Recomendaciones de AWS

Implementación de controles de seguridad en AWS

Recomendaciones de AWS: Implementación de controles de seguridad en AWS

Table of Contents

Implementación de controles de seguridad en AWS

Lucia Vanta, Gurpreet Kaur Cheema, Wasim Hossain, Iqbal Umair, Joseph Nguyen y San Brar de Amazon Web Services (AWS)

Diciembre de 2022 (historial de documentos (p. 16))

La seguridad es fundamental para todas las empresas y es un pilar clave en el Marco de AWS Well-Architected. Sin embargo, muchos no saben cómo abordar las consideraciones de seguridad y crear una estrategia integral y automatizada de pruebas y corrección de la seguridad para sus entornos. Mediante el uso de Servicios de AWS y herramientas, como AWS Config, Amazon GuardDuty y AWS CloudFormation, puede crear una estrategia de pruebas de seguridad e incorporarla a su entorno de Nube de AWS.

A fin de ayudar a cumplir con las políticas y los estándares de seguridad de su empresa, los controles de seguridad son las barreras de protección técnicas o administrativas que ayudan a prevenir, detectar o reducir la capacidad de un agente de amenazas para aprovechar una vulnerabilidad de seguridad. Se han diseñado para proteger la confidencialidad, la integridad y la disponibilidad de los recursos y los datos. Los siguientes son ejemplos de controles de seguridad:

- Implementar la autenticación multifactor para los usuarios que necesitan iniciar sesión en una aplicación
- Acciones de consulta, registro y monitoreo con el fin de realizar auditorías en tiempo real de la actividad de la cuenta
- Asegurarse de que los datos confidenciales se encuentren cifrados
- Asegurarse de que los registros se almacenen de acuerdo con la política de retención de su empresa

Existen tres tipos de controles de seguridad: preventivo, de detección y de respuesta. En esta guía, se describe cada tipo con más detalle y se hace hincapié en cómo implementar y automatizar estos controles en la Nube de AWS. En esta guía, se brinda orientación sobre cómo pensar en los controles de seguridad que sean continuos y proactivos.

Destinatarios previstos

Esta guía se ha diseñado para arquitectos e ingenieros de seguridad responsables de implementar los controles de seguridad en la Nube de AWS. Si su empresa no ha definido una política de seguridad, objetivos de control o estándares, como se describe en Controles de seguridad en el marco de gobernanza (p. 3), le recomendamos que complete estas tareas de gobernanza antes de continuar con esta guía.

Resultados empresariales específicos

Las empresas utilizan los controles de seguridad a fin de mitigar o emplear medidas correctivas frente a los riesgos para sus sistemas de información. Los controles definen la base de los requisitos para satisfacer los principales objetivos de seguridad de un programa de TI y su estrategia de seguridad. Contar con controles mejora la posición de seguridad de una empresa al proteger la confidencialidad, integridad y disponibilidad de sus datos y activos de TI. Sin controles, sería difícil saber dónde hay que invertir los esfuerzos para establecer una base de seguridad.

Los controles de seguridad se pueden utilizar para abordar una variedad de escenarios. Los ejemplos incluyen cumplir con los requisitos derivados de las evaluaciones de riesgos, alcanzar los estándares del sector o cumplir con las normativas. Cumplir con los controles de seguridad demuestra que se ha medido el riesgo para un sistema, se ha determinado el nivel de protección necesario y se han implementado soluciones de forma proactiva. Otros factores, como el negocio, la industria y la geografía, pueden determinar los controles de seguridad que necesita.

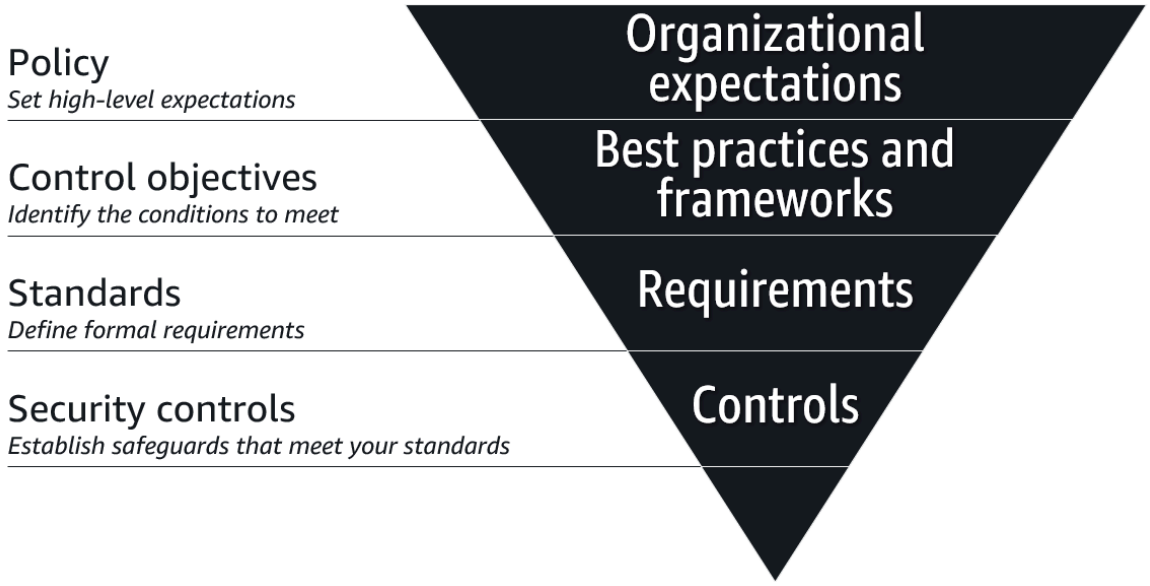
Los siguientes son casos de uso comunes para la implementación de los controles de seguridad:

- En la evaluación de seguridad de una aplicación se ha identificado la necesidad de controles de acceso en función de la confidencialidad de los datos que se procesan.
- Debe cumplir con los estándares de seguridad, como las Normas de seguridad de datos del sector de las tarjetas de pago (PCI DSS), la HIPAA (Ley de Portabilidad y Responsabilidad de Seguros de Salud) o el Instituto Nacional de Estándares y Tecnología (NIST).
- Debe proteger la información confidencial para las transacciones empresariales.
- Su empresa se ha expandido a una región geográfica que requiere controles de seguridad, como una región que exige la conformidad con el Reglamento General de Protección de Datos (RGPD).

