opciones de cifrado), clasificar sus recursos y usar las herramientas de IAM para aplicar los permisos adecuados.

Sin embargo, el modelo de responsabilidad compartida cambia al añadir contenedores y otros servicios que trasladan el modelo de operaciones al proveedor de servicios. Según nos desplazamos hacia la izquierda del modelo operativo (lejos de IaaS y centros de datos hacia PaaS), aumenta la responsabilidad del proveedor de servicios. Un cliente tiene menos responsabilidades en la nube

y opera con más facilidad cuando usa la migración a la izquierda del gráfico. Tenga en cuenta las ilustraciones siguientes y las diferencias en la capacidad de operar en la nube. A medida que cambia su responsabilidad compartida en la nube, también cambian sus opciones de respuesta ante incidentes o análisis forense. Como cliente, al planificar la respuesta ante incidentes, deberá asegurarse también de realizar una planificación según las capacidades que tiene en su modelo operativo y de planear las posibles interacciones antes de que se produzcan en el modelo que haya elegido. Planificar y comprender estos compromisos y adaptarlos a sus necesidades de gobernanza es un paso crucial en la respuesta ante incidentes.

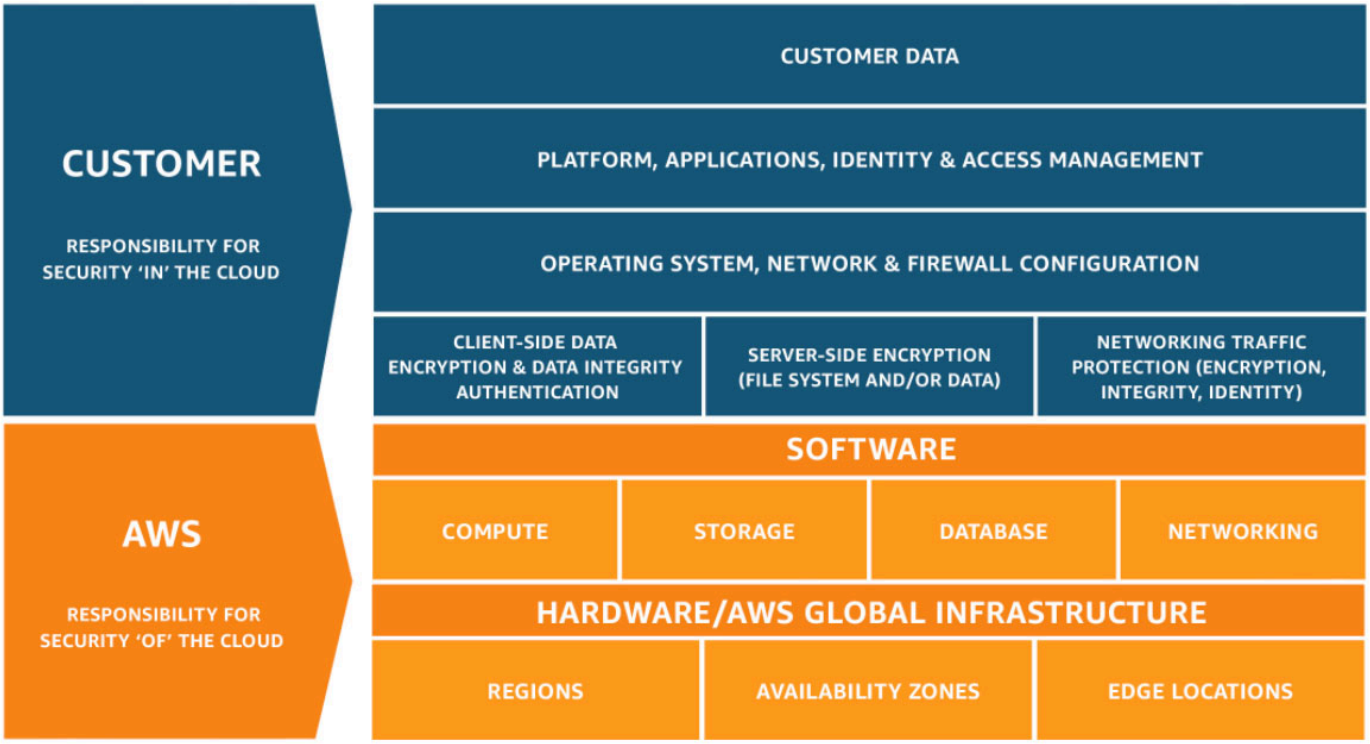

Ilustración 1: Modelo de responsabilidad compartida

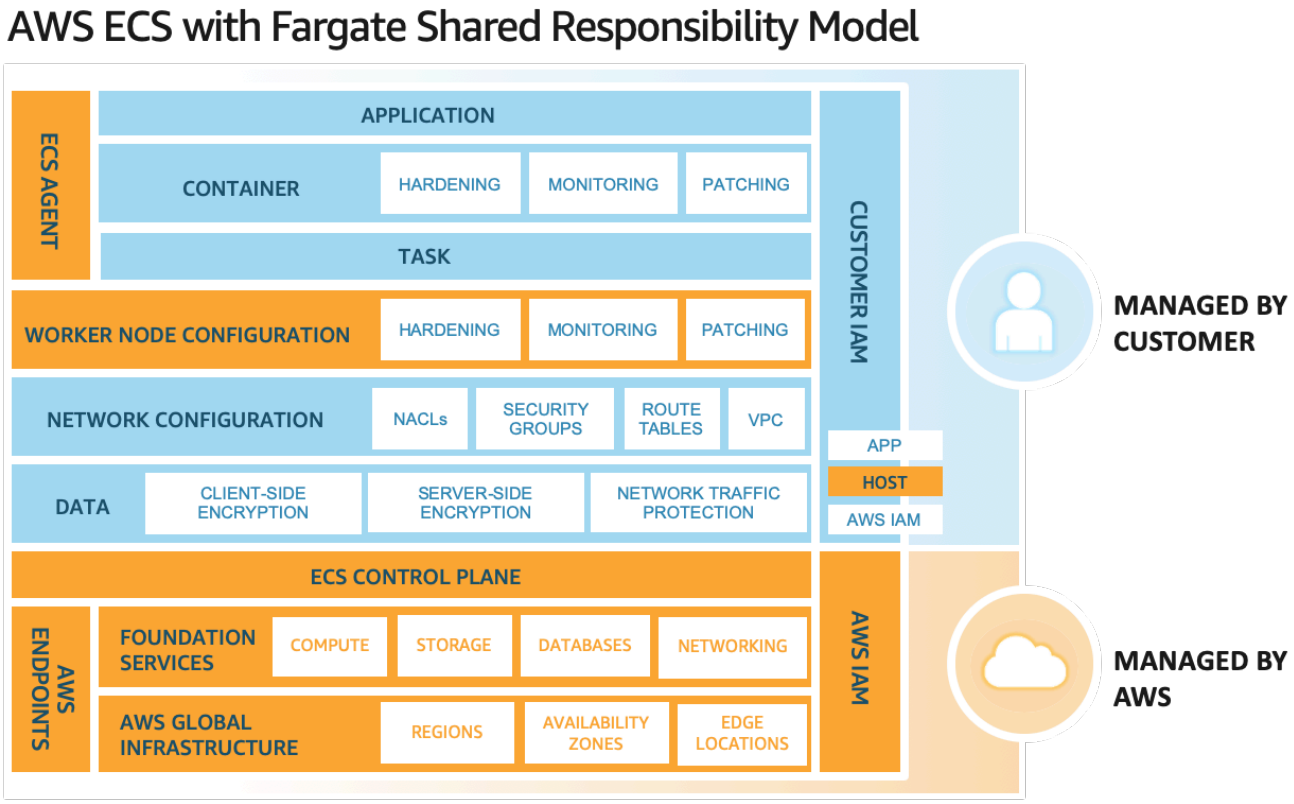

Ilustración 2: Amazon Elastic Container Service (Amazon ECS) con el modelo de responsabilidad compartida de AWS Fargate

Además de la relación directa que tiene con AWS, puede haber otras entidades que tengan responsabilidades en su modelo de responsabilidad particular. Por ejemplo, puede tener unidades organizativas internas que asuman la responsabilidad de algunos aspectos de sus operaciones. También puede contar con socios o terceros que desarrollen, operen o administren parte de su tecnología en la nube.

Es muy importante crear un runbook de respuesta ante incidentes y análisis forense adecuado que coincida con su modelo operativo. Su éxito depende de que entienda los tipos de herramientas que debe crear o las herramientas que necesita comprar para el modelo operativo que ha seleccionado. Cuanto mejor comprenda su organización las herramientas disponibles, mejor preparado estará para satisfacer las necesidades del modelo de gobernanza, riesgo y cumplimiento (GRC) de su empresa.

Respuesta frente a incidentes en la nube

Objetivos de diseño de la respuesta en la nube

Si bien los procesos y los mecanismos generales de respuesta ante incidentes (como los que se definen en la guía de administración de incidentes de seguridad informática NIST SP 800-61) siguen siendo aplicables, recomendamos considerar estos objetivos de diseño específicos que son relevantes para la respuesta ante incidentes de seguridad en un entorno de nube:

- Establezca objetivos de respuesta: trabaje con las partes interesadas, sus asesores jurídicos y la dirección de la organización para determinar el objetivo de respuesta ante un incidente. Entre algunos de los objetivos habituales se incluyen la contención y mitigación del problema, la recuperación de los recursos afectados, la protección de los datos para el análisis forense y la atribución.
- Responda mediante la nube: implemente sus patrones de respuesta donde ocurre el evento y están los datos.
- Conozca lo que tiene y lo que necesita: copie los registros, las instantáneas y cualquier otra prueba en una cuenta de seguridad centralizada en la nube para conservarlos. Use etiquetas, metadatos y mecanismos que permitan aplicar las políticas de retención. Por ejemplo, puede optar por usar el comando dd de Linux o un equivalente de Windows para realizar una copia completa de los datos con fines de investigación.
- Use mecanismos de reimplementación: si una anomalía de seguridad puede atribuirse a una configuración incorrecta, la corrección puede ser tan simple como eliminar la variación mediante la reimplementación de los recursos con la configuración adecuada. Siempre que sea posible, haga que sus mecanismos de respuesta sean seguros para ejecutarse más de una vez y en estados desconocidos.
- Automatice siempre que sea posible: si ve que los problemas o incidentes se repiten, cree mecanismos que clasifiquen y respondan mediante programación a situaciones habituales. Use respuestas humanas para incidentes únicos, nuevos y delicados.
- Elija soluciones escalables: esfuércese por adaptarse a la escalabilidad del enfoque de su organización a la computación en la nube y reduzca el tiempo entre la detección y la respuesta.
- Aprenda y mejore su proceso: si detecta deficiencias en su proceso, herramientas o personal, planifique solucionarlas. Las simulaciones son métodos seguros para encontrar lagunas y mejorar los procesos.

Los objetivos de diseño de NIST recuerdan que es necesario revisar la arquitectura para poder llevar a cabo tanto la respuesta ante incidentes como la detección de amenazas. Al planificar la implementación en la nube, piense en cómo responder a un incidente o a un evento forense. En algunos casos, esto significa que puede tener varias organizaciones, cuentas y herramientas configuradas específicamente para estas tareas de respuesta. Estas herramientas y funciones deben ponerse a disposición de la respuesta ante incidentes mediante la canalización de la implementación y no deben ser estáticas, ya que esto provocaría un riesgo mayor.

Incidentes de seguridad en la nube

Temas

Dominios de incidentes

La responsabilidad del cliente incluye tres dominios en los que pueden producirse incidentes de seguridad: servicio, infraestructura y aplicación. La diferencia entre estos dominios está relacionada con las herramientas que se usan al responder. Tenga en cuenta estos dominios:

- Dominio de servicio: los incidentes del dominio de servicio afectan a la cuenta de AWS del cliente, los permisos de IAM, los metadatos de los recursos, la facturación y otras áreas. Un evento del dominio de servicio es aquel al que se responde exclusivamente con los mecanismos de la API de AWS o que tiene causas raíz asociadas a los permisos de configuración o recurso y puede tener registros relacionados orientados al servicio.
- Dominio de infraestructura: los incidentes del dominio de infraestructura incluyen actividades relacionadas con los datos o la red, como el tráfico a las instancias de Amazon EC2 en la VPC, los procesos y los datos de las instancias de Amazon EC2 y otras áreas, como los contenedores o servicios futuros adicionales. A menudo, la respuesta a los eventos del dominio de infraestructura implica la recuperación, restauración o adquisición de datos relacionados con incidentes para su análisis forense. Puede incluir la interacción con el sistema operativo de una instancia y, en algunos casos, también puede implicar mecanismos de la API de AWS.
- Dominio de aplicación: los incidentes del 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 los runbooks de detección y respuesta ante amenazas en la nube y puede incorporar respuestas similares a las del dominio de infraestructura. Con una arquitectura de aplicaciones

adecuada y meditada, puede administrar este dominio con herramientas en la nube, mediante procesos de análisis forense, recuperación e implementación automatizados.

En estos dominios, debe tener en cuenta los factores que pueden actuar contra la cuenta, los recursos o los datos. Use un marco de riesgos, interno o externo, para determinar cuáles son los riesgos específicos de la organización y prepararse en consecuencia.

En el dominio de servicio, se trabaja para lograr los objetivos exclusivamente con las API de AWS. Por ejemplo, la gestión de un incidente de divulgación de datos de un bucket de Amazon S3 implica llamadas a la API para recuperar la política del bucket, el análisis de los registros de acceso de S3 y, posiblemente, la consulta de registros de AWS CloudTrail. En este ejemplo, es poco probable que la investigación implique herramientas de análisis forense de datos o herramientas de análisis del tráfico de red.

En el dominio de infraestructura, puede usar una combinación de las API de AWS y software de análisis forense digital y respuesta ante incidentes (DFIR) conocido dentro del sistema operativo de una estación de trabajo, como una instancia de Amazon EC2 que haya preparado para trabajar en la respuesta a incidentes. Los incidentes del dominio de infraestructura pueden implicar el análisis de capturas de paquetes de red, bloques de disco en un volumen de Amazon Elastic Block Store (Amazon EBS) o memoria volátil adquirida de una instancia.

Indicadores de eventos de seguridad en la nube

Hay muchos eventos de seguridad que puede que no se clasifiquen como incidentes, pero que sería prudente investigar. Para detectar eventos relacionados con la seguridad en el entorno de la nube de AWS, puede usar estos mecanismos. Si bien no es una lista exhaustiva, tenga en cuenta los ejemplos siguientes de algunos indicadores potenciales:

- Registros y monitores: revise los registros de AWS (como Amazon CloudTrail, los registros de acceso de Amazon S3 y los registros de flujo de VPC), así como los servicios de monitoreo de la seguridad (como Amazon GuardDuty, Amazon Detective, AWS Security Hub CSPM y Amazon Macie). Además, use monitores como las comprobaciones de estado de Amazon Route 53 y las alarmas de Amazon CloudWatch. Del mismo modo, use eventos de Windows, registros de syslog de Linux y otros registros específicos de aplicaciones que pueda generar en las aplicaciones e inicie sesión en Amazon CloudWatch mediante los agentes correspondientes.
- Actividad de facturación: un cambio repentino en la actividad de facturación puede ser indicativo de un evento de seguridad.

- Inteligencia de amenazas: si se suscribe a una fuente de inteligencia de amenazas de terceros, puede correlacionar esa información con otras herramientas de registro y supervisión para identificar posibles indicadores de eventos.
- Herramientas de socios: los miembros de la Red de socios de AWS (APN) ofrecen cientos de productos líderes de la industria que pueden ayudar a cumplir los objetivos de seguridad. Para obtener más información, consulte Socios con competencia en seguridad de AWS y Soluciones de seguridad en AWS Marketplace.
- Contacto por parte de AWS: AWS Support puede ponerse en contacto con usted en caso de identificar actividades abusivas o malintencionadas. Para obtener más información, consulte la sección Respuesta de AWS frente a abusos y riesgos.
- Contacto único: dado que pueden ser sus clientes, sus desarrolladores u otro personal de su organización los que observen algo inusual, es importante contar con un método bien establecido y conocido por todos para ponerse en contacto con el equipo de seguridad. Entre las opciones más populares se incluyen los sistemas de tickets, direcciones de correo electrónico de contacto y formularios web. Si la organización trabaja con el público en general, puede que también necesite un mecanismo de contacto de seguridad orientado al público.

Una de las herramientas que AWS ofrece para la automatización y la detección es AWS Security Hub CSPM. Security Hub ofrece una visión integral de las alertas de seguridad de máxima prioridad y el estado de cumplimiento en todas las cuentas de AWS en un solo lugar, lo que permite una mayor visibilidad de estos indicadores. AWS Security Hub CSPM no es un software de administración de eventos e información de seguridad (SIEM) y no almacena datos de registro, sino que incorpora, organiza y prioriza las alertas de seguridad o los resultados de varios servicios de AWS. Security Hub también ofrece la posibilidad de crear información personalizada que puede provenir de varias fuentes. Esto proporciona al equipo de operaciones de seguridad diversas opciones y una mejor comprensión de la información cuando se produce un evento. Security Hub monitorea de manera continua su entorno mediante comprobaciones de cumplimiento automatizadas que se basan en las prácticas recomendadas de AWS y en los estándares de la industria que sigue su organización.

