Creación de un programa de gestión de vulnerabilidades escalable sobre AWS

AWS Guía prescriptiva

AWS Guía prescriptiva: Creación de un programa de gestión de vulnerabilidades escalable sobre AWS

Table of Contents

Creación de un programa de gestión de vulnerabilidades escalable en AWS

Anna McAbee y Megan O'Neil, Amazon Web Services ()AWS

Octubre de 2023 (historial del documento)

Según la tecnología subyacente que utilice, una variedad de herramientas y análisis pueden generar resultados de seguridad en un entorno en la nube. Si no se implementan procesos para gestionar estos resultados, pueden empezar a acumularse y, a menudo, dar lugar a miles o decenas de miles de resultados en un breve periodo de tiempo. Sin embargo, con un programa estructurado de administración de vulnerabilidades y una operacionalización adecuada de las herramientas, su organización puede gestionar y clasificar una gran cantidad de resultados de diversos orígenes.

La administración de vulnerabilidades se centra en descubrir, priorizar, evaluar, corregir y notificar las vulnerabilidades. La administración de revisiones, por otro lado, se centra en aplicar revisiones en el software o actualizarlo para eliminar o corregir las vulnerabilidades de seguridad. La administración de revisiones es solo un aspecto de la administración de vulnerabilidades. Por lo general, se recomienda establecer un patch-in-place proceso (también conocido como mitigate-in-placeproceso) para abordar situaciones críticas en las que se debe aplicar el parche ahora, y un proceso estándar que ejecute de forma regular para lanzar Amazon Machine Images (AMIs), contenedores o paquetes de software parcheados. Estos procesos ayudan a preparar a su organización para responder rápidamente a una vulnerabilidad de día cero. Para los sistemas críticos de un entorno de producción, utilizar un patch-in-place proceso puede ser más rápido y fiable que implementar una nueva AMI en toda la flota. En el caso de las revisiones programadas con regularidad, como las revisiones del sistema operativo (SO) y del software, le recomendamos que las cree y pruebe mediante procesos de desarrollo estándar, como haría con cualquier cambio de nivel de software. Esto proporciona una mayor estabilidad para los modos de funcionamiento estándar. Puede utilizar Patch Manager, una funcionalidad u otros productos de terceros como patch-in-place soluciones. AWS Systems Manager Para obtener más información sobre el uso del Administrador de parches, consulte Patch management en AWS Cloud Adoption Framework: Operations Perspective. Además, puede utilizar EC2 Image Builder para automatizar la creación, la administración y el despliegue de imágenes personalizadas up-to-date y de servidor.

La creación de un programa de gestión de vulnerabilidades escalable AWS implica gestionar las vulnerabilidades tradicionales de software y red, además de los riesgos de configuración de la nube. Un riesgo de configuración de la nube, como un bucket de Amazon Simple Storage Service (Amazon

S3) sin cifrar, debería seguir un proceso de clasificación y corrección similar al de una vulnerabilidad de software. En ambos casos, el equipo de aplicaciones debe ser el propietario y responsable de la seguridad de la aplicación, incluida la infraestructura subyacente. Esta distribución de la propiedad es clave para un programa de administración de vulnerabilidades eficaz y escalable.

En esta guía se explica cómo agilizar la identificación y la corrección de las vulnerabilidades para reducir el riesgo general. Utilice las siguientes secciones para crear su programa de administración de vulnerabilidades e iterar en él:

1. Preparación: prepare a su personal, los procesos y la tecnología para identificar, evaluar y corregir las vulnerabilidades de su entorno.
2. Clasificación y corrección: remita los resultados de seguridad a las partes interesadas pertinentes, identifique la medida correctiva adecuada y, a continuación, tome dicha medida.
3. Notificación y mejora: utilice los mecanismos de notificación para identificar las oportunidades de mejora y, a continuación, itere en su programa de administración de vulnerabilidades.

La creación de un programa de administración de vulnerabilidades en la nube suele implicar iteraciones. Dé prioridad a las recomendaciones de esta guía y revisite periódicamente sus tareas pendientes para mantenerse al día con los cambios tecnológicos y los requisitos de su empresa.

Destinatarios previstos

Esta guía está destinada a grandes empresas que cuentan con tres equipos principales responsables de los hallazgos relacionados con la seguridad: un equipo de seguridad, un centro de excelencia (CCoE) o equipo de nube y equipos de aplicaciones (o desarrolladores). En esta guía se utilizan los modelos operativos empresariales más comunes y se basa en esos modelos operativos para permitir una respuesta más eficiente ante los resultados de seguridad y mejorar los resultados de seguridad. Las organizaciones que lo utilizan AWS pueden tener estructuras y modelos operativos diferentes; sin embargo, puede modificar muchos de los conceptos de esta guía para adaptarlos a diferentes modelos operativos y organizaciones más pequeñas.

Objetivos

Esta guía puede ayudarlos a usted y a su organización a lo siguiente:

- Desarrollar políticas para agilizar la administración de vulnerabilidades y garantizar la responsabilidad.

- Establecer mecanismos para distribuir la responsabilidad en materia de seguridad entre los equipos de aplicaciones.
- Configure Servicios de AWS según las mejores prácticas para una gestión escalable de vulnerabilidades
- Distribuir la propiedad de los resultados de seguridad.
- Establecer mecanismos para notificar el programa de administración de vulnerabilidades e iterar en él.
- Mejorar la visibilidad de los resultados de seguridad y mejorar la postura general de seguridad.

Preparación del programa de administración de vulnerabilidades escalable

Prepararse para crear un programa de administración de vulnerabilidades escalable implica capacitar a las personas, desarrollar procesos e implementar la tecnología adecuada de acuerdo con las prácticas recomendadas. Las personas, los procesos y la tecnología son igual de importantes para que un programa de administración de vulnerabilidades sea eficaz y es necesario integrarlos estrechamente para administrar las vulnerabilidades a escala.

En esta sección de la guía se revisan las medidas fundamentales que puede tomar para preparar su programa de administración de vulnerabilidades escalable en AWS.

Temas

Definición de un plan de administración de vulnerabilidades

El primer paso a la hora de preparar su programa de administración de vulnerabilidades en la nube consiste en definir su plan de administración de vulnerabilidades. Este plan incluye las políticas y los procesos que sigue su organización. Este plan debe estar documentado y ser accesible para todas las partes interesadas. Un plan de administración de vulnerabilidades es un documento de alto nivel que normalmente incluye las siguientes secciones:

- Objetivos y alcance: describa los objetivos, las funciones y el alcance de la administración de vulnerabilidades.
- Roles y responsabilidades: indique las partes interesadas en la administración de vulnerabilidades y detalle sus responsabilidades.

- Definiciones de gravedad y priorización de las vulnerabilidades: determine cómo clasificar la gravedad de una vulnerabilidad y cómo priorizarla.
- Acuerdos de nivel de servicio (SLAs) para la remediación: para cada nivel de gravedad, defina el tiempo máximo del que dispone el propietario de la remediación para resolver un problema de seguridad. Dado que el cumplimiento de los SLA es una parte integral de contar con un programa de gestión de vulnerabilidades eficaz y escalable, considere cómo comprobar si los está cumpliendo. SLAs
- Proceso de excepciones: detalle el proceso de presentación, aprobación y actualización de las excepciones. Este proceso debe garantizar que las excepciones sean legítimas, tengan un límite de tiempo y se rastreen.
- Orígenes de información sobre vulnerabilidades: indique los orígenes o las herramientas que generan resultados de seguridad. Para obtener más información sobre Servicios de AWS estas posibles fuentes de hallazgos de seguridad, consulta Configure AWS los servicios de seguridad esta guía.

Aunque estas secciones son comunes en empresas de diferentes tamaños y de diferentes sectores, el plan de administración de vulnerabilidades de cada organización es único. Debe elaborar el plan de administración de vulnerabilidades que mejor se adapte a su organización. Espere iterar el plan con el tiempo para incorporar las lecciones aprendidas y las tecnologías en evolución.

Distribución de la propiedad de seguridad

El modelo de responsabilidad AWS compartida define cómo AWS y sus clientes comparten la responsabilidad por la seguridad y el cumplimiento de la nube. En este modelo, AWS protege la infraestructura en la que se ejecutan todos los servicios que se ofrecen en él Nube de AWS, y AWS los clientes son responsables de proteger sus datos y aplicaciones.

Puede reflejar este modelo en su organización y distribuir las responsabilidades entre sus equipos de la nube y de aplicaciones. Esto lo ayuda a escalar sus programas de seguridad en la nube de forma más eficaz, ya que los equipos de aplicaciones se hacen cargo de determinados aspectos de seguridad de sus aplicaciones. La interpretación más sencilla del Modelo de responsabilidad compartida es que si tiene acceso para configurar el recurso, es responsable de la seguridad de ese recurso.

Una parte clave de la distribución de las responsabilidades de seguridad entre los equipos de aplicaciones consiste en crear herramientas de seguridad de autoservicio que ayuden a los equipos

de aplicaciones a automatizar. Inicialmente, esto puede ser un esfuerzo conjunto. El equipo de seguridad puede traducir los requisitos de seguridad en herramientas de análisis de código y, a continuación, los equipos de aplicaciones pueden usar esas herramientas para crear y compartir soluciones con su comunidad interna de desarrolladores. Esto contribuye a aumentar la eficiencia de otros equipos que deben cumplir con requisitos de seguridad similares.

En la siguiente tabla se describen los pasos para distribuir la propiedad entre los equipos de aplicaciones y se proporcionan ejemplos.

Paso	Action	Ejemplo
1	Definición de sus requisitos de seguridad: ¿qué intenta lograr? Esto puede provenir de un estándar de seguridad o de un requisito de cumplimiento.	Un ejemplo de requisito de seguridad es el acceso con privilegio mínimo para las identidades de las aplicaciones.
2	Enumeración de los controles de un requisito de seguridad: ¿qué significa realmente este requisito desde el punto de vista del control? ¿Qué debo hacer para lograrlo?	Para lograr el privilegio mínimo para las identidades de las aplicaciones, a continuación se muestran dos ejemplos de controles: • Utilice funciones AWS Identity and Access Management (IAM) • No usar comodines en las políticas de IAM.
3	Documentación de pautas para los controles: con estos controles, ¿qué pautas puede proporcionar a un desarrollador para ayudarlo a cumplir con el control?	En primer lugar, puede empezar por documentar políticas de ejemplo sencillas, tales como políticas de IAM y políticas de bucket de Amazon Simple Storage Service (Amazon S3) seguras

Paso	Action	Ejemplo
		y no seguras. A continuación, puede incrustar soluciones de análisis de políticas en las canalizaciones de integración continua y entrega continua (CI/CD), por ejemplo, mediante reglas de AWS Config para la evaluación proactiva.
4	Desarrollo de artefactos reutilizables: con estas pautas, ¿podrá hacerlo aún más fácil y desarrollar artefactos reutilizables para los desarrolladores?	Puede crear infraestructura como código (IaC) para implementar políticas de IAM que sigan el principio de privilegio mínimo. Puede almacenar estos artefactos reutilizables en un repositorio de código.

Es posible que el autoservicio no funcione para todos los requisitos de seguridad, pero puede funcionar en escenarios estándar. Al seguir estos pasos, las organizaciones pueden capacitar a sus equipos de aplicaciones para que se ocupen de una mayor parte de sus propias responsabilidades de seguridad de forma escalable. En general, el modelo de responsabilidad distribuida conduce a prácticas de seguridad más colaborativas en muchas organizaciones.

Desarrollo de un programa de divulgación de vulnerabilidades

Para defense-in-depthadoptar un enfoque de la gestión de vulnerabilidades, cree un programa de divulgación de vulnerabilidades para que las personas de su organización o ajenas a ella puedan denunciar las vulnerabilidades o los riesgos de seguridad.

Para las personas de su organización, establezca un proceso para enviar los riesgos o las vulnerabilidades. Esto se puede hacer mediante un sistema de tickets o por correo electrónico. Independientemente del proceso que elija, es fundamental que sus empleados conozcan el proceso y puedan enviar fácilmente cualquier vulnerabilidad o riesgo al que se enfrenten.

Para las personas ajenas a su organización, establezca una página web externa para enviar las posibles vulnerabilidades de seguridad. A modo de ejemplo, consulte la página web AWS Vulnerability Reporting. Esta página web también debe contener directrices de divulgación para ayudar a proteger los datos y los activos de su organización. Un programa de divulgación de vulnerabilidades no debe fomentar actividades potencialmente dañinas, por lo que es esencial contar con una política clara con directrices. Crear un programa de divulgación responsable y maduro es un objetivo por el que hay que esforzarse a medida que vaya madurando el programa. La mayoría de las organizaciones no comienza con un programa de divulgación externo, y hacerlo bien lleva tiempo.

Prepare su AWS entorno

Antes de implementar cualquier herramienta de administración de vulnerabilidades, asegúrese de que su entorno de AWS esté diseñado para admitir un programa de administración de vulnerabilidades escalable. La estructura de sus políticas de etiquetado Cuentas de AWS y las de su organización puede simplificar el proceso de creación de un programa de gestión de vulnerabilidades escalable.

Desarrolle una estructura Cuenta de AWS

AWS Organizationsayuda a gestionar y gobernar un AWS entorno de forma centralizada a medida que su empresa crece y amplía sus AWS recursos. Una organización los AWS Organizations consolida Cuentas de AWS en grupos lógicos, o unidades organizativas, para que pueda administrarlos como una sola unidad. La administración de AWS Organizations se efectúa desde una cuenta dedicada, denominada cuenta de administración. Para obtener más información, consulte Terminología y conceptos de AWS Organizations.

Le recomendamos que administre su entorno de AWS múltiples cuentas en. AWS Organizations Esto ayuda a crear un inventario completo de las cuentas y los recursos de su empresa. Este inventario completo de activos es un aspecto fundamental de la administración de vulnerabilidades. Los equipos de aplicaciones no deben utilizar cuentas que estén fuera de la organización.

AWS Control Towerle ayuda a configurar y gobernar un entorno de AWS múltiples cuentas, siguiendo las mejores prácticas prescriptivas. Si aún no ha establecido un entorno de múltiples cuentas, AWS Control Tower es un buen punto de partida.

Recomendamos utilizar la estructura de cuentas dedicada y las prácticas recomendadas que se describen en la Arquitectura AWS de referencia de seguridad (AWS SRA). La cuenta de

herramientas de seguridad debe servir como administradora delegada de sus servicios de seguridad. Más adelante en esta guía encontrará más información sobre la configuración de las herramientas de administración de vulnerabilidades en esta cuenta. Aloje aplicaciones en cuentas dedicadas en la unidad organizativa (UO) de cargas de trabajo. Esto establece un fuerte aislamiento en el nivel de carga de trabajo y límites de seguridad explícitos para cada aplicación. Para obtener información sobre los principios de diseño y las ventajas de utilizar un enfoque de cuentas múltiples, consulte Cómo organizar su AWS entorno con varias cuentas (documentoAWS técnico).

Disponer de una estructura de cuentas intencionada y administrar de forma centralizada los servicios de seguridad desde una cuenta dedicada son aspectos fundamentales de un programa de administración de vulnerabilidades escalable.

Definición, implementación y aplicación de etiquetas

Las etiquetas son pares clave-valor que actúan como metadatos para organizar los recursos. AWS Para obtener más información, consulte Etiquetado de los recursos de AWS. Puede utilizar etiquetas para proporcionar un contexto empresarial, como la unidad de negocio, el propietario de la aplicación, el entorno y el centro de costos. En la siguiente tabla se muestra un conjunto de etiquetas de ejemplo.

Clave	Valor
BusinessUnit	HumanResources
CostCenter	CC101
ApplicationTeam	HumanResourcesTechnology
Entorno	Producción

Las etiquetas pueden ayudarlo a priorizar los resultados. Por ejemplo, pueden ayudarlo a lo siguiente:

- Identificar al propietario de un recurso responsable de aplicar una revisión a una vulnerabilidad.
- Hacer un seguimiento de qué aplicaciones o unidades de negocio tienen una gran número de resultados.

- Escalar la gravedad de los resultados de determinadas clasificaciones de datos, como la información de identificación personal (PII) o los datos de la industria de tarjetas de pago (PCI).
- Identificar el tipo de datos del entorno, como los datos de prueba en un entorno de desarrollo de nivel inferior o los datos de producción.