Tras leer esta guía, debería familiarizarse con los tres tipos de controles de seguridad, comprender de qué manera forman parte de su marco de gobernanza de seguridad, y estar preparado para comenzar a implementar y automatizar los controles de seguridad en la Nube de AWS.

Controles de seguridad en el marco de gobernanza

Es importante planificar desde un nivel básico. ¿Cómo se comienza? En la siguiente figura, se muestra cómo se puede crear una estrategia de gobernanza de la seguridad basada en una política, objetivos de control, estándares y controles de seguridad.



Los siguientes son los componentes jerárquicos de una estrategia de gobernanza de la seguridad:

- Política: una política es la base de cualquier estrategia de gobernanza de ciberseguridad. Es un documento que establece las expectativas de la empresa, como las obligaciones legales, reglamentarias o contractuales que debe cumplir. Las políticas pueden variar en función del sector y la región.
- Objetivos de control: los objetivos de control son metas, como las prácticas recomendadas reconocidas en el sector, que ayudan a cumplir la intención de una política. En el caso de la computación en la nube, muchas empresas adoptan la Matriz de controles en la nube (CCM) (sitio web de Cloud Security Alliance), que es un marco de objetivos de control de ciberseguridad.
- Estándares: los estándares son requisitos que se establecen de manera formal y satisfacen un objetivo de control. Los estándares pueden incluir procesos, acciones o configuraciones, y son cuantificables para que pueda medir el rendimiento en comparación con el estándar.
- Controles de seguridad: los controles de seguridad son los mecanismos técnicos o administrativos que se llevan a cabo para implementar los estándares. Todos los controles de seguridad se ajustan a los estándares, pero no todos los estándares se ajustan a los controles de seguridad. Las pruebas de los controles de seguridad se han diseñado para monitorear y medir si se cumplen de manera efectiva los estándares definidos.

Esta guía se enfoca en cómo diseñar e implementar los tipos comunes de controles de seguridad en la Nube de AWS.

Tipos de controles de seguridad

Existen tres tipos de controles de seguridad principales:

- Controles preventivos (p. 4): estos controles se han diseñado para evitar que ocurra un evento.
- Controles de detección (p. 7): estos controles se han diseñado para detectar, registrar y alertar después de que se produzca un evento.
- Controles de respuesta (p. 10): estos controles se han diseñado para corregir los eventos adversos o las desviaciones con respecto a su base de seguridad.

Una estrategia de seguridad eficaz incluye los tres tipos de controles de seguridad. Los controles preventivos son la primera línea de defensa para evitar el acceso no autorizado o los cambios no deseados en la red. Sin embargo, es importante asegurarse de establecer controles de detección y de respuesta a fin de saber cuándo se produce un evento y poder tomar las medidas adecuadas e inmediatas para solucionarlo.

En las siguientes secciones, se describe cada tipo de control en más detalle. Se analizan los objetivos, el proceso de implementación, los casos de uso, las consideraciones tecnológicas y los resultados esperados de cada tipo de control.

Controles preventivos

Los controles preventivos son controles de seguridad que se han diseñado para evitar que ocurra un evento. Estas barreras de protección son la primera línea de defensa para evitar el acceso no autorizado o los cambios no deseados en la red. Un ejemplo de control preventivo es un rol de AWS Identity and Access Management (IAM) que tiene acceso de solo lectura porque ayuda a evitar acciones de escritura no deseadas por parte de usuarios no autorizados.

Objetivos

El objetivo principal de los controles preventivos es minimizar o evitar la probabilidad de que se produzca una amenaza. El control debe ayudar a evitar el acceso no autorizado al sistema e impedir que los cambios no intencionados afecten al sistema. Los objetivos de los controles preventivos son los siguientes:

- División de funciones: los controles preventivos pueden establecer límites lógicos que restringen los privilegios, de manera de que con los permisos solo se realicen tareas específicas en cuentas o entornos designados. Entre los ejemplos se incluyen:
  - Segmentar las cargas de trabajo en diferentes cuentas para servicios específicos
  - Separar y contabilizar en entornos aislados de producción, desarrollo y pruebas
  - Delegar el acceso y las responsabilidades a varias entidades para que desempeñen funciones específicas, como utilizar roles de IAM o roles asumidos a fin de permitir que solo funciones laborales específicas realicen determinadas acciones
- Control de acceso: los controles preventivos pueden conceder o denegar el acceso a los recursos y datos del entorno de forma sistemática. Entre los ejemplos se incluyen:
  - Impedir que los usuarios superen los permisos previstos, lo que se conoce como escalado de privilegios
  - Restringir el acceso a aplicaciones y datos solo a los usuarios y servicios autorizados
  - Mantener el grupo de administradores reducido y evitar el uso de las credenciales del usuario raíz

- Cumplimiento: los controles preventivos pueden ayudar a su empresa a cumplir con sus políticas, directrices y estándares. Entre los ejemplos se incluyen:
  - Bloquear configuraciones que sirvan como base de seguridad mínima
  - Implementar medidas de seguridad adicionales, como la autenticación multifactor
  - Evitar tareas y acciones no estándar que realizan los roles no aprobados

Proceso

La asignación de control preventivo es el proceso de asignar controles a los requisitos y utilizar políticas para implementar esos controles mediante la restricción, la desactivación o el bloqueo. Al asignar los controles, tenga en cuenta el efecto proactivo que tienen en el entorno, los recursos y los usuarios. Las siguientes son prácticas recomendadas para la asignación de controles:

- Los controles estrictos que prohíben una actividad se deben asignar a los entornos de producción en los que la acción requiera procesos de revisión, aprobación y cambio.
- Los entornos de desarrollo o confinados pueden tener menos controles preventivos para ofrecer la agilidad que se necesita para crear y probar.
- La clasificación de datos, el nivel de riesgo de un activo y la política de administración de riesgos determinan los controles preventivos.
- Asigne los marcos existentes como prueba de la conformidad con los estándares y reglamentos.
- Implemente controles preventivos por ubicación geográfica, entorno, cuentas, redes, usuarios, roles o recursos.