También puede tomar medidas como respuesta a estos resultados de seguridad y cumplimiento mediante su investigación en Amazon Detective o Amazon Athena o mediante el uso de reglas del bus de eventos o de Amazon CloudWatch Events para enviar los resultados a herramientas de tickets, chat, SIEM, automatización y respuesta de orquestación de seguridad (SOAR) y administración de incidentes o a los manuales de corrección de errores personalizados. La automatización basada en eventos permite responder de forma automática a los incidentes o eventos

que se producen. Este enfoque cambia la seguridad y la forma en que se gestionan los eventos en la nube en comparación con los entornos locales.

Comprensión de las capacidades de la nube

AWS ofrece una amplia gama de capacidades de seguridad que puede usar para investigar eventos de seguridad en todos los dominios. Por ejemplo, AWS proporciona varios mecanismos de registro, como los registros de AWS CloudTrail, Amazon CloudWatch Logs, los registros de acceso de Amazon S3 y muchos más. Debe tener en cuenta los servicios que utiliza y asegurarse de haber activado los registros correspondientes a esos servicios. AWS también ofrece una solución de registro centralizado, que puede ayudar a comprender cómo centralizar y almacenar los tipos comunes de registros en la nube. Después de haber habilitado estas fuentes de registro, debe decidir cómo quiere analizarlas, por ejemplo, mediante el uso de Amazon Athena para consultar los registros almacenados en los buckets de Amazon S3.

Además, existen varios productos de los socios de AWS que pueden simplificar el proceso al analizar estos registros, como los que se describen en el programa de socios con competencia en seguridad de AWS. Existen también varios servicios de AWS que pueden ayudarle a obtener información valiosa sobre estos datos, como Amazon GuardDuty (un servicio de detección de amenazas) y AWS Security Hub CSPM, que permite ver de manera integral las alertas de seguridad de máxima prioridad y el estado de cumplimiento en todas las cuentas de AWS. Además, Amazon Detective recopila datos de registro de sus recursos de AWS y usa el machine learning, el análisis estadístico y la teoría de grafos para ayudar a identificar la causa raíz de posibles problemas de seguridad o actividades sospechosas. Para obtener más información sobre otras capacidades de la nube que puede aprovechar durante sus investigaciones, consulte el Apéndice A: Definiciones de las capacidades en la nube.

Temas

- Privacidad de datos
- Respuesta de AWS frente a abusos y riesgos

Privacidad de datos

Sabemos que los clientes se preocupan mucho por la confidencialidad y la seguridad de los datos, por lo que implementamos controles técnicos y físicos sólidos y sofisticados que están diseñados para evitar el acceso no autorizado al contenido del cliente o su divulgación. Tenemos el compromiso permanente de mantener la confianza de los clientes. Puede encontrar más información sobre los

compromisos de privacidad de datos de AWS en nuestra página de Preguntas frecuentes sobre privacidad de datos.

Estos controles deliberados y autoimpuestos limitan la capacidad de AWS para ayudar a responder en el entorno de un cliente. Por ello, centrarse en comprender y desarrollar capacidades dentro del modelo de responsabilidad compartida es un factor clave para el éxito en la nube de AWS. Si bien es importante habilitar las capacidades de registro y supervisión en las cuentas de AWS antes de que se produzca un incidente, hay otros aspectos de la respuesta ante incidentes que son imprescindibles para un programa satisfactorio.

Privacidad de los datos de los consumidores de California

La Ley de Privacidad del Consumidor de California de 2018 (CCPA) otorga a los «consumidores diversos derechos con respecto a la información personal relacionada con el consumidor que posee una empresa» que está sujeta a la CCPA. Para obtener información sobre las políticas de privacidad y seguridad de los datos de AWS en relación con los clientes sujetos a la CCPA, consulte el documento técnico Preparación para la Ley de Privacidad del Consumidor de California para obtener orientación.

Reglamento general de protección de datos

El Reglamento General de Protección de Datos (RGPD) es una ley de privacidad europea (Reglamento 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016) que entró en vigor el 25 de mayo de 2018. El RGPD deroga la Directiva de Protección de Datos de la UE (Directiva 95/46/EC) y su objetivo es unificar las leyes de protección de datos de toda la Unión Europea (UE) mediante la instauración de una única ley de protección de datos que sea vinculante en todos los estados miembros. Para obtener información sobre el cumplimiento de AWS en relación con el RGPD, consulte el documento técnico sobre Navegación de la guía de RGPD en AWS.

Respuesta de AWS frente a abusos y riesgos

Las actividades abusivas son comportamientos de las instancias o de otros recursos de los clientes de AWS que pueden considerarse malintencionados, ofensivos, ilegales o que podrían dañar otros sitios de Internet. AWS trabaja con sus clientes para detectar y abordar las actividades sospechosas y malintencionadas de los recursos de AWS. Un comportamiento inesperado o sospechoso de los recursos de AWS puede indicar que dichos recursos se han visto comprometidos, lo que podría suponer un riesgo para su negocio. Recuerde que tiene métodos de contacto alternativos en su cuenta de AWS. Asegúrese de aplicar las prácticas recomendadas al añadir contactos, tanto para la seguridad como para la facturación. Aunque el correo electrónico de su cuenta raíz es el objetivo

principal de las comunicaciones de AWS, AWS también comunica los problemas de seguridad y de facturación a las direcciones de correo electrónico secundarias. La adición de una dirección de correo electrónico destinada a una sola persona significa que ha añadido un único punto de error a su cuenta de AWS. Asegúrese de haber añadido al menos una lista de distribución a sus contactos.

AWS detecta actividades abusivas en sus recursos mediante mecanismos como los siguientes:

- Supervisión interna de eventos de AWS
- Inteligencia de seguridad externa con respecto al espacio de direcciones de red de AWS
- Denuncias de actividades abusivas en Internet contra los recursos de AWS

Aunque el equipo de respuesta a actividades abusivas de AWS monitorea y anula con contundencia las actividades no autorizadas que se ejecutan en AWS, la mayoría de las quejas sobre abuso están relacionadas con clientes que tienen negocios legítimos en AWS. A continuación, se indican algunos ejemplos de las causas habituales de actividades abusivas involuntarias:

- Recurso vulnerable: una instancia de Amazon EC2 sin revisiones podría infectarse y convertirse en un agente de botnet.
- Abuso involuntario: un rastreador web demasiado agresivo podría clasificarse como un ataque de denegación de servicio en algunos sitios de Internet.
- Abuso secundario: un usuario final del servicio proporcionado por un cliente de AWS podría publicar archivos de malware en un bucket público de Amazon S3.
- Denuncias falsas: a veces, los usuarios de Internet informan erróneamente de actividades legítimas como si se tratara de abuso.

AWS se compromete a trabajar con sus clientes para prevenir, detectar y mitigar las prácticas abusivas, así como para defenderse de futuras prácticas reincidentes. Recomendamos leer la Política de uso aceptable de AWS, que describe los usos prohibidos de los servicios web que ofrecen Amazon Web Services y sus filiales. Para poder responder de forma oportuna a las notificaciones de abuso de AWS, asegúrese de que la información de contacto de su cuenta de AWS sea correcta. Si se recibe una advertencia de abuso de AWS, el personal de seguridad y operaciones deberá investigar inmediatamente el asunto. Un retraso puede ampliar el impacto en la reputación y las implicaciones legales para usted y otras personas. Y lo que es más importante: el recurso implicado en el abuso podría verse amenazado por usuarios malintencionados. Omitir este peligro podría intensificar los daños de su negocio.

Preparación: personas

Los procesos automatizados permiten a las organizaciones dedicar más tiempo a centrarse en medidas para incrementar la seguridad de sus aplicaciones y su entorno en la nube. La respuesta automatizada ante incidentes también permite que haya personas disponibles para correlacionar eventos, practicar simulaciones, diseñar nuevos procedimientos de respuesta, realizar investigaciones, desarrollar nuevas habilidades y probar o crear herramientas nuevas. A pesar del incremento de la automatización, los analistas y los agentes de repuesta de una organización de seguridad siguen teniendo mucho trabajo. Los equipos homogéneos pueden crear puntos ciegos, por lo que es esencial crear un equipo variado que ofrezca distintos sistemas de pensamiento, perspectivas culturales y experiencia laboral y de vida en situaciones complejas inestables. Una de las cosas más efectivas que podemos hacer cuando planificamos los eventos es asegurarnos de tener diversidad en nuestros equipos y planes de respuesta. Un equipo que integre diversas perspectivas puede identificar puntos ciegos que hayan pasado inadvertidos e identificar soluciones que, de otro modo, no se habrían planteado.

Temas

Definición de roles y responsabilidades

Las habilidades y los mecanismos de respuesta ante incidentes son más importantes cuando se gestionan eventos nuevos o a gran escala. Estos eventos se basan en los estándares escritos que el equipo ha desarrollado y en la práctica adquirida. No podemos predecir ni codificar todos los rumbos posibles que puede tomar un evento, por lo que confiamos en la automatización para las tareas simples y repetitivas (como la recopilación de memoria de instancias o registros de diagnóstico) y dejamos que las personas tomen las decisiones difíciles. La gestión de eventos de seguridad poco claros requiere disciplina entre organizaciones, una predisposición a las acciones decisivas y capacidad para obtener resultados. Dentro de su estructura organizativa, debe haber muchas personas responsables, aprobadoras, consultadas o informadas (RACI) durante un incidente, tales como representantes del departamento de recursos humanos (RR. HH.), el equipo ejecutivo y el departamento jurídico. Tenga en cuenta estos roles y responsabilidades y piense si debe participar

alguna tercera parte. No olvide que, en muchas ubicaciones, existen leyes locales que rigen lo que se puede hacer y lo que no. Aunque crear un gráfico de responsables, aprobadores, consultados e informados (RACI) para un incidente puede parecer un trámite burocrático, al hacerlo se posibilita una comunicación rápida y directa y se describe claramente el liderazgo en las distintas etapas del evento.

Los socios de confianza pueden participar en la investigación o la respuesta, donde aportan experiencia adicional y un escrutinio valioso. Si su equipo no dispone de estas habilidades, puede contratar a una tercera parte externa para obtener ayuda. En ese caso, asegúrese de que la parte externa proporcione formación a los miembros de su equipo. Cuando las partes externas trabajan con sus desarrolladores y operadores internos, pueden ampliar las habilidades de los miembros de su equipo y esa nueva experiencia puede resultar valiosa para su programa de respuesta a incidentes en el futuro.

Durante un incidente, la inclusión de los propietarios y los desarrolladores de las aplicaciones y los recursos afectados es clave, ya que son expertos en la materia (SME) que pueden proporcionar información y contexto. Asegúrese de practicar y de establecer relaciones con los desarrolladores y los propietarios de las aplicaciones antes de confiar en su experiencia para responder ante los incidentes. Es posible que los expertos en la materia o los propietarios de las aplicaciones se vean obligados a actuar en situaciones en las que el entorno les resulte desconocido, que tengan una complejidad imprevista o en las que el personal encargado de la respuesta no tenga acceso. Los expertos en las aplicaciones deben practicar y sentirse cómodos al trabajar con el equipo de respuesta a incidentes.

Proporcionar formación

Para reducir las dependencias y disminuir el tiempo de respuesta, asegúrese de que los equipos de seguridad y los encargados de proporcionar respuesta hayan recibido la formación adecuada en relación con los servicios en la nube y que tengan oportunidades de practicar con las plataformas de nube específicas que su organización utiliza. Parte de esta formación proviene de la creación de equipos y del runbook que se crea al principio del proceso. El hecho de incluir a tantas personas como sea posible en el paso inicial de la formación de runbooks aporta una mejor comprensión a los equipos internos. Esta formación se consolida a medida que los equipos comienzan a seguir estos runbooks en ejercicios de simulación.

AWS y otras terceras partes también ofrecen talleres de seguridad en línea (AWS Security Workshops) que se pueden descargar para trabajar con ellos. También puede resultar beneficioso para la organización ofrecer formación adicional al personal para que adquiera conocimientos sobre

programación, procesos de desarrollo (incluidos los sistemas de control de versiones y las prácticas de implementación) y automatización de la infraestructura.

AWS ofrece varias opciones de formación y rutas de aprendizaje a través de la formación digital, la formación presencial, los socios de AWS y las certificaciones. Para obtener más información, consulte la Formación y certificación de AWS.

Definición de los mecanismos de respuesta

El mecanismo de respuesta depende del modelo de gobernanza, riesgos y cumplimiento (GRC). Lo ideal es crear el modelo de GRC antes de planificar la respuesta ante incidentes. Si aún no ha comenzado a crear un modelo de GRC, este es un primer paso necesario para disponer de un mecanismo óptimo de respuesta ante incidentes. Cuando se plantee su enfoque de respuesta ante incidentes en la nube, al unísono con otros equipos (como los asesores legales, el equipo directivo y las partes corporativas interesadas, entre otros), debe comprender qué tiene y qué necesita. Identifique a las partes interesadas y a los contactos relevantes y asegúrese de tener el acceso adecuado para llevar a cabo la respuesta necesaria.

Si bien la nube puede proporcionar una mayor visibilidad y más capacidades a través de las API de servicio, su modelo de GRC muestra cómo usarlas a la hora de responder. Identifique los números de cuenta de AWS de su equipo, los rangos de IP de sus nubes virtuales privadas (VPC), los diagramas de red correspondientes, los registros, las ubicaciones de los datos y las clasificaciones de estos. Muchos de estos procesos tecnológicos están incluidos en la sección Preparación: tecnología. Después, comience a documentar los procedimientos de respuesta ante incidentes (conocidos habitualmente como procedimientos o runbooks) que definen los pasos para investigar un incidente y corregirlo.

Creación de una cultura de seguridad receptiva y adaptable

En AWS, hemos aprendido que nuestros clientes y nuestros equipos internos tienen más éxito cuando los equipos de seguridad son facilitadores cooperativos para el negocio y sus desarrolladores y fomentan una cultura que garantiza que todas las partes interesadas cooperen y escalen para mantener una posición de seguridad ágil con una alta capacidad de respuesta. Si bien mejorar la cultura de seguridad de la organización no es el tema central de este documento, puede obtener información relevante del resto del personal si el equipo de seguridad es receptivo. Cuando el equipo de seguridad tiene una actitud abierta y accesible, con el apoyo de la dirección, es más probable que reciba notificaciones, colaboraciones y respuestas adicionales y oportunas para los eventos de seguridad.

En algunas organizaciones, el personal puede temer represalias si informa sobre un problema de seguridad. A veces, simplemente no saben cómo notificarlo. En otros casos, es posible que no quieran perder el tiempo o que se sientan avergonzados de notificar un posible incidente de seguridad que al final resulte no ser un problema. Desde el equipo directivo hacia abajo, es importante promover una cultura de aceptación e invitar a todos a formar parte de la seguridad de la organización. Proporcione un canal claro para que cualquiera pueda crear un ticket de gravedad alta, siempre que se crea que puede haber un riesgo o una amenaza potencial. Reciba estas notificaciones de buena gana y con una mente abierta y, lo que es más importante, deje claro al personal no relacionado con la seguridad que aprecia estas notificaciones. Enfatice que prefiere recibir más notificaciones de las necesarias sobre posibles problemas que no recibir ninguna en absoluto. Es mucho mejor que un desarrollador notifique su propio error que esperar a que un investigador lo señale en un artículo público.

Estas notificaciones ofrecen oportunidades valiosas para practicar investigaciones receptivas en situaciones de estrés. Pueden servir como un bucle de retroalimentación importante mientras desarrolla sus procedimientos de respuesta.

Predicción de la respuesta

Dado que es imposible predecir todos los eventos posibles, debe seguir confiando en el análisis humano. Tomarse el tiempo necesario para formar al personal y preparar a la organización de forma minuciosa ayuda a anticipar situaciones inesperadas; sin embargo, no es necesario preparar a la organización de forma aislada. Colaborar con socios de seguridad de confianza para identificar eventos de seguridad inesperados ofrece a las organizaciones la ventaja de contar con visibilidad e información adicionales.

Los socios y la ventana de respuesta

El traspaso a la nube es único para cada organización. Sin embargo, hay patrones y prácticas que otras organizaciones ya han descubierto y que un socio de seguridad de confianza puede indicarle. Se recomienda identificar socios de seguridad de AWS externos que puedan proporcionarle experiencia externa y una perspectiva distinta para aumentar sus capacidades de respuesta. Los socios de seguridad de confianza pueden ayudar a identificar posibles riesgos o amenazas con los que quizás no esté familiarizado.

En 1955, Joseph Luft y Harrington Ingham crearon la ventana de Johari, un ejercicio para asignar rasgos a distintas categorías. La ventana se representa como una cuadrícula que consta de cuatro cuadrantes, similar al diagrama siguiente.