Para ayudarle a lograr un etiquetado eficaz a gran escala, siga las instrucciones que se indican en Cómo crear una estrategia de etiquetado, en el documento técnico Best Practices for Tagging AWS Resources (documento técnico).AWS

AWS Supervise los boletines de seguridad

Recomendamos encarecidamente supervisar los boletines de seguridad de AWS de forma regular y frecuente. Los boletines de seguridad pueden notificarle cualquier nueva vulnerabilidad relacionada con la seguridad, los servicios afectados y las actualizaciones aplicables. También puede suscribirse a una fuente RSS para recibir los boletines de seguridad y crear un proceso para ingerir y abordar estos boletines como parte de su programa de administración de vulnerabilidades.

Configure AWS los servicios de seguridad

AWS ofrece una variedad de servicios de seguridad diseñados para ayudar a proteger su AWS entorno. Para su programa de gestión de vulnerabilidades, le recomendamos que habilite lo siguiente Servicios de AWS en cada cuenta:

- Amazon GuardDuty ayuda a detectar las amenazas activas en su entorno. Un GuardDuty hallazgo podría ayudarle a identificar una vulnerabilidad desconocida que se ha explotado en su entorno. También podría ayudarlo a comprender los efectos de una vulnerabilidad sin revisiones.
- AWS Healthproporciona una visibilidad continua del rendimiento de sus recursos y de la disponibilidad de sus Servicios de AWS cuentas.
- AWS Identity and Access Management Access Analyzer analiza las políticas basadas en recursos de su entorno de AWS para identificar los recursos que se comparten con una entidad externa. Esto puede ayudarlo a identificar las vulnerabilidades asociadas con el acceso no deseado a sus recursos y datos. Para cada instancia de un recurso compartido fuera de su cuenta, el Analizador de acceso de IAM genera un resultado.
- Amazon Inspector es un servicio de gestión de vulnerabilidades que analiza continuamente sus AWS cargas de trabajo en busca de vulnerabilidades de software y exposición no intencionada a la red.

- AWS Security Hub CSPMle ayuda a comprobar su AWS entorno con respecto a los estándares del sector de la seguridad y puede identificar los riesgos de configuración de la nube. También proporciona una visión completa del estado de su AWS seguridad mediante la agregación de los resultados de otros servicios de AWS seguridad y herramientas de seguridad de terceros.

En esta sección se explica cómo activar y configurar Amazon Inspector y Security Hub CSPM para ayudarle a establecer un programa de gestión de vulnerabilidades escalable.

Uso de Amazon Inspector en el programa de administración de vulnerabilidades

Amazon Inspector es un servicio de administración de vulnerabilidades que analiza continuamente las instancias de Amazon Elastic Compute Cloud (Amazon EC2), las imágenes de contenedores de Amazon Elastic Container Registry (Amazon ECR) y las funciones de AWS Lambda en busca de vulnerabilidades de software y exposiciones de la red no deseadas. Puede utilizar Amazon Inspector para obtener visibilidad y priorizar la resolución de las vulnerabilidades de software en sus AWS entornos.

Amazon Inspector evalúa su entorno de forma continua durante todo el ciclo de vida de sus recursos. Vuelve a analizar automáticamente los recursos en respuesta a los cambios que podrían introducir una nueva vulnerabilidad. Por ejemplo, se vuelve a analizar cuando se instala un paquete nuevo en una instancia de EC2, cuando se instala una revisión o cuando se publica una nueva entrada sobre vulnerabilidades y exposiciones comunes (CVE) que afecta al recurso. Cuando Amazon Inspector detecta una vulnerabilidad o una ruta de red abierta, produce un resultado que puede investigar. El resultado proporciona información completa sobre la vulnerabilidad, entre la que se incluye lo siguiente:

- Puntuación de riesgo de Amazon Inspector
- Puntuación del sistema de clasificación de vulnerabilidades comunes (CVSS)
- Recurso afectado
- Datos de inteligencia de vulnerabilidades sobre el CVE de Amazon, Recorded Future y Cybersecurity and Infrastructure Security Agency (CISA)
- Recomendaciones de corrección

Para obtener instrucciones sobre la configuración de Amazon Inspector, consulte Getting started with Amazon Inspector. En el paso de activación de Amazon Inspector de este tutorial se proporcionan

dos opciones de configuración: un entorno de una cuenta independiente y un entorno de varias cuentas. Le recomendamos que utilice la opción de entorno de varias cuentas si desea monitorizar varias cuentas Cuentas de AWS que sean miembros de una organización. AWS Organizations

Cuando configura Amazon Inspector para un entorno de varias cuentas, designa una cuenta de la organización como administradora delegada de Amazon Inspector. El administrador delegado puede administrar los resultados y algunos parámetros para los miembros de la organización. Por ejemplo, el administrador delegado puede ver detalles de resultados agregados de todas las cuentas de miembros, habilitar o deshabilitar análisis de cuentas de miembros y revisar los recursos analizados. La AWS SRA recomienda crear una cuenta de Security Tooling y utilizarla como administrador delegado de Amazon Inspector.

Utilícela AWS Security Hub CSPM en su programa de gestión de vulnerabilidades

La creación de un programa de gestión de vulnerabilidades escalable AWS implica gestionar las vulnerabilidades tradicionales de software y red, además de los riesgos de configuración de la nube. AWS Security Hub CSPMle ayuda a comparar su AWS entorno con los estándares del sector de la seguridad y puede identificar los riesgos de configuración de la nube. Security Hub CSPM también proporciona una visión integral del estado de su seguridad al agregar los hallazgos AWS de seguridad de otros servicios de seguridad y herramientas de AWS seguridad de terceros.

En las siguientes secciones, ofrecemos prácticas recomendadas y recomendaciones para configurar Security Hub CSPM para respaldar su programa de gestión de vulnerabilidades:

- Configuración de Security Hub (CSPM)
- Habilitación de los estándares CSPM de Security Hub
- Gestión de las conclusiones del CSPM de Security Hub
- Agregación de los resultados de otros servicios y herramientas de seguridad

Configuración de Security Hub (CSPM)

Para obtener instrucciones sobre la configuración, consulte Setting up AWS Security Hub CSPM. Para usar Security Hub CSPM, debe habilitarlo. AWS Config Para obtener más información, consulte Habilitación y configuración AWS Config en la documentación de Security Hub CSPM.

Si está integrado con AWS Organizations, desde la cuenta de administración de la organización, designa una cuenta para que sea el administrador delegado de CSPM de Security Hub. Para obtener instrucciones, consulte Designación del administrador delegado de CSPM de Security Hub. La AWS SRA recomienda crear una cuenta de Security Tooling y utilizarla como administrador delegado de CSPM de Security Hub.

El administrador delegado tiene acceso automáticamente para configurar Security Hub CSPM para todas las cuentas de los miembros de la organización y para ver los hallazgos asociados a esas cuentas. Le recomendamos que habilite AWS Config Security Hub CSPM en todos Regiones de AWS y cada uno de sus. Cuentas de AWS Puede configurar Security Hub CSPM para tratar automáticamente las nuevas cuentas de la organización como cuentas de miembros de Security Hub CSPM. Consulte las instrucciones en Managing member accounts that belong to an organization.

Habilitación de los estándares CSPM de Security Hub

Security Hub CSPM genera hallazgos mediante la ejecución de comprobaciones de seguridad automatizadas y continuas contra los controles de seguridad. Las verificaciones están asociadas a uno o más estándares de seguridad. Los controles ayudan a determinar si se cumplen los requisitos de un estándar.

Al habilitar un estándar en Security Hub CSPM, Security Hub CSPM habilita automáticamente los controles que se aplican al estándar. Security Hub CSPM utiliza AWS Config reglas para realizar la mayoría de las comprobaciones de seguridad de los controles. Puede activar o desactivar los estándares CSPM de Security Hub en cualquier momento. Para obtener más información, consulte Controles y estándares de seguridad en. AWS Security Hub CSPM Para obtener una lista completa de estándares, consulte la referencia de estándares CSPM de Security Hub.

Si su organización aún no tiene un estándar de seguridad preferido, le recomendamos que utilice el estándar Prácticas recomendadas de seguridad básica de AWS (FSBP). Este estándar está diseñado para detectar cuándo Cuentas de AWS y los recursos se desvían de las mejores prácticas de seguridad. AWS selecciona este estándar y lo actualiza periódicamente para incluir nuevas funciones y servicios. Tras evaluar los resultados de FSBP, considere la posibilidad de habilitar otros estándares.

Gestión de las conclusiones del CSPM de Security Hub

Security Hub CSPM ofrece varias funciones que le ayudan a abordar grandes volúmenes de hallazgos de toda la organización y a comprender el estado de seguridad de su AWS entorno. Para

ayudarle a gestionar los hallazgos, le recomendamos que habilite las dos funciones siguientes de CSPM de Security Hub:

- Utilice la agregación entre regiones para agregar los hallazgos, encontrar actualizaciones, información, controlar los estados de cumplimiento y las puntuaciones de seguridad de varias regiones de agregación Regiones de AWS a una sola región de agregación.
- Use los resultados de verificaciones consolidados para reducir el ruido de los resultados mediante la eliminación de los resultados duplicados. Cuando los hallazgos de control consolidados están activados en su cuenta, Security Hub CSPM genera un único hallazgo nuevo o una actualización de hallazgos para cada comprobación de seguridad de un control, incluso si un control se aplica a varios estándares habilitados.

Agregación de los resultados de otros servicios y herramientas de seguridad

Además de generar hallazgos de seguridad, puede usar Security Hub CSPM para agregar datos de búsqueda de varias Servicios de AWS soluciones de seguridad de terceros compatibles. Esta sección se centra en el envío de los resultados de seguridad a Security Hub CSPM. En la siguiente sección Preparación para asignar resultados de seguridad, se explica cómo puede integrar Security Hub CSPM con productos que puedan recibir las conclusiones del Security Hub CSPM.

Hay muchos Servicios de AWS productos de terceros y soluciones de código abierto disponibles que puede integrar con Security Hub CSPM. Si acaba de empezar, le recomendamos que haga lo siguiente:

1. Habilitar la integración Servicios de AWS: la mayoría de Servicio de AWS las integraciones que envían los resultados al Security Hub CSPM se activan automáticamente después de habilitar tanto el Security Hub CSPM como el servicio integrado. Para su programa de gestión de vulnerabilidades, le recomendamos que habilite Amazon Inspector GuardDuty AWS Health, Amazon e IAM Access Analyzer en cada cuenta. Estos servicios envían automáticamente sus hallazgos a Security Hub CSPM. Para obtener una lista completa de Servicio de AWS las integraciones compatibles, consulte la sección Enviar Servicios de AWS los resultados a Security Hub CSPM.

   > **Note**
   >
   > AWS Health envía los resultados al Security Hub CSPM si se cumple una de las siguientes condiciones:

- El hallazgo está asociado a un AWS servicio de seguridad
- El valor de typecode del resultado contiene las palabras `security`, `abuse` o `certificate`.
- El AWS Health servicio de búsqueda es `risk` o `abuse`

2. Configuración de integraciones de terceros: para obtener una lista de las integraciones compatibles en este momento, consulte Available third-party partner product integrations. Seleccione cualquier herramienta adicional que pueda enviar o recibir hallazgos de Security Hub CSPM. Es posible que ya tenga algunas de estas herramientas de terceros. Siga las instrucciones del producto para configurar la integración con Security Hub CSPM.

Preparación para asignar resultados de seguridad

En esta sección, configura las herramientas que utilizan sus equipos para administrar y asignar los resultados de seguridad. En esta sección se incluyen las siguientes opciones:

- Administración de los resultados en las herramientas y los flujos de trabajo existentes— Esta opción se integra AWS Security Hub CSPM con los sistemas existentes que sus equipos utilizan para gestionar sus tareas diarias, como la cartera de productos pendientes. Esta opción se recomienda para los equipos que han establecido herramientas para administrar sus flujos de trabajo.
- Gestione los hallazgos en Security Hub (CSPM)— Esta opción configura las notificaciones de los eventos de CSPM de Security Hub para que el equipo correspondiente reciba una alerta y pueda abordar el hallazgo en Security Hub CSPM.

Decida qué flujo de trabajo funcionaría mejor para sus equipos y asegúrese de que los resultados de seguridad lleguen rápidamente a sus respectivos propietarios.

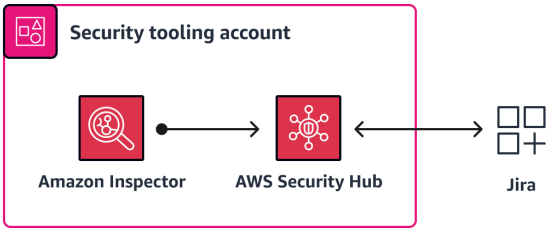
Administración de los resultados en las herramientas y los flujos de trabajo existentes

Recomendamos integraciones adicionales de Security Hub CSPM para las organizaciones empresariales que cuentan con herramientas establecidas que los equipos utilizan para gestionar o realizar sus tareas diarias. Puede importar los datos de búsqueda de CSPM de Security Hub a varias plataformas tecnológicas. Entre los ejemplos se incluyen:

- Los sistemas de gestión de información y eventos de seguridad (SIEM) ayudan a los equipos de seguridad a clasificar los eventos de seguridad operativos. Los sistemas de SIEM proporcionan análisis en tiempo real de las alertas de seguridad generadas por las aplicaciones y el hardware de la red.
- Los sistemas de gobernanza, riesgo y cumplimiento (GRC) ayudan a los equipos de cumplimiento y gobernanza a supervisar los datos de administración de riesgos e informar sobre ellos. Las herramientas de GRC son aplicaciones de software que las empresas pueden utilizar para administrar las políticas, evaluar los riesgos, controlar el acceso de los usuarios y agilizar el cumplimiento. Puede utilizar las herramientas de GRC para integrar los procesos empresariales, reducir los costos y mejorar la eficiencia.
- Los sistemas de tickets y tareas pendientes de productos ayudan a los equipos de aplicaciones y de la nube a administrar las características y priorizar las tareas de desarrollo. Atlassian Jira y Microsoft Azure DevOps son ejemplos de estos sistemas.

La integración de los hallazgos del CSPM de Security Hub directamente con estos sistemas empresariales existentes puede mejorar el tiempo medio de recuperación (MTTR) y los resultados de seguridad, ya que el flujo de trabajo operativo diario no tiene por qué cambiar. Los equipos pueden responder ante los resultados de seguridad y aprender de ellos mucho más rápido, ya que no tienen que utilizar flujos de trabajo y herramientas independientes. La integración hace que abordar los resultados de seguridad sea parte del flujo de trabajo normal y estándar.

Security Hub CSPM se integra con varios productos de socios de terceros. Para obtener una lista completa y las instrucciones, consulte las integraciones de productos de socios externos disponibles en la documentación de CSPM de Security Hub. Las integraciones más comunes incluyen Atlassian - Jira Service Managementla integración bidireccional con el software y. AWS Security Hub CSPM Jira ServiceNow – ITSM El siguiente diagrama muestra cómo puede configurar Amazon Inspector para que envíe las conclusiones al Security Hub CSPM y, a continuación, configurar Security Hub CSPM para que envíe todas las conclusiones. Jira



Gestione los hallazgos en Security Hub (CSPM)

Puede crear un sistema de notificaciones basado en la nube para los hallazgos de CSPM de Security Hub mediante EventBridge las reglas de Amazon y los temas del Servicio de Notificación Simple de Amazon (Amazon SNS). Este sistema notifica al equipo correspondiente acerca de un resultado cuando se crea. Para este enfoque, la estrategia de varias cuentas descrita en la sección Desarrolle una estructura Cuenta de AWS es fundamental porque las aplicaciones se dividen en cuentas dedicadas. Esto lo ayuda a notificar cada resultado a los equipos correctos.

Los equipos de seguridad o de nube pueden optar por recibir eventos de todos. Cuentas de AWS En este caso, cree una EventBridge regla en la cuenta de administrador delegado de CSPM de Security Hub y suscríbase a un tema de Amazon SNS que notifique a estos equipos. Para los equipos de aplicaciones, configure una EventBridge regla y un tema de SNS en sus respectivas cuentas de aplicaciones. Cuando se produce un hallazgo de CSPM de Security Hub en una cuenta de aplicación, se notifica al equipo responsable sobre el hallazgo.

Security Hub CSPM ya envía automáticamente todos los nuevos hallazgos y todas las actualizaciones de los hallazgos existentes EventBridge como Security Hub CSPM Findings: Imported events. Cada evento CSPM Findings - Imported de Security Hub contiene un único hallazgo. Puede aplicar filtros a las EventBridge reglas para que un hallazgo inicie la regla solo si el hallazgo coincide con los filtros. Para obtener instrucciones, consulte Configurar una EventBridge regla para el envío automático de los resultados. Para obtener más información sobre cómo crear temas de Amazon SNS y suscribirse a ellos, consulte Configuring Amazon SNS.