Casos de uso

Gestión de datos

Se crea un rol que puede acceder a todos los datos de una cuenta. Si hay datos confidenciales y cifrados, los privilegios excesivamente permisivos pueden suponer un riesgo, en función de los usuarios o grupos que puedan asumir ese rol. Mediante el uso de una política de claves en AWS Key Management Service (AWS KMS), puede controlar quién tiene acceso a la clave y puede descifrar los datos.

Escalado de privilegios

Si los permisos administrativos y de escritura se asignan de una forma demasiado amplia, el usuario puede eludir los límites de los permisos previstos y concederse privilegios adicionales. El usuario que crea y administra un rol puede asignar un límite de permisos, que define los privilegios máximos permitidos para el rol.

Bloqueo de carga de trabajo

Si su empresa no tiene una necesidad previsible de utilizar servicios específicos, habilite un política de control de servicio que limita los servicios que pueden operar en las cuentas de los miembros de una organización o restringe los servicios en función de la Región de AWS. Este control preventivo puede reducir el alcance del impacto si un agente de amenazas logra comprometer una cuenta de su organización y acceder a ella. Para obtener más información, consulte Políticas de control de servicios (p. 6).

Impacto en otras aplicaciones

Los controles preventivos pueden imponer el uso de servicios y características, como IAM, el cifrado y el registro, para cumplir con los requisitos de seguridad de las aplicaciones. También puede utilizar estos

controles para protegerse contra las vulnerabilidades al limitar las acciones que un agente de amenazas puede aprovechar debido a errores involuntarios o a una mala configuración.

Tecnología

Políticas de control de servicios

En AWS Organizations, las políticas de control de servicio (SCP) definen los permisos máximos disponibles para las cuentas de los miembros de una organización. Estas políticas ayudan a las cuentas a cumplir con las directrices de control de acceso de la organización. Tenga en cuenta lo siguiente al diseñar las SCP para su organización:

- Las SCP son controles preventivos porque definen y hacen cumplir los permisos máximos permitidos para los roles o usuarios de IAM en las cuentas de los miembros de la organización.
- Las SCP solo afectan a los roles o usuarios de IAM en las cuentas de los miembros de la organización. No afectan a los usuarios ni a los roles de la cuenta de administración de la organización.
- Puede hacer que una SCP sea más detallada al definir los permisos máximos para cada Región de AWS.

Límites de permisos de IAM

En AWS Identity and Access Management (IAM), el límite de permisos se utiliza para establecer los permisos máximos que una política basada en identidades puede conceder a una entidad de IAM (usuarios o roles). Un límite de permisos para una entidad le posibilita realizar solo las acciones que le permitan tanto sus políticas basadas en identidades como sus límites de permisos. Tenga en cuenta lo siguiente al establecer los límites de permisos:

- Puede utilizar una política administrada por AWS o una política administrada por el cliente a fin de configurar el límite para una entidad de IAM.
- Un límite de permisos no concede permisos por sí mismo. La política de límite de permisos limita los permisos que se conceden a la entidad de IAM.

Resultados empresariales

Ahorro de tiempo

- Al agregar la automatización después de configurar los controles preventivos, puede reducir la necesidad de intervención y reducir la frecuencia de los errores.
- El uso de los límites de permisos como control preventivo ayuda a los equipos de seguridad y de IAM a centrarse en tareas críticas, como la gobernanza y el soporte.

Conformidad normativa

- Es posible que las empresas deban cumplir con las normas internas o industriales. Pueden ser restricciones regionales, de usuarios y roles, o de servicio. Las SCP pueden ayudarlo a cumplir con las normas y evitar sanciones por infracción.

Reducción de riesgos

- Con el crecimiento, aumenta la cantidad de solicitudes para crear y administrar políticas y roles nuevos. Resulta cada vez más difícil comprender el contexto de lo que se requiere a fin de crear los permisos

para cada aplicación de forma manual. El establecimiento de controles preventivos actúa como punto de partida y ayuda a evitar que los usuarios realicen acciones no deseadas, incluso si se les ha concedido el acceso de forma accidental.

- La aplicación de controles preventivos a las políticas de acceso brinda una capa adicional para ayudar a proteger los datos y activos.

Controles de detección

Los controles de detección son controles de seguridad que se han diseñado para detectar, registrar y alertar después de que se produzca un evento. Los controles de detección son una parte fundamental de los marcos de gobernanza. Estas barreras de protección son una segunda línea de defensa, ya que le notifican los problemas de seguridad que han eludido los controles preventivos.

Por ejemplo, puede aplicar un control de detección para detectar y notificar si un bucket de Amazon Simple Storage Service (Amazon S3) pasa a ser de acceso público. Si bien es posible que disponga de controles preventivos que inhabiliten el acceso público a los buckets de S3 a nivel de cuenta y, posteriormente, inhabiliten el acceso a través de las SCP, un agente de amenazas puede eludir estos controles preventivos si inicia sesión como usuario administrativo. En estas situaciones, un control de detección puede alertarlo sobre los errores de configuración y la posible amenaza.

Objetivos

- Los controles de detección lo ayudan a mejorar los procesos de operaciones de seguridad y los procesos de calidad.
- Los controles de detección lo ayudan a cumplir con las obligaciones reglamentarias, legales o de conformidad.
- Los controles de detección ofrecen visibilidad a los equipos de operaciones de seguridad para responder a los problemas de seguridad, incluidas las amenazas avanzadas que eluden los controles preventivos.
- Los controles de detección pueden ayudarlo a identificar la respuesta adecuada a los problemas de seguridad y las posibles amenazas.