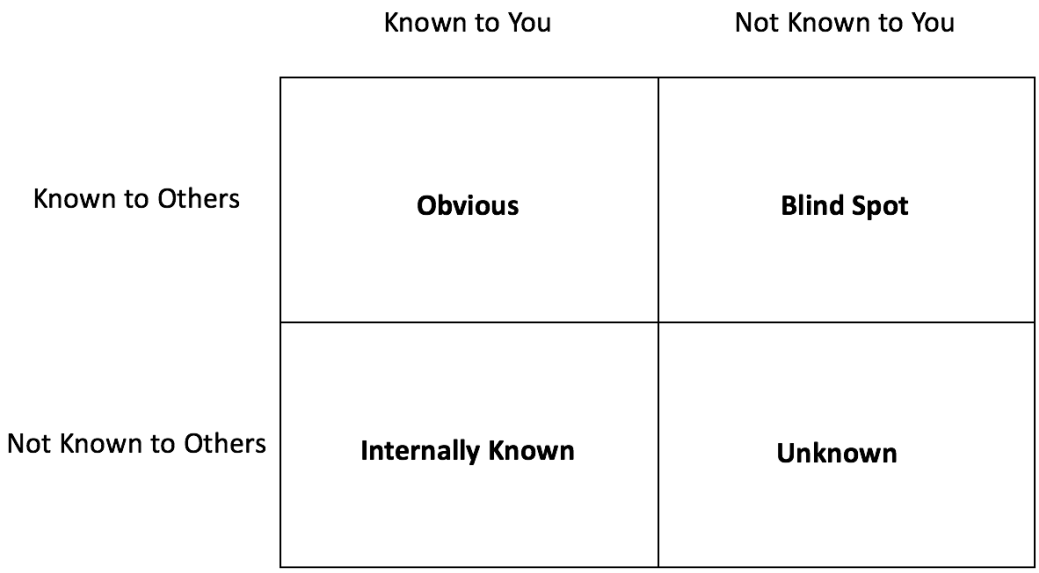

Figura 3: Ventana de Johari modificada para la respuesta ante incidentes

Aunque la ventana de Johari no se diseñó para la seguridad de la información, se puede ajustar el concepto a fin de usarlo como un modelo mental simple para considerar la dificultad en la evaluación de las amenazas de una organización. En nuestro concepto modificado, los cuatro cuadrantes son los siguientes:

- Obvio: riesgo que conocen tanto su equipo como el socio de AWS.
- Conocido internamente: riesgo con el que el equipo está familiarizado, pero no así el socio de AWS. Esto puede significar que dispone de experiencia interna o conocimientos transmitidos oralmente.
- Punto ciego: riesgo con el que el socio de AWS está familiarizado, pero su equipo no.
- Desconocido: riesgo con el que ni usted ni su socio de AWS están familiarizados.

Si bien este diagrama es sencillo, representa el valor que pueden aportar los socios de confianza de AWS. Lo más importante es que puede haber puntos ciegos que no conoce, pero sobre los que un socio de AWS con la experiencia adecuada pueda llamar su atención. Si bien es posible que ambos estén familiarizados con esos riesgos en el cuadrante Obvio, el socio de AWS podría recomendarle controles y soluciones con los que no esté familiarizado. Además, aunque es posible que llame la atención de su socio de AWS sobre los riesgos del cuadrante Conocido internamente, también cabe la posibilidad de que este pueda identificar controles optimizados para mitigar el riesgo en cuestión.

Mientras se pone a prueba a sí mismo para mejorar, póngase en contacto con su socio de AWS para que le proporcione asesoramiento experto.

Riesgo desconocido

Si se ha centrado en adaptar las alertas, mejorar los procedimientos de respuesta ante incidentes con la automatización y aumentar las defensas de seguridad, puede que se pregunte qué puede mejorarse a continuación. Es posible que sienta curiosidad por los riesgos desconocidos, tal y como se representa en la categoría Desconocido de la Figura 3. Puede reducir los riesgos desconocidos a través de los métodos siguientes:

- Afirmaciones de seguridad definidas: ¿cuáles son algunas de las verdades que puede afirmar? ¿Cuáles son los fundamentos de seguridad que deben ser absolutamente ciertos en su entorno? La definición clara de estos aspectos permite localizar los opuestos. Este proceso es más fácil de hacer al principio del traspaso a la nube, en lugar de intentar aplicar ingeniería inversa a sus afirmaciones de seguridad más adelante.
- Educación, comunicación e investigación: forme a expertos de seguridad en la nube entre su personal o incluya socios expertos que le ayuden a examinar su entorno. Cuestione sus suposiciones y desconfíe del razonamiento sutil. Cree bucles de retroalimentación en sus procesos y ofrezca mecanismos para que los equipos de ingeniería se comuniquen con los equipos de seguridad. También puede ampliar su enfoque para monitorear las listas de correo de seguridad y las divulgaciones de seguridad de la información relevantes.
- Reducción de la superficie de ataque: mejore su defensa para evitar los riesgos y tener más tiempo frente a ataques desconocidos. Bloquee y ralentice a los atacantes y oblíguelos a hacerse notar.
- Inteligencia de amenazas: suscríbase a una fuente continua de información sobre amenazas, riesgos e indicadores actuales y relevantes de todo el mundo.
- Alertas: genere notificaciones que alerten sobre actividades inusuales, malintencionadas o costosas. Por ejemplo, puede crear una notificación para las actividades que se produzcan en regiones o servicios que no utilice.
- Machine Learning: use el machine learning para identificar anomalías complejas en una organización específica o para personas concretas. Como ayuda para identificar comportamientos inusuales, también puede generar un perfil de las características normales de sus redes, usuarios y sistemas.

La inteligencia de amenazas se convierte en el tema principal a la hora de considerar los puntos ciegos y los riesgos desconocidos. La ventana de Johari muestra cómo categorizar lo que sabe y lo que no sabe, pero la inteligencia de amenazas muestra cómo explicar lo que aún no sabe. Este tipo de inteligencia es una disciplina que ayuda a las empresas a ver más allá del modelo de amenazas, para encontrar amenazas que la empresa aún no sabe que existen.

En general, la inteligencia de amenazas incluye lo siguiente:

1. Localización de nuevas amenazas
2. Definición de patrones nuevos
3. Definición de nuevas técnicas automatizadas de adquisición
4. Repetición de estos procesos

Si bien este tipo de práctica puede resultar útil, el cuidado y el mantenimiento de un equipo de inteligencia de amenazas pueden suponer una sobrecarga para muchas empresas, incluso aquellas de gran tamaño. Al final, la cuestión se reduce a adaptarse a su modelo de amenazas, tamaño y desafío en cuanto a riesgos. Tenga en cuenta estas preguntas:

- ¿Su modelo de amenazas es lo suficientemente diferente del perfil estándar en el que se encuentra la empresa?
- ¿Es su tolerancia al riesgo lo suficientemente baja como para necesitar un equipo de este tipo?
- ¿Es una decisión económicamente acertada disponer de un equipo para su empresa?
- ¿Es su perfil de riesgo lo suficientemente interesante como para atraer una cantidad de talento razonable a su causa?

Si la respuesta a alguna de estas preguntas es no, lo más acertado sería encontrar un socio de inteligencia de amenazas. Muchas empresas importantes y conocidas ofrecen servicios competitivos de este tipo.

AWS proporciona las herramientas y los servicios necesarios para que pueda administrar estos problemas por su cuenta. El uso del machine learning para identificar patrones malintencionados es un campo de estudio investigado en profundidad, con patrones que implementan los clientes, los Servicios profesionales de AWS, los socios de AWS y a través de servicios de AWS como Amazon GuardDuty y Amazon Macie. Algunos de estos patrones se han debatido en las sesiones de las conferencias AWS re:Invent. Para obtener más información, consulte la sección Multimedia de este documento técnico.

Los clientes también están ampliando sus lagos de datos tradicionalmente centrados en la actividad empresarial para aprovechar patrones de arquitectura similares cuando desarrollan lagos de datos de seguridad. Los equipos de operaciones de seguridad también están ampliando su uso de las herramientas tradicionales de registro y monitoreo, tales como Amazon OpenSearch Service y OpenSearch Dashboards, a arquitecturas de macrodatos.

Esos clientes recopilan datos internos de registros de eventos de AWS CloudTrail, registros de flujo de VPC, registros de acceso de Amazon CloudFront, registros de bases de datos y registros de aplicaciones y, a continuación, combinan estos datos con datos públicos e inteligencia de amenazas. Los clientes han usado estos valiosos datos para ir aún más lejos e incluir competencias de ciencia de datos y de ingeniería de datos en sus equipos de operaciones de seguridad a fin de aprovechar herramientas como Amazon EMR, Amazon Kinesis Data Analytics, Amazon Redshift, Amazon QuickSight, AWS Glue, Amazon SageMaker y Apache MXNet en AWS para crear soluciones personalizadas que identifiquen y prevean anomalías exclusivas de su negocio.

Por último, consulte las soluciones de los socios con competencia en seguridad para conocer cientos de productos líderes del sector de los socios de AWS equivalentes, idénticos o integrados en los controles existentes en sus entornos locales. Estos productos complementan a los servicios de AWS existentes para que pueda implementar una arquitectura de seguridad integral y disfrutar de una experiencia más fluida tanto en la nube como en las instalaciones.

Preparación: tecnología

Temas

Preparación del acceso a las cuentas de AWS

Durante un incidente, los equipos de respuesta ante incidentes deben tener acceso a los entornos y los recursos involucrados. Asegúrese de que los equipos tengan el acceso adecuado para llevar a cabo sus tareas antes de que ocurra un evento. Para ello, debe saber el nivel de acceso que requieren los miembros del equipo (por ejemplo, qué tipo de acciones es probable que realicen) y debe aprovisionar el acceso con antelación. Este acceso se deriva de las políticas de gobernanza, administración de riesgos y cumplimiento (GRC) de la empresa. La autenticación y la autorización de los miembros del equipo deben haberse documentado y probado mucho antes de que se produzca un evento para garantizar que puedan responder de forma oportuna y sin demora. Parte de la preparación para responder a un incidente de forma correcta debe consistir en revisar cómo se han diseñado las cuentas de AWS y cómo se permiten y organizan los roles entre cuentas.

En esta etapa, debe trabajar en estrecha colaboración con los desarrolladores, arquitectos, socios, equipos de gobernanza y equipos de cumplimiento para comprender qué nivel de acceso es necesario para los agentes de respuesta. Identifique y debata la estrategia de cuentas de AWS y la estrategia de identidades en la nube con los arquitectos de la nube de su organización para comprender los métodos de autenticación y autorización que se han configurado, 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 entre varias cuentas de AWS.
- Autenticación: un usuario se autentica como usuario de AWS IAM creado dentro de una sola cuenta de AWS.

Estos valores definen las opciones técnicas para la autenticación en AWS y cómo puede obtener acceso durante una respuesta, pero algunas organizaciones pueden confiar en otro equipo o en un socio como ayuda a la hora de responder. Las cuentas de usuario que se crean de forma específica

para responder ante un incidente de seguridad suelen tener privilegios con el fin de proporcionar un acceso suficiente. Por lo tanto, el uso de estas cuentas de usuario debe restringirse y no deben utilizarse para las actividades cotidianas.

Antes de crear nuevos mecanismos de acceso, trabaje con los equipos de la nube para comprender cómo se organizan y se gobiernan las cuentas de AWS. Muchos clientes usan AWS Organizations como ayuda para administrar la facturación de forma centralizada, compartir recursos a través de sus cuentas de AWS y controlar el acceso, el cumplimiento y la seguridad. Una de las características básicas de Organizations es que se puede aprovechar para aplicar políticas de control de servicios a grupos de cuentas, lo que le permite disfrutar de una administración de políticas a escala. Para obtener más información sobre la implementación de mecanismos de gobernanza a escala, consulte Gobernanza de AWS a escala. Una vez que comprenda la forma en que la organización dispone y gobierna las cuentas de AWS, analice los patrones de respuesta generalizados siguientes como ayuda para identificar los enfoques adecuados para su organización.

Temas

Acceso indirecto

Si usa el acceso indirecto, los propietarios de las cuentas o los equipos de aplicaciones deben realizar las correcciones autorizadas en sus cuentas de AWS con la orientación táctica del equipo de respuesta ante incidentes, que son los expertos en seguridad. Este método es una forma más lenta y compleja de ejecutar tareas, pero puede resultar eficaz cuando los agentes de respuesta no están familiarizados con el entorno de las cuentas o la nube.

Acceso directo

Para otorgar acceso directo a los encargados de la respuesta ante incidentes, implemente un rol de AWS IAM en las cuentas de AWS que los ingenieros de seguridad o los agentes de respuesta ante incidentes puedan asumir durante un evento de seguridad. El personal de respuesta ante incidentes se autentica mediante un proceso federado normal o mediante un proceso de emergencia especial,

si el incidente afecta al proceso de autenticación normal. Los permisos que se otorgan al rol de IAM de respuesta ante incidentes dependen de las acciones que prevea que van a realizar los agentes de respuesta.

Acceso alternativo

Si considera que un evento de seguridad afecta a sus sistemas de seguridad, identidad o comunicación, es posible que deba buscar formas de acceso y mecanismos alternativos para investigar y corregir el impacto. Con el uso de una cuenta de AWS nueva personalizada, los agentes de respuesta pueden colaborar y trabajar desde una infraestructura alternativa y segura.

Por ejemplo, pueden aprovechar cualquier infraestructura nueva lanzada en la nube, como estaciones de trabajo remotas que utilizan Amazon WorkSpaces y los servicios de correo electrónico que proporciona Amazon WorkMail. Debe preparar controles de acceso adecuados (con políticas de IAM) para delegar el acceso, de modo que su cuenta de AWS alternativa y segura pueda asumir los permisos de la cuenta de AWS afectada.

Después de haber delegado el acceso adecuado, puede usar las API de AWS en la cuenta afectada para compartir datos relevantes (como registros e instantáneas de volúmenes) a fin de realizar trabajos de investigación en el entorno aislado. Para obtener más información sobre este acceso entre cuentas, consulte Tutorial de IAM: Delegación del acceso entre cuentas de AWS mediante roles de IAM.

Acceso de automatización

Al migrar a la automatización como modo de respuesta para los eventos de seguridad, debe crear roles de IAM para su uso específico por parte de los recursos de automatización (como instancias de Amazon EC2 o funciones de AWS Lambda). Estos recursos podrán asumir los roles de IAM y heredar los permisos asignados al rol. En lugar de crear y distribuir credenciales de AWS, se delega permiso a su función de AWS Lambda o a la instancia de Amazon EC2. El recurso de AWS recibe de forma automática un conjunto de credenciales temporales y las usa para firmar las solicitudes de la API.

También puede plantearse el uso de un método seguro para que la automatización o las herramientas se autentiquen y se ejecuten en el sistema operativo de la instancia de Amazon EC2. Si bien hay muchas herramientas que pueden realizar esta automatización, considere usar AWS Systems Manager Run Command, que permite administrar las instancias de forma remota y segura mediante un agente que se instala en el sistema operativo de la instancia de Amazon EC2.

AWS Systems Manager Agent (SSM Agent) se instala de forma predeterminada en algunas imágenes de máquina de Amazon (AMI) de Amazon EC2, por ejemplo, para Microsoft Windows Server y Amazon Linux. Sin embargo, puede que tenga que instalar el agente de forma manual en otras versiones de instancias de Linux e híbridas. Tanto si usa Run Command como cualquier otra herramienta, debe completar la instalación y la configuración de los requisitos previos antes de recibir la primera alerta relacionada con la seguridad para su investigación.

Acceso a servicios administrados

Es posible que su organización ya esté asociada con algún proveedor de tecnología de la información que se encargue de administrar los servicios y las soluciones en su nombre. Estos socios tienen la responsabilidad compartida de respaldar la seguridad de su organización y es importante comprender esta relación con claridad antes de que se produzca una anomalía. Tanto si ya trabaja con un socio Proveedor de Servicios Administrados (MSP) de AWS, con AWS Managed Services o con un socio de servicios de seguridad administrados, debe identificar las responsabilidades de cada socio en relación con sus entornos en la nube, el acceso con el que cuenta cada proveedor en sus servicios en la nube, el acceso que necesitan y los puntos de contacto o las rutas de escalada cuando requiera su ayuda. Por último, practique los puntos indicados con su socio para asegurarse de que sus planes de respuesta sean predecibles y eficaces.

Preparación de procesos

Una vez que se haya aprovisionado y probado el acceso adecuado, el equipo de respuesta ante incidentes debe definir y preparar los procesos relativos necesarios para la investigación y la corrección. Esta etapa requiere gran cantidad de esfuerzo, ya que debe planificar una respuesta adecuada y suficiente para los eventos de seguridad dentro de sus entornos en la nube.

