Guía de CrowdStrike

CROWDSTRIKE

GUÍA RÁPIDA PARA PROTEGER LAS APPS NATIVAS DE LA NUBE

GUÍA RÁPIDA PARA PROTEGER LAS APPS NATIVAS DE LA NUBE

El ciclo de vida de las aplicaciones actualmente da prioridad a la velocidad, lo que obliga a los equipos de la nube a crear aplicaciones nativas basadas en una infraestructura programable que permita a las empresas cambiar y reconfigurar sobre la marcha. Además, la metodología de integración continua/entrega continua (IC/EC) introduce la automatización y la supervisión permanentes a lo largo del ciclo de vida de las aplicaciones, desde la integración y las pruebas, hasta la entrega y el despliegue, lo que redunda en una innovación más rápida.

Cuando vaya a realizar la migración a la nube, es fundamental conocer los entresijos de la seguridad. Compartirá y/o almacenará datos de la empresa en el proveedor de servicios que elija.

Para garantizar la seguridad de sus datos, hay muchos factores que deben tenerse en cuenta, desde la responsabilidad compartida hasta si los estándares de seguridad del proveedor elegido satisfacen sus propios requisitos. Todo esto puede resultar abrumador, especialmente si no es un experto en seguridad.

Para ayudarle, hemos elaborado una guía de inicio rápido para proteger las aplicaciones nativas de la nube.

1. **Implemente autenticación multifactor en el usuario raíz y los usuarios de IAM:** la autenticación multifactor (MFA) es esencial para proteger un entorno de nube, ya que permite disuadir a aquellos atacantes que, aunque pueden poner en riesgo las credenciales para acceder al entorno, no pueden comprometer el dispositivo MFA asociado a ellas. Además, en AWS, con la MFA en el usuario raiz, para los atacantes es más difícil recuperar la cuenta, lo que añade todavía más seguridad.

2. **Aplique una política estricta de contraseñas de IAM:** las políticas de contraseñas estrictas pueden impedir que se comprometa a los usuarios a través de ataques de fuerza bruta o con hashes filtrados. El empleo de una contraseña fuerte es fundamental para la seguridad básica de un entorno de nube.

3. **Activación del registro de API global:** para la seguridad de un entorno de nube es crucial activar servicios como AWS CloudTrail. De esta forma, puede rastrear, reaccionar y almacenar todos los eventos que se produzcan en su entorno de nube.

4. **Utilice servicios adecuados de administración de secretos para su almacenamiento:** servicios como AWS Systems Manager Parameter Store y AWS Secrets Manager permiten guardar y recuperar con seguridad los valores secretos. Este tipo de servicios son preferibles a la alternativa de almacenar los secretos directamente en código, variables de entorno u otros lugares en los que se pueden visualizar en texto sin cifrar.

5. **Utilice el cifrado en todos sitios:** algunos proveedores de nube, como GCP, aplican cifrado en todos sitios de forma predeterminada, sin embargo otros no. Para garantizar el cumplimiento normativo y la seguridad, se deben cifrar los datos en reposo y en tránsito con los controles adecuados que proporciona el proveedor de servicios de nube.

6. **Active y controle los servicios de supervisión de la seguridad:** servicios como AWS GuardDuty o GCP Event Threat Detection identifican cualquier actividad potencialmente maliciosa en un entorno. Estos servicios deben activarse y controlarse convenientemente para garantizar la identificación de toda actividad maliciosa.

7. **Cree copias de seguridad automáticas y manuales:** es importante utilizar copias de seguridad automáticas y manuales para los servicios de datos, como AWS Simple Storage Service (S3), AWS Relational Database Service (RDS) y AWS Elastic Block Store (EBS). Las copias de seguridad automáticas crean copias periódicas de los datos sin intervención del usuario, por otro lado, las copias de seguridad manuales ofrecen más confianza de que los datos no se han perdido si algo le ocurriera a la copia de seguridad automática.

8. **Aplique el principio del mínimo de privilegios:** si solo y exclusivamente concede a los usuarios los permisos necesarios para realizar su trabajo, la onda expansiva en caso de compromiso de una cuenta se minimiza. Además, el principio del mínimo de privilegios reduce el riesgo contra amenazas internas e incluso el de llamadas a API accidentales que puedan ser destructivas.

ACERCA DE CROWDSTRIKE

CrowdStrike, líder mundial en ciberseguridad, redefine la seguridad en la era de la nube mediante una plataforma de protección de endpoints que ha sido construida desde la base con el objetivo de detener las brechas de la seguridad. La arquitectura de un solo agente ligero de CrowdStrike Falcon® aprovecha la inteligencia artificial a escala de la nube y ofrece protección en tiempo real y visibilidad en toda la empresa, evitando los ataques a los endpoints, estén o no conectados a la red. Gracias a CrowdStrike Threat Graph®, CrowdStrike Falcon correlaciona a la semana, en tiempo real, más de 4 billones de eventos relativos a los endpoints en todo el planeta, alimentando una de las plataformas de datos para seguridad más avanzadas del mundo.

© 2021 CrowdStrike, Inc. Todos los derechos reservados.

SEGURIDAD DE LA NUBE DE CROWDSTRIKE

Idear, crear, proteger

FALCON CLOUD WORKLOAD PROTECTION

Proporciona una protección completa contra las brechas de seguridad en los entornos de nube privada, híbrida y multinube, lo que permite a los clientes adoptar y proteger rápidamente nuevas tecnologías con independencia del tipo de carga de trabajo.

FALCON HORIZON™

Ofrece visibilidad multinube, supervisión continua y detección de amenazas, y garantiza el cumplimiento normativo, permitiendo a DevOps desplegar aplicaciones con mayor velocidad y eficiencia. Es la solución que simplifica la administración de la seguridad de la nube.

SEGURIDAD DE LOS CONTENEDORES

Acelera las tareas críticas de detección, investigación y caza de amenazas en los contenedores, incluso en los que son efímeros tras ser inutilizados, para que los equipos de seguridad puedan proteger contenedores al ritmo de DevOps, sin añadir interrupciones.

EVALUACIÓN DE SEGURIDAD DE LA NUBE

Permite probar y evaluar la infraestructura de nube para determinar si se han implementado los niveles adecuados de seguridad y administración para superar los retos de seguridad inherentes al entorno.