Proceso

Los controles de detección se implementan en dos fases. En primer lugar, debe configurar el sistema para registrar los eventos y los estados de los recursos en una ubicación centralizada, como los Registros de Amazon CloudWatch. Una vez que se establece el registro centralizado, estos se analizan para detectar anomalías que puedan indicar una amenaza. Cada análisis es un control que se asigna a sus requisitos y políticas originales. Por ejemplo, puede crear un control de detección que busque un patrón específico en los registros y genere una alerta si coincide. Los equipos de seguridad utilizan los controles de detección para mejorar su visibilidad general de las amenazas y los riesgos a los que su sistema podría estar expuesto.

Casos de uso

Detección de comportamiento sospechoso

Los controles de detección ayudan a identificar cualquier actividad anómala, como credenciales de usuarios privilegiados comprometidas o el acceso o la fuga de datos confidenciales. Estos controles son factores reactivos importantes que pueden ayudar a su empresa a identificar y comprender el alcance de la actividad anómala.

Detección de fraude

Estos controles ayudan a detectar e identificar una amenaza dentro de la empresa, como un usuario que elude las políticas y realiza transacciones no autorizadas.

Conformidad

Los controles de detección ayudan a cumplir los requisitos de conformidad, como las Normas de seguridad de datos del sector de las tarjetas de pago (PCI DSS), y pueden ayudar a prevenir el robo de identidad. Estos controles pueden ayudarlo a descubrir y proteger la información confidencial que se encuentra sujeta a la conformidad normativa, como la información de identificación personal.

Análisis automatizado

Los controles de detección pueden analizar de forma automática los registros para detectar anomalías y otros indicadores de actividad no autorizada.

Puede analizar de forma automática los registros de diferentes orígenes, como registros de AWS CloudTrail, Registro de flujo de la VPC y registros del sistema de nombres de dominio (DNS) para indicar una actividad potencialmente maliciosa. Para ayudar a la organización, agrupe las alertas de seguridad o los resultados de varios Servicios de AWS a una ubicación centralizada.

Tecnología

Un control de detección habitual consiste en implementar uno o más servicios de monitoreo, que pueden analizar los orígenes de datos, como los registros, para identificar las amenazas de seguridad. En la Nube de AWS, puede analizar orígenes como registros de AWS CloudTrail, registros de acceso a Amazon S3 y registros de flujo de Amazon Virtual Private Cloud para ayudar a detectar actividades inusuales. Los servicios de seguridad de AWS, como Amazon GuardDuty, Amazon Detective, AWS Security Hub y Amazon Macie, cuentan con funciones de monitoreo integradas.

GuardDuty y Security Hub

Amazon GuardDuty utiliza técnicas de inteligencia sobre amenazas, machine learning y detección de anomalías para monitorear de forma continua los orígenes de registro en busca de actividades maliciosas o no autorizadas. El panel de control brinda información sobre el estado en tiempo real de sus Cuentas de AWS y cargas de trabajo. Puede integrar GuardDuty con AWS Security Hub, un servicio de administración de la posición de seguridad en la nube que comprueba el cumplimiento de las prácticas recomendadas, agrega alertas y permite la corrección automática. GuardDuty envía los resultados a Security Hub como una forma de centralizar la información. Puede integrar aún más Security Hub con las soluciones de administración de eventos e información de seguridad (SIEM) para ampliar las capacidades de monitoreo y alerta de su organización.

Macie

Amazon Macie es un servicio de privacidad y seguridad de datos completamente administrado que utiliza machine learning y coincidencia de patrones para ayudar a descubrir y proteger los datos confidenciales en AWS. Las siguientes son algunas de las características y controles de detección disponibles en Macie:

- Macie inspecciona el inventario de bucket y todos los objetos almacenados en Amazon S3. Esta información se puede presentar en una única vista de panel, lo que brinda visibilidad y lo ayuda a evaluar la seguridad de los buckets.
- Para descubrir datos confidenciales, Macie utiliza identificadores de datos administrados e integrados y también admite identificadores de datos personalizados.

- Macie se integra de forma nativa con otros Servicios de AWS y herramientas. Por ejemplo, Macie publica los resultados como eventos de Amazon EventBridge, que se envían a Security Hub de forma automática.

Las siguientes son prácticas recomendadas para configurar los controles de detección en Macie:

- Habilite Macie en todas las cuentas. Al utilizar la característica de administración delegada, habilite a Macie en varias cuentas mediante AWS Organizations.
- Utilice Macie para evaluar la posición de seguridad de los buckets de S3 de sus cuentas. Esto ayuda a evitar la pérdida de datos y brinda visibilidad de la ubicación y el acceso a los datos. Para obtener más información, consulte Análisis de su posición de seguridad de Amazon S3 (documentación de Macie).
- Automatice la detección de datos confidenciales en sus buckets de S3 al ejecutar y programar tareas automatizadas de procesamiento y descubrimiento de datos. Esto inspecciona los buckets de S3 en busca de datos confidenciales de forma periódica.

AWS Config

AWS Config audita y registra la conformidad de los recursos de AWS. AWS Config descubre los recursos de AWS existentes y genera un inventario completo, junto con los detalles de configuración de cada recurso. Si hay algún cambio en la configuración, registra esos cambios y envía una notificación. Esto puede ayudarlo a detectar y revertir los cambios de infraestructura no autorizados. Puede utilizar las reglas administradas por AWS y crear reglas personalizadas.

Las siguientes son prácticas recomendadas para configurar los controles de detección en AWS Config:

- Habilite AWS Config para cada cuenta de miembro de la organización y para cada Región de AWS que contenga los recursos que desea proteger.
- Configure las alertas de Amazon Simple Notification Service (Amazon SNS) para cualquier cambio de configuración.
- Guarde los datos de configuración en un bucket de S3 y utilice Amazon Athena para analizarlos.
- Automatice la corrección de los recursos no conformes mediante el uso de la Automatización, una capacidad de AWS Systems Manager.
- Utilice EventBridge o Amazon SNS para configurar las notificaciones sobre recursos de AWS no conformes.