Trabaje en estrecha colaboración con sus socios y sus equipos internos de servicios en la nube a fin de identificar las tareas necesarias para garantizar que estos procesos sean posibles. Pueden colaborar o asignarse mutuamente las tareas de actividades de respuesta y debe asegurarse de que se hayan implementado las configuraciones de cuenta necesarias. Se recomienda preparar los procesos y las configuraciones de requisitos previos por adelantado para que la organización tenga las capacidades de respuesta siguientes.

Temas

- Árboles de toma de decisiones
- Uso de cuentas alternativas

- Visualización o copia de datos
- Uso compartido de instantáneas de Amazon EBS
- Uso compartido de Amazon CloudWatch Logs
- Uso del almacenamiento inmutable
- Lanzamiento de recursos cerca del evento
- Aislamiento de recursos
- Lanzamiento de estaciones de trabajo forenses

Árboles de toma de decisiones

A veces, distintas condiciones pueden requerir acciones o pasos diferentes. Por ejemplo, puede realizar distintas acciones en función del tipo de cuenta de AWS (desarrollo o producción), las etiquetas de los recursos, el estado de cumplimiento de las reglas de AWS Config de esos recursos u otras consideraciones.

Como ayuda a la hora de crear y documentar estas decisiones, se recomienda que elabore un árbol de toma de decisiones con el resto de equipos y partes interesadas. Al igual que un diagrama de flujo, un árbol de decisiones es una herramienta que puede aprovecharse para respaldar la toma de decisiones, ya que sirve como guía para determinar las acciones y los resultados óptimos en función de las condiciones y las entradas potenciales, incluidas las probabilidades.

Uso de cuentas alternativas

Si bien puede que sea necesario responder a un evento en la cuenta afectada, lo ideal es investigar los datos fuera de esa cuenta. Algunos clientes cuentan con un proceso para crear entornos de cuentas de AWS separados y aislados, con plantillas para preconfigurar los recursos que deben aprovisionarse. Estas plantillas se implementan a través de un servicio, como AWS CloudFormation o Terraform, que proporciona un método sencillo para crear una colección de recursos de AWS relacionados y aprovisionarlos de forma ordenada y predecible.

La preconfiguración de estas cuentas mediante mecanismos con plantillas ayuda a eliminar la interacción humana durante las etapas iniciales de un incidente y garantiza la preparación del entorno y de los recursos de forma repetible y predecible, lo que puede verificarse mediante una auditoría. Además, este mecanismo también aumenta la capacidad de mantener la seguridad y la contención de los datos en el entorno forense.

Este enfoque requiere que trabaje con sus equipos de arquitectos y servicios en la nube a fin de determinar un proceso adecuado para las cuentas de AWS que pueda utilizarse en las investigaciones. Por ejemplo, los equipos de servicios en la nube pueden usar AWS Organizations para generar cuentas nuevas y ayudar a preconfigurarlas con un método basado en plantillas o scripts.

Este método de segmentación es mejor cuando se necesita mantener a una organización de mayor tamaño alejada de una amenaza potencial. Esta segmentación (que utiliza una cuenta de AWS nueva y, en gran medida, sin conexión) significa que un usuario de la organización, etiquetado en la documentación de varias cuentas como la unidad organizativa (OU) de seguridad, puede acceder a la cuenta, realizar las actividades forenses necesarias y, potencialmente, entregar la cuenta en su totalidad a una entidad legal, si es necesario. Este método de análisis forense y atribución requiere una revisión y planificación importantes y debe alinearse con las políticas de GRC de la empresa. Aunque esta no es una tarea sencilla, es mucho más fácil llevarla a cabo antes de crear una base de cuentas grande.

Visualización o copia de datos

El personal de respuesta requiere acceso a los registros o a otros tipos de pruebas para analizarlos y debe asegurarse de tener la capacidad de ver o copiar datos. Como mínimo, la política de permisos de IAM para el personal de respuesta debe proporcionar acceso de solo lectura para poder investigar. Para habilitar un acceso adecuado, puede usar algunas políticas administradas de AWS predefinidas, como SecurityAudit o ViewOnlyAccess.

Por ejemplo, puede que los agentes de respuesta quieran hacer una copia de los datos en un momento dado, como los registros de AWS CloudTrail, de un bucket de Amazon S3 en una cuenta a un bucket de Amazon S3 en otra. Los permisos proporcionados por la política administrada ReadOnlyAccess, por ejemplo, permiten al personal de respuesta realizar estas acciones. Para comprender cómo utilizar AWS Command Line Interface (CLI) para estas tareas, consulte ¿Cómo se pueden copiar todos los objetos de un bucket de Amazon S3 en otro bucket?

Uso compartido de instantáneas de Amazon EBS

Muchos clientes utilizan instantáneas de Amazon Elastic Block Store (Amazon EBS) como parte de la investigación de eventos de seguridad que implican a sus instancias de Amazon EC2. Las instantáneas de los volúmenes de Amazon EBS son copias de seguridad progresivas. Para obtener más información sobre las instantáneas progresivas de Amazon EBS, consulte Instantáneas de Amazon EBS.

Para realizar una investigación de un volumen de Amazon EBS en una cuenta separada y aislada, debe modificar los permisos de la instantánea para compartirla con las demás cuentas de AWS especificadas. Los usuarios a los que haya autorizado pueden usar las instantáneas que comparta como base para crear sus propios volúmenes de EBS, mientras que la instantánea original no se modifica. Para obtener más información, consulte Compartir una instantánea de Amazon EBS.

Si la instantánea está cifrada, también debe compartir la clave administrada por el cliente (CMK) personalizada de AWS Key Management Service (AWS KMS) que se usó para cifrar la instantánea. Puede aplicar permisos entre cuentas a una CMK personalizada al crearla o bien en un momento posterior. Las instantáneas están restringidas a la región en la que se crean, pero puede compartir una instantánea con otra región si la copia en esa región. Para obtener más información, consulte Copiar una instantánea de Amazon EBS.

Uso compartido de Amazon CloudWatch Logs

Los registros que se crean en Amazon CloudWatch Logs (como los registros de flujo de Amazon VPC) pueden compartirse con otra cuenta (como la cuenta de seguridad centralizada) a través de una suscripción a CloudWatch Logs. Por ejemplo, los datos de los eventos de registro se pueden leer desde un flujo de Amazon Kinesis centralizado para realizar un procesamiento y un análisis personalizados. El procesamiento personalizado resulta especialmente útil cuando se recopilan datos de registro de muchas cuentas. Lo ideal es crear esta configuración en una etapa inicial del traspaso a la nube, antes de que se produzca un evento relacionado con la seguridad. Para obtener más información, consulte Uso compartido de datos de registro entre cuentas con suscripciones.

Uso del almacenamiento inmutable

Al copiar registros y otras pruebas en una cuenta alternativa, asegúrese de que los datos replicados estén protegidos. Además de proteger las pruebas secundarias, también debe proteger la integridad de los datos en la fuente. Estos mecanismos, que se conocen como almacenamiento inmutable, protegen la integridad de los datos al prevenir que estos se alteren o se eliminen.

Con las características nativas de Amazon S3, puede configurar un bucket de Amazon S3 para proteger la integridad de los datos. Por ejemplo, si usa el Bloqueo de objetos de S3, puede evitar que se elimine o se sobrescriba un objeto durante un período de tiempo determinado o de manera indefinida. La administración de los permisos de acceso con políticas de buckets de S3, la configuración del control de versiones de S3 y la habilitación de la eliminación de MFA son otras formas de restringir cómo se pueden escribir o leer los datos. Este tipo de configuración resulta útil para almacenar las pruebas y los registros de investigación y suele denominarse escritura única,

lectura múltiple (WORM). Otra forma de proteger los datos es mediante el cifrado del lado del servidor con AWS Key Management Service (AWS KMS) y la verificación de que solo las entidades principales de IAM adecuadas estén autorizadas para descifrarlos.

Además, si quiere conservar los datos de forma segura en un almacenamiento a largo plazo una vez finalizada la investigación, puede trasladar los datos de Amazon S3 a Amazon S3 Glacier con políticas de ciclo de vida de los objetos. Amazon S3 Glacier es un servicio de almacenamiento en la nube seguro, duradero y de muy bajo coste para el archivado de datos y las copias de seguridad a largo plazo. Está diseñado para ofrecer una durabilidad del 99,999999999 % y ofrece funciones integrales de seguridad y cumplimiento.

Además, puede proteger los datos en Amazon S3 Glacier mediante el bloqueo de almacenes de Amazon S3 Glacier, que permite implementar y aplicar fácilmente los controles de cumplimiento para almacenes individuales de Amazon S3 Glacier con una política de bloqueo de almacenes. Puede especificar controles de seguridad, como WORM, en una política de bloqueo de almacenes y bloquear la política para que no se puedan hacer modificaciones en el futuro. Una vez bloqueada, la política no se puede cambiar. Amazon S3 Glacier aplica los controles establecidos en la política de bloqueo de almacenes para ayudar a lograr los objetivos de cumplimiento, por ejemplo, para la retención de datos. Puede implementar distintos controles de cumplimiento en una política de bloqueo de almacenes mediante el lenguaje de políticas de AWS Identity and Access Management (IAM).

Lanzamiento de recursos cerca del evento

Para los agentes de respuesta que sean nuevos en la nube, puede resultar tentador intentar llevar a cabo investigaciones de la nube en las instalaciones donde se encuentran las herramientas existentes. Según nuestra experiencia, los clientes de AWS que responden a los incidentes mediante tecnologías en la nube logran mejores resultados: los aislamientos se pueden automatizar, se pueden hacer copias más fácilmente, las pruebas están listas para su análisis en menos tiempo y el análisis se puede completar más rápido.

La práctica recomendada es realizar las investigaciones y los análisis forenses en la nube, donde están los datos, en lugar de intentar transferirlos a un centro de datos antes de investigar. Puede usar las capacidades de computación y de almacenamiento seguras de la nube en prácticamente cualquier parte del mundo para realizar operaciones de respuesta seguras. Muchos clientes optan por preconfigurar una cuenta de AWS independiente que esté lista para realizar una investigación, aunque puede haber casos en los que elija realizar el análisis en la misma cuenta de AWS. Si se espera que su organización conserve los registros por motivos legales y de cumplimiento, puede

ser prudente mantener cuentas separadas para las actividades legales y el almacenamiento a largo plazo.

También se recomienda llevar a cabo la investigación en la misma región de AWS en la que se produjo el evento, en lugar de replicar los datos en otra región. La recomendación de esta práctica se debe principalmente al tiempo adicional que se requiere para transferir los datos entre las regiones. En cada región de AWS en la que opere, asegúrese de que tanto el proceso de respuesta ante incidentes como el personal de respuesta cumplan con las leyes de privacidad de datos relevantes. Si necesita trasladar datos entre las regiones, tenga en cuenta las implicaciones legales de mover datos entre jurisdicciones. En general, la práctica recomendada es mantener los datos dentro de la misma jurisdicción nacional.

Si considera que un evento de seguridad afecta a sus sistemas de seguridad, identidad o comunicación, es posible que deba buscar formas de acceso y mecanismos alternativos para investigar y corregir el impacto. AWS ofrece la posibilidad de lanzar rápidamente infraestructura nueva que se puede utilizar para entornos de trabajo alternativos y seguros. Por ejemplo, mientras investiga la posible gravedad de la situación, puede que quiera crear una cuenta de AWS nueva con las herramientas seguras que necesitan su asesor legal, el departamento de relaciones públicas y los equipos de seguridad para comunicarse y seguir trabajando. Servicios como AWS WorkSpaces (para escritorios virtuales), AWS WorkMail (para correo electrónico) y Amazon Chime (para la comunicación) pueden proporcionar a sus equipos de respuesta, a la dirección y a otros participantes las capacidades y la conectividad que necesitan para comunicarse, investigar y corregir un problema.

Aislamiento de recursos

Durante el curso de la investigación, es posible que tenga que aislar recursos como parte de la respuesta ante una anomalía de seguridad. El aislamiento se aplica para limitar el impacto potencial, evitar una mayor propagación de los recursos afectados, limitar la exposición involuntaria de los datos y prevenir otros accesos no autorizados.

Al igual que con cualquier otra respuesta, pueden aplicarse consideraciones empresariales, normativas, legales o de otro tipo. Asegúrese de sopesar las acciones previstas con respecto a las consecuencias esperadas e inesperadas. Si los equipos de la nube usan etiquetas de recursos, estas pueden ayudar a identificar la importancia del recurso o el propietario con el que hay que ponerse en contacto.

Lanzamiento de estaciones de trabajo forenses

Algunas de las actividades de respuesta ante incidentes pueden incluir el análisis de imágenes de disco, sistemas de archivos, volcados de RAM u otros artefactos implicados en un incidente. Muchos de los clientes crean una estación de trabajo forense personalizada que pueden usar para montar copias de cualquier volumen de datos afectado (conocidas como instantáneas de EBS). Para hacerlo, siga estos pasos básicos:

1. Elija una imagen de máquina de Amazon (AMI) básica (como Linux o Microsoft Windows) que se pueda usar como estación de trabajo forense.
2. Lance una instancia de Amazon EC2 desde esa AMI básica.
3. Refuerce el sistema operativo, elimine los paquetes de software innecesarios y configure mecanismos de auditoría y registro relevantes.
4. Instale su conjunto preferido de kits de herramientas privadas o de código abierto, así como el software y los paquetes que necesite de cualquier proveedor.
5. Detenga la instancia de Amazon EC2 y cree una AMI desde la instancia detenida.
6. Cree un proceso semanal o mensual para actualizar y recompilar la AMI con las últimas revisiones de software.

Una vez que el sistema forense se haya aprovisionado con una AMI, el equipo de respuesta ante incidentes puede usar esta plantilla para crear una AMI nueva y lanzar una nueva estación de trabajo forense para cada investigación. El proceso de lanzamiento de la AMI como instancia de Amazon EC2 puede preconfigurarse para simplificar el proceso de implementación. Por ejemplo, puede crear una plantilla de los recursos de infraestructura forense que necesita en un archivo de texto e implementarla en la cuenta de AWS mediante AWS CloudFormation.

Cuando los recursos están disponibles para implementarlos de forma rápida a partir de una plantilla, los expertos forenses con la formación adecuada pueden usar nuevas estaciones de trabajo forenses para cada investigación, en lugar de reutilizar la infraestructura. Este proceso le permite asegurarse de que no haya contaminación cruzada con otros exámenes forenses.

Tipos de instancias y ubicaciones

Amazon EC2 ofrece una amplia variedad de tipos de instancias optimizadas para diferentes casos de uso. Los tipos de instancia abarcan varias combinaciones de capacidad de CPU, memoria, almacenamiento y redes; además, ofrecen la flexibilidad necesaria para elegir la combinación de

recursos adecuada para sus aplicaciones. Muchos tipos de instancias incluyen varios tamaños, lo que le permite escalar los recursos según los requisitos de la carga de trabajo objetivo. Para las instancias de respuesta ante incidentes, siga las políticas de GRC de la empresa para la ubicación y la segmentación desde la red que ejecuta las instancias de producción.

Las redes mejoradas de AWS utilizan la virtualización de E/S de raíz única (SR-IOV) para ofrecer capacidades de redes de alto rendimiento en los tipos de instancias admitidos. SR-IOV es un método de virtualización de dispositivos que ofrece un mayor rendimiento de E/S y una menor utilización de CPU en comparación con las interfaces de red virtualizadas tradicionales. Las redes mejoradas proporcionan un mayor ancho de banda, un rendimiento superior de paquetes por segundo (PPS) y menores latencias entre instancias de manera constante. El uso de las redes mejoradas no supone ningún cargo adicional. Para obtener información sobre qué tipos de instancias admiten velocidades de red de 10 o 25 Gbps y otras funciones avanzadas, consulte Tipos de instancias de Amazon EC2.

Soporte para proveedores en la nube

Temas

- AWS Managed Services
- AWS Support
- Soporte para la respuesta a DDoS

AWS Managed Services

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

Como operador de infraestructura, AMS asume la responsabilidad de implementar un conjunto de controles de detección de seguridad y proporciona una primera línea de respuesta ante alertas, las 24 horas del día y los 7 días de la semana, con un modelo de ajuste a las zonas horarias. Cuando se desencadena una alerta, AMS sigue un conjunto estándar de runbooks automatizados y manuales para garantizar una respuesta coherente. Estos runbooks se comparten con los clientes de AMS durante su incorporación para que puedan desarrollar y coordinar la respuesta con AMS. AMS

fomenta la ejecución conjunta de simulaciones de respuestas de seguridad con los clientes para desarrollar la capacidad operativa antes de que se produzca un incidente real.

AWS Support

AWS Support ofrece una serie de planes que proporcionan acceso a herramientas y conocimientos que contribuyen al éxito y a la eficiencia operativa de sus soluciones de AWS. Todos los planes de soporte proporcionan acceso ininterrumpido al servicio de atención al cliente, documentación de AWS, documentos técnicos y foros de ayuda. Si necesita soporte técnico y recursos adicionales que le ayuden a planificar, implementar y optimizar su entorno de AWS, puede seleccionar un plan de soporte técnico acorde con su caso de uso de AWS.

