Documento técnico

CROWDSTRIKE

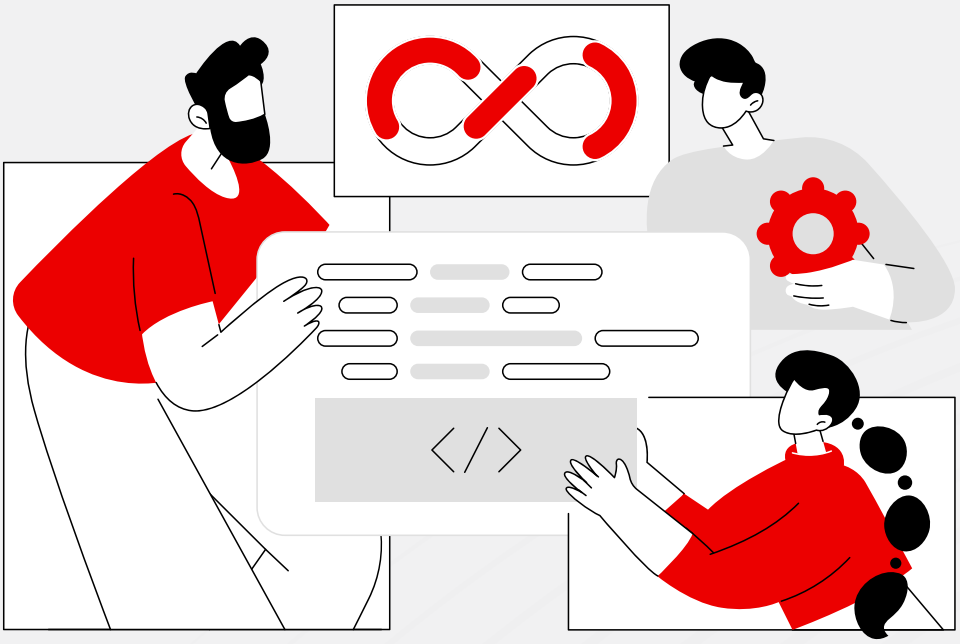
Las cinco prácticas recomendadas de seguridad en la nube para DevSecOps

Índice

Una introducción breve sobre DevSecOps

DevSecOps es la integración intencionada de la seguridad en la metodología de DevOps. La seguridad es primordial en un panorama en el que los equipos de desarrollo crean software cada vez más rápido. Al incluir la seguridad en el proceso de desarrollo, en lugar de pensar en ella en el último momento, los equipos pueden diseñar software seguros de manera eficiente y eficaz.

En este documento técnico se incluyen cinco prácticas recomendadas para garantizar que DevSecOps prospere en tu empresa. No se trata de prácticas infalibles, pero sin duda son un punto de partida certero para los profesionales de la seguridad y los desarrolladores en sus esfuerzos de crear, reconsiderar o mejorar sus programas de seguridad en la nube.



Práctica recomendada n.° 1: Asegurar el código en las fases tempranas de desarrollo

Es fundamental hacer hincapié en adoptar prácticas de codificación segura desde que se empieza a desarrollar el software para crear aplicaciones resilientes. La integración de medidas de seguridad en las primeras etapas del ciclo de vida del desarrollo del software ayuda a identificar y mitigar vulnerabilidades antes de que estas se incorporen al código base. De esta forma se reduce significativamente el riesgo de que se aprovechen tales vulnerabilidades. Los escáneres de seguridad, como las herramientas de pruebas estáticas de seguridad de aplicaciones (SAST), analizan continuamente el código para detectar patrones de codificación dudosos y posibles amenazas. Además, los equipos deben aprovechar herramientas como el escaneo de la infraestructura como código (IaC) para analizar con antelación sus plantillas de código y comprobar que no tengan vulnerabilidades que puedan abordarse fácilmente antes de la etapa de producción. Al implementar principios de codificación segura desde el principio, los desarrolladores podrán abordar los problemas de seguridad de manera proactiva. Así, el proceso de desarrollo será más eficiente y rentable a largo plazo.