Trusted Advisor

Se puede utilizar AWS Trusted Advisor como un servicio para los controles de detección. Mediante una serie de comprobaciones, Trusted Advisor identifica las áreas en las que puede optimizar su infraestructura, mejorar el rendimiento y la seguridad, o reducir los costos. Trusted Advisor brinda recomendaciones basadas en las prácticas recomendadas de AWS que puede seguir para mejorar sus servicios y recursos. Los planes Business y Enterprise Support brindan acceso a todas las comprobaciones disponibles para los pilares del Marco de AWS Well-Architected.

Las siguientes son prácticas recomendadas para configurar los controles de detección en Trusted Advisor:

- Analice el resumen del nivel de comprobación.
- Implemente recomendaciones específicas de recursos para los estados de advertencia y error.
- Compruebe Trusted Advisor con frecuencia para revisar e implementar sus recomendaciones de forma activa.

Amazon Inspector

Amazon Inspector es un servicio automatizado de administración de vulnerabilidades que, después de habilitarse, analiza de forma continua las cargas de trabajo en busca de cualquier exposición de la red no deseada o vulnerabilidades de software. Contextualiza los resultados en una puntuación de riesgo que puede ayudarlo a determinar los próximos pasos, como corregir o confirmar el estado de conformidad.

Las siguientes son prácticas recomendadas para configurar los controles de detección en Amazon Inspector:

- Habilite Amazon Inspector en todas las cuentas e intégrelo en EventBridge y Security Hub para configurar los informes y las notificaciones de las vulnerabilidades de seguridad.
- Priorice las correcciones y otras medidas en función de la puntuación de riesgo de Amazon Inspector.

Resultados empresariales

Menos errores y esfuerzo humano

Puede lograr la automatización mediante el uso de la infraestructura como código (IaC). La automatización de la implementación y la configuración de los servicios y herramientas de monitoreo y corrección reduce el riesgo de errores manuales y la cantidad de tiempo y esfuerzo necesarios para escalar estos controles de detección. La automatización ayuda a desarrollar manuales de procedimientos de seguridad y reduce las operaciones manuales para los analistas de seguridad. Las revisiones periódicas ayudan a ajustar las herramientas de automatización y a iterar y mejorar los controles de detección de forma continua.

Medidas adecuadas contra las posibles amenazas

Registrar y analizar los eventos a partir de registros y métricas es fundamental para ganar visibilidad. Esto ayuda a los analistas a actuar ante los eventos de seguridad y las posibles amenazas para proteger las cargas de trabajo. La capacidad de identificar las vulnerabilidades que existen con rapidez ayuda a los analistas a tomar las medidas adecuadas para abordarlas y solucionarlas.

Mejor respuesta a incidentes y gestión de la investigación

La automatización de las herramientas de control de detección puede aumentar la velocidad de detección, investigación y recuperación. Las alertas y notificaciones automatizadas basadas en condiciones definidas permiten a los analistas de seguridad investigar y responder de manera adecuada. Estos factores de respuesta pueden ayudarlo a identificar y comprender el alcance de la actividad anómala.

Controles de respuesta

Los controles de respuesta son controles de seguridad que se han diseñado para corregir los eventos adversos o las desviaciones con respecto a su base de seguridad. Algunos ejemplos de controles de respuesta técnica incluyen la aplicación de revisiones a un sistema, el aislamiento de un virus, el cierre de un proceso o el reinicio de un sistema.

Objetivos

- Los controles de respuesta pueden ayudarlo a crear manuales de procedimientos para los tipos de ataques más comunes, como la suplantación de identidad o los ataques de fuerza bruta.
- Los controles de respuesta pueden implementar respuestas automatizadas a posibles problemas de seguridad.

- Los controles de respuesta pueden corregir de forma automática las acciones no deseadas o no aprobadas en recursos de AWS, como eliminar buckets de S3 no cifrados.
- Los controles de respuesta se pueden orquestar para que funcionen con controles preventivos y de detección, a fin de crear un enfoque integral y proactivo para abordar los posibles incidentes de seguridad.

Proceso

Los controles de detección son un requisito previo para establecer controles de respuesta. Debe poder detectar el problema de seguridad antes de poder solucionarlo. Luego, puede establecer una política o una respuesta al problema de seguridad. Por ejemplo, en caso de un ataque de fuerza bruta, se implementaría un proceso de corrección. Una vez que finalice el proceso de corrección, se puede automatizar y ejecutar como un script mediante un lenguaje de programación, como un script del intérprete de comandos.

Considere si el control de respuesta podría interrumpir una carga de trabajo de producción existente. Por ejemplo, si el control de seguridad de detección es Los buckets de S3 no deben ser de acceso público y la corrección es desactivar el acceso público a Amazon S3, esto podría tener consecuencias importantes para su empresa y sus clientes. Si el bucket de S3 brinda servicio a un sitio web público, desactivar el acceso público podría provocar una interrupción. Las bases de datos son un ejemplo similar. Si una base de datos no debe ser de acceso público a través de Internet, desactivar el acceso público podría afectar a la conectividad con la aplicación.

Casos de uso

- Respuesta automática a los eventos de seguridad detectados
- Corrección automática de las vulnerabilidades de seguridad detectadas
- Control de recuperación automatizado para reducir el tiempo de inactividad operativo

Tecnología

Security Hub

AWS Security Hub envía de forma automática todos los resultados nuevos y todas las actualizaciones de los resultados existentes a EventBridge como eventos. También puede crear acciones personalizadas que envíen los resultados y los resultados de información seleccionados a EventBridge. Puede configurar EventBridge para que responda a cada tipo de evento. El evento puede iniciar una función de AWS Lambda que realiza la acción correctiva.