Debe considerar el Centro de asistencia de la Consola de administración de AWS como el punto de contacto central para obtener asistencia en relación con los problemas que afecten a sus recursos de AWS. IAM controla el acceso a AWS Support. Para obtener más información sobre cómo acceder a las características de soporte de AWS, consulte cómo acceder a Support.

Además, si necesita informar sobre un abuso de Amazon EC2, póngase en contacto con el equipo de respuesta frente a abusos de AWS.

Soporte para la respuesta a DDoS

Un ataque de denegación de servicio (DoS) provoca que el sitio web o la aplicación no estén disponibles para los usuarios finales. Los atacantes usan diversas técnicas que consumen ancho de banda de la red u otros recursos, lo que interrumpe el acceso de los usuarios finales legítimos. En su forma más sencilla, un atacante aislado lanza un ataque DoS contra un objetivo desde un solo origen.

En un ataque de denegación de servicio distribuido (DDoS), el atacante usa varios orígenes, que pueden verse comprometidos o estar controlados por un grupo de colaboradores, para orquestar un ataque contra un objetivo. En un ataque de DDoS, todos los colaboradores o hosts vulnerables participan en el ataque, lo que genera una avalancha de paquetes o solicitudes para desbordar al objetivo previsto.

AWS ofrece a los clientes AWS Shield, que proporciona un servicio administrado de protección contra ataques de denegación de servicio distribuido (DDoS) para proteger a las aplicaciones web que se ejecutan en AWS. AWS Shield proporciona una mitigación en línea automática y detección siempre activa que minimizan el tiempo de inactividad y la latencia de las aplicaciones, por lo que no

es necesario recurrir a AWS Support para beneficiarse de la protección frente a DDoS. Existen dos niveles de AWS Shield: Standard y Advanced.

Todos los clientes de AWS se benefician de la protección automática gratuita de AWS Shield Standard. AWS Shield Standard protege frente a los ataques DDoS más comunes y frecuentes que se suelen producir en la capa de red y transporte dirigidos contra su sitio web o sus aplicaciones. Cuando utiliza AWS Shield Standard con Amazon CloudFront y Amazon Route 53, recibe una protección de disponibilidad integral frente a todos los ataques conocidos a la infraestructura (capas 3 y 4).

Si quiere obtener un nivel de protección superior contra ataques dirigidos a sus aplicaciones web ejecutadas en recursos de Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (ELB), Amazon CloudFront y Amazon Route 53, puede suscribirse a AWS Shield Advanced. Además, AWS Shield Advanced proporciona acceso ininterrumpido al equipo de respuesta a DDoS (DRT) de AWS. Para obtener más información sobre AWS Shield Standard y AWS Shield Advanced, consulte AWS Shield.

Simulación

Temas

Simulaciones de respuesta ante incidentes de seguridad

Las simulaciones de respuesta ante incidentes de seguridad (SIRS) son eventos internos que ofrecen una oportunidad estructurada para practicar el plan y los procedimientos de respuesta ante incidentes en un escenario realista. Los eventos SIRS consisten fundamentalmente en estar preparados y mejorar iterativamente las capacidades de respuesta. A continuación, se indican algunas de las razones por las que los clientes consideran interesante realizar actividades de SIRS:

- Validación de la preparación
- Desarrollo de la confianza gracias al aprendizaje obtenido de las simulaciones y la formación del personal
- Observación de las obligaciones de cumplimiento o contractuales
- Generación de artefactos para la acreditación
- Desarrollo de agilidad y mejora progresiva con enfoque
- Mejora de la velocidad y las herramientas
- Perfeccionamiento de la comunicación y la elevación a instancias superiores
- Capacidad de adaptarse a situaciones raras e inesperadas

Por estos motivos, el valor derivado de participar en una actividad de SIRS aumenta la efectividad de una organización durante eventos estresantes. El desarrollo de una actividad de SIRS que sea realista y beneficiosa puede ser un ejercicio difícil. Si bien probar los procedimientos o automatizar eventos conocidos tiene ciertas ventajas, es igualmente valioso participar en actividades de SIRS creativas para ponerse a prueba frente a situaciones inesperadas.

Pasos de la simulación

Independientemente de que diseñe sus propias SIRS o de que tenga un socio de confianza que le proporcione el trabajo preliminar, las simulaciones generalmente siguen estos pasos:

1. Encontrar un problema importante: defina el desencadenador que debe provocar una respuesta.
2. Identificar ingenieros de seguridad cualificados: una simulación requiere un creador y un comprobador.
3. Crear un sistema de modelo realista: la simulación debe ser realista y adecuada. Si no es realista, es posible que los participantes no valoren el ejercicio. Si es demasiado simple, el ejercicio puede considerarse trivial. Comience con ejercicios sencillos y avance hacia un evento completo.
4. Crear y probar los elementos del escenario: puede que sea necesario crear material de simulación relevante, como artefactos de registro, notificaciones y alertas por correo electrónico, así como posibles runbooks.
5. Invitar a otras personas del equipo de seguridad y a participantes de otras organizaciones: invite a todos los usuarios que necesiten formarse y participar. Si su asesor legal, los ejecutivos y el personal de relaciones públicas participan en la simulación, también debe invitarlos.
6. Ejecutar la simulación: elija si el personal debe esperar el evento de SIRS o si la simulación debe realizarse sin previo aviso.
7. Celebrar, medir, mejorar y repetir: la simulación tiene factores de estrés, por lo que es importante alentar a los participantes y celebrar sus esfuerzos. Después del estímulo, se presenta la oportunidad de medir, mejorar e iterar para la próxima simulación. AWS recomienda que estas actividades se conviertan en un hábito.

> **Important**
>
> Si está planeando una simulación de respuesta ante incidentes de seguridad (SIRS), consulte Pruebas de penetración y revise la sección Otros eventos simulados para obtener la información más reciente sobre cómo actuar.

Ejemplos de simulación

Las simulaciones de seguridad deben ser realistas para proporcionar el valor esperado. Cuando usted o sus socios trabajen para crear sus propias simulaciones, tenga siempre en cuenta los

eventos pasados reales como una fuente valiosa para posibles ejercicios de simulación. A continuación, se muestran algunos ejemplos que los clientes de AWS han considerado útiles para sus simulaciones iniciales:

- Cambios no autorizados en los recursos o la configuración de la red
- Credenciales expuestas públicamente por error debido a una configuración incorrecta del desarrollador
- Contenido confidencial accesible públicamente por error debido a una configuración incorrecta del desarrollador
- Aislamiento de un servidor web que se comunica con direcciones IP sospechosas de ser malintencionadas

Además de un valioso aprendizaje práctico, la realización de actividades de SIRS aporta otros resultados, como el aprendizaje de lecciones que se pueden usar como aportaciones en el proceso siguiente de su programa: la iteración.

Iteración

En la sección anterior, se definieron algunas de las ventajas de las actividades de SIRS. Entre ellas se mencionaba adquirir agilidad a través de mejoras progresivas. Las simulaciones deben generar resultados valiosos que pueda aprovechar para mejorar su respuesta de seguridad. Proporcionan un bucle de retroalimentación a la organización sobre lo que funciona y lo que no. Estos conocimientos pueden ayudarle a crear procedimientos de forma progresiva o a actualizar los ya existentes para mejorar su respuesta.

Temas

Runbooks

Cuando se detecta una anomalía de seguridad, retener el evento y volver a un estado correcto conocido son elementos importantes de un plan de respuesta. Por ejemplo, si la anomalía se debe a una configuración de seguridad incorrecta, la solución puede ser tan simple como eliminar la desviación a través de una reimplementación de los recursos con la configuración adecuada. Para ello, tendrá que planificar con antelación y definir sus propios procedimientos de respuesta de seguridad, que a menudo se denominan runbooks.

Un runbook es la forma documentada de los procedimientos de una organización para realizar una tarea o una serie de tareas. Esta documentación suele almacenarse en un sistema digital interno o en formato impreso. Puede que ya tenga runbooks de respuesta ante incidentes o que deba crearlos para cumplir con un marco de garantía de seguridad. Sin embargo, cuando se siguen de forma manual los runbooks escritos, aumenta la posibilidad de cometer errores. En su lugar, se recomienda automatizar todas las tareas repetibles. Gracias a la automatización, su equipo de respuesta se libera de las tareas habituales y queda disponible para tareas más importantes, como correlacionar eventos, practicar en simulaciones, diseñar nuevos procedimientos de respuesta, realizar investigaciones, desarrollar nuevas competencias y probar o crear nuevas herramientas. Sin embargo, antes de poder descomponer las tareas en lógica programable e iterar hacia una automatización adecuada, debe comenzar por escribir un runbook.

Creación de runbooks

Si quiere crear runbooks para la nube, se recomienda que primero se centre en las alertas que genera actualmente. Si se genera una alerta, es importante investigarla. Comience por definir las descripciones de los procesos manuales que realiza. Después, pruebe los procesos e itere el patrón del runbook para mejorar la lógica básica de la respuesta. Determine cuáles son las excepciones y las resoluciones alternativas para esos escenarios. Por ejemplo, en un entorno de desarrollo, puede que quiera terminar una instancia de Amazon EC2 mal configurada. Sin embargo, si el mismo evento se produce en un entorno de producción, en lugar de terminar la instancia, puede detenerla y verificar con las partes interesadas que no se pierdan datos críticos y si la terminación es aceptable.

Después de determinar cuál es la mejor solución, puede descomponer la lógica en una solución basada en código que el personal de respuesta pueden usar como herramienta para automatizar la respuesta y para eliminar las discrepancias o suposiciones. Esto acelera el ciclo de vida de una respuesta. El objetivo siguiente es hacer que este código esté completamente automatizado cuando las alertas o los eventos lo invoquen, en lugar de que el personal de respuesta lo ejecute.

Introducción

Si no está seguro de por dónde empezar, considere comenzar con las alertas que podrían generar AWS Trusted Advisor, el Estándar de prácticas de seguridad básicas recomendadas de AWS Security Hub y Reglas de AWS Config (incluido el repositorio de GitHub de Reglas de AWS Config). Después, céntrese en los eventos generados por los servicios que describen los sistemas que le interesan.

Amazon GuardDuty y Access Analyzer describen muchos de los dominios que una aplicación usará en AWS, motivo por el que se suelen sugerir; sin embargo, Amazon Inspector y Amazon Macie ofrecen usos específicos para aquellos que están preocupados por los datos y los puntos de acceso. En la Guía del usuario de Amazon GuardDuty tiene disponible información sobre los resultados de Amazon GuardDuty. Los resultados de Access Analyzer están disponibles en la Guía del usuario de Amazon Access Analyzer. Los resultados de Macie están disponibles en la Guía del usuario de Amazon Macie. Los resultados de Amazon Inspector están disponibles en la Guía del usuario de Amazon Inspector. Security Hub ofrece la posibilidad de unificar esos resultados en un solo lugar y reaccionar ante ellos de forma unificada con baja latencia, por lo que se sugiere como ubicación central para la corrección.

Todos los servicios anteriores envían notificaciones a través de Amazon CloudWatch Events cuando se produce cualquier cambio en los resultados o las alertas, incluidas las alertas generadas recientemente y las actualizaciones de las alertas existentes. Puede configurar las reglas de

Amazon CloudWatch Events para desencadenar las funciones AWS Lambda para que lleven a cabo una respuesta basada en eventos. Sin embargo, la capacidad de crear información personalizada y de añadir sus propios resultados desde el dominio de la aplicación se suma a las razones de peso para usar Security Hub en su lugar. Para obtener más información, consulte la sección Respuesta basada en eventos.

Automatización

La automatización es un multiplicador de fuerza, es decir, impulsa los esfuerzos del personal de respuesta para que se ajuste a la velocidad de la organización. Pasar de los procesos manuales a procesos automatizados permite dedicar más tiempo a aumentar la seguridad del entorno de la nube de AWS.

Temas

- Automatización de la respuesta ante incidentes
- Respuesta basada en eventos

Automatización de la respuesta ante incidentes

Para automatizar las funciones de ingeniería y operaciones de seguridad, puede usar un conjunto completo de API y herramientas de AWS. Puede automatizar por completo las capacidades de administración de identidades, seguridad de la red, protección de datos y supervisión. Al automatizar la seguridad, el sistema puede monitorear, revisar e iniciar una respuesta, en lugar de hacer que el personal monitoree la posición de seguridad y reaccione de forma manual a los eventos.

Si los equipos de respuesta ante incidentes siguen respondiendo a las alertas de la misma manera, corren el riesgo de sufrir fatiga por alertas. Con el tiempo, el equipo puede volverse insensible a las alertas y cometer errores al gestionar situaciones habituales o pasar por alto alertas inusuales. La automatización ayuda a evitar la fatiga respecto a las alertas mediante el uso de funciones que procesan las alertas repetitivas y habituales, lo que deja que las personas gestionen los incidentes delicados y puntuales.

Para mejorar los procesos manuales, automatice mediante programación los pasos del proceso. Después de definir el patrón de resolución de un evento, puede descomponer ese patrón en lógica procesable y escribir el código para ejecutar la lógica. El personal de respuesta puede ejecutar ese código para solucionar el problema. Con el tiempo, puede automatizar cada vez más pasos y, en última instancia, gestionar de forma automática clases enteras de incidentes habituales.

Sin embargo, el objetivo debe ser reducir aún más el intervalo de tiempo entre los mecanismos de detección y los mecanismos de respuesta. Históricamente, este intervalo de tiempo puede ser de horas, días o incluso meses. En una encuesta sobre respuesta ante incidentes realizada por SANS en 2016, el 21 % de los encuestados declaró que su tiempo hasta la detección oscilaba entre dos y siete días y solo el 29 % de los encuestados pudo corregir los eventos dentro del mismo marco temporal. En la nube, puede reducir ese intervalo de tiempo de respuesta a segundos mediante la creación de capacidades de respuesta basadas en eventos.

Temas

Opciones de automatización de la respuesta

Es importante asegurarse de equilibrar la implementación empresarial y la estructura organizativa. En la figura 4 se ilustran las diferencias entre los atributos técnicos de cada opción de respuesta automatizada en su implementación de AWS con un gráfico radial. En el gráfico, cuanto más lejos esté el atributo técnico del centro del gráfico, mayor será la fuerza de dicho atributo para la respuesta de automatización correspondiente. Por ejemplo, AWS Lambda ofrece la mayor velocidad y requiere menos habilidades técnicas. AWS Fargate ofrece más flexibilidad y requiere menos habilidades técnicas y mantenimiento. En la tabla 1 se ofrece información general de estas opciones de automatización y un resumen de los atributos técnicos de cada una.