Tenga en cuenta lo siguiente cuando utilice este método:

- Para los equipos de aplicaciones, cree EventBridge reglas dentro de cada uno de ellos Cuenta de AWS y en el Región de AWS lugar donde se aloja la aplicación.
- Para los equipos de seguridad y de nube, cree EventBridge reglas en la cuenta de administrador delegado CSPM de Security Hub. Esto notifica a los equipos sobre todos los resultados en las cuentas de miembros.
- Amazon SNS envía una notificación todos los días si el estado del resultado de seguridad es `NEW`. Si quieres desactivar las notificaciones diarias, puedes crear una AWS Lambda función personalizada que cambie el estado del hallazgo de `NEW` a `NOTIFIED` después de que el suscriptor de Amazon SNS reciba la notificación.

Clasifique y corrija los hallazgos de seguridad en su entorno AWS

La clasificación de un resultado de seguridad implica dirigirlo a la parte interesada correspondiente, evaluarlo y priorizarlo y, a continuación, corregirlo. En esta sección se analiza cada uno de estos pasos en detalle y se proporcionan recomendaciones de escalabilidad y eficiencia. También incluye ejemplos para ayudar a ilustrar el proceso de clasificación y corrección.

Temas

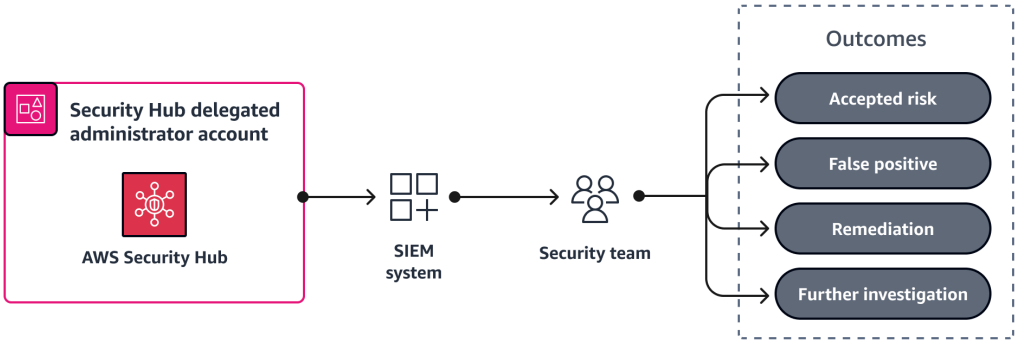
Definición de la propiedad de los resultados de seguridad

Definir un modelo de propiedad para clasificar los resultados de seguridad puede ser difícil, pero no tiene por qué serlo. El panorama de la seguridad cambia constantemente y los profesionales deben ser flexibles para adaptarse a estos cambios. Adopte un enfoque flexible para desarrollar su modelo de propiedad para los resultados de seguridad. Su modelo inicial debería permitir a sus equipos actuar de inmediato. Recomendamos empezar con una lógica de propiedad básica y refinarla con el tiempo. Si se demora en definir los criterios de propiedad perfectos, el número de resultados de seguridad seguirá aumentando.

Para facilitar la asignación de los hallazgos a los equipos y recursos adecuados, recomendamos integrarlos AWS Security Hub CSPM con cualquier sistema existente que sus equipos utilicen para gestionar sus tareas diarias. Por ejemplo, puede integrar Security Hub CSPM con los sistemas de gestión de eventos e información de seguridad (SIEM) o con los sistemas de registro de productos y venta de entradas. Para obtener más información, consulte la sección Preparación para asignar resultados de seguridad de esta guía.

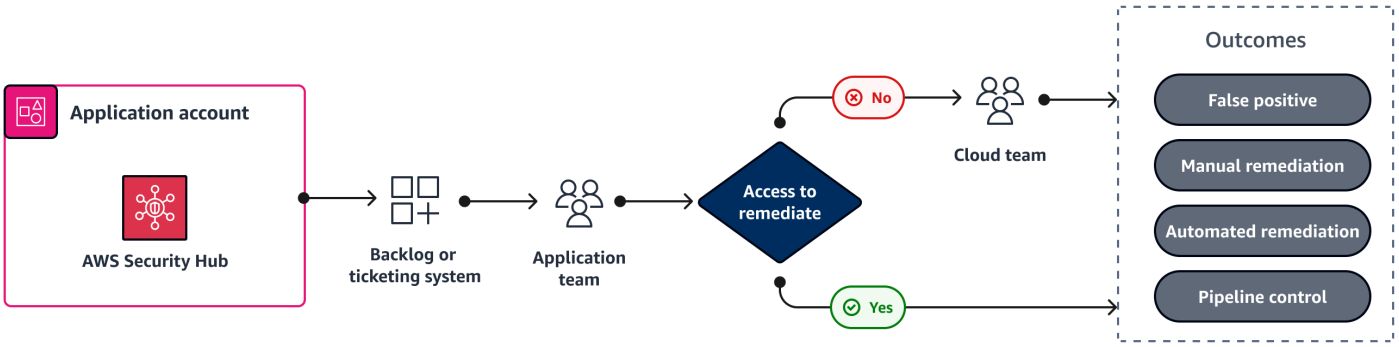
A continuación, se incluye un ejemplo de modelo de propiedad que puede utilizar como punto de partida:

- El equipo de seguridad analiza las posibles amenazas activas y ayuda a evaluar y priorizar los resultados de seguridad. El equipo de seguridad tiene la experiencia y las herramientas para evaluar adecuadamente el contexto. Comprende los datos adicionales relacionados con la seguridad que lo ayudan a evaluar y priorizar las vulnerabilidades e investigar los eventos de detección de amenazas. Si es necesario determinar la gravedad del resultado o aplicar refinamientos adicionales, consulte la sección Evaluación y priorización de los resultados de seguridad de esta guía. Para ver un ejemplo, consulte Ejemplo del equipo de seguridad en esta guía.



- Distribución de los resultados de seguridad entre los equipos de la nube y de aplicaciones: como se explica en la sección Distribución de la propiedad de seguridad, el equipo que tiene acceso para configurar el recurso es responsable de su configuración segura. Los equipos de aplicaciones son responsables de los resultados de seguridad relacionados con los recursos que crean y configuran, y el equipo de la nube es responsable de los resultados de seguridad relacionados con las configuraciones de amplio alcance. En la mayoría de los casos, los equipos de aplicaciones no tienen acceso a cambiar las configuraciones de gran alcance y Servicios de AWS, por ejemplo, las políticas de control de servicios (SCPs) en AWS Organizations las configuraciones de VPC relacionadas con la red y el Centro de identidad de IAM. AWS Control TowerAWS

  En el caso de entornos con varias cuentas que separan las aplicaciones en cuentas dedicadas, normalmente se pueden integrar los resultados relacionados con la seguridad de la cuenta en el sistema de tareas pendientes de productos o de tickets de la aplicación. Desde ese sistema, el equipo de la nube o de aplicaciones pueden abordar el resultado. Para ver ejemplos, consulte Ejemplo del equipo en la nube o Ejemplo del equipo de aplicaciones en esta guía.



- Asignación al equipo de la nube de los resultados restantes sin resolver: los resultados residuales pueden estar relacionados con la configuración predeterminada o con configuraciones de amplio alcance que el equipo de la nube pueda abordar. Es probable que este equipo sea el que tenga más conocimientos históricos y acceso para resolver el resultado. En general, este suele ser un subconjunto significativamente menor del total de los resultados.

Evaluación y priorización de los resultados de seguridad

Un componente fundamental de un programa eficaz de administración de vulnerabilidades es la capacidad de evaluar y priorizar los resultados de seguridad. Aquí es donde entra en juego el contexto, el historial de la organización y el refinamiento de los sistemas de detección. La priorización de los resultados de seguridad ayuda a establecer la velocidad adecuada para el nivel de respuesta.

En el caso de Amazon Inspector y Amazon GuardDuty, los resultados contienen una etiqueta o puntuación de gravedad. AWS Security Hub CSPM Recomendamos priorizar la investigación de todos los hallazgos críticos y de alta gravedad en Security Hub CSPM, incluidos los hallazgos relacionados con el estándar Foundational Security Best Practices (FSBP), Amazon Inspector y. GuardDuty Las etiquetas y puntuaciones de gravedad de los resultados se determinan de la siguiente manera:

- La puntuación de Amazon Inspector es una puntuación altamente contextualizada para cada resultado. Para calcularla, se correlaciona la información de la puntuación básica del sistema de clasificación de vulnerabilidades comunes (CVSS) con los resultados de accesibilidad de la red y los datos de explotabilidad. Con esta puntuación, puede priorizar los resultados para centrarse en los resultados más críticos y en los recursos vulnerables. Además de la puntuación, Amazon Inspector también proporciona inteligencia de vulnerabilidades mejorada sobre vulnerabilidades y exposiciones comunes (CVE). En esta sección se resume la inteligencia disponible sobre las CVE de Amazon y otros orígenes de inteligencia de seguridad estándar en el sector, como Recorded

Future and Cybersecurity and Infrastructure Security Agency (CISA). Por ejemplo, Amazon Inspector puede proporcionar los nombres de los kits de malware conocidos que se utilizan para aprovechar una vulnerabilidad. Para obtener más información, consulte Vulnerability Intelligence.

- Cada GuardDuty hallazgo tiene un nivel de gravedad y un valor asignados que reflejan el riesgo potencial del hallazgo para su entorno. Los ingenieros de seguridad de AWS determinan este nivel y este valor. Por ejemplo, el nivel de seguridad `High` indica que un recurso está en peligro y que se está utilizando de forma activa para fines no autorizados. Le recomendamos que dé prioridad a `High` la GuardDuty determinación de la gravedad y que la corrija de inmediato para evitar un uso no autorizado posterior.
- La gravedad de una constatación de control CSPM de Security Hub viene determinada por la dificultad de explotación y la probabilidad de que se ponga en peligro. La dificultad viene determinada por el grado de sofisticación o complejidad que se requiere para utilizar la debilidad para llevar a cabo un escenario de amenaza. La probabilidad de que se ponga en peligro indica la probabilidad de que el escenario de amenaza provoque una interrupción o una violación de sus recursos o de sus recursos Servicios de AWS .

Para ajustar los resultados, puede suprimir o archivar resultados específicos directamente en la consola del servicio correspondiente o mediante la API del servicio. Además, puede realizar cambios en los hallazgos de Security Hub CSPM mediante reglas de automatización. GuardDuty y las conclusiones de Amazon Inspector se envían automáticamente a Security Hub (CSPM). Puede utilizar reglas de automatización para actualizar automáticamente (por ejemplo, cambiar la gravedad) o suprimir los resultados casi en tiempo real, en función de los criterios que defina. Al crear reglas de automatización, le recomendamos agregar contexto a la descripción de la regla, como la fecha de creación o modificación, quién la creó y por qué es necesaria la regla. Esta información suele ser útil para consultarla en el futuro.

Corrección de los resultados de seguridad

Después de evaluar y priorizar un resultado, la siguiente acción es corregirlo. Hay muchas medidas diferentes que puede tomar para corregir un resultado. En el caso de las vulnerabilidades de software, puede actualizar el sistema operativo o aplicar una revisión. En el caso de los resultados de configuración de la nube, puede actualizar la configuración de los recursos. En general, las medidas de corrección que se toman se pueden agrupar en uno de los siguientes resultados:

- Solución manual: usted proporciona manualmente una solución a la vulnerabilidad, por ejemplo, modificando las propiedades de un AWS recurso para habilitar el cifrado. Si el hallazgo proviene

de una comprobación gestionada en Security Hub (CSPM), el hallazgo incluye un enlace a instrucciones para corregir manualmente el hallazgo.

- Artefacto reutilizable: actualiza la infraestructura como código (IaC) para corregir la vulnerabilidad y saber que otras personas podrían beneficiarse de una solución similar. Considere la posibilidad de cargar la IaC actualizada y un breve resumen de la resolución en un repositorio de código interno compartido.
- Corrección automatizada: la vulnerabilidad se corrige automáticamente mediante los mecanismos que usted creó.
- Control de canalizaciones: aplica un control en su canalización de integración y entrega continuas (CI/CD) que impide la implementación si la vulnerabilidad está presente.
- Riesgo aceptado: no toma ninguna medida ni implementa ningún control compensatorio, y acepta el riesgo que presenta la vulnerabilidad. Haga un seguimiento del riesgo aceptado en una ubicación específica, como un registro de riesgos.
- Falso positivo: no toma ninguna medida porque ha determinado que el resultado no identificó correctamente una vulnerabilidad.

En esta guía no se incluye una lista completa de las diversas medidas y herramientas que puede utilizar para corregir una vulnerabilidad. Sin embargo, vale la pena mencionar algunos servicios y herramientas que pueden ayudarlo a corregir las vulnerabilidades a escala:

- El administrador de parches, una capacidad de AWS Systems Manager, automatiza el proceso de parchear los nodos gestionados tanto con actualizaciones relacionadas con la seguridad como con otros tipos de actualizaciones. Puede utilizar Patch Manager para aplicar parches a los sistemas operativos y a las aplicaciones.
- AWS Firewall Managerle ayuda a configurar y administrar de forma centralizada las reglas de firewall en todas sus cuentas y aplicaciones en. AWS Organizations A medida que se crean nuevas aplicaciones, Firewall Manager facilita el cumplimiento de las nuevas aplicaciones y recursos mediante la aplicación de un conjunto común de reglas de seguridad.
- Automated Security AWS Response on es una AWS solución que funciona con Security Hub CSPM y proporciona acciones de respuesta y remediación predefinidas basadas en los estándares de cumplimiento de la industria y las mejores prácticas para las amenazas de seguridad.

Ejemplos de clasificación y corrección de los resultados de seguridad

En esta sección se proporcionan ejemplos del proceso de clasificación para los equipos de seguridad, la nube y aplicaciones. Se analizan los tipos de resultados que suele abordar cada equipo y se proporciona un ejemplo de cómo responder ante ellos. También se incluye una guía de corrección de alto nivel.

Los siguientes ejemplos se incluyen en esta sección:

- Ejemplo de equipo de seguridad: creación de una regla de automatización CSPM de Security Hub
- Ejemplo del equipo de la nube: cambio de configuraciones de VPC
- Ejemplo del equipo de aplicaciones: creación de una regla AWS Config

Ejemplo de equipo de seguridad: creación de una regla de automatización CSPM de Security Hub

El equipo de seguridad recibe las conclusiones relacionadas con la detección de amenazas, incluidas las de Amazon GuardDuty . Para obtener una lista completa de los tipos de GuardDuty búsqueda clasificados por tipo de AWS recurso, consulte Búsqueda de tipos en la GuardDuty documentación. Los equipos de seguridad deben estar familiarizados con todos estos tipos de resultados.

Para este ejemplo, el equipo de seguridad acepta el nivel de riesgo asociado a los hallazgos de seguridad en un Cuenta de AWS documento que se utiliza estrictamente con fines de aprendizaje y no incluye datos importantes o confidenciales. El nombre de esta cuenta es `sandbox` y el ID de la cuenta es `123456789012`. El equipo de seguridad puede crear una regla de AWS Security Hub CSPM automatización que suprima todos los GuardDuty hallazgos de esta cuenta. Puede crear una regla a partir de una plantilla, que abarca muchos casos de uso comunes, o puede crear una regla personalizada. En Security Hub CSPM, recomendamos obtener una vista previa de los resultados de los criterios para confirmar que la regla arroja los resultados esperados.

> **Note**
>
> En este ejemplo, se destaca la funcionalidad de las reglas de automatización. No recomendamos suprimir todos los GuardDuty resultados de una cuenta. El contexto es

importante, y cada organización debe elegir qué resultados suprimir en función del tipo de datos, la clasificación y los controles de mitigación.

A continuación, se incluyen los parámetros que se utilizan para crear esta regla de automatización:

- Regla:
  - El nombre de la regla es `Suppress findings from Sandbox account`.
  - La descripción de la regla es `Date: 06/25/23 Authored by: John Doe Reason: Suppress GuardDuty findings from the sandbox account`.
- Criterios:
  - `AwsAccountId` = `123456789012`
  - `ProductName` = `GuardDuty`
  - `WorkflowStatus` = `NEW`
  - `RecordState` = `ACTIVE`
- Acción automatizada:
  - `Workflow.status` es `SUPPRESSED`

Para obtener más información, consulte Reglas de automatización en la documentación de Security Hub CSPM. Los equipos de seguridad disponen de muchas opciones para investigar y corregir los resultados relacionados con las amenazas detectadas. Para obtener más información, consulte Guía sobre Respuesta ante incidentes de seguridad de AWS. Recomendamos consultar esta guía para confirmar que haya establecido procesos sólidos de respuesta ante incidentes.