AWS Config

AWS Config utiliza reglas para evaluar sus recursos de AWS y lo ayuda a corregir los recursos no conformes. AWS Config aplica la corrección mediante Automatización de AWS Systems Manager. En los documentos de la Automatización, define las acciones que desea realizar en los recursos que AWS Config determina que no son conformes. Después de crear los documentos de Automatización, puede utilizarlos en Systems Manager a través de la AWS Management Console o mediante las API. Puede elegir corregir de forma manual o automática los recursos no conformes.

Resultados empresariales

Minimizar la pérdida de datos

Tras un incidente de ciberseguridad, el uso de controles de seguridad de respuesta puede ayudar a minimizar la pérdida de datos y los daños al sistema o la red. Los controles de respuesta también pueden

ayudar a restaurar los sistemas y procesos empresariales importantes lo más rápido posible, lo que aumenta la resistencia de las cargas de trabajo.

Reducir los costos

La automatización reduce los costos asociados a los recursos humanos porque los miembros del equipo no tienen que responder de forma manual a los incidentes ni administrarlos caso por caso.

Pasos siguientes

Tras leer esta guía, debería familiarizarse con los tres tipos de controles de seguridad, comprender de qué manera forman parte de su marco de gobernanza de seguridad, y estar preparado para comenzar a implementar y automatizar los controles de seguridad en la Nube de AWS. Para obtener más información, recomendamos que repase las referencias que se incluyen en la sección Recursos (p. 15).

También le recomendamos que siga los pasos siguientes para evaluar la seguridad de su infraestructura en la nube y comenzar a implementar controles de seguridad:

1. Habilite y configure AWS Security Hub. Como práctica recomendada, sugerimos habilitar los controles de estándares disponibles. Para obtener más información, consulte Estándares y controles de seguridad (documentación de Security Hub).
2. Habilite y configure AWS Config. Para obtener más información, consulte Introducción (documentación de AWS Config).
3. Mediante los Servicios de AWS, como AWS Security Hub, Amazon Macie, AWS Config, AWS Trusted Advisor y Amazon Inspector, evalúe la infraestructura de su organización y cuentas, identifique las áreas que necesitan mejoras, y analice y recomiende estos servicios. Utilice la característica de control de seguridad de Security Hub a fin de generar una puntuación de seguridad para un estándar de seguridad. Para obtener más información, consulte Determinación de la puntuación de seguridad de un estándar de seguridad (documentación de Security Hub).
4. Implemente controles de seguridad preventivos, de detección y receptivos en función de las mejoras identificadas.
5. Realice una evaluación de seguridad de seguimiento para evaluar la eficacia de los controles de seguridad implementados. En AWS Security Hub, determine si la puntuación de seguridad ha mejorado. Realice iteraciones para mejorar o agregar controles de seguridad nuevos.
6. Establezca una frecuencia regular para realizar las evaluaciones de seguridad, por ejemplo, una vez al año.

Preguntas frecuentes

¿En qué debo enfocarme si tengo tiempo y recursos limitados y no puedo implementar todos estos tipos de controles?

Recomendamos implementar AWS Security Hub. Security Hub cuenta con un conjunto de controles de seguridad automatizados denominado Estándar de Prácticas recomendadas de seguridad básica de AWS (documentación de Security Hub). Se trata de un conjunto seleccionado de prácticas recomendadas de seguridad que administran expertos en seguridad de AWS. Puede ejecutar estos controles estándar de forma continua, siempre que se produzcan cambios en los recursos asociados, o de manera periódica, siguiendo un programa regular. Cada control cuenta con una puntuación de gravedad específica para ayudarlo a priorizar sus esfuerzos de remediación. Para obtener más información, consulte Ejecución de controles de seguridad (documentación de Security Hub).

Recursos

Documentación de AWS

- Arquitectura de referencia de seguridad de AWS (SRA de AWS)
- Perspectiva de seguridad de AWS Cloud Adoption Framework (AWS CAF)
- Prácticas recomendadas para seguridad, identidad y conformidad
- Respuesta de seguridad automatizada en AWS (Solución de AWS)
  - Página de inicio de la solución
  - Guía de implementación

Publicaciones de blog de AWS

- Guía de Identity: controles preventivos con AWS Identity, SCP
- Cómo implementar una política de control de servicio (SCP) de solo lectura para las cuentas en AWS Organizations
- Prácticas recomendadas para las políticas de control de servicio de AWS Organizations en un entorno de varias cuentas
- Mantener la conformidad mediante las políticas de control de servicio y asegurarse de que se apliquen siempre
- Cuándo y dónde utilizar los límites de permisos de IAM

Otros recursos

- Matriz de controles en la nube (CCM) (Cloud Security Alliance)
- Límites de permisos de ejemplo (GitHub)

Historial de documentos

En la siguiente tabla, se describen cambios significativos de esta guía. Si quiere recibir notificaciones de futuras actualizaciones, puede suscribirse a las notificaciones RSS.

Cambio	Descripción	Fecha
Publicación inicial (p. 16)	—	12 de diciembre de 2022

Glosario de las Recomendaciones de AWS

Los siguientes son términos de uso común en las estrategias, guías y patrones que se ofrecen en las Recomendaciones de AWS. Para sugerir entradas, utilice el enlace Enviar comentarios al final del glosario.