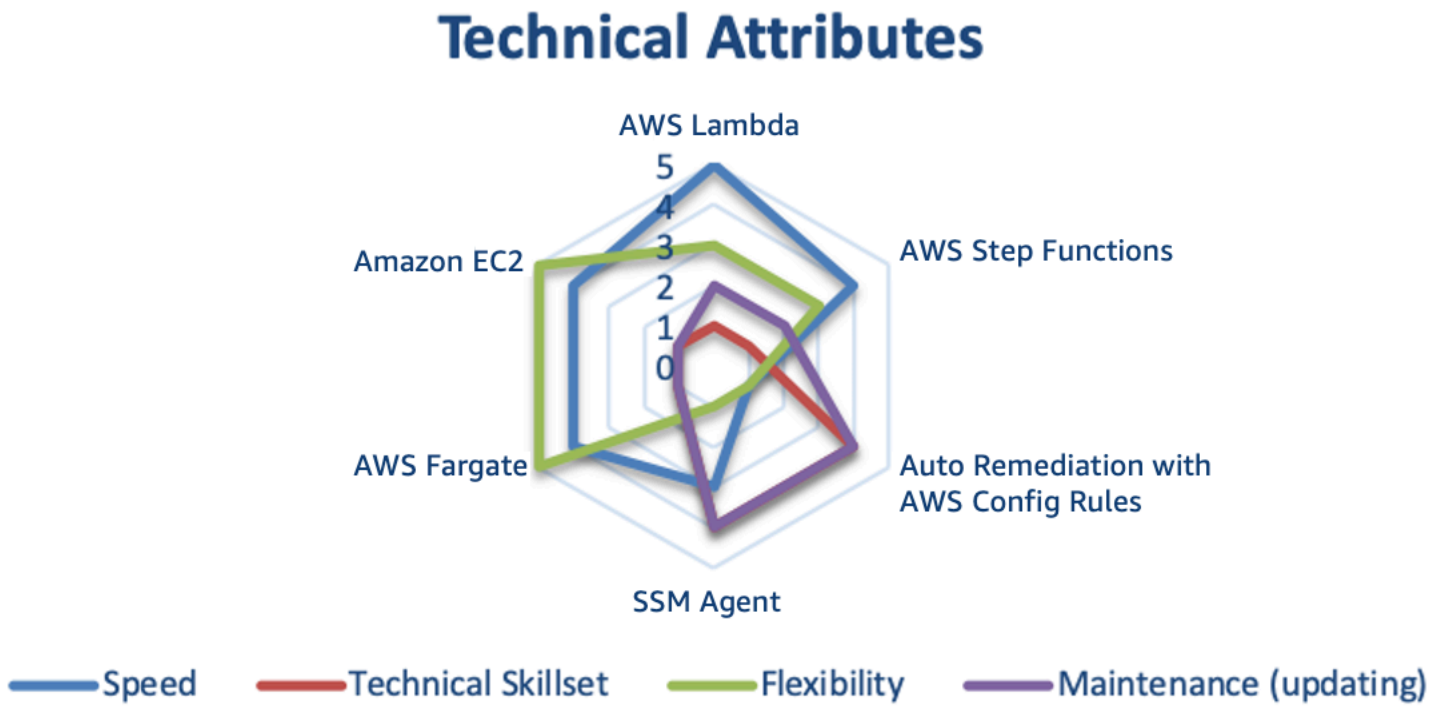

Figura 4: Diferencias entre los atributos técnicos de los enfoques de respuesta automatizada

Tabla 1: Opciones para la respuesta automatizada

Servicio o característica de AWS	Descripción	Resumen de atributos*
AWS Lambda	Sistema que solo usa AWS Lambda, con el lenguaje empresarial de su organización.	Velocidad Flexibilidad Mantenimiento Habilidades
AWS Step Functions	Sistema que usa AWS Step Functions, Lambda y SSM Agent.	Velocidad Flexibilidad Mantenimiento Habilidades

Servicio o característica de AWS	Descripción	Resumen de atributos*
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.	Mantenimiento y habilidades Velocidad y flexibilidad
SSM Agent	Conjunto de reglas y documentos de automatización que revisan muchas partes de los entornos y los sistemas internos y realizan correcciones.	Mantenimiento y habilidades Velocidad Flexibilidad
AWS Fargate	Sistema de AWS Fargate que usa código de función escalonada de código abierto y los eventos de Amazon CloudWatch, así como otros sistemas, para impulsar la detección y la corrección.	Flexibilidad Velocidad Mantenimiento y habilidades
Amazon EC2	Sistema que se ejecuta en una instancia completa, similar a la opción de AWS Fargate.	Flexibilidad Velocidad Mantenimiento Habilidades

* Los atributos se enumeran en orden descendente para cada servicio o característica. Por ejemplo, AWS Lambda ofrece la mayor velocidad y requiere menos habilidades técnicas. AWS Fargate ofrece más flexibilidad y requiere menos habilidades técnicas y mantenimiento.

Al considerar estas opciones de automatización en el entorno de AWS, también debe tener en cuenta la centralización y el periodo de análisis (eventos por segundo [EPS]).

La centralización hace referencia a una cuenta central que controla todas las actividades de detección y corrección de una organización. Este enfoque parece la mejor opción disponible y es la práctica recomendada actualmente. Sin embargo, en algunas circunstancias es necesario desviarse de este enfoque; comprender cuándo depende de la forma en que gestione sus cuentas subordinadas. Se recomienda empezar por aprovechar el enfoque de la cuenta de herramientas de seguridad en el marco de varias cuentas de AWS Organizations o AWS Control Tower.

Tabla 2: Ventajas y desventajas de la centralización

	Centralización	Descentralización
Ventajas	Administración de configuración sencilla No se puede cancelar ni modificar la respuesta	Arquitectura sencilla Configuración inicial más rápida
Desventajas	Mayor complejidad de la arquitectura Incorporación y desvinculación de cuentas y recursos	Más recursos para administrar Dificultad para mantener una referencia de software

Una comparación de costes de estas implementaciones también puede contribuir a su decisión empresarial a la hora de determinar la mejor opción. La métrica de eventos por segundo (EPS) se utiliza para realizar la mejor estimación de los costes. En última instancia, puede resultar mucho más fácil y más barato aplicar enfoques centralizados o descentralizados, pero nos resulta imposible analizar cómo evaluará ese coste específicamente en su cuenta. Asegúrese de tener en cuenta el valor de EPS al enviar esos eventos a una cuenta central para obtener una respuesta. Cuanto mayor sea el valor de EPS, mayor será el coste de enviar esos eventos a una cuenta centralizada.

Comparaciones de costes en métodos de análisis

Los costes también vienen determinados por el método de análisis mediante el que se detecta una anomalía y el plazo entre validaciones. Para los métodos de análisis, puede elegir entre una revisión

basada en eventos o periódica. En la tabla 3 se muestran las ventajas y las desventajas de ambos enfoques.

Tabla 3: Ventajas y desventajas de los distintos métodos de análisis

	Basado en eventos	Análisis periódico
Ventajas	Menos tiempo desde el evento hasta la respuesta Necesidad limitada de consultar llamadas a la API adicionales	Imagen completa en un punto concreto del tiempo
Desventajas	Contexto de estado limitado en torno al recurso Los eventos desencadenados pueden ser para un recurso no disponible	Cuotas de servicio en cuentas grandes Existe la posibilidad de limitación controlada debido al alto volumen de llamadas a la API

En muchos casos, una combinación de ambos enfoques de análisis es probablemente la mejor opción en una organización con plena madurez. AWS Security Hub CSPM y el Estándar de prácticas de seguridad básicas recomendadas de AWS proporcionan una combinación de ambos métodos de análisis.

En la figura 5 se proporciona un gráfico radial que ilustra la comparación de costes de los eventos por segundo (EPS) para cada uno de los enfoques de automatización. Por ejemplo, Amazon EC2 y AWS Fargate tienen los costes más elevados para ejecutar de 0 a 10 EPS, mientras que AWS Lambda y AWS Step Functions tienen los costes más altos para ejecutar más de 76 EPS.

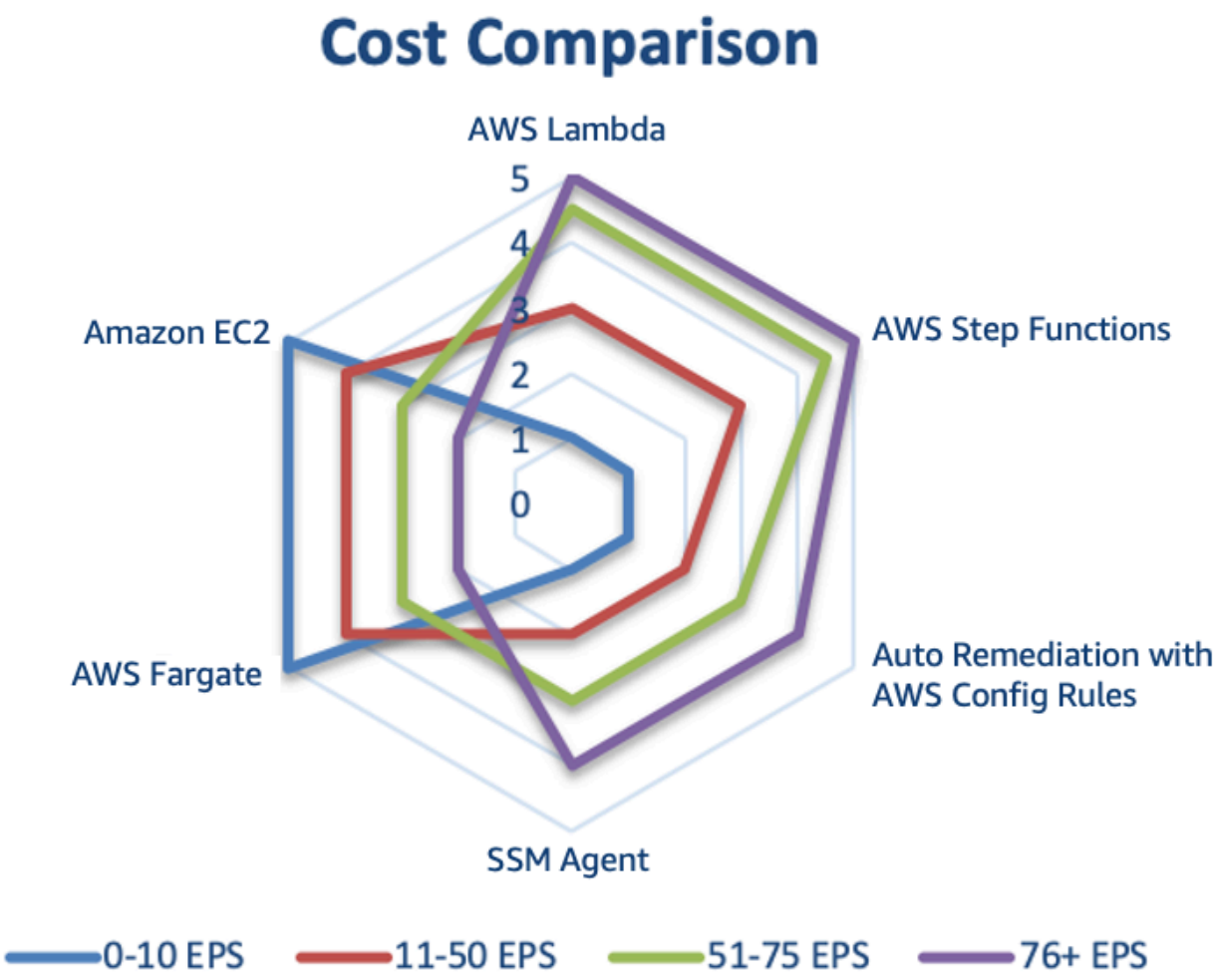

Figura 5: Comparación de costes de los métodos de análisis de las opciones de automatización (eventos por segundo [EPS])

Respuesta basada en eventos

Con un sistema de respuesta basada en eventos, un mecanismo de detección desencadena un mecanismo de respuesta para corregir el evento de forma automática. Puede usar las capacidades de respuesta basada en eventos para reducir el tiempo hasta la obtención de valor entre los mecanismos de detección y los mecanismos de respuesta. Para crear esta arquitectura basada en eventos, puede usar AWS Lambda, que es un servicio de computación sin servidor que ejecuta su código como respuesta a eventos y administra automáticamente los recursos de computación subyacentes.

Por ejemplo, supongamos que tiene una cuenta de AWS con el servicio AWS CloudTrail habilitado. Si AWS CloudTrail se deshabilita alguna vez (mediante la API `cloudtrail:StopLogging`), el

procedimiento de respuesta consiste en volver a habilitar el servicio e investigar al usuario que ha deshabilitado el registro de AWS CloudTrail. En lugar de realizar estos pasos de forma manual en la Consola de administración de AWS, puede volver a habilitar el registro mediante programación (a través de la API `cloudtrail:StartLogging`). Si se implementa con código, el objetivo de la respuesta es llevar a cabo esta tarea lo más rápido posible y notificar al personal de respuesta que esta se ha efectuado.

Puede descomponer la lógica en código simple para ejecutarlo en una función AWS Lambda a fin de realizar estas tareas. Después, puede usar Amazon CloudWatch Events para monitorear el evento `cloudtrail:StopLogging` específico e invocar la función si se produce. Cuando Amazon CloudWatch Events invoca esta función AWS Lambda de respuesta, puede pasarle los detalles del evento específico con la información de la entidad principal que deshabilitó AWS CloudTrail, cuándo se deshabilitó, el recurso específico afectado y otra información relevante. Puede usar esta información para complementar los resultados de los registros y, después, generar una notificación o una alerta solo con los valores específicos que un analista de respuesta requeriría.

El objetivo ideal de la respuesta basada en eventos es que la función Lambda de respuesta realice las tareas de respuesta y, después, notifique al personal de respuesta que la anomalía se ha resuelto correctamente, junto con cualquier información contextual pertinente. Corresponde entonces al personal de respuesta decidir cómo determinar por qué ha ocurrido y cómo podrían prevenirse reincidencias futuras. Este bucle de retroalimentación mejora aún más la seguridad en los entornos de nube. Para lograr este objetivo, debe tener una cultura que permita a su equipo de seguridad trabajar más estrechamente con los equipos de desarrollo y operaciones.

Ejemplos de respuesta ante incidentes

Temas

Incidentes del dominio de servicios

Por lo general, los incidentes del dominio de servicios se gestionan exclusivamente a través de las API de AWS.

Identidades

AWS proporciona API a nuestros servicios en la nube que utilizan millones de clientes para crear aplicaciones e impulsar los resultados empresariales. Estas API pueden invocarse a través de muchos métodos, como los kits de desarrollo de software (SDK), la CLI de AWS y la Consola de administración de AWS. Para interactuar con AWS a través de estos métodos, el servicio de IAM ayuda a controlar el acceso a los recursos de AWS de forma segura. Puede usar IAM para controlar quién está autenticado (tiene una sesión iniciada) y autorizado (tiene permisos) para usar recursos en el nivel de cuenta. Para obtener una lista de los servicios de AWS que puede usar con IAM, consulte Servicios de AWS que funcionan con IAM.

Cuando crea una cuenta de AWS por primera vez, comienza por una identidad de inicio de sesión único (SSO) 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 obtiene acceso a ella mediante el inicio de sesión con la dirección de correo electrónico y la contraseña que utilizó para crear la cuenta. Se recomienda encarecidamente no utilizar el usuario raíz en las tareas cotidianas y, en particular, para las tareas administrativas. En lugar de ello, siga la práctica recomendada, que consiste en utilizar el usuario raíz solo para crear el primer usuario de IAM, almacenar de forma segura las credenciales de usuario raíz y utilizarlas para realizar solo unas pocas tareas de administración de servicios y cuentas. Para obtener más información, consulte Crear usuarios de IAM individuales.

Si bien estas API proporcionan valor a millones de clientes, algunos de ellos pueden sufrir un abuso si las personas equivocadas obtienen acceso a su cuenta de IAM o a sus credenciales de usuario raíz. Por ejemplo, puede usar las API para habilitar el registro en su cuenta, como

AWS CloudTrail. Sin embargo, si los atacantes obtienen sus credenciales, también pueden usar la API para desactivar estos registros. Para evitar este tipo de abuso, configure los permisos de IAM apropiados que sigan un modelo de privilegios mínimos y proteja de forma adecuada sus credenciales de IAM. Para obtener más información, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de AWS Identity and Access Management. Si se produce este tipo de evento, hay varios controles de detección para identificar que el registro de AWS CloudTrail se ha deshabilitado, incluidos AWS CloudTrail, AWS Config, AWS Trusted Advisor, Amazon GuardDuty y AWS CloudWatch Events.

Recursos

Otras características de las que se puede abusar o que se pueden configurar de forma incorrecta varían de una organización a otra, según la forma en que cada cliente opere en la nube. Por ejemplo, algunas organizaciones tienen la intención de poner ciertos datos o aplicaciones a disposición del público, mientras que otras mantienen sus aplicaciones y datos con carácter interno y confidencial. No todos los eventos de seguridad son malintencionados por naturaleza; algunos pueden ser el resultado de configuraciones involuntarias o incorrectas. Determine las API o las características que tienen un gran impacto en su organización y si las usa con mucha o poca frecuencia.

Puede identificar muchas configuraciones incorrectas de seguridad con el uso de herramientas y servicios. Por ejemplo, AWS Trusted Advisor proporciona una serie de comprobaciones de las prácticas recomendadas. Los socios de AWS también ofrecen cientos de productos líderes del sector que son equivalentes o idénticos a los controles existentes en sus entornos locales o bien se integran en ellos. El programa de competencias de socios de AWS ha preseleccionado varios de estos productos y soluciones. Se recomienda visitar la sección Análisis de puntos vulnerables y configuraciones del programa de socios con competencia en seguridad de AWS para examinar estas soluciones y determinar si pueden satisfacer sus requisitos.

Incidentes del dominio de infraestructura

El dominio de infraestructura suele incluir los datos de la aplicación o la actividad relacionada con la red, como el tráfico hacia las instancias de Amazon EC2 dentro de la VPC y los procesos que se ejecutan en los sistemas operativos de las instancias de Amazon EC2.

Por ejemplo, supongamos que su solución de supervisión le ha notificado una posible anomalía de seguridad en la instancia de Amazon EC2. Estos son algunos pasos habituales para abordar esta situación:

1. Capture los metadatos de la instancia de Amazon EC2 antes de realizar cambios en su entorno.
2. Proteja la instancia de Amazon EC2 de la terminación accidental; para ello, habilite la protección de terminación para la instancia.
3. Aísle la instancia de Amazon EC2 mediante el cambio del grupo de seguridad de la VPC. Sin embargo, tenga en cuenta el seguimiento de la conexión de VPC y otras técnicas de contención.
4. Desconecte la instancia de Amazon EC2 de cualquier grupo de AWS Auto Scaling.
5. Anule el registro de la instancia de Amazon EC2 de cualquier servicio de Elastic Load Balancing relacionado.
6. Realice una instantánea de los volúmenes de datos de Amazon EBS asociados a la instancia de EC2 para su protección y para realizar investigaciones de seguimiento.
7. Etiquete la instancia de Amazon EC2 para indicar que se encuentra en cuarentena para la investigación y añada cualquier metadato pertinente, como el ticket de incidencia asociado a la investigación.