Ejemplo del equipo de la nube: cambio de configuraciones de VPC

El equipo de la nube es responsable de clasificar y corregir los hallazgos de seguridad que tienen tendencias comunes, como los cambios en la configuración AWS predeterminada que podrían no adaptarse a su caso de uso. Estos hallazgos suelen afectar a muchos Cuentas de AWS recursos, como las configuraciones de VPC, o incluyen una restricción que debería aplicarse a todo el entorno. En su mayor parte, el equipo de la nube hace cambios manuales y puntuales, como agregar o actualizar una política.

Una vez que su organización haya utilizado un AWS entorno durante algún tiempo, es posible que se esté desarrollando un conjunto de antipatrones. Un antipatrón es una solución que se utiliza con

frecuencia para un problema recurrente en el que la solución es contraproducente, ineficaz o menos eficaz que una alternativa. Como alternativa a estos antipatrones, su organización puede utilizar restricciones que afecten a todo el entorno y que sean más eficaces, como las políticas de control de AWS Organizations servicios (SCPs) o los conjuntos de permisos del IAM Identity Center. SCPs y los conjuntos de permisos pueden proporcionar restricciones adicionales para los tipos de recursos, como impedir que los usuarios configuren un bucket público de Amazon Simple Storage Service (Amazon S3). Aunque puede resultar tentador restringir todas las configuraciones de seguridad posibles, las políticas tienen límites de tamaño SCPs y conjuntos de permisos. Recomendamos un enfoque equilibrado de los controles preventivos y de detección.

Los siguientes son algunos controles del estándar de mejores prácticas de seguridad AWS Security Hub CSPM fundamentales (FSBP) de los que podría ser responsable el equipo de la nube:

- [EC2.2] El grupo de seguridad predeterminado de la VPC no debe permitir el tráfico entrante ni saliente
- [EC2.6] El registro de flujo de VPC debe estar habilitado en todos VPCs
- [EC2.23] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC
- [CloudTrail.1] CloudTrail debe habilitarse y configurarse con al menos un registro multirregional que incluya eventos de administración de lectura y escritura
- [Config.1] AWS Config debe estar activado

Para este ejemplo, el equipo de la nube aborda un resultado relativo al control EC2.2 de FSBP. En la documentación de este control se recomienda no utilizar el grupo de seguridad predeterminado, ya que permite un amplio acceso mediante las reglas de entrada y salida predeterminadas. Dado que el grupo de seguridad predeterminado no se puede eliminar, se recomienda cambiar la configuración de reglas para restringir el tráfico entrante y saliente. Para abordar este problema de manera eficiente, el equipo de nube debe usar los mecanismos establecidos para modificar las reglas de los grupos de seguridad para todos, VPCs ya que cada VPC tiene este grupo de seguridad predeterminado. En la mayoría de los casos, los equipos de la nube administran las configuraciones de VPC mediante personalizaciones de AWS Control Tower o una herramienta de infraestructura como código (IaC), como HashiCorp Terraform o AWS CloudFormation.

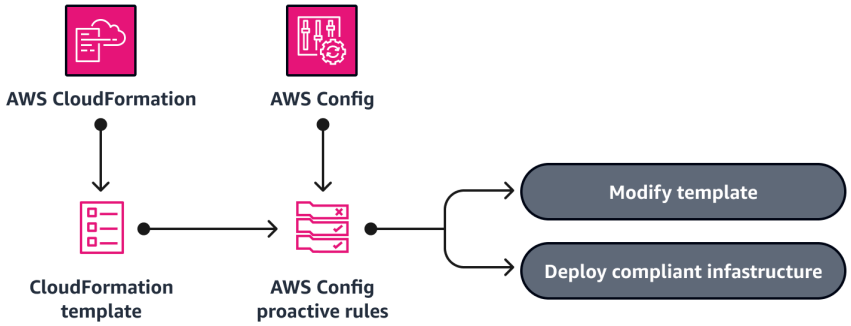
Ejemplo del equipo de aplicaciones: creación de una regla AWS Config

Los siguientes son algunos controles del estándar de seguridad Security Hub CSPM Foundational Security Best Practices (FSBP) de los que podría ser responsable la aplicación o el equipo de desarrollo:

- [CloudFront.1] las CloudFront distribuciones deben tener configurado un objeto raíz predeterminado
- [EC2.19] Los grupos de seguridad no deben permitir el acceso ilimitado a los puertos de alto riesgo
- [CodeBuild.1] CodeBuild GitHub o el repositorio fuente de Bitbucket deberían usar URLs OAuth
- [ECS.4] Los contenedores de ECS deben ejecutarse sin privilegios
- [ELB.1] Application Load Balancer debe configurarse para redirigir todas las solicitudes HTTP a HTTPS

Para este ejemplo, el equipo de aplicaciones aborda un resultado relativo al control EC2.19 de FSBP. Este control comprueba si el tráfico entrante ilimitado de los grupos de seguridad es accesible para los puertos especificados que tienen el mayor riesgo. Este control falla si alguna de las reglas de un grupo de seguridad permite la entrada de tráfico desde `0.0.0.0/0` o `::/0` para esos puertos. En la documentación de este control se recomienda eliminar las reglas que permiten este tráfico.

Además de abordar la regla del grupo de seguridad individual, este es un excelente ejemplo de un hallazgo que debería dar como resultado una nueva regla. AWS Config Al utilizar el modo de evaluación proactiva, puede ayudar a evitar la implementación de reglas de grupos de seguridad de riesgo en el futuro. El modo proactivo evalúa los recursos antes de que se implementen para evitar los recursos mal configurados y los resultados de seguridad asociados a ellos. Al implementar un nuevo servicio o una nueva funcionalidad, los equipos de aplicaciones pueden ejecutar reglas en modo proactivo como parte de su canalización de integración y entrega continuas (CI/CD) para identificar los recursos que no cumplen con los requisitos. La siguiente imagen muestra cómo puede utilizar una AWS Config regla proactiva para confirmar que la infraestructura definida en una AWS CloudFormation plantilla es compatible.



En este ejemplo se puede obtener otra eficiencia importante. Cuando un equipo de aplicaciones crea una AWS Config regla proactiva, puede compartirla en un repositorio de código común para que otros equipos de aplicaciones puedan usarla.

Cada hallazgo asociado a un control CSPM de Security Hub contiene detalles sobre el hallazgo y un enlace a las instrucciones para solucionar el problema. Si bien los equipos de la nube pueden encontrar resultados que requieran una corrección manual y puntual, cuando proceda, recomendamos crear controles proactivos que identifiquen los problemas lo antes posible en el proceso de desarrollo.

Notificación y mejora del programa de administración de vulnerabilidades

Un proceso eficaz de notificaciones en materia de administración de vulnerabilidades implica revisar los datos, supervisar las tendencias y compartir los conocimientos. Esto proporciona visibilidad y ayuda a los equipos a mejorar la postura de seguridad de sus organizaciones en la Nube de AWS.

Organización de reuniones mensuales sobre operaciones de seguridad

Las reuniones mensuales sobre operaciones de seguridad son un mecanismo eficaz para promover la titularidad, la responsabilidad y la alineación continuas entre los equipos. En la reunión, las partes interesadas de los equipos de seguridad, nube y aplicaciones revisan los datos para detectar hallazgos de seguridad sobresalientes, hallazgos fuera de los acuerdos de nivel de servicio (SLAs) y los equipos que tienen más hallazgos.

Estas reuniones ayudan a sus equipos a identificar antipatrones, como las oportunidades de agregar más restricciones. Los controles preventivos y las oportunidades de automatización también se pueden descubrir y compartir. Las reuniones también ayudan a identificar lo que funciona y lo que no funciona bien en el programa de administración de vulnerabilidades para poder aplicar mejoras.

Al revisar los datos, identificar los antipatrones y los problemas, y compartir información sobre los controles y las automatizaciones, los equipos pueden obtener información valiosa y realizar mejoras continuas que pueden reforzar su postura de seguridad y reducir los problemas relacionados con la seguridad. SLAs

Utilice los conocimientos de CSPM de Security Hub para identificar antipatrones

La información de AWS Security Hub CSPM también puede ayudarlo a identificar los antipatrones y a hacer un seguimiento de sus avances en la corrección de los resultados. La información sobre el CSPM de Security Hub es una colección de hallazgos relacionados. Identifica un área de seguridad que requiere atención e intervención. Los conocimientos de CSPM de Security Hub pueden ayudarlo a identificar requisitos específicos y desarrollar informes. Security Hub CSPM ofrece varios

conocimientos gestionados integrados. Para realizar un seguimiento de los problemas de seguridad que son exclusivos de su AWS entorno y uso, puede crear información personalizada.

Conclusión y siguientes pasos

En resumen, un programa de administración de vulnerabilidades eficaz requiere una preparación minuciosa y disponer de las herramientas e integraciones adecuadas, refinarlas, clasificar los problemas de manera eficiente y notificar y mejorar continuamente. Al seguir las mejores prácticas de esta guía, las organizaciones pueden crear un programa de gestión de vulnerabilidades escalable AWS para ayudar a proteger sus entornos de nube.

Puede ampliar este programa para incluir vulnerabilidades y hallazgos adicionales relacionados con la seguridad, como las vulnerabilidades de seguridad de las aplicaciones. AWS Security Hub CSPM admite integraciones de productos personalizadas. Considere utilizar Security Hub CSPM como punto de integración para herramientas y productos de seguridad adicionales. Esta integración le permite aprovechar los procesos y flujos de trabajo que ya ha establecido en su programa de administración de vulnerabilidades, como la integración directa con las tareas pendientes de los productos y las reuniones mensuales de revisión de seguridad.

En la siguiente tabla se resumen las fases y los elementos de acción que se describen en esta guía.

Fase	Elementos de acción
Preparación	• Definir un plan de administración de vulnerabilidades. • Distribuir la propiedad de los resultados. • Desarrollar un programa de divulgación de vulnerabilidades. • Desarrolle una estructura Cuenta de AWS . • Definir, implementar y aplicar etiquetas. • Supervise los boletines de AWS seguridad. • Habilitar Amazon Inspector con un administr ador delegado. • Habilite el CSPM de Security Hub con un administrador delegado. • Habilite los estándares CSPM de Security Hub.

Fase	Elementos de acción
	• Configure la agregación entre regiones de Security Hub CSPM. • Habilite los hallazgos de control consolidados en Security Hub CSPM. • Configure y gestione las integraciones de Security Hub (CSPM), incluidas las integraciones descendentes aplicables con SIEM, GRC o los sistemas de venta de entradas o cartera de productos
Clasificación y corrección	• Remitir los resultados en función de una estrategia de varias cuentas. • Remitir los resultados a los equipos de seguridad, la nube y aplicaciones o desarrolladores. • Ajustar los resultados de seguridad para asegurarse de que sean aplicables a su entorno específico. • Desarrollar mecanismos de corrección automatizados, siempre que sea posible. • Siempre que sea posible, implemente controles de CI/CD tuberías u otras barreras que ayuden a evitar problemas de seguridad. • Utilice las reglas de automatización de CSPM de Security Hub para aumentar o suprimir los hallazgos.
Notificación y mejora	• Organizar reuniones mensuales sobre operaciones de seguridad. • Utilice los conocimientos de CSPM de Security Hub para identificar los antipatrones.

Recursos

AWS documentación de servicio

- Product integrations (AWS Security Hub CSPM)
- Integrating AWS Security Hub CSPM in Jira Service Management Cloud (AWS Security Hub CSPM)
- Automation rules (AWS Security Hub CSPM)
- Proactive evaluation rules (AWS Config)
- Patch Manager (AWS Systems Manager)

Otros recursos de AWS

- Best practices for tagging AWS resources (documento técnico de AWS)
- Automated Security Response on AWS (Biblioteca de soluciones de AWS)
- AWS Security Incident Response Guide (guía técnica de AWS)
- Boletines de seguridad de AWS

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	—	12 de octubre de 2023

AWS Glosario de orientación prescriptiva

Los siguientes son términos de uso común en las estrategias, guías y patrones proporcionados por la Guía AWS prescriptiva. Para sugerir entradas, utilice el enlace Enviar comentarios al final del glosario.

Números

Las 7 R

Siete estrategias de migración comunes para trasladar aplicaciones a la nube. Estas estrategias se basan en las 5 R que Gartner identificó en 2011 y consisten en lo siguiente:

- Refactorizar/rediseñar: traslade una aplicación y modifique su arquitectura mediante el máximo aprovechamiento de las características nativas en la nube para mejorar la agilidad, el rendimiento y la escalabilidad. Por lo general, esto implica trasladar el sistema operativo y la base de datos. Ejemplo: Migrar la base de datos de Oracle en las instalaciones a Amazon Aurora PostgreSQL-Compatible Edition.
- Redefinir la plataforma (transportar y redefinir): traslade una aplicación a la nube e introduzca algún nivel de optimización para aprovechar las capacidades de la nube. Ejemplo: Migrar la base de datos Oracle en las instalaciones a Amazon Relational Database Service (Amazon RDS) para Oracle en la nube de Nube de AWS.
- Recomprar (readquirir): cambie a un producto diferente, lo cual se suele llevar a cabo al pasar de una licencia tradicional a un modelo SaaS. Ejemplo: Migrar el sistema de administración de las relaciones con los clientes (CRM) a Salesforce.com.
- Volver a alojar (migrar mediante lift-and-shift): traslade una aplicación a la nube sin realizar cambios para aprovechar las capacidades de la nube. Ejemplo: Migrar la base de datos de Oracle en las instalaciones a Oracle en una instancia de EC2 en la Nube de AWS.
- Reubicar: (migrar el hipervisor mediante lift and shift): traslade la infraestructura a la nube sin comprar equipo nuevo, reescribir aplicaciones o modificar las operaciones actuales. Los servidores se migran de una plataforma en las instalaciones a un servicio en la nube para la misma plataforma. Ejemplo: migrar una Microsoft Hyper-V aplicación a AWS.
- Retener (revisitar): conserve las aplicaciones en el entorno de origen. Estas pueden incluir las aplicaciones que requieren una refactorización importante, que desee posponer para más adelante, y las aplicaciones heredadas que desee retener, ya que no hay ninguna justificación empresarial para migrarlas.

- Retirar: retire o elimine las aplicaciones que ya no sean necesarias en un entorno de origen.

A

ABAC

Consulte control de acceso basado en atributos.

servicios abstractos

Consulte servicios administrados.

ACID

Consulte atomicidad, consistencia, aislamiento, durabilidad.

migración activa-activa

Método de migración de bases de datos en el que las bases de datos de origen y destino se mantienen sincronizadas (mediante una herramienta de replicación bidireccional o mediante operaciones de escritura doble) y ambas bases de datos gestionan las transacciones de las aplicaciones conectadas durante la migración. Este método permite la migración en lotes pequeños y controlados, en lugar de requerir una transición única. Es más flexible, pero requiere más trabajo que una migración activa-pasiva.

migración activa-pasiva

Método de migración de bases de datos en el que las bases de datos de origen y destino se mantienen sincronizadas, pero solo la de origen gestiona las transacciones de las aplicaciones conectadas, mientras los datos se replican en la de destino. La base de datos de destino no acepta ninguna transacción durante la migración.

función de agregación

Función SQL que actúa en un grupo de filas y calcula un único valor de devolución para el grupo. Entre los ejemplos de funciones de agregación se incluyen `SUM` y `MAX`.

IA

Consulte inteligencia artificial.

AIOps

Consulte operaciones de inteligencia artificial

anonimización

El proceso de eliminar permanentemente la información personal de un conjunto de datos. La anonimización puede ayudar a proteger la privacidad personal. Los datos anonimizados ya no se consideran datos personales.

antipatrones

Una solución que se utiliza con frecuencia para un problema recurrente en el que la solución es contraproducente, ineficaz o menos eficaz que una alternativa.

control de aplicaciones

Enfoque de seguridad que permite usar de manera exclusiva aplicaciones aprobadas para ayudar a proteger un sistema contra el malware.

cartera de aplicaciones

Recopilación de información detallada sobre cada aplicación que utiliza una organización, incluido el costo de creación y mantenimiento de la aplicación y su valor empresarial. Esta información es clave para el proceso de detección y análisis de la cartera y ayuda a identificar y priorizar las aplicaciones que se van a migrar, modernizar y optimizar.

inteligencia artificial (IA)

El campo de la informática que se dedica al uso de tecnologías informáticas para realizar funciones cognitivas que suelen estar asociadas a los seres humanos, como el aprendizaje, la resolución de problemas y el reconocimiento de patrones. Para más información, consulte ¿Qué es la inteligencia artificial?

operaciones de inteligencia artificial (AIOps)

El proceso de utilizar técnicas de machine learning para resolver problemas operativos, reducir los incidentes operativos y la intervención humana, y mejorar la calidad del servicio. Para obtener más información sobre cómo AIOps se utiliza en la estrategia de AWS migración, consulte la guía de integración de operaciones.