Términos de seguridad

control de acceso basado en atributos (ABAC)

: La práctica de crear permisos detallados basados en los atributos del usuario, como el departamento, el puesto de trabajo y el nombre del equipo. A fin de obtener más información, consulte ABAC para AWS en la documentación de AWS Identity and Access Management (IAM).

cifrado asimétrico

: Algoritmo de cifrado que utiliza un par de claves, una clave pública para el cifrado y una clave privada para el descifrado. Puede compartir la clave pública porque no se utiliza para el descifrado, pero el acceso a la clave privada debe estar sumamente restringido.

gráfico de comportamiento

: Una vista unificada e interactiva del comportamiento de los recursos y de las interacciones a lo largo del tiempo. Puede utilizar un gráfico de comportamiento con Amazon Detective para examinar los intentos de inicio de sesión fallidos, las llamadas sospechosas a la API y acciones similares. Para obtener más información, consulte Datos en un gráfico de comportamiento en la documentación de Detective.

cifrado de lado del cliente

: Cifrado de datos de forma local, antes de que el Servicio de AWS de destino los reciba.

paquete de conformidad

: Una colección de acciones correctivas y reglas de AWS Config que puede reunir para personalizar sus controles de seguridad y conformidad. Puede implementar un paquete de conformidad como una sola entidad en una región y Cuenta de AWS, o en toda una organización, mediante una plantilla YAML. Para obtener más información, consulte Paquetes de conformidad en la documentación de AWS Config.

datos en reposo

: Datos que están estacionarios en la red, como los datos que se encuentran almacenados.

clasificación de datos

: Un proceso para identificar y clasificar los datos de su red en función de su importancia y sensibilidad. Es un componente fundamental de cualquier estrategia de administración de riesgos de ciberseguridad porque lo ayuda a determinar los controles de protección y retención adecuados para los datos. La clasificación de datos es un componente del pilar de seguridad del Marco de AWS Well-Architected. Para obtener más información, consulte Clasificación de datos.

datos en tránsito

: Datos que se mueven de forma activa por la red, por ejemplo, entre los recursos de la red.

defensa en profundidad

: Un enfoque de seguridad de la información en el que se distribuyen cuidadosamente una serie de mecanismos y controles de seguridad en una red informática para proteger la confidencialidad, la

integridad y la disponibilidad de la red y de los datos que contiene. Cuando se adopta esta estrategia en AWS, se suman varios controles en diferentes capas de la estructura de AWS Organizations para ayudar a proteger los recursos.

administrador delegado

En AWS Organizations, un servicio compatible puede registrar una cuenta de miembro de AWS a fin de administrar las cuentas de la organización y los permisos para ese servicio. Esta cuenta se denomina administrador delegado para ese servicio. Para obtener más información y una lista de servicios compatibles, consulte Servicios que funcionan con AWS Organizations en la documentación de AWS Organizations.

control de detección

Un control de seguridad que se ha diseñado para detectar, registrar y alertar después de que se produzca un evento. Estos controles son una segunda línea de defensa, ya que lo advierten sobre los eventos de seguridad que han eludido los controles preventivos establecidos. Para obtener más información, consulte Controles de detección en Implementación de controles de seguridad en AWS.

clave de cifrado

Cadena criptográfica de bits aleatorios que se genera mediante un algoritmo de cifrado. Las claves pueden variar en longitud y cada una se ha diseñado para ser impredecible y única.

servicio de punto de conexión

Servicio que puede alojar en una nube privada virtual (VPC) para compartir con otros usuarios. Puede crear un servicio de punto de conexión con AWS PrivateLink y conceder permisos a otras Cuentas de AWS o a las entidades principales de IAM. Estas cuentas o entidades principales pueden conectarse a su servicio de punto de conexión de forma privada mediante la creación de puntos de conexión de VPC de interfaz. Para obtener más información, consulte Creación de un servicio de punto de conexión en la documentación de Amazon VPC.

cifrado de sobre

El proceso de cifrar una clave de cifrado con otra clave de cifrado. Para obtener más información, consulte Cifrado de sobre en la documentación de AWS Key Management Service (AWS KMS).

restricciones geográficas (bloqueo geográfico)

En Amazon CloudFront, una opción para impedir que los usuarios de países específicos accedan a las distribuciones de contenido. Puede utilizar una lista de permitidos o bloqueados para especificar los países aprobados y prohibidos. Para obtener más información, consulte Restricción de la distribución geográfica de su contenido en la documentación de CloudFront.

barrera de protección

Una regla de alto nivel que ayuda a regular los recursos, las políticas y la conformidad en todas las unidades organizativas (OU). Las barreras de protección preventivas aplican políticas para garantizar la alineación con los estándares de conformidad. Se implementan mediante políticas de control de servicios y límites de permisos de IAM. Las barreras de protección de detección detectan las vulneraciones de las políticas y los problemas de conformidad, y generan alertas para su corrección. Se implementan mediante el uso de AWS Config, AWS Security Hub, Amazon GuardDuty, AWS Trusted Advisor, Amazon Inspector y comprobaciones de AWS Lambda personalizadas.

políticas basadas en identidad

Una política asociada a una o más entidades principales de IAM que define sus permisos en el entorno de la Nube de AWS.

VPC entrante (de entrada)

En una arquitectura de varias cuentas de AWS, una VPC que acepta, inspecciona y enruta las conexiones de red desde fuera de una aplicación. La Arquitectura de referencia de seguridad de AWS

recomienda configurar su cuenta de red con VPC entrantes, salientes y de inspección para proteger la interfaz bidireccional entre su aplicación e Internet en general.

VPC de inspección

En una arquitectura de varias cuentas de AWS, una VPC centralizada que administra las inspecciones del tráfico de red entre VPC (en la misma o en diferentes Regiones de AWS), Internet y las redes en las instalaciones. La Arquitectura de referencia de seguridad de AWS recomienda configurar su cuenta de red con VPC entrantes, salientes y de inspección para proteger la interfaz bidireccional entre su aplicación e Internet en general.

privilegio mínimo

La práctica recomendada de seguridad que consiste en conceder los permisos mínimos necesarios para realizar una tarea. Para obtener más información, consulte Aplicar permisos de privilegio mínimo en la documentación de IAM.

cuenta miembro

Todas las Cuentas de AWS distintas de las cuentas de administración que forman parte de una organización en AWS Organizations. Una cuenta no puede pertenecer a más de una organización a la vez.

registro de seguimiento organizativo

Registro de seguimiento creado por AWS CloudTrail que registra todos los eventos para todas las Cuentas de AWS en una organización en AWS Organizations. Este registro de seguimiento se crea en cada Cuenta de AWS que forma parte de la organización y realiza un seguimiento de la actividad en cada cuenta. Para obtener más información, consulte Creación de un registro de seguimiento para una organización en la documentación de CloudTrail.