Puede realizar todos los pasos anteriores con las API de AWS, los SDK de AWS, AWS CLI y la Consola de administración de AWS. Para interactuar con AWS mediante estos métodos, el servicio de IAM ayuda a controlar el acceso a los recursos de AWS de forma segura. Use IAM para controlar quién está autenticado y autorizado para utilizar recursos en el nivel de cuenta. El servicio IAM proporciona la autenticación y la autorización necesarias para que pueda realizar estas acciones e interactuar con el dominio de servicio.

Una instantánea de un volumen de Amazon EBS es una copia puntual en el nivel de bloque de un volumen de datos de EBS, que se realiza de forma asíncrona y puede tardar un tiempo en completarse, pero indica la diferencia con respecto a esos datos en el futuro. Puede crear nuevos volúmenes de EBS a partir de estas copias y montarlos en la instancia de EC2 forense para que los investigadores correspondientes la analicen en profundidad sin conexión. El diagrama siguiente muestra una versión simplificada del resultado y no describe todos los componentes de la red (como las subredes, las tablas de enrutamiento y las listas de control de acceso a la red).

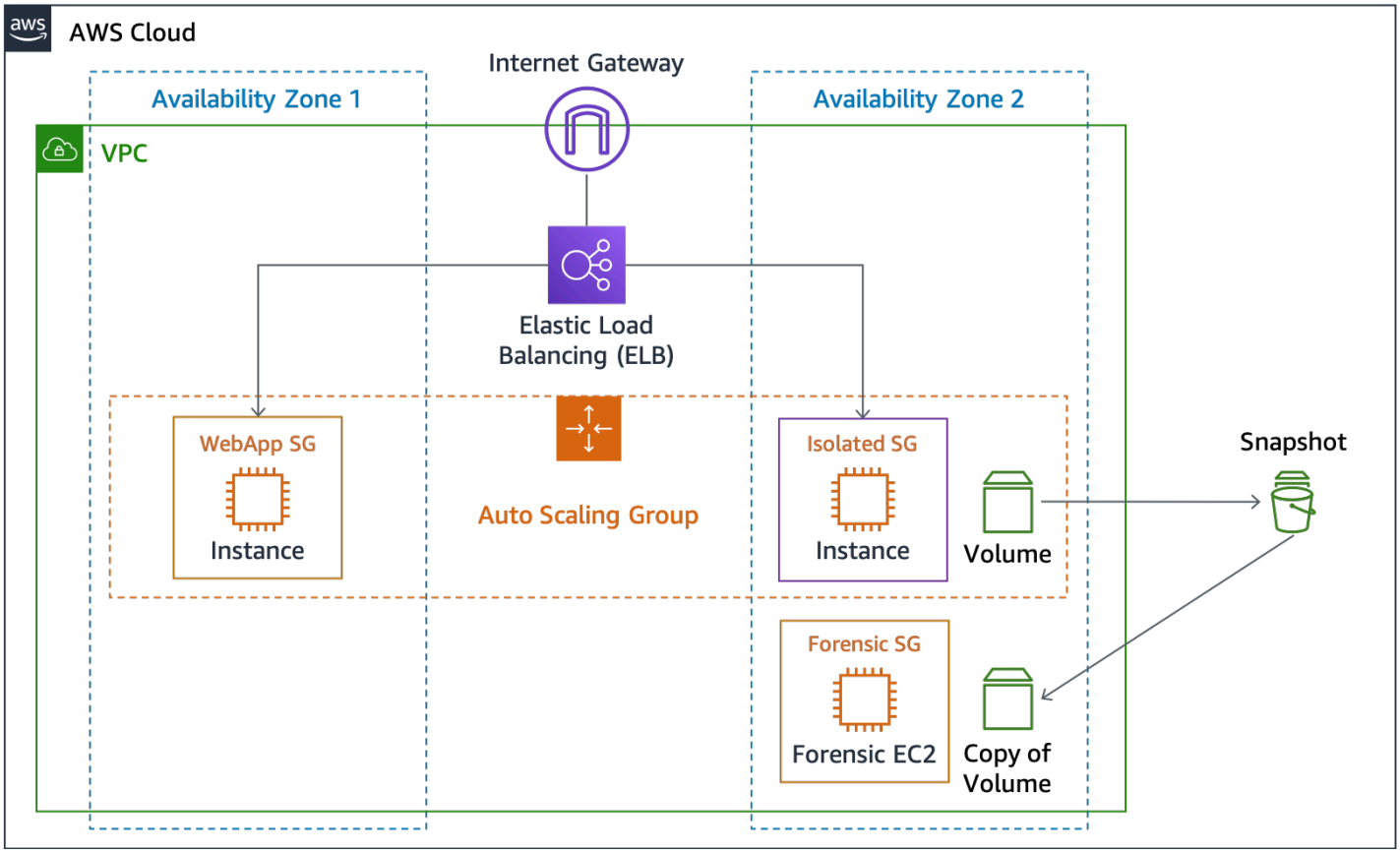

Figura 6: Aislamiento de instancias de EC2 e instantáneas

Temas

- Decisiones de investigación
- Captura de datos volátiles
- Uso de AWS Systems Manager
- Automatización de la captura

Decisiones de investigación

En este punto, puede elegir entre una investigación sin conexión (cerrar la instancia de forma inmediata) o una investigación en línea (mantener la instancia en funcionamiento). Una ventaja de la investigación sin conexión es que, una vez que la instancia se cierra, ya no puede afectar al entorno existente. Además, puede crear una copia de la instancia afectada a partir de las instantáneas de EBS y revisarla en una cuenta de AWS aislada con un entorno aislado que se haya diseñado específicamente para la investigación. Sin embargo, puede optar por no cerrar la instancia de forma

inmediata, si una investigación en línea permite capturar pruebas volátiles del sistema operativo host, como la memoria o el tráfico de red.

Captura de datos volátiles

Si bien es posible que decida no llevar a cabo la investigación en línea, es importante comprender los mecanismos necesarios para capturar datos volátiles de una instancia. Una investigación en línea requiere la interacción con el sistema operativo que se ejecuta en la instancia de Amazon EC2. En este escenario, necesita más que el servicio AWS IAM para ejecutar tareas en una instancia de Amazon EC2. Aunque puede autenticarse directamente en la máquina con un método estándar (como Secure Shell (SSH) de Linux o Escritorio remoto (RDP) de Microsoft Windows), la interacción manual con el sistema operativo no es una práctica recomendada. Se recomienda utilizar una herramienta de automatización mediante programación para ejecutar tareas en un host.

Uso de AWS Systems Manager

AWS Systems Manager Run Command ayuda a realizar de forma remota y segura los cambios bajo demanda mediante la ejecución de scripts de shell de Linux y comandos de Windows PowerShell en una instancia de destino. Si bien puede invocar Run Command a través de los permisos del servicio AWS IAM, primero debe activar las instancias de Amazon EC2 como instancias administradas, instalar SSM Agent en sus máquinas (si no está instalado de forma predeterminada) y configurar los permisos de AWS IAM. Si quiere usar Run Command para actividades de automatización o respuesta, asegúrese de completar las actividades previas requeridas antes de tener que realizar una investigación.

AWS Systems Manager, que incluye Run Command, se integra con AWS CloudTrail, un servicio que captura las llamadas a la API realizadas por o en nombre de una instancia de Systems Manager y entrega los archivos de registro en un bucket de Amazon S3 especificado. Gracias a la información recopilada por AWS CloudTrail, puede determinar qué solicitud se realizó, la dirección IP de origen que realizó la solicitud, quién hizo la solicitud y cuándo, entre otros datos. CloudTrail crea registros de todas las acciones de la API de Systems Manager, incluidas las solicitudes de API para ejecutar comandos con Run Command o para crear documentos de Systems Manager.

Puede usar el servicio AWS Systems Manager Run Command para invocar la instancia de SSM Agent que ejecuta scripts de shell de Linux y comandos de Windows PowerShell. Estos scripts pueden cargar y ejecutar herramientas específicas para capturar datos adicionales del host, como el módulo de kernel Linux Memory Extractor (LiME). A continuación, puede transferir la captura de memoria a la instancia forense de Amazon EC2 en la red VPC o a un bucket de Amazon S3 para su almacenamiento de larga duración.

Automatización de la captura

Un método para invocar SSM Agent consiste en dirigir Run Command a través de Amazon CloudWatch Events cuando la instancia se haya etiquetado de forma específica. Por ejemplo, si aplica la etiqueta `Response=Isolate+MemoryCapture` a una instancia afectada, puede configurar Amazon CloudWatch Events para desencadenar dos acciones:

- Una función Lambda que realiza las actividades de aislamiento
- Una instancia de Run Command que ejecuta un comando de shell para exportar la memoria de Linux a través de SSM Agent

Esta respuesta basada en etiquetas es otro método de respuesta basada en eventos.

Conclusión

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

Recursos adicionales

Para obtener información adicional, consulte la siguiente documentación:

- AWS Well-Architected
- Página de AWS Cloud Adoption Framework
- Solución de registro centralizada de AWS
- Visualice los registros de AWS CloudTrail con AWS Glue y Amazon QuickSight
- How to Monitor Host-Based Intrusion Detection System Alerts on Amazon EC2 Instances
- Almacenar y monitorizar los archivos de registro del sistema operativo y de las aplicaciones con Amazon CloudWatch
- Identity and Access Management in Amazon S3
- Usar el control de versiones (Amazon S3)
- Uso de eliminación con MFA
- Protección de los datos con el cifrado del lado del servidor con claves administradas por AWS KMS (SSE-KMS)
- Respuesta ante incidentes con la CLI y la consola de AWS
- Preparación para la Ley de privacidad del consumidor de California

Medios

- AWS re:Invent 2014 (SEC402): Intrusion Detection in the Cloud
- AWS re:Invent 2014 (SEC404): Incident Response in the Cloud
- AWS re:Invent 2015 (SEC308): Wrangling Security Events in The Cloud
- AWS re:Invent 2015 (SEC316): Harden Your Architecture with Security Incident Response Simulations
- AWS re:Invent 2016 (SEC313): Automating Security Event Response, from Idea to Code to Execution
- AWS re:Invent 2017 (SID302): Force Multiply Your Security Team with Automation and Alexa
- AWS re:Invent 2016 (SAC316): Security Automation: Spend Less Time Securing Your Applications
- AWS re:Invent 2016 (SAC304): Predictive Security: Using Big Data to Fortify Your Defenses

- AWS re:Invent 2017 (SID325): Amazon Macie: Data Visibility Powered by Machine Learning for Security and Compliance Workloads
- Cumbre de AWS en Londres en 2018: Automating Incident Response and Forensics in AWS

Herramientas de terceros

Los enlaces siguientes a herramientas de terceros son externos y no están avalados por AWS. AWS no ofrece garantías ni representaciones de ningún tipo sobre estas herramientas o páginas.

- AWS_IR: utilidad de línea de comandos que se puede instalar en Python para mitigar las vulnerabilidades de los hosts y las claves.
- MargaritaShotgun: herramienta de adquisición de memoria remota.
- ThreatPrep: módulo de Python para la evaluación de las prácticas recomendadas para las cuentas de AWS en relación con la preparación para la gestión de incidentes.
- ThreatResponse Web: plataforma de análisis basada en web para su uso con la herramienta de la línea de comandos AWS_IR.
- GRR Rapid Response: análisis forense remoto en directo para la respuesta ante incidentes.
- Linux Write Blocker: revisión de kernel y herramientas de espacio de usuarios para habilitar el bloqueo de escritura de software de Linux.

Referencias de la industria

- NIST SP 800-61R2: guía de administración de incidentes de seguridad informática

Revisiones del documento

Para recibir notificaciones sobre las actualizaciones de este documento técnico, suscríbase a la fuente RSS.

update-history-change	update-history-description	update-history-date
Actualizaciones menores	Errores corregidos y numerosos cambios menores generales.	2 de junio de 2021
Actualización menor	Enlaces rotos corregidos.	5 de marzo de 2021
Documento técnico actualizado	Enlaces rotos corregidos y numerosos cambios de texto para mejorar la legibilidad.	23 de noviembre de 2020
Actualización menor	Enlace corregido a «Respuesta ante incidentes con la CLI y la consola de AWS».	30 de junio de 2020
Documento técnico actualizado	Actualización para nuevos servicios de seguridad, inteligencia de amenazas, responsabilidad compartida para los contenedores, automatización y CCPA. Apéndices añadidos con un runbook y un árbol de toma de decisiones de ejemplo.	11 de junio de 2020
Publicación inicial	Documento técnico publicado por primera vez	1 de junio de 2019

Apéndice A: Definiciones de las capacidades de la nube

AWS proporciona más de 150 servicios en la nube y miles de características. Muchos de estos ofrecen capacidades de detección, prevención y respuesta de tipo nativo y otros se pueden usar para diseñar soluciones de seguridad personalizadas. En esta sección se incluye un subconjunto de los servicios más relevantes para la respuesta ante incidentes en la nube.

Temas

Registro y eventos

AWS CloudTrail: AWS CloudTrail es un servicio que permite la gobernanza, el cumplimiento, la auditoría operativa y la auditoría de riesgos de su cuenta de AWS. Con CloudTrail, puede registrar, monitorear de manera continua y retener la actividad de la cuenta relacionada con acciones en toda su infraestructura de AWS. CloudTrail proporciona un historial de eventos de la actividad de la cuenta de AWS, incluidas las acciones realizadas a través de la Consola de administración de AWS, los SDK de AWS, las herramientas de la línea de comandos y otros servicios de AWS. Este historial de eventos simplifica los análisis de seguridad, el seguimiento de cambios de los recursos y la resolución de problemas.

Los archivos de registro validados son muy valiosos para las investigaciones de seguridad y forenses. Para determinar si un archivo de registro se ha modificado, eliminado o continúa igual después del envío de CloudTrail, puede usar la validación de la integridad de los archivos de registro de CloudTrail. Esta característica se integra mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. De ese modo, resulta imposible modificar, eliminar o falsificar los archivos de registro de CloudTrail por medios informáticos sin que se sepa.

De forma predeterminada, a los archivos de registro entregados por CloudTrail al bucket se les aplica el cifrado del lado del servidor de Amazon. Opcionalmente, puede usar las claves administradas de AWS Key Management Service (AWS KMS) (SSE-KMS) para los archivos de registro de CloudTrail.

Amazon CloudWatch Events: Amazon CloudWatch Events proporciona un flujo de eventos del sistema en tiempo casi real que describen los 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. CloudWatch Events detecta los cambios operativos a medida que se producen. CloudWatch Events puede responder a estos cambios operativos y emprender acciones correctivas según sea necesario mediante el envío de mensajes para responder al entorno, la activación de funciones, la realización de cambios y la captura de información de estado. Algunos servicios de seguridad, como Amazon GuardDuty, generan sus resultados en forma de CloudWatch Events.

AWS Config: AWS Config es un servicio que permite examinar, auditar y evaluar las configuraciones de los recursos de AWS. Config monitorea y registra constantemente las configuraciones de sus recursos de AWS y permite automatizar la evaluación de las configuraciones registradas con respecto a las configuraciones deseadas. Con Config, puede revisar los cambios en las configuraciones y las relaciones entre los recursos de AWS de forma manual o automática. Puede revisar los historiales detallados de configuración de recursos y determinar el cumplimiento general con respecto a las configuraciones especificadas en sus directrices internas. Esto permite simplificar las auditorías de cumplimiento, los análisis de seguridad, la administración de cambios y la resolución de problemas operativos.

Registros de acceso de Amazon S3: si almacena información confidencial en un bucket de Amazon S3, puede habilitar los registros de acceso de S3 para registrar cada carga, descarga y modificación de esos datos. Este registro es independiente de los registros de CloudTrail que registran los cambios en el bucket en sí (como los cambios en las políticas de acceso y en las políticas de ciclo de vida) y los complementa.

Amazon CloudWatch Logs: puede usar Amazon CloudWatch Logs para monitorear, almacenar y acceder a los archivos de registro (por ejemplo, del sistema operativo, las aplicaciones y los archivos de registro personalizados) desde sus instancias de Amazon Elastic Compute Cloud (Amazon EC2) con el agente de CloudWatch Logs. Además, Amazon CloudWatch Logs puede capturar registros de AWS CloudTrail, consultas de DNS de Amazon Route 53, registros de flujo de VPC, funciones de Lambda y otros orígenes. Luego, puede recuperar los datos de registro asociados desde CloudWatch Logs.

Registros de flujo de Amazon VPC: los registros de flujo de VPC permiten capturar información sobre el tráfico IP hacia y desde las interfaces de red en la VPC. Una vez creado un registro de flujo, puede ver y recuperar sus datos en Amazon CloudWatch Logs. Los registros de flujo de VPC pueden ayudarle en diversas tareas. Por ejemplo, puede usar registros de flujo para solucionar problemas

por los que determinado tráfico no llega a una instancia, lo cual puede ayudarle a diagnosticar reglas de grupo de seguridad excesivamente restrictivas. También puede utilizar los registros de flujo como herramienta de seguridad para monitorear el tráfico hacia la instancia.