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.

atomicidad, consistencia, aislamiento, durabilidad (ACID)

Conjunto de propiedades de software que garantizan la validez de los datos y la fiabilidad operativa de una base de datos, incluso en caso de errores, cortes de energía u otros problemas.

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. Para obtener más información, consulte ABAC AWS en la documentación AWS Identity and Access Management (IAM).

origen de datos fidedigno

Ubicación en la que se almacena la versión principal de los datos, que se considera la fuente de información más fiable. Puede copiar los datos del origen de datos autorizado a otras ubicaciones con el fin de procesarlos o modificarlos, por ejemplo, anonimizarlos, redactarlos o seudonimizarlos.

Zona de disponibilidad

Una ubicación distinta dentro de una Región de AWS que está aislada de los fallos en otras zonas de disponibilidad y que proporciona una conectividad de red económica y de baja latencia a otras zonas de disponibilidad de la misma región.

AWS Marco de adopción de la nube (AWS CAF)

Un marco de directrices y mejores prácticas AWS para ayudar a las organizaciones a desarrollar un plan eficiente y eficaz para migrar con éxito a la nube. AWS CAF organiza la orientación en seis áreas de enfoque denominadas perspectivas: negocios, personas, gobierno, plataforma, seguridad y operaciones. Las perspectivas empresariales, humanas y de gobernanza se centran en las habilidades y los procesos empresariales; las perspectivas de plataforma, seguridad y operaciones se centran en las habilidades y los procesos técnicos. Por ejemplo, la perspectiva humana se dirige a las partes interesadas que se ocupan de los Recursos Humanos (RR. HH.), las funciones del personal y la administración de las personas. Desde esta perspectiva, AWS CAF proporciona orientación para el desarrollo, la formación y la comunicación de las personas a fin de preparar a la organización para una adopción exitosa de la nube. Para obtener más información, consulte la Página web de AWS CAF y el Documento técnico de AWS CAF.

AWS Marco de calificación de la carga de trabajo (AWS WQF)

Herramienta que evalúa las cargas de trabajo de migración de bases de datos, recomienda estrategias de migración y proporciona estimaciones de trabajo. AWS WQF se incluye con AWS

Schema Conversion Tool ().AWS SCT Analiza los esquemas de bases de datos y los objetos de código, el código de las aplicaciones, las dependencias y las características de rendimiento y proporciona informes de evaluación.

B

bot malicioso

Bot destinado a causar interrupciones o daños a personas u organizaciones.

BCP

Consulte planificación de la continuidad del negocio.

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.

sistema big-endian

Un sistema que almacena primero el byte más significativo. Consulte también endianidad.

clasificación binaria

Un proceso que predice un resultado binario (una de las dos clases posibles). Por ejemplo, es posible que su modelo de ML necesite predecir problemas como “¿Este correo electrónico es spam o no es spam?” o “¿Este producto es un libro o un automóvil?”.

filtro de floración

Estructura de datos probabilística y eficiente en términos de memoria que se utiliza para comprobar si un elemento es miembro de un conjunto.

implementación azul/verde

Estrategia de implementación en la que se crean dos entornos separados, pero idénticos. La versión actual de la aplicación se ejecuta en un entorno (azul) y la nueva versión de la aplicación se ejecuta en el otro entorno (verde). Esta estrategia lo ayuda a hacer reversiones rápidas con un impacto mínimo.

bot

Aplicación de software que ejecuta tareas automatizadas a través de Internet y simula la actividad o interacción humana. Algunos bots son útiles o beneficiosos, como los rastreadores web que indexan la información de Internet. Otros bots, conocidos como bots maliciosos, tienen como objetivo causar interrupciones o daños a personas u organizaciones.

botnet

Redes de bots infectadas por malware y que están bajo el control de una sola parte, conocida como pastor de bots u operador de bots. Las botnets son el mecanismo más conocido para escalar los bots y su impacto.

branch

Área contenida de un repositorio de código. La primera rama que se crea en un repositorio es la rama principal. Puede crear una rama nueva a partir de una rama existente y, a continuación, desarrollar características o corregir errores en la rama nueva. Una rama que se genera para crear una característica se denomina comúnmente rama de característica. Cuando la característica se encuentra lista para su lanzamiento, se vuelve a combinar la rama de característica con la rama principal. Para obtener más información, consulte Acerca de las sucursales (GitHub documentación).

acceso de emergencia

En circunstancias excepcionales y mediante un proceso aprobado, es una forma rápida de que un usuario pueda acceder a un Cuenta de AWS sitio al que normalmente no tiene permisos de acceso. Para más información, consulte el indicador Implement break-glass procedures en la guía de AWS Well-Architected.

estrategia de implementación sobre infraestructura existente

La infraestructura existente en su entorno. Al adoptar una estrategia de implementación sobre infraestructura existente para una arquitectura de sistemas, se diseña la arquitectura en función de las limitaciones de los sistemas y la infraestructura actuales. Si está ampliando la infraestructura existente, puede combinar las estrategias de implementación sobre infraestructuras existentes y de implementación desde cero.

caché de búfer

El área de memoria donde se almacenan los datos a los que se accede con más frecuencia.

capacidad empresarial

Lo que hace una empresa para generar valor (por ejemplo, ventas, servicio al cliente o marketing). Las arquitecturas de microservicios y las decisiones de desarrollo pueden estar impulsadas por las capacidades empresariales. Para obtener más información, consulte la sección Organizado en torno a las capacidades empresariales del documento técnico Ejecutar microservicios en contenedores en AWS.

planificación de la continuidad del negocio (BCP)

Plan que aborda el posible impacto de un evento disruptivo, como una migración a gran escala en las operaciones y permite a la empresa reanudar las operaciones rápidamente.

C

CAF

Consulte AWS Cloud Adoption Framework.

implementación canario

Lanzamiento lento e incremental de una versión para los usuarios finales. Cuando tenga mayor confianza en la nueva versión, la implementa y reemplaza la versión actual en su totalidad.

CCoE

Consulte Centro de excelencia en la nube.

CDC

Consulte captura de datos de cambios.

captura de datos de cambio (CDC)

Proceso de seguimiento de los cambios en un origen de datos, como una tabla de base de datos, y registro de los metadatos relacionados con el cambio. Puede utilizar los CDC para diversos fines, como auditar o replicar los cambios en un sistema de destino para mantener la sincronización.

ingeniería del caos

Introducción intencionada de fallos o eventos disruptivos para poner a prueba la resiliencia de un sistema. Puedes usar AWS Fault Injection Service (AWS FIS) para realizar experimentos que estresen tus AWS cargas de trabajo y evalúen su respuesta.

CI/CD

Consulte integración continua y entrega continua.

clasificación

Un proceso de categorización que permite generar predicciones. Los modelos de ML para problemas de clasificación predicen un valor discreto. Los valores discretos siempre son distintos entre sí. Por ejemplo, es posible que un modelo necesite evaluar si hay o no un automóvil en una imagen.

cifrado del cliente

Cifrado de datos localmente, antes de que el objetivo los Servicio de AWS reciba.

Centro de excelencia en la nube (CCoE)

Equipo multidisciplinario que impulsa los esfuerzos de adopción de la nube en toda la organización, incluido el desarrollo de las prácticas recomendadas en la nube, la movilización de recursos, el establecimiento de plazos de migración y la dirección de la organización durante las transformaciones a gran escala. Para obtener más información, consulte las publicaciones de CCo E en el blog de estrategia Nube de AWS empresarial.

computación en la nube

La tecnología en la nube que se utiliza normalmente para la administración de dispositivos de IoT y el almacenamiento de datos de forma remota. La computación en la nube suele estar relacionada con la tecnología de computación de periferia.

modelo operativo en la nube

En una organización de TI, el modelo operativo que se utiliza para crear, madurar y optimizar uno o más entornos de nube. Para obtener más información, consulte Creación de su modelo operativo de nube.

etapas de adopción de la nube

Las siguientes son las cuatro fases por las que suelen pasar las empresas cuando migran a la Nube de AWS:

- Proyecto: ejecución de algunos proyectos relacionados con la nube con fines de prueba de concepto y aprendizaje
- Fundamento: realizar inversiones fundamentales para escalar su adopción de la nube (p. ej., crear una landing zone, definir una CCo E, establecer un modelo de operaciones)

- Migración: migración de aplicaciones individuales
- Reinvención: optimización de productos y servicios e innovación en la nube

Stephen Orban definió estas etapas en la entrada del blog The Journey Toward Cloud-First & the Stages of Adoption en el blog Nube de AWS Enterprise Strategy. Para obtener información sobre su relación con la estrategia de AWS migración, consulte la guía de preparación para la migración.

CMDB

Consulte base de datos de administración de configuración.

repositorio de código

Una ubicación donde el código fuente y otros activos, como documentación, muestras y scripts, se almacenan y actualizan mediante procesos de control de versiones. Algunos repositorios en la nube comunes son GitHub o Bitbucket Cloud. Cada versión del código se denomina rama. En una estructura de microservicios, cada repositorio se encuentra dedicado a una única funcionalidad. Una sola canalización de CI/CD puede utilizar varios repositorios.

caché en frío

Una caché de búfer que está vacía no está bien poblada o contiene datos obsoletos o irrelevantes. Esto afecta al rendimiento, ya que la instancia de la base de datos debe leer desde la memoria principal o el disco, lo que es más lento que leer desde la memoria caché del búfer.

datos fríos

Datos a los que se accede con poca frecuencia y que suelen ser históricos. Al consultar este tipo de datos, normalmente se aceptan consultas lentas. Trasladar estos datos a niveles o clases de almacenamiento de menor rendimiento y menos costosos puede reducir los costos.

visión artificial (CV)

Campo de la IA que utiliza el machine learning para analizar y extraer información de formatos visuales, como imágenes y videos digitales. Por ejemplo, Amazon SageMaker AI proporciona algoritmos de procesamiento de imágenes para CV.

deriva de configuración

En el caso de una carga de trabajo, un cambio en la configuración con respecto al estado esperado. Podría provocar que la carga de trabajo deje de cumplir las normas y, por lo general, es gradual e involuntaria.

base de datos de administración de configuración (CMDB)

Repositorio que almacena y administra información sobre una base de datos y su entorno de TI, incluidos los componentes de hardware y software y sus configuraciones. Por lo general, los datos de una CMDB se utilizan en la etapa de detección y análisis de la cartera de productos durante la migración.

paquete de conformidad

Un conjunto de AWS Config reglas y medidas correctivas que puede reunir para personalizar sus controles de conformidad y seguridad. Puede implementar un paquete de conformidad como una entidad única en una región Cuenta de AWS y, o en una organización, mediante una plantilla YAML. Para obtener más información, consulta los paquetes de conformidad en la documentación. AWS Config

integración y entrega continuas (CI/CD)

El proceso de automatización de las etapas de origen, compilación, prueba, puesta en escena y producción del proceso de publicación del software. CI/CD se describe comúnmente como una canalización. CI/CD puede ayudarlo a automatizar los procesos, mejorar la productividad, mejorar la calidad del código y entregar más rápido. Para obtener más información, consulte Beneficios de la entrega continua. CD también puede significar implementación continua. Para obtener más información, consulte Entrega continua frente a implementación continua.

CV

Consulte visión artificial.

D

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 AWS Well-Architected Framework. Para obtener más información, consulte Clasificación de datos.

deriva de datos

Una variación significativa entre los datos de producción y los datos que se utilizaron para entrenar un modelo de machine learning, o un cambio significativo en los datos de entrada a lo largo del tiempo. La deriva de datos puede reducir la calidad, la precisión y la imparcialidad generales de las predicciones de los modelos de machine learning.

datos en tránsito

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

malla de datos

Marco de arquitectura que proporciona una propiedad de datos distribuida y descentralizada con una administración y una gobernanza centralizadas.

minimización de datos

El principio de recopilar y procesar solo los datos estrictamente necesarios. Practicar la minimización de los datos Nube de AWS puede reducir los riesgos de privacidad, los costos y la huella de carbono de la analítica.

perímetro de datos

Un conjunto de barreras preventivas en su AWS entorno que ayudan a garantizar que solo las identidades confiables accedan a los recursos confiables desde las redes esperadas. Para obtener más información, consulte Crear un perímetro de datos sobre. AWS

preprocesamiento de datos

Transformar los datos sin procesar en un formato que su modelo de ML pueda analizar fácilmente. El preprocesamiento de datos puede implicar eliminar determinadas columnas o filas y corregir los valores faltantes, incoherentes o duplicados.

procedencia de los datos

El proceso de rastrear el origen y el historial de los datos a lo largo de su ciclo de vida, por ejemplo, la forma en que se generaron, transmitieron y almacenaron los datos.

titular de los datos

Persona cuyos datos se recopilan y procesan.

almacenamiento de datos

Sistema de administración de datos que respalda la inteligencia empresarial, como los análisis. Los almacenes de datos suelen contener grandes cantidades de datos históricos y, por lo general, se utilizan para las consultas y los análisis.

lenguaje de definición de datos (DDL)

Instrucciones o comandos para crear o modificar la estructura de tablas y objetos de una base de datos.

lenguaje de manipulación de datos (DML)

Instrucciones o comandos para modificar (insertar, actualizar y eliminar) la información de una base de datos.

DDL

Consulte lenguaje de definición de bases de datos.

conjunto profundo

Combinar varios modelos de aprendizaje profundo para la predicción. Puede utilizar conjuntos profundos para obtener una predicción más precisa o para estimar la incertidumbre de las predicciones.

aprendizaje profundo

Un subcampo del ML que utiliza múltiples capas de redes neuronales artificiales para identificar el mapeo entre los datos de entrada y las variables objetivo de interés.

defense-in-depth

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. Al adoptar esta estrategia AWS, se añaden varios controles en diferentes capas de la AWS Organizations estructura para ayudar a proteger los recursos. Por ejemplo, un defense-in-depth enfoque podría combinar la autenticación multifactorial, la segmentación de la red y el cifrado.

administrador delegado

En AWS Organizations, un servicio compatible puede registrar una cuenta de AWS miembro para administrar las cuentas de la organización y gestionar los permisos de 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 .

Implementación

El proceso de hacer que una aplicación, características nuevas o correcciones de código se encuentren disponibles en el entorno de destino. La implementación abarca implementar cambios en una base de código y, a continuación, crear y ejecutar esa base en los entornos de la aplicación.

entorno de desarrollo

Consulte entorno.

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.

asignación de flujos de valor para el desarrollo (DVSM)

Proceso que se utiliza para identificar y priorizar las restricciones que afectan negativamente a la velocidad y la calidad en el ciclo de vida del desarrollo de software. DVSM amplía el proceso de asignación del flujo de valor diseñado originalmente para las prácticas de fabricación ajustada. Se centra en los pasos y los equipos necesarios para crear y transferir valor a través del proceso de desarrollo de software.

gemelo digital

Representación virtual de un sistema del mundo real, como un edificio, una fábrica, un equipo industrial o una línea de producción. Los gemelos digitales son compatibles con el mantenimiento predictivo, la supervisión remota y la optimización de la producción.

tabla de dimensiones

En un esquema en estrella, tabla más pequeña que contiene los atributos de datos sobre los datos cuantitativos en una tabla de hechos. Los atributos de la tabla de dimensiones suelen ser campos de texto o números discretos que se comportan como texto. Estos atributos se suelen utilizar para restringir consultas, filtrarlas y etiquetar los conjuntos de resultados.

desastre

Un evento que impide que una carga de trabajo o un sistema cumplan sus objetivos empresariales en su ubicación principal de implementación. Estos eventos pueden ser desastres naturales, fallos técnicos o el resultado de acciones humanas, como una configuración incorrecta involuntaria o un ataque de malware.

recuperación de desastres (DR)

Estrategia y proceso que utiliza para minimizar el tiempo de inactividad y la pérdida de datos a causa de un desastre. Para obtener más información, consulte Recuperación ante desastres de cargas de trabajo en AWS: Recovery in the Cloud in the AWS Well-Architected Framework.