VPC saliente (de salida)

En una arquitectura de varias cuentas de AWS, una VPC que gestiona las conexiones de red que se inician desde una aplicación. La Arquitectura de referencia de seguridad de AWS recomienda configurar su cuenta de red con VPC entrantes, salientes y de inspección para proteger la interfaz bidireccional entre su aplicación e Internet en general.

control de acceso de origen (OAC)

En CloudFront, una opción mejorada para restringir el acceso a su contenido de Amazon Simple Storage Service (Amazon S3). El OAC es compatible con todos los buckets de S3 en todas las Regiones de AWS, cifrado del servidor con AWS KMS (SSE-KMS), y solicitudes `PUT` y `DELETE` dinámicas al bucket de S3.

identidad de acceso de origen (OAI)

En CloudFront, una opción para restringir el acceso al contenido de Amazon S3. Cuando utiliza la OAI, CloudFront crea una entidad principal con la que Amazon S3 puede autenticarse. Las entidades principales autenticadas solo pueden acceder al contenido de un bucket de S3 a través de una distribución de CloudFront específica. Consulte también el OAC (p. 19), que proporciona un control de acceso más detallado y mejorado.

límite de permisos

Una política de administración de IAM que se adjunta a las entidades principales de IAM para establecer los permisos máximos que puede tener el usuario o el rol. Para obtener más información, consulte Límites de permisos en la documentación de IAM.

política

Un objeto que se puede definir permisos (consulte políticas basadas en identidad (p. 18)), especificar las condiciones de acceso (consulte política basada en recursos (p. 20)) o definir los permisos máximos para todas las cuentas de una organización en AWS Organizations (consulte política de control de servicios (p. 20)).

control preventivo

Un control de seguridad diseñado para evitar que ocurra un evento. Estos controles son la primera línea de defensa para evitar el acceso no autorizado o los cambios no deseados en la red. Para obtener más información, consulte Controles preventivos en Implementación de controles de seguridad en AWS.

principal

Una entidad de AWS que puede realizar acciones y obtener acceso a los recursos. Esta entidad suele ser un usuario raíz de una Cuenta de AWS, un rol de IAM o un usuario. Para obtener más información, consulte Entidad principal en Términos y conceptos de roles en la documentación de IAM.

ransomware

Software malicioso que se ha diseñado para bloquear el acceso a un sistema informático o a los datos hasta que se efectúe un pago.

política basada en recursos

Una política asociada a un recurso, como un bucket de Amazon S3, un punto de conexión o una clave de cifrado. Este tipo de política especifica a qué entidades principales se les permite el acceso, las acciones compatibles y cualquier otra condición que deba cumplirse.

control receptivo

Un control de seguridad que se ha diseñado para corregir los eventos adversos o las desviaciones con respecto a su base de seguridad. Para obtener más información, consulte Controles receptivos en Implementación de controles de seguridad en AWS.

SAML 2.0

Un estándar abierto que utilizan muchos proveedores de identidades (IdP). Esta característica permite el inicio de sesión único (SSO) federado a fin de que los usuarios puedan iniciar sesión en la AWS Management Console o llamar a la API de AWS sin necesidad de crear un usuario de IAM para cada persona de la organización. Para obtener más información sobre la federación basada en SAML 2.0, consulte Acerca de la federación basada en SAML 2.0 en la documentación de IAM.

control de seguridad

Barrera de protección técnica o administrativa que impide, detecta o reduce la capacidad de un agente de amenazas para aprovechar una vulnerabilidad de seguridad. Existen tres tipos principales de controles de seguridad: preventivo (p. 20), de detección (p. 18) y receptivo (p. 20).

refuerzo de la seguridad

Proceso de reducir la superficie expuesta a ataques para hacerla más resistente a los ataques. Esto puede incluir acciones, como la eliminación de los recursos que ya no se necesitan, la implementación de prácticas recomendadas de seguridad consistente en conceder privilegios mínimos o la desactivación de características innecesarias en los archivos de configuración.

sistema de información sobre seguridad y administración de eventos (SIEM)

Herramientas y servicios que combinan sistemas de administración de información sobre seguridad (SIM) y de administración de eventos de seguridad (SEM). Un sistema de SIEM recopila, monitorea y analiza los datos de servidores, redes, dispositivos y otras fuentes para detectar amenazas y brechas de seguridad y generar alertas.

cifrado del servidor

Cifrado de los datos en su destino, por parte del Servicio de AWS que los recibe.

política de control de servicio (SCP)

Una política que proporciona un control centralizado de los permisos de todas las cuentas de una organización en AWS Organizations. Las SCP definen barreras de protección o establecen límites a las acciones que un administrador puede delegar en los usuarios o roles. Puede utilizar las SCP

como listas de permitidos o rechazados, para especificar qué servicios o acciones se encuentra permitidos o prohibidos. Para obtener más información, consulte Políticas de control de servicio en la documentación de AWS Organizations.

modelo de responsabilidad compartida

Modelo que describe la responsabilidad que comparte con AWS en cuanto a la conformidad y la seguridad en la nube. AWS es responsable de la seguridad de la nube, mientras que usted es responsable de la seguridad en la nube. Para obtener más información, consulte el Modelo de responsabilidad compartida.

cifrado simétrico

Un algoritmo de cifrado que utiliza la misma clave para cifrar y descifrar los datos.

acceso de confianza

Concesión de permisos a un servicio que especifique para realizar tareas en su organización en AWS Organizations y en sus cuentas en su nombre. El servicio de confianza crea un rol vinculado al servicio en cada cuenta, cuando ese rol es necesario, para realizar las tareas de administración por usted. Para obtener más información, consulte Uso de AWS Organizations con otros servicios de AWS en la documentación de AWS Organizations.

carga de trabajo

Conjunto de recursos y código que ofrece valor comercial, como una aplicación orientada al cliente o un proceso de backend.