Registros de AWS WAF: AWS WAF admite ahora el registro completo de todas las solicitudes web inspeccionadas por el servicio. Puede almacenar estos registros en Amazon S3 para satisfacer sus necesidades de cumplimiento y auditoría, así como usarlos para depuración y análisis forenses adicionales. Estos registros ayudan a comprender por qué se desencadenan ciertas reglas y por qué se bloquean determinadas solicitudes web. También puede integrar los registros con sus herramientas de SIEM y análisis de registros.

Otros registros de AWS: dado el ritmo de innovación, seguimos implementando características y capacidades nuevas para los clientes prácticamente todos los días, lo que significa que hay docenas de servicios de AWS que ofrecen capacidades de registro y monitoreo. Para obtener información sobre las características disponibles para cada servicio de AWS, consulte la documentación de AWS del servicio en cuestión.

Visibilidad y alertas

AWS Security Hub CSPM: AWS Security Hub CSPM permite ver de manera integral las alertas de seguridad de alta prioridad y el estado de cumplimiento en todas las cuentas de AWS. Con Security Hub, dispone de un único lugar donde se incorporan, organizan y priorizan las alertas de seguridad o los resultados de varios servicios de AWS, como Amazon GuardDuty, Amazon Inspector y Amazon Macie, así como de soluciones de socios de AWS. Los resultados se resumen visualmente en tableros integrados con gráficos y tablas que se pueden procesar. También puede monitorear continuamente su entorno utilizando comprobaciones de conformidad automatizadas basadas en las prácticas recomendadas de AWS y en 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 y ayuda a proteger sus cargas de trabajo y cuentas de AWS. Monitoriza actividades como llamadas a la API inusuales o implementaciones potencialmente no autorizadas que pueden indicar una posible vulneración de la cuenta. GuardDuty también detecta instancias potencialmente vulneradas o actividades de reconocimiento por parte de atacantes.

GuardDuty identifica a los atacantes sospechosos a través de fuentes integradas de inteligencia de amenazas y utiliza machine learning para detectar anomalías en las actividades de las cuentas y las cargas de trabajo. Cuando se detecta una amenaza potencial, el servicio emite un alerta de

seguridad detallada a la consola de GuardDuty y a AWS CloudWatch Events. Esto permite poder actuar sobre las alertas e integrarlas fácilmente en los sistemas de administración de eventos y de flujos de trabajo existentes.

Amazon Macie: Amazon Macie es un servicio de seguridad con tecnología de IA que ayuda a evitar la pérdida de datos mediante la identificación, la clasificación y la protección automáticas de la información confidencial almacenada en AWS. Amazon Macie usa machine learning para reconocer información confidencial, como información de identificación personal (PII) o propiedad intelectual, asigna un valor empresarial y proporciona visibilidad de la ubicación donde se almacenan los datos y cómo se utilizan en su organización. Amazon Macie monitorea la actividad de acceso a los datos constantemente en busca de anomalías y envía alertas cuando detecta un riesgo de acceso no autorizado o filtraciones de datos involuntarias.

Reglas de AWS Config: una regla de AWS Config representa las configuraciones preferidas para un recurso y se evalúa con respecto a los cambios de configuración realizados en los recursos relevantes, según los registró AWS Config. Los resultados de la evaluación de una regla con respecto a la configuración de un recurso pueden verse en un panel. Con las reglas de Config, puede evaluar su estado general de cumplimiento y riesgo desde el punto de vista de la configuración, ver las tendencias de cumplimiento a lo largo del tiempo e identificar qué cambio en la configuración ha provocado que un recurso no cumpla una regla.

AWS Trusted Advisor: AWS Trusted Advisor es un recurso en línea que ayuda a reducir costes, aumentar el rendimiento y mejorar la seguridad mediante la optimización de su entorno de AWS. Trusted Advisor proporciona orientación en tiempo real que le ayuda a aprovisionar sus recursos al seguir las prácticas recomendadas de AWS. El conjunto completo de comprobaciones de Trusted Advisor, incluida la integración de CloudWatch Events, se encuentra disponible para los clientes de los planes Business Support y Enterprise Support.

Amazon CloudWatch: Amazon CloudWatch es un servicio de supervisión para los recursos de la nube de AWS y las aplicaciones que se ejecutan en AWS. Puede utilizar Amazon CloudWatch para recopilar y realizar el seguimiento de métricas y registros, establecer alarmas y reaccionar automáticamente a los cambios en sus recursos de AWS. Amazon 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 que las aplicaciones y los servicios generan y archivos de registro generados por las aplicaciones. Puede usar Amazon CloudWatch para obtener visibilidad de todo el sistema sobre la utilización de recursos, el rendimiento de las aplicaciones y el estado operativo. Estas observaciones se pueden usar para reaccionar en consecuencia y mantener la ejecución de su aplicación sin problemas.

AWS Inspector: Amazon Inspector es un servicio automático de evaluación de seguridad que ayuda a mejorar la seguridad y cumplimiento de las aplicaciones implementadas en AWS. Amazon Inspector evalúa automáticamente las aplicaciones en busca de vulnerabilidades o desviaciones de las prácticas recomendadas. Después de la evaluación, Amazon Inspector genera una lista detallada de problemas de seguridad ordenados 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 datos de registro de manera automática a partir de sus recursos de AWS y utiliza el machine learning, el análisis estadístico y la teoría de grafos para crear un conjunto de datos vinculado que permite llevar a cabo fácilmente investigaciones sobre la seguridad más rápidas y eficientes. Con este servicio, se pueden analizar billones de eventos de diversos orígenes de datos, como los registros de flujos de Virtual Private Cloud (VPC), AWS CloudTrail y Amazon GuardDuty, además de crear de manera automática una vista unificada e interactiva de los recursos, los usuarios y las interacciones entre ellos a lo largo del tiempo. Gracias a esta visión unificada, puede 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.

Automatización

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. Puede usar Lambda para ampliar otros servicios de AWS con lógica personalizada o crear sus propios servicios back-end que funcionan según la escala, el rendimiento y la seguridad de AWS. Lambda ejecuta el código en una infraestructura de computación de alta disponibilidad y lleva a cabo toda la administración de los recursos informáticos de forma automática. Entre otras cosas, se encarga del mantenimiento de servidores y sistemas operativos, del aprovisionamiento de capacidad y del escalado automático, de la implementación de código y de revisiones de seguridad, así como de la supervisión y el registro del código. Lo único que tiene que hacer es proporcionar el código.

AWS Step Functions: AWS Step Functions facilita la coordinación de los componentes de aplicaciones y microservicios distribuidos con flujos de trabajo visuales. Step Functions proporciona una consola gráfica para ordenar y visualizar los componentes de su aplicación en varios pasos. De este modo, crear y ejecutar aplicaciones de varios pasos resulta sencillo. Step Functions activa y monitoriza 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, lo que permite desarrollar fácilmente su aplicación e innovar con más rapidez. AWS Step Functions forma parte de la plataforma sin servidor de AWS y facilita la orquestación de las funciones de AWS Lambda para las aplicaciones sin servidor. También puede usar Step Functions para la orquestación de microservicios mediante recursos de computación como Amazon EC2 y Amazon ECS.

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

Almacenamiento seguro

Amazon S3: Amazon S3 es un servicio de almacenamiento de objetos creado para almacenar y recuperar cualquier volumen de datos desde cualquier ubicación. Está diseñado para ofrecer una durabilidad del 99,999999999 % y almacena datos de millones de aplicaciones que utilizan líderes del mercado de todas las industrias. Amazon S3 presta servicios integrales de seguridad y está diseñado para cumplir con los requisitos normativos. Ofrece a los clientes flexibilidad respecto a los métodos que usan para administrar datos en relación con las actividades de optimización de costes, control de acceso y cumplimiento. Amazon S3 proporciona funcionalidad de consulta in situ, lo que permite ejecutar análisis exhaustivos directamente en los datos en reposo en Amazon S3. Además, Amazon S3 es el servicio de almacenamiento en la nube con mayor nivel de compatibilidad disponible, ya que se integra con la mayoría de las 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 muy bajo coste para archivar datos y realizar copias de seguridad a largo plazo. Ofrece una durabilidad del 99,999999999 %, presta servicios integrales de seguridad y está diseñado para cumplir los requisitos normativos. Amazon S3 Glacier proporciona funcionalidad de consulta in situ, lo que permite ejecutar análisis exhaustivos directamente en los datos archivados en reposo. Para mantener un coste bajo pero seguir siendo apto para diversas necesidades de

recuperación, Amazon S3 Glacier ofrece tres opciones de acceso a los archivos, que ocupan desde unos pocos minutos hasta varias horas.

Personalizado

Las características y los servicios mencionados anteriormente no componen una lista exhaustiva. AWS agrega nuevas capacidades continuamente. Para obtener más información, se recomienda consultar las páginas ¿Qué novedades hay en AWS? y Seguridad en la nube de AWS. Además de los servicios de seguridad que AWS ofrece como servicios nativos en la nube, puede que le interese desarrollar sus propias capacidades en los servicios de AWS.

Si bien recomendamos habilitar un conjunto básico de servicios de seguridad en sus cuentas, como AWS CloudTrail, Amazon GuardDuty y Amazon Macie, puede que a la larga quiera ampliar estas capacidades para obtener un valor adicional de sus activos de registro. Existen varias herramientas de socios disponibles, como las que se enumeran en nuestro programa de socios con competencia de seguridad de AWS. También puede que quiera escribir sus propias consultas para realizar búsquedas en los registros. La gran cantidad de servicios administrados que AWS ofrece lo hace más fácil que nunca. Hay muchos servicios adicionales de AWS de ayuda a la investigación que quedan fuera del alcance de este documento, como Amazon Athena, Amazon OpenSearch Service, Amazon QuickSight, Amazon Machine Learning y Amazon EMR.

Apéndice B: Código de muestra

Evento AWS CloudTrail de ejemplo

En el ejemplo siguiente se muestra que una usuaria de IAM llamada `Alice` utilizó AWS CLI para llamar a la acción `StopInstancesaction` de Amazon EC2 mediante `ec2-stop-instances`.


```
{"Records": [{
    "eventVersion": "1.0",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-03-06T21:01:59Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StopInstances",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "205.251.233.176",
    "userAgent": "ec2-api-tools 1.6.12.2",
    "requestParameters": {
        "instancesSet": {"items": [{"instanceId": "i-ebeaf9e2"}]},
        "force": false
    },
    "responseElements": {"instancesSet": {"items": [{
        "instanceId": "i-ebeaf9e2",
        "currentState": {
            "code": 64,
            "name": "stopping"
        },
        "previousState": {
            "code": 16,
            "name": "running"
        }
    }]}}
}]}
```

Evento AWS CloudWatch de ejemplo

El evento de ejemplo de Amazon CloudWatch siguiente muestra que una usuaria de AWS IAM llamada `jane-roe-test` se expuso públicamente en `www.github.com` y podría ser víctima de abuso por parte de usuarios no autorizados.

```
{
  "check-name": "Exposed Access Keys",
  "check-item-detail": {
    "Case ID": "02648f3b-e18f-4019-8d68-ce25efe080ff",
    "Usage (USD per Day)": "0",
    "User Name (IAM or Root)": "jane-roe-test",
    "Deadline": "1440453299248",
    "Access Key ID": "AKIAIOSFODNN7EXAMPLE",
    "Time Updated": "1440021299248",
    "Fraud Type": "Exposed",
    "Location": "www.github.com"
  },
  "status": "ERROR",
  "resource_id": "",
  "uuid": "cce6d28f-e44b-4e61-aba1-5b4af96a0f59"
}
```

Actividades de la CLI del dominio de infraestructura de ejemplo

Los comandos de AWS CLI siguientes muestran un ejemplo de respuesta a un evento dentro del dominio de infraestructura. En este ejemplo, se usan las API de AWS para realizar muchas de las actividades iniciales de respuesta ante incidentes que se describen en este documento.

```
# Anomaly detected on IP X.X.X.X. Capture that instance's metadata
> aws ec2 describe-instances --filters "Name=ip-address,Values=X.X.X.X"
```

```
# Protect that instance from accidental termination
> aws ec2 modify-instance-attribute --instance-id i-abcd1234 --attribute
 disableApiTermination --value true
```

```
# Switch the EC2 instance's Security Group to a restricted Security Group
> aws ec2 modify-instance-attribute --instance-id i-abcd1234 --groups sg-a1b2c3d4
```

```
# Detach from the Auto Scaling Group
> aws autoscaling detach-instances --instance-ids i-abcd1234 --auto-scaling-group-name
 web-asg
```

```
# Deregister the instance from the Elastic Load Balancer
> aws elb deregister-instances-from-load-balancer --instances i-abcd1234 --load-
balancer-name web-load-balancer
```

```
# Create an EBS snapshot
> aws ec2 create-snapshot --volume vol-12xxxx78 --description "ResponderName-Date-
REFERENCE-ID"
```

```
# Create a new EC2 instance from the Forensic Workstation AMI
> aws ec2 run-instances --image-id ami-4n6x4n6x --count 1 --instance-type c4.8xlarge --
key-name forensicPublicKey --security-group-ids sg-1a2b3c4d --subnet-id subnet-6e7f819e
```

```
# Create a new EBS volume copy from the EBS snapshot
> aws ec2 create-volume --region us-east-1 --availability-zone us-east-1a --snapshot-id
 snap-abcd1234 --volume-type io1 --iops 10000
```

```
# Attach the volume to the forensic workstation
> aws ec2 attach-volume --volume-id vol-1234abcd --instance-id i-new4n6x --device /dev/
sdf
```

```
# Create a security group rule to allow the new Forensic Workstation to communicate to
 the contaminated instance.
> aws ec2 authorize-security-group-ingress --group-id sg-a1b2c3d4 --protocol tcp --port
 0-65535 --source-group sg-1a2b3c4d
```

```
# Tag the contaminated instance with the ticket or reference ID
> aws ec2 create-tags -resources i-abcd1234 -tags
 Key=Environment,Value=Quarantine:REFERENCE-ID
```

Apéndice C: Ejemplo de runbook

El ejemplo de runbook siguiente representa una sola entrada de un runbook más extenso. Este runbook no es oficial y se proporciona solo como ejemplo. A medida que elabore sus runbooks, cada uno de los escenarios puede evolucionar en elementos más grandes que tienen comienzos e indicadores de riesgo distintos, pero todos con resultados o acciones similares que deben realizarse. Efectuar este cambio también puede dar lugar a otras situaciones que generen respuestas mejores o más minuciosas.

Runbook de respuesta ante incidentes: uso de la cuenta raíz

Objetivo

El objetivo de este runbook es proporcionar orientación específica sobre cómo administrar el uso de la cuenta raíz de AWS. Este runbook no sustituye a una estrategia de respuesta ante incidentes exhaustiva. Se centra en el ciclo de vida de la respuesta ante incidentes:

- Establecimiento de control
- Determinación del impacto
- Recuperación según sea necesario
- Investigación de la causa raíz
- Mejora

Los indicadores de riesgo (IOC), los pasos iniciales (detener la «hemorragia») y los comandos detallados de la CLI necesarios para ejecutar esos pasos se enumeran a continuación.

Supuestos

- CLI configurada e instalada
- Proceso de generación de informes existente
- Trusted Advisor activo
- Security Hub activo

Indicadores de vulnerabilidad

- Actividad que es anormal para la cuenta.
  - Creación de usuarios de IAM
  - CloudTrail desactivado
  - CloudWatch desactivado
  - SNS en pausa
  - Step Functions en pausa
- Lanzamiento de AMI nuevas o inesperadas
- Cambios en los contactos de la cuenta

Pasos de corrección: establecimiento de medidas de control

La documentación de AWS para una cuenta posiblemente vulnerable indica las tareas específicas que se enumeran a continuación. La documentación para una cuenta posiblemente vulnerable puede encontrarse en la página sobre qué hacer si se observa una actividad no autorizada en la cuenta de AWS.

1. Póngase en contacto con AWS Support y el administrador técnico de la cuenta (TAM) lo antes posible.
2. Cambie y rote la contraseña raíz y agregue un dispositivo MFA asociado a la cuenta raíz.
3. Rote las contraseñas, las claves de acceso/secretas y los comandos de la CLI relevantes para los pasos de corrección.
4. Revise las acciones que realiza el usuario raíz.
5. Abra los runbooks correspondientes a esas acciones.
6. Cierre el incidente.
7. Revise el incidente e intente comprender lo que ha pasado.
8. Solucione los problemas subyacentes, implemente mejoras y actualice el runbook según sea necesario.

Elementos de acción adicionales: determinación del impacto

Revise los elementos creados y las llamadas modificadas. Puede haber elementos que se hayan creado para permitir el acceso en el futuro. Algunos de los elementos que deben tenerse en cuenta son los siguientes:

- Roles entre cuentas de IAM
- Usuarios de IAM
- Buckets de S3
- Instancias de EC2
- [Su aplicación e infraestructura determinarán esta lista].

Avisos

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