DML

Consulte lenguaje de manipulación de bases de datos.

diseño basado en el dominio

Un enfoque para desarrollar un sistema de software complejo mediante la conexión de sus componentes a dominios en evolución, o a los objetivos empresariales principales, a los que sirve cada componente. Este concepto lo introdujo Eric Evans en su libro, Diseño impulsado por el dominio: abordando la complejidad en el corazón del software (Boston: Addison-Wesley Professional, 2003). Para obtener información sobre cómo utilizar el diseño basado en dominios con el patrón de higos estranguladores, consulte Modernización gradual de los servicios web antiguos de Microsoft ASP.NET (ASMX) mediante contenedores y Amazon API Gateway.

DR

Consulte recuperación ante desastres.

Detección de desviaciones

Seguimiento de las desviaciones con respecto a una configuración con línea de base. Por ejemplo, puedes usarlo AWS CloudFormation para detectar desviaciones en los recursos del sistema o puedes usarlo AWS Control Tower para detectar cambios en tu landing zone que puedan afectar al cumplimiento de los requisitos de gobierno.

DVSM

Consulte asignación de flujos de valor para el desarrollo.

E

EDA

Consulte análisis de datos de tipo exploratorio.

EDI

Consulte intercambio electrónico de datos.

computación en la periferia

La tecnología que aumenta la potencia de cálculo de los dispositivos inteligentes en la periferia de una red de IoT. En comparación con la computación en la nube, la computación de periferia puede reducir la latencia de la comunicación y mejorar el tiempo de respuesta.

intercambio electrónico de datos (EDI)

Intercambio automatizado de documentos comerciales entre organizaciones. Para más información, consulte ¿Qué es el intercambio electrónico de datos?

cifrado

Proceso de computación que transforma datos de texto plano, que son legibles por humanos, en texto cifrado.

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.

endianidad

El orden en el que se almacenan los bytes en la memoria del ordenador. Los sistemas big-endianos almacenan primero el byte más significativo. Los sistemas Little-Endian almacenan primero el byte menos significativo.

punto de conexión

Consulte punto de conexión de servicio.

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 final AWS PrivateLink y conceder permisos a otros Cuentas de AWS o a responsables AWS Identity and Access Management (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 Virtual Private Cloud (Amazon VPC).

planificación de recursos empresariales (ERP)

Sistema que automatiza y administra los procesos empresariales clave (como la contabilidad, MES y la administración de proyectos) de una empresa.

cifrado de sobre

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

entorno

Una instancia de una aplicación en ejecución. Los siguientes son los tipos de entornos más comunes en la computación en la nube:

- entorno de desarrollo: instancia de una aplicación en ejecución que solo se encuentra disponible para el equipo principal responsable del mantenimiento de la aplicación. Los entornos de desarrollo se utilizan para probar los cambios antes de promocionarlos a los entornos superiores. Este tipo de entorno a veces se denomina entorno de prueba.
- entornos inferiores: todos los entornos de desarrollo de una aplicación, como los que se utilizan para las compilaciones y pruebas iniciales.
- entorno de producción: instancia de una aplicación en ejecución a la que pueden acceder los usuarios finales. En un CI/CD proceso, el entorno de producción es el último entorno de implementación.
- entornos superiores: todos los entornos a los que pueden acceder usuarios que no sean del equipo de desarrollo principal. Esto puede incluir un entorno de producción, entornos de preproducción y entornos para las pruebas de aceptación por parte de los usuarios.

epopeya

En las metodologías ágiles, son categorías funcionales que ayudan a organizar y priorizar el trabajo. Las epopeyas brindan una descripción detallada de los requisitos y las tareas de implementación. Por ejemplo, las epopeyas AWS de seguridad de CAF incluyen la gestión de identidades y accesos, los controles de detección, la seguridad de la infraestructura, la protección de datos y la respuesta a incidentes. Para obtener más información sobre las epopeyas en la estrategia de migración de AWS , consulte la Guía de implementación del programa.

ERP

Consulte planificación de recursos empresariales.

análisis de datos de tipo exploratorio (EDA)

El proceso de analizar un conjunto de datos para comprender sus características principales. Se recopilan o agregan datos y, a continuación, se realizan las investigaciones iniciales para encontrar patrones, detectar anomalías y comprobar las suposiciones. El EDA se realiza mediante el cálculo de estadísticas resumidas y la creación de visualizaciones de datos.

F

tabla de hechos

Tabla central de un esquema en estrella. Almacena datos cuantitativos sobre operaciones empresariales. Por lo general, una tabla de hechos contiene dos tipos de columnas: las que contienen medidas y las que contienen una clave externa para una tabla de dimensiones.

Fail Fast

Filosofía que utiliza pruebas frecuentes e incrementales para reducir el ciclo de vida del desarrollo. Es una parte fundamental de los enfoques ágiles.

límite de aislamiento de errores

En el Nube de AWS, un límite, como una zona de disponibilidad Región de AWS, un plano de control o un plano de datos, que limita el efecto de una falla y ayuda a mejorar la resiliencia de las cargas de trabajo. Para más información, consulte AWS Fault Isolation Boundaries.

rama de característica

Consulte rama.

características

Los datos de entrada que se utilizan para hacer una predicción. Por ejemplo, en un contexto de fabricación, las características pueden ser imágenes que se capturan periódicamente desde la línea de fabricación.

importancia de las características

La importancia que tiene una característica para las predicciones de un modelo. Por lo general, esto se expresa como una puntuación numérica que se puede calcular mediante diversas

técnicas, como las explicaciones aditivas de Shapley (SHAP) y los gradientes integrados. Para obtener más información, consulte Interpretabilidad del modelo de aprendizaje automático con. AWS

transformación de funciones

Optimizar los datos para el proceso de ML, lo que incluye enriquecer los datos con fuentes adicionales, escalar los valores o extraer varios conjuntos de información de un solo campo de datos. Esto permite que el modelo de ML se beneficie de los datos. Por ejemplo, si divide la fecha del “27 de mayo de 2021 00:15:37” en “jueves”, “mayo”, “2021” y “15”, puede ayudar al algoritmo de aprendizaje a aprender patrones matizados asociados a los diferentes componentes de los datos.

peticiones con pocos pasos

Proporcionar a un LLM una pequeña cantidad de ejemplos que demuestren la tarea y el resultado deseado antes de pedirle que lleve a cabo una tarea similar. Esta técnica es una aplicación del aprendizaje contextual, mediante el que los modelos aprenden a partir de ejemplos (pasos) incrustados en las peticiones. La técnica de peticiones con pocos pasos puede ser eficaz para las tareas que requieren un formato, un razonamiento o un conocimiento del dominio específicos. Consulte también peticiones desde cero.

FGAC

Consulte control de acceso detallado.

control de acceso preciso (FGAC)

El uso de varias condiciones que tienen por objetivo permitir o denegar una solicitud de acceso.

migración relámpago

Método de migración de bases de datos que utiliza la replicación continua de datos mediante la captura de datos de cambio para migrar los datos en el menor tiempo posible, en lugar de utilizar un enfoque gradual. El objetivo es reducir al mínimo el tiempo de inactividad.

FM

Consulte modelo fundacional.

Modelo fundacional (FM)

Una gran red neuronal de aprendizaje profundo que se ha estado entrenando con conjuntos de datos masivos de datos generalizados y sin etiquetar. FMs son capaces de realizar una

amplia variedad de tareas generales, como comprender el lenguaje, generar texto e imágenes y conversar en lenguaje natural. Para más información, consulte ¿Qué son los modelos fundacionales?

G

IA generativa

Subconjunto de modelos de IA que se entrenaron con grandes cantidades de datos y que pueden utilizar una simple petición de texto para crear contenido y artefactos nuevos, como imágenes, videos, texto y audio. Para más información, consulte ¿Qué es la IA generativa?

bloqueo geográfico

Consulte restricciones geográficas.

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, consulta la sección Restringir la distribución geográfica del contenido en la CloudFront documentación.

Flujo de trabajo de Gitflow

Un enfoque en el que los entornos inferiores y superiores utilizan diferentes ramas en un repositorio de código fuente. El flujo de trabajo de Gitflow se considera heredado, mientras que el flujo de trabajo basado en enlaces troncales es el enfoque moderno preferido.

imagen dorada

Instantánea de un sistema o software que se usa como plantilla para implementar nuevas instancias de ese sistema o software. Por ejemplo, en la fabricación, una imagen dorada se puede utilizar para aprovisionar software en varios dispositivos y ayuda a mejorar la velocidad, la escalabilidad y la productividad de las operaciones de fabricación de dispositivos.

estrategia de implementación desde cero

La ausencia de infraestructura existente en un entorno nuevo. Al adoptar una estrategia de implementación desde cero para una arquitectura de sistemas, puede seleccionar todas las tecnologías nuevas sin que estas deban ser compatibles con una infraestructura existente, lo que también se conoce como implementación sobre infraestructura existente. Si está

ampliando la infraestructura existente, puede combinar las estrategias de implementación sobre infraestructuras existentes y de implementación desde cero.

barrera de protección

Una regla de alto nivel que ayuda a regular los recursos, las políticas y el cumplimiento en todas las unidades organizativas (OUs). 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 Amazon AWS Config AWS Security Hub CSPM GuardDuty AWS Trusted Advisor, Amazon Inspector y AWS Lambda cheques personalizados.

H

HA

Consulte alta disponibilidad.

migración heterogénea de bases de datos

Migración de la base de datos de origen a una base de datos de destino que utilice un motor de base de datos diferente (por ejemplo, de Oracle a Amazon Aurora). La migración heterogénea suele ser parte de un esfuerzo de rediseño de la arquitectura y convertir el esquema puede ser una tarea compleja. AWS ofrece AWS SCT, lo cual ayuda con las conversiones de esquemas.

alta disponibilidad (HA)

La capacidad de una carga de trabajo para funcionar de forma continua, sin intervención, en caso de desafíos o desastres. Los sistemas de alta disponibilidad están diseñados para realizar una conmutación por error automática, ofrecer un rendimiento de alta calidad de forma constante y gestionar diferentes cargas y fallos con un impacto mínimo en el rendimiento.

modernización histórica

Un enfoque utilizado para modernizar y actualizar los sistemas de tecnología operativa (TO) a fin de satisfacer mejor las necesidades de la industria manufacturera. Un histórico es un tipo de base de datos que se utiliza para recopilar y almacenar datos de diversas fuentes en una fábrica.

datos de reserva

Parte de los datos históricos etiquetados que se ocultan de un conjunto de datos que se utiliza para entrenar un modelo de machine learning. Puede utilizar los datos de reserva para evaluar el rendimiento del modelo mediante la comparación de las predicciones del modelo con los datos de reserva.

migración homogénea de bases de datos

Migración de la base de datos de origen a una base de datos de destino que comparte el mismo motor de base de datos (por ejemplo, Microsoft SQL Server a Amazon RDS para SQL Server). La migración homogénea suele formar parte de un esfuerzo para volver a alojar o redefinir la plataforma. Puede utilizar las utilidades de bases de datos nativas para migrar el esquema.

datos recientes

Datos a los que se accede con frecuencia, como datos en tiempo real o datos traslacionales recientes. Por lo general, estos datos requieren un nivel o una clase de almacenamiento de alto rendimiento para proporcionar respuestas rápidas a las consultas.

hotfix

Una solución urgente para un problema crítico en un entorno de producción. Debido a su urgencia, una revisión suele realizarse fuera del flujo de trabajo de DevOps publicación típico.

periodo de hiperatención

Periodo, inmediatamente después de la transición, durante el cual un equipo de migración administra y monitorea las aplicaciones migradas en la nube para solucionar cualquier problema. Por lo general, este periodo dura de 1 a 4 días. Al final del periodo de hiperatención, el equipo de migración suele transferir la responsabilidad de las aplicaciones al equipo de operaciones en la nube.

I

IaC

Consulte infraestructura como código.

políticas basadas en identidades

Política asociada a uno o más directores de IAM que define sus permisos en el entorno. Nube de AWS

aplicación inactiva

Aplicación que utiliza un promedio de CPU y memoria de entre 5 y 20 por ciento durante un periodo de 90 días. En un proyecto de migración, es habitual retirar estas aplicaciones o mantenerlas en las instalaciones.

IIoT

Consulte Internet de las cosas industrial.

infraestructura inmutable

Modelo que implementa una nueva infraestructura para las cargas de trabajo de producción en lugar de actualizar o modificar la infraestructura existente o aplicarle revisiones. Las infraestructuras inmutables son de manera intrínseca más coherentes, fiables y predecibles que las infraestructuras mutables. Para más información, consulte la práctica recomendada Implementación mediante una infraestructura inmutable en el Marco de AWS Well-Architected.

VPC entrante (de entrada)

En una arquitectura de AWS cuentas múltiples, una VPC que acepta, inspecciona y enruta las conexiones de red desde fuera de una aplicación. La arquitectura AWS de referencia de seguridad recomienda configurar la cuenta de red con entradas, salidas e inspección VPCs para proteger la interfaz bidireccional entre la aplicación y el resto de Internet.

migración gradual

Estrategia de transición en la que se migra la aplicación en partes pequeñas en lugar de realizar una transición única y completa. Por ejemplo, puede trasladar inicialmente solo unos pocos microservicios o usuarios al nuevo sistema. Tras comprobar que todo funciona correctamente, puede trasladar microservicios o usuarios adicionales de forma gradual hasta que pueda retirar su sistema heredado. Esta estrategia reduce los riesgos asociados a las grandes migraciones.

Industria 4.0

Término que introdujo Klaus Schwab en 2016 para referirse a la modernización de los procesos de fabricación mediante los avances en la conectividad, los datos en tiempo real, la automatización, el análisis, la IA y el ML.

infraestructura

Todos los recursos y activos que se encuentran en el entorno de una aplicación.

infraestructura como código (IaC)

Proceso de aprovisionamiento y administración de la infraestructura de una aplicación mediante un conjunto de archivos de configuración. La IaC se ha diseñado para ayudarlo a centralizar la administración de la infraestructura, estandarizar los recursos y escalar con rapidez a fin de que los entornos nuevos sean repetibles, fiables y consistentes.

Internet de las cosas industrial (T) IIo

El uso de sensores y dispositivos conectados a Internet en los sectores industriales, como el productivo, el eléctrico, el automotriz, el sanitario, el de las ciencias de la vida y el de la agricultura. Para obtener más información, consulte Creación de una estrategia de transformación digital de la Internet de las cosas (IIoT) industrial.

VPC de inspección

En una arquitectura de AWS cuentas múltiples, una VPC centralizada que gestiona las inspecciones del tráfico de red VPCs entre Internet y las redes locales (en una misma o Regiones de AWS diferente). La arquitectura AWS de referencia de seguridad recomienda configurar su cuenta de red con entrada, salida e inspección VPCs para proteger la interfaz bidireccional entre la aplicación e Internet en general.

Internet de las cosas (IoT)

Red de objetos físicos conectados con sensores o procesadores integrados que se comunican con otros dispositivos y sistemas a través de Internet o de una red de comunicación local. Para obtener más información, consulte ¿Qué es IoT?.

interpretabilidad

Característica de un modelo de machine learning que describe el grado en que un ser humano puede entender cómo las predicciones del modelo dependen de sus entradas. Para obtener más información, consulte Interpretabilidad del modelo de aprendizaje automático con. AWS

IoT

Consulte Internet de las cosas.

biblioteca de información de TI (ITIL)

Conjunto de prácticas recomendadas para ofrecer servicios de TI y alinearlos con los requisitos empresariales. La ITIL proporciona la base para la ITSM.

administración de servicios de TI (ITSM)

Actividades asociadas con el diseño, la implementación, la administración y el soporte de los servicios de TI para una organización. Para obtener información sobre la integración de las operaciones en la nube con las herramientas de ITSM, consulte la Guía de integración de operaciones.

ITIL

Consulte biblioteca de información de TI.

ITSM

Consulte administración de servicios de TI.

L

control de acceso basado en etiquetas (LBAC)

Una implementación del control de acceso obligatorio (MAC) en la que a los usuarios y a los propios datos se les asigna explícitamente un valor de etiqueta de seguridad. La intersección entre la etiqueta de seguridad del usuario y la etiqueta de seguridad de los datos determina qué filas y columnas puede ver el usuario.

zona de aterrizaje

Una landing zone es un AWS entorno multicuenta bien diseñado, escalable y seguro. Este es un punto de partida desde el cual las empresas pueden lanzar e implementar rápidamente cargas de trabajo y aplicaciones con confianza en su entorno de seguridad e infraestructura. Para obtener más información sobre las zonas de aterrizaje, consulte Configuración de un entorno de AWS seguro y escalable con varias cuentas.

modelo de lenguaje de gran tamaño (LLM)

Modelo de IA de aprendizaje profundo que se entrenó previamente con una gran cantidad de datos. Un LLM puede llevar a cabo varias tareas, como responder preguntas, resumir documentos, traducir textos a otros idiomas y completar oraciones. Para obtener más información, consulte Qué son. LLMs

migración grande

Migración de 300 servidores o más.

LBAC

Consulte control de acceso basado en etiquetas.

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.

migrar mediante lift-and-shift

Consulte Las 7 R.

sistema little-endian

Un sistema que almacena primero el byte menos significativo. Consulte también endianidad.

LLM

Consulte modelo de lenguaje de gran tamaño.

entornos inferiores

Consulte entorno.

M

machine learning (ML)

Un tipo de inteligencia artificial que utiliza algoritmos y técnicas para el reconocimiento y el aprendizaje de patrones. El ML analiza y aprende de los datos registrados, como los datos del Internet de las cosas (IoT), para generar un modelo estadístico basado en patrones. Para más información, consulte Machine learning.

rama principal

Consulte rama.

malware

Software diseñado para comprometer la seguridad o la privacidad de la computadora. El malware podría interrumpir los sistemas informáticos, filtrar información confidencial u obtener acceso

no autorizado. Algunos ejemplos de malware son los virus, los gusanos, el ransomware, los troyanos, el spyware y los registradores de pulsaciones de teclas.

Servicios administrados

Servicios de AWS para lo cual AWS opera la capa de infraestructura, el sistema operativo y las plataformas, y se accede a los puntos finales para almacenar y recuperar datos. Amazon Simple Storage Service (Amazon S3) y Amazon DynamoDB son ejemplos de servicios administrados. También se conocen como servicios abstractos.

sistema de ejecución de fabricación (MES)

Sistema de software para seguir, supervisar, documentar y controlar los procesos de producción que convierten las materias primas en productos acabados en la zona de producción.

MAP

Consulte Programa de aceleración de la migración.

mecanismo

Proceso completo mediante el que se crea una herramienta, se impulsa su adopción y, a continuación, se inspeccionan los resultados para hacer ajustes. Un mecanismo es un ciclo que se refuerza y mejora por sí mismo a medida que funciona. Para obtener más información, consulte Creación de mecanismos en el AWS Well-Architected Framework.

cuenta de miembro

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

MES

Consulte sistema de ejecución de fabricación.

Message Queuing Telemetry Transport (MQTT)

Un protocolo de comunicación ligero machine-to-machine (M2M), basado en el patrón de publicación/suscripción, para dispositivos de IoT con recursos limitados.

microservicio

Un servicio pequeño e independiente que se comunica a través de una red bien definida APIs y que, por lo general, es propiedad de equipos pequeños e independientes. Por ejemplo,

un sistema de seguros puede incluir microservicios que se adapten a las capacidades empresariales, como las de ventas o marketing, o a subdominios, como las de compras, reclamaciones o análisis. Los beneficios de los microservicios incluyen la agilidad, la escalabilidad flexible, la facilidad de implementación, el código reutilizable y la resiliencia. Para obtener más información, consulte Integrar microservicios mediante AWS servicios sin servidor.

arquitectura de microservicios

Un enfoque para crear una aplicación con componentes independientes que ejecutan cada proceso de la aplicación como un microservicio. Estos microservicios se comunican a través de una interfaz bien definida mediante un uso ligero. APIs Cada microservicio de esta arquitectura se puede actualizar, implementar y escalar para satisfacer la demanda de funciones específicas de una aplicación. Para obtener más información, consulte Implementación de microservicios en. AWS

Programa de aceleración de la migración (MAP)

Un AWS programa que proporciona soporte de consultoría, formación y servicios para ayudar a las organizaciones a crear una base operativa sólida para migrar a la nube y para ayudar a compensar el costo inicial de las migraciones. El MAP incluye una metodología de migración para ejecutar las migraciones antiguas de forma metódica y un conjunto de herramientas para automatizar y acelerar los escenarios de migración más comunes.

migración a escala

Proceso de transferencia de la mayoría de la cartera de aplicaciones a la nube en oleadas, con más aplicaciones desplazadas a un ritmo más rápido en cada oleada. En esta fase, se utilizan las prácticas recomendadas y las lecciones aprendidas en las fases anteriores para implementar una fábrica de migración de equipos, herramientas y procesos con el fin de agilizar la migración de las cargas de trabajo mediante la automatización y la entrega ágil. Esta es la tercera fase de la estrategia de migración de AWS.

fábrica de migración

Equipos multifuncionales que agilizan la migración de las cargas de trabajo mediante enfoques automatizados y ágiles. Los equipos de las fábricas de migración suelen incluir a analistas y propietarios de operaciones, empresas, ingenieros de migración, desarrolladores y DevOps profesionales que trabajan a pasos agigantados. Entre el 20 y el 50 por ciento de la cartera de aplicaciones empresariales se compone de patrones repetidos que pueden optimizarse mediante un enfoque de fábrica. Para obtener más información, consulte la discusión sobre las fábricas de migración y la Guía de fábricas de migración a la nube en este contenido.

metadatos de migración

Información sobre la aplicación y el servidor que se necesita para completar la migración. Cada patrón de migración requiere un conjunto diferente de metadatos de migración. Algunos ejemplos de metadatos de migración son la subred de destino, el grupo de seguridad y AWS la cuenta.

patrón de migración

Tarea de migración repetible que detalla la estrategia de migración, el destino de la migración y la aplicación o el servicio de migración utilizados. Ejemplo: rehospede la migración a Amazon EC2 AWS con Application Migration Service.

Migration Portfolio Assessment (MPA)

Herramienta en línea que proporciona información a fin de validar los argumentos comerciales necesarios para migrar a la Nube de AWS. La MPA ofrece una evaluación detallada de la cartera (adecuación del tamaño de los servidores, precios, comparaciones del costo total de propiedad, análisis de los costos de migración), así como una planificación de la migración (análisis y recopilación de datos de aplicaciones, agrupación de aplicaciones, priorización de la migración y planificación de oleadas). La herramienta MPA (requiere iniciar sesión) está disponible de forma gratuita para todos los AWS consultores y consultores de los socios de APN.

Evaluación de la preparación para la migración (MRA)

Proceso que consiste en obtener información sobre el estado de preparación de una organización para la nube, identificar sus puntos fuertes y débiles y elaborar un plan de acción para cerrar las brechas identificadas mediante el AWS CAF. Para obtener más información, consulte la Guía de preparación para la migración. La MRA es la primera fase de la estrategia de migración de AWS.

estrategia de migración

Enfoque utilizado para migrar una carga de trabajo a la Nube de AWS. Para más información, consulte la entrada Las 7 R de este glosario y también Mobilize your organization to accelerate large-scale migrations.

ML

Consulte machine learning.

modernización

Transformar una aplicación obsoleta (antigua o monolítica) y su infraestructura en un sistema ágil, elástico y de alta disponibilidad en la nube para reducir los gastos, aumentar la eficiencia

y aprovechar las innovaciones. Para más información, consulte Strategy for modernizing applications in the Nube de AWS.

evaluación de la preparación para la modernización

Evaluación que ayuda a determinar la preparación para la modernización de las aplicaciones de una organización; identifica los beneficios, los riesgos y las dependencias; y determina qué tan bien la organización puede soportar el estado futuro de esas aplicaciones. El resultado de la evaluación es un esquema de la arquitectura objetivo, una hoja de ruta que detalla las fases de desarrollo y los hitos del proceso de modernización y un plan de acción para abordar las brechas identificadas. Para más información, consulte Evaluating modernization readiness for applications in the Nube de AWS.

aplicaciones monolíticas (monolitos)

Aplicaciones que se ejecutan como un único servicio con procesos estrechamente acoplados. Las aplicaciones monolíticas presentan varios inconvenientes. Si una característica de la aplicación experimenta un aumento en la demanda, se debe escalar toda la arquitectura. Agregar o mejorar las características de una aplicación monolítica también se vuelve más complejo a medida que crece la base de código. Para solucionar problemas con la aplicación, puede utilizar una arquitectura de microservicios. Para obtener más información, consulte Descomposición de monolitos en microservicios.

MPA

Consulte Migration Portfolio Assessment.

MQTT

Consulte Message Queuing Telemetry Transport.

clasificación multiclase

Un proceso que ayuda a generar predicciones para varias clases (predice uno de más de dos resultados). Por ejemplo, un modelo de ML podría preguntar “¿Este producto es un libro, un automóvil o un teléfono?” o “¿Qué categoría de productos es más interesante para este cliente?”.

infraestructura mutable

Modelo que actualiza y modifica la infraestructura actual para las cargas de trabajo de producción. Para mejorar la coherencia, la fiabilidad y la previsibilidad, el AWS Well-Architected Framework recomienda el uso de una infraestructura inmutable como práctica recomendada.

O

OAC

Consulte control de acceso de origen.

OAI

Consulte identidad de acceso de origen.

OCM

Consulte administración del cambio organizacional.

migración fuera de línea

Método de migración en el que la carga de trabajo de origen se elimina durante el proceso de migración. Este método implica un tiempo de inactividad prolongado y, por lo general, se utiliza para cargas de trabajo pequeñas y no críticas.

OI

Consulte integración de operaciones.

OLA

Consulte acuerdo de nivel operativo.

migración en línea

Método de migración en el que la carga de trabajo de origen se copia al sistema de destino sin que se desconecte. Las aplicaciones que están conectadas a la carga de trabajo pueden seguir funcionando durante la migración. Este método implica un tiempo de inactividad nulo o mínimo y, por lo general, se utiliza para cargas de trabajo de producción críticas.

OPC-UA

Consulte Open Process Communications: arquitectura unificada.

Open Process Communications: arquitectura unificada (OPC-UA)

Un protocolo de machine-to-machine comunicación (M2M) para la automatización industrial. OPC-UA establece un estándar de interoperabilidad con esquemas de autenticación, autorización y cifrado de datos.

acuerdo de nivel operativo (OLA)

Acuerdo que aclara lo que los grupos de TI operativos se comprometen a ofrecerse entre sí, para respaldar un acuerdo de nivel de servicio (SLA).

revisión de la preparación operativa (ORR)

Lista de comprobación de preguntas y prácticas recomendadas asociadas que son útiles para comprender, evaluar, prevenir o reducir el alcance de los incidentes y posibles errores. Para más información, consulte Operational Readiness Reviews (ORR) en el Marco de AWS Well-Architected.

tecnología operativa (TO)

Sistemas de hardware y software que funcionan con el entorno físico para controlar las operaciones, los equipos y la infraestructura industriales. En el sector de la fabricación, la integración de los sistemas de TO y tecnología de la información (TI) es un enfoque clave para las transformaciones de la industria 4.0.

integración de operaciones (OI)

Proceso de modernización de las operaciones en la nube, que implica la planificación de la preparación, la automatización y la integración. Para obtener más información, consulte la Guía de integración de las operaciones.

registro de seguimiento organizativo

Un registro creado por y AWS CloudTrail que registra todos los eventos para todos los miembros Cuentas de AWS de una organización. 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 Crear un registro para una organización en la CloudTrail documentación.

administración del cambio organizacional (OCM)

Marco para administrar las transformaciones empresariales importantes y disruptivas desde la perspectiva de las personas, la cultura y el liderazgo. La OCM ayuda a las empresas a prepararse para nuevos sistemas y estrategias y a realizar la transición a ellos, al acelerar la adopción de cambios, abordar los problemas de transición e impulsar cambios culturales y organizacionales. En la estrategia de AWS migración, este marco se denomina aceleración de personal, debido a la velocidad de cambio que requieren los proyectos de adopción de la nube. Para obtener más información, consulte la Guía de OCM.

control de acceso de origen (OAC)

En CloudFront, una opción mejorada para restringir el acceso y proteger el contenido del Amazon Simple Storage Service (Amazon S3). El OAC admite todos los buckets de S3 Regiones de AWS, el cifrado del lado del servidor AWS KMS (SSE-KMS) y las solicitudes dinámicas `PUT` y `DELETE` dirigidas al bucket de S3.

identidad de acceso de origen (OAI)

En CloudFront, una opción para restringir el acceso y proteger el contenido de Amazon S3. Cuando utiliza OAI, CloudFront crea un principal con el que Amazon S3 puede autenticarse. Los directores autenticados solo pueden acceder al contenido de un bucket de S3 a través de una distribución específica. CloudFront Consulte también el OAC, que proporciona un control de acceso más detallado y mejorado.

ORR

Consulte revisión de la preparación operativa.

OT

Consulte tecnología operativa.

VPC saliente (de salida)

En una arquitectura de AWS cuentas múltiples, una VPC que gestiona las conexiones de red que se inician desde una aplicación. La arquitectura AWS de referencia de seguridad recomienda configurar la cuenta de red con entradas, salidas e inspección VPCs para proteger la interfaz bidireccional entre la aplicación e Internet en general.

P

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.

información de identificación personal (PII)

Información que, vista directamente o combinada con otros datos relacionados, puede utilizarse para deducir de manera razonable la identidad de una persona. Algunos ejemplos de información de identificación personal son los nombres, las direcciones y la información de contacto.

PII

Consulte información de identificación personal.

manual de estrategias

Conjunto de pasos predefinidos que capturan el trabajo asociado a las migraciones, como la entrega de las funciones de operaciones principales en la nube. Un manual puede adoptar la forma de scripts, manuales de procedimientos automatizados o resúmenes de los procesos o pasos necesarios para operar un entorno modernizado.

PLC

Consulte controlador lógico programable.

PLM

Consulte administración del ciclo de vida del producto.

policy

Objeto que puede definir permisos (consulte política basada en identidad), especificar las condiciones de acceso (consulte política basada en recursos) o definir los permisos máximos para todas las cuentas de una organización de AWS Organizations (consulte política de control de servicio).

persistencia políglota

Elegir de forma independiente la tecnología de almacenamiento de datos de un microservicio en función de los patrones de acceso a los datos y otros requisitos. Si sus microservicios tienen la misma tecnología de almacenamiento de datos, pueden enfrentarse a desafíos de implementación o experimentar un rendimiento deficiente. Los microservicios se implementan más fácilmente y logran un mejor rendimiento y escalabilidad si utilizan el almacén de datos que mejor se adapte a sus necesidades.

evaluación de cartera

Proceso de detección, análisis y priorización de la cartera de aplicaciones para planificar la migración. Para obtener más información, consulte la Evaluación de la preparación para la migración.

predicate

Condición de consulta que devuelve `true` o `false`. En general, se encuentra en una cláusula `WHERE`.

inserción de predicados

Técnica de optimización de consultas en bases de datos que filtra los datos de la consulta antes de transferirlos. Esta técnica reduce la cantidad de datos de la base de datos relacional que se tienen que recuperar y procesar. Además, mejora el rendimiento de las consultas.

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.

entidad principal

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

Privacidad desde el diseño

Enfoque de ingeniería de sistemas que tiene en cuenta la privacidad durante todo el proceso de desarrollo.

zonas alojadas privadas

Un contenedor que contiene información sobre cómo desea que Amazon Route 53 responda a las consultas de DNS de un dominio y sus subdominios dentro de uno o más VPCs. Para obtener más información, consulte Uso de zonas alojadas privadas en la documentación de Route 53.

control proactivo

Control de seguridad que se diseñó para evitar la implementación de recursos que no cumplan con la normativa. Estos controles analizan los recursos antes de aprovisionarlos. Si el recurso no cumple con los requisitos del control, no se aprovisiona. Para obtener más información, consulte la guía de referencia de controles en la AWS Control Tower documentación y consulte Controles proactivos en la sección Implementación de controles de seguridad en AWS.

administración del ciclo de vida del producto (PLM)

Administración de los datos y los procesos de un producto a lo largo de todo su ciclo de vida, desde el diseño, el desarrollo y el lanzamiento, pasando por el crecimiento y la madurez, hasta la reducción de su uso y su retirada.

entorno de producción

Consulte entorno.

controlador lógico programable (PLC)

En el sector de la fabricación, computadora adaptable y altamente fiable que supervisa las máquinas y automatiza los procesos de fabricación.

encadenamiento de peticiones

Uso de la salida de una petición de LLM como entrada para la siguiente petición a fin de generar mejores respuestas. Esta técnica se utiliza para dividir una tarea compleja en tareas secundarias o para refinar o ampliar de forma iterativa una respuesta preliminar. Ayuda a mejorar la precisión y la relevancia de las respuestas de un modelo y permite obtener resultados más detallados y personalizados.

seudonimización

El proceso de reemplazar los identificadores personales de un conjunto de datos por valores de marcadores de posición. La seudonimización puede ayudar a proteger la privacidad personal. Los datos seudonimizados siguen considerándose datos personales.

publish/subscribe (pub/sub)

Patrón que permite establecer comunicaciones asíncronas entre microservicios para mejorar la escalabilidad y la capacidad de respuesta. Por ejemplo, en un MES basado en microservicios, un microservicio puede publicar mensajes de eventos en un canal al que se pueden suscribir otros microservicios. El sistema puede agregar nuevos microservicios sin cambiar el servicio de publicación.

Q

plan de consulta

Serie de pasos, como instrucciones, que se utilizan para acceder a los datos de un sistema de base de datos relacional SQL.

regresión del plan de consulta

El optimizador de servicios de la base de datos elige un plan menos óptimo que antes de un cambio determinado en el entorno de la base de datos. Los cambios en estadísticas,

restricciones, configuración del entorno, enlaces de parámetros de consultas y actualizaciones del motor de base de datos PostgreSQL pueden provocar una regresión del plan.

R

Matriz RACI

Consulte responsable, fiable, consultada e informada (RACI).

RAG

Consulte generación aumentada por recuperación.

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.

Matriz RASCI

Consulte responsable, fiable, consultada e informada (RACI).

RCAC

Consulte control de acceso por filas y columnas.

réplica de lectura

Una copia de una base de datos que se utiliza con fines de solo lectura. Puede enrutar las consultas a la réplica de lectura para reducir la carga en la base de datos principal.

rediseñar

Consulte Las 7 R.

objetivo de punto de recuperación (RPO)

La cantidad de tiempo máximo aceptable desde el último punto de recuperación de datos. Esto determina qué se considera una pérdida de datos aceptable entre el último punto de recuperación y la interrupción del servicio.

objetivo de tiempo de recuperación (RTO)

La demora máxima aceptable entre la interrupción del servicio y el restablecimiento del servicio.

refactorizar

Consulte Las 7 R.

Region

Conjunto de AWS recursos en un área geográfica. Cada uno Región de AWS está aislado e independiente de los demás para proporcionar tolerancia a las fallas, estabilidad y resiliencia. Para más información, consulte Specify which Regiones de AWS your account can use.

regresión

Una técnica de ML que predice un valor numérico. Por ejemplo, para resolver el problema de "¿A qué precio se venderá esta casa?", un modelo de ML podría utilizar un modelo de regresión lineal para predecir el precio de venta de una vivienda en función de datos conocidos sobre ella (por ejemplo, los metros cuadrados).

volver a alojar

Consulte Las 7 R.

versión

En un proceso de implementación, el acto de promover cambios en un entorno de producción.

reubicar

Consulte Las 7 R.

redefinir la plataforma

Consulte Las 7 R.

recomprar

Consulte Las 7 R.

resiliencia

Capacidad de una aplicación para resistir interrupciones o recuperarse de ellas. Al planificar la resiliencia en la Nube de AWS, la alta disponibilidad y la recuperación ante desastres son consideraciones comunes. Para más información, consulte Resiliencia en la Nube de AWS.

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.

matriz responsable, confiable, consultada e informada (RACI)

Una matriz que define las funciones y responsabilidades de todas las partes involucradas en las actividades de migración y las operaciones de la nube. El nombre de la matriz se deriva de los tipos de responsabilidad definidos en la matriz: responsable (R), contable (A), consultado (C) e informado (I). El tipo de soporte (S) es opcional. Si incluye el soporte, la matriz se denomina matriz RASCI y, si la excluye, se denomina matriz RACI.

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.

retain

Consulte Las 7 R.

retirar

Consulte Las 7 R.

Generación aumentada de recuperación (RAG)

Tecnología de IA generativa mediante la que un LLM hace referencia a un origen de datos autorizado que se encuentra fuera de sus orígenes de datos de entrenamiento antes de generar una respuesta. Por ejemplo, un modelo de RAG podría hacer una búsqueda semántica en la base de conocimientos o en los datos personalizados de una organización. Para más información, consulte ¿Qué es RAG (generación aumentada por recuperación)?

rotación

Proceso mediante el que periódicamente se actualiza un secreto para que resulte más difícil que un atacante pueda acceder a las credenciales.

control de acceso por filas y columnas (RCAC)

El uso de expresiones SQL básicas y flexibles que tienen reglas de acceso definidas. El RCAC consta de permisos de fila y máscaras de columnas.

RPO

Consulte objetivo de punto de recuperación.

RTO

Consulte objetivo de tiempo de recuperación.

manual de procedimientos

Conjunto de procedimientos manuales o automatizados necesarios para realizar una tarea específica. Por lo general, se diseñan para agilizar las operaciones o los procedimientos repetitivos con altas tasas de error.

S

SAML 2.0

Un estándar abierto que utilizan muchos proveedores de identidad (IdPs). Esta función permite el inicio de sesión único (SSO) federado, de modo que los usuarios pueden iniciar sesión Consola de administración de AWS o llamar a las operaciones de la AWS API sin tener que crear un usuario en IAM para todos los miembros 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.

SCADA

Consulte control de supervisión y adquisición de datos.

SCP

Consulte política de control de servicio.

secreta

En AWS Secrets Manager, información confidencial o restringida, como una contraseña o credenciales de usuario, que se almacena de forma cifrada. Se compone del valor del secreto y de sus metadatos. El valor del secreto puede ser binario, una sola cadena o varias cadenas. Para más información, consulte What's in a Secrets Manager secret? en la documentación de Secrets Manager.

seguridad desde el diseño

Enfoque de ingeniería de sistemas que tiene en cuenta la seguridad durante todo el proceso de desarrollo.

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 cuatro tipos de controles de seguridad principales: preventivos, de detección, de respuesta y proactivos.

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.

automatización de la respuesta de seguridad

Acción predefinida y programada que está diseñada para responder automáticamente a un evento de seguridad o corregirlo. Estas automatizaciones sirven como controles de seguridad preventivos o adaptables que le ayudan a implementar las mejores prácticas AWS de seguridad. La modificación de un grupo de seguridad de VPC, la aplicación de revisiones a una instancia de Amazon EC2 o la rotación de credenciales son algunos ejemplos de acciones de respuesta automatizadas.

cifrado del servidor

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

política de control de servicio (SCP)

Política que proporciona un control centralizado de los permisos de todas las cuentas de una organización en AWS Organizations. SCPs defina barreras o establezca límites a las acciones que un administrador puede delegar en usuarios o roles. Puede utilizarlas SCPs como listas de permitidos o rechazados para especificar qué servicios o acciones están permitidos o prohibidos. Para obtener más información, consulte las políticas de control de servicios en la AWS Organizations documentación.

punto de enlace de servicio

La URL del punto de entrada de un Servicio de AWS. Para conectarse mediante programación a un servicio de destino, puede utilizar un punto de conexión. Para obtener más información, consulte Puntos de conexión de Servicio de AWS en Referencia general de AWS.

acuerdo de nivel de servicio (SLA)

Acuerdo que aclara lo que un equipo de TI se compromete a ofrecer a los clientes, como el tiempo de actividad y el rendimiento del servicio.

indicador de nivel de servicio (SLI)

Medición de un aspecto del rendimiento de un servicio, como la tasa de errores, la disponibilidad o el rendimiento.

objetivo de nivel de servicio (SLO)

Métrica objetivo que representa el estado de un servicio medido mediante un indicador de nivel de servicio.

modelo de responsabilidad compartida

Un modelo que describe la responsabilidad con AWS la que compartes la seguridad y el cumplimiento de 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.

SIEM

Consulte sistema de administración de eventos e información de seguridad.

único punto de error (SPOF)

Error en un único componente crítico de una aplicación que puede interrumpir el sistema.

SLA

Consulte acuerdo de nivel de servicio.

SLI

Consulte indicador de nivel de servicio.

SLO

Consulte objetivo de nivel de servicio.

split-and-seed modelo

Un patrón para escalar y acelerar los proyectos de modernización. A medida que se definen las nuevas funciones y los lanzamientos de los productos, el equipo principal se divide para

crear nuevos equipos de productos. Esto ayuda a ampliar las capacidades y los servicios de su organización, mejora la productividad de los desarrolladores y apoya la innovación rápida. Para más información, consulte Phased approach to modernizing applications in the Nube de AWS.

SPOF

Consulte único punto de error.

esquema en estrella

Estructura organizativa de una base de datos que utiliza una tabla de hechos de gran tamaño para almacenar datos transaccionales o medidos y una o varias tablas dimensionales más pequeñas para almacenar los atributos de los datos. Esta estructura está diseñada para utilizarse en un almacén de datos o con fines de inteligencia empresarial.

patrón de higo estrangulador

Un enfoque para modernizar los sistemas monolíticos mediante la reescritura y el reemplazo gradual de las funciones del sistema hasta que se pueda desmantelar el sistema heredado. Este patrón utiliza la analogía de una higuera que crece hasta convertirse en un árbol estable y, finalmente, se apodera y reemplaza a su host. El patrón fue presentado por Martin Fowler como una forma de gestionar el riesgo al reescribir sistemas monolíticos. Para ver un ejemplo con la aplicación de este patrón, consulte Modernización gradual de los servicios web antiguos de Microsoft ASP.NET (ASMX) mediante contenedores y Amazon API Gateway.

subred

Un intervalo de direcciones IP en la VPC. Una subred debe residir en una sola zona de disponibilidad.

control de supervisión y adquisición de datos (SCADA)

En el sector de la fabricación, sistema que utiliza hardware y software para supervisar los activos físicos y las operaciones de producción.

cifrado simétrico

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

pruebas sintéticas

Prueba de un sistema de manera que simule las interacciones de los usuarios para detectar posibles problemas o supervisar el rendimiento. Puede usar Amazon CloudWatch Synthetics para crear estas pruebas.

petición del sistema

Técnica para proporcionar contexto, instrucciones o pautas a un LLM para dirigir su comportamiento. Las peticiones del sistema ayudan a establecer el contexto y las reglas para las interacciones con los usuarios.

T

etiquetas

Pares clave-valor que actúan como metadatos para organizar los recursos. AWS Las etiquetas pueden ayudar a administrar, identificar, organizar, buscar y filtrar recursos de . Para obtener más información, consulte Etiquetado de los recursos de AWS.

variable de destino

El valor que intenta predecir en el ML supervisado. Esto también se conoce como variable de resultado. Por ejemplo, en un entorno de fabricación, la variable objetivo podría ser un defecto del producto.

lista de tareas

Herramienta que se utiliza para hacer un seguimiento del progreso mediante un manual de procedimientos. La lista de tareas contiene una descripción general del manual de procedimientos y una lista de las tareas generales que deben completarse. Para cada tarea general, se incluye la cantidad estimada de tiempo necesario, el propietario y el progreso.

entorno de prueba

Consulte entorno.

entrenamiento

Proporcionar datos de los que pueda aprender su modelo de ML. Los datos de entrenamiento deben contener la respuesta correcta. El algoritmo de aprendizaje encuentra patrones en los datos de entrenamiento que asignan los atributos de los datos de entrada al destino (la respuesta que desea predecir). Genera un modelo de ML que captura estos patrones. Luego, el modelo de ML se puede utilizar para obtener predicciones sobre datos nuevos para los que no se conoce el destino.

puerta de enlace de tránsito

Un centro de tránsito de red que puede usar para interconectar sus redes con VPCs las locales. Para obtener más información, consulte Qué es una pasarela de tránsito en la AWS Transit Gateway documentación.

flujo de trabajo basado en enlaces troncales

Un enfoque en el que los desarrolladores crean y prueban características de forma local en una rama de característica y, a continuación, combinan esos cambios en la rama principal. Luego, la rama principal se adapta a los entornos de desarrollo, preproducción y producción, de forma secuencial.

acceso de confianza

Otorgar permisos a un servicio que especifique para realizar tareas en su organización 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 AWS Organizations Utilización con otros AWS servicios en la AWS Organizations documentación.

ajuste

Cambiar aspectos de su proceso de formación a fin de mejorar la precisión del modelo de ML. Por ejemplo, puede entrenar el modelo de ML al generar un conjunto de etiquetas, incorporar etiquetas y, luego, repetir estos pasos varias veces con diferentes ajustes para optimizar el modelo.

equipo de dos pizzas

Un DevOps equipo pequeño al que puedes alimentar con dos pizzas. Un equipo formado por dos integrantes garantiza la mejor oportunidad posible de colaboración en el desarrollo de software.

U

incertidumbre

Un concepto que hace referencia a información imprecisa, incompleta o desconocida que puede socavar la fiabilidad de los modelos predictivos de ML. Hay dos tipos de incertidumbre: la incertidumbre epistémica se debe a datos limitados e incompletos, mientras que la incertidumbre aleatoria se debe al ruido y la aleatoriedad inherentes a los datos. Para más información, consulte la guía Cuantificación de la incertidumbre en los sistemas de aprendizaje profundo.

tareas indiferenciadas

También conocido como tareas arduas, es el trabajo que es necesario para crear y operar una aplicación, pero que no proporciona un valor directo al usuario final ni proporciona una ventaja competitiva. Algunos ejemplos de tareas indiferenciadas son la adquisición, el mantenimiento y la planificación de la capacidad.

entornos superiores

Consulte entorno.

V

succión

Una operación de mantenimiento de bases de datos que implica limpiar después de las actualizaciones incrementales para recuperar espacio de almacenamiento y mejorar el rendimiento.

control de versión

Procesos y herramientas que realizan un seguimiento de los cambios, como los cambios en el código fuente de un repositorio.

Emparejamiento de VPC

Una conexión entre dos VPCs que le permite enrutar el tráfico mediante direcciones IP privadas. Para obtener más información, consulte ¿Qué es una interconexión de VPC? en la documentación de Amazon VPC.

vulnerabilidad

Defecto de software o hardware que pone en peligro la seguridad del sistema.

W

caché caliente

Un búfer caché que contiene datos actuales y relevantes a los que se accede con frecuencia. La instancia de base de datos puede leer desde la caché del búfer, lo que es más rápido que leer desde la memoria principal o el disco.

datos templados

Datos a los que el acceso es infrecuente. Al consultar este tipo de datos, normalmente se aceptan consultas moderadamente lentas.

función de ventana

Función SQL que hace un cálculo en un grupo de filas que se relacionan de alguna manera con el registro actual. Las funciones de ventana son útiles para las tareas de procesamiento, como calcular una media móvil o acceder al valor de las filas en función de la posición relativa de la fila actual.

carga de trabajo

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

flujo de trabajo

Grupos funcionales de un proyecto de migración que son responsables de un conjunto específico de tareas. Cada flujo de trabajo es independiente, pero respalda a los demás flujos de trabajo del proyecto. Por ejemplo, el flujo de trabajo de la cartera es responsable de priorizar las aplicaciones, planificar las oleadas y recopilar los metadatos de migración. El flujo de trabajo de la cartera entrega estos recursos al flujo de trabajo de migración, que luego migra los servidores y las aplicaciones.

WORM

Consulte escritura única y lectura múltiple.

WQF

Consulte AWS Workload Qualification Framework.

escritura única y lectura múltiple (WORM)

Modelo de almacenamiento que escribe los datos una sola vez y evita que se eliminen o modifiquen. Los usuarios autorizados pueden leer los datos tantas veces como sea necesario, pero no los pueden cambiar. Esta infraestructura de almacenamiento de datos se considera inmutable.

Z

ataque de día cero

Ataque, normalmente de malware, que se aprovecha de una vulnerabilidad de día cero.

vulnerabilidad de día cero

Un defecto o una vulnerabilidad sin mitigación en un sistema de producción. Los agentes de amenazas pueden usar este tipo de vulnerabilidad para atacar el sistema. Los desarrolladores suelen darse cuenta de la vulnerabilidad a raíz del ataque.

peticiones desde cero

Proporcionar a un LLM instrucciones para llevar a cabo una tarea, pero sin ejemplos (pasos) que puedan ayudar a guiarlo. El LLM debe usar los conocimientos del entrenamiento previo para llevar a cabo la tarea. La eficacia de la petición desde cero depende de la complejidad de la tarea y de la calidad de la petición. Consulte también peticiones con pocos pasos.

aplicación zombi

Aplicación que utiliza un promedio de CPU y memoria menor al 5 por ciento. En un proyecto de migración, es habitual retirar estas aplicaciones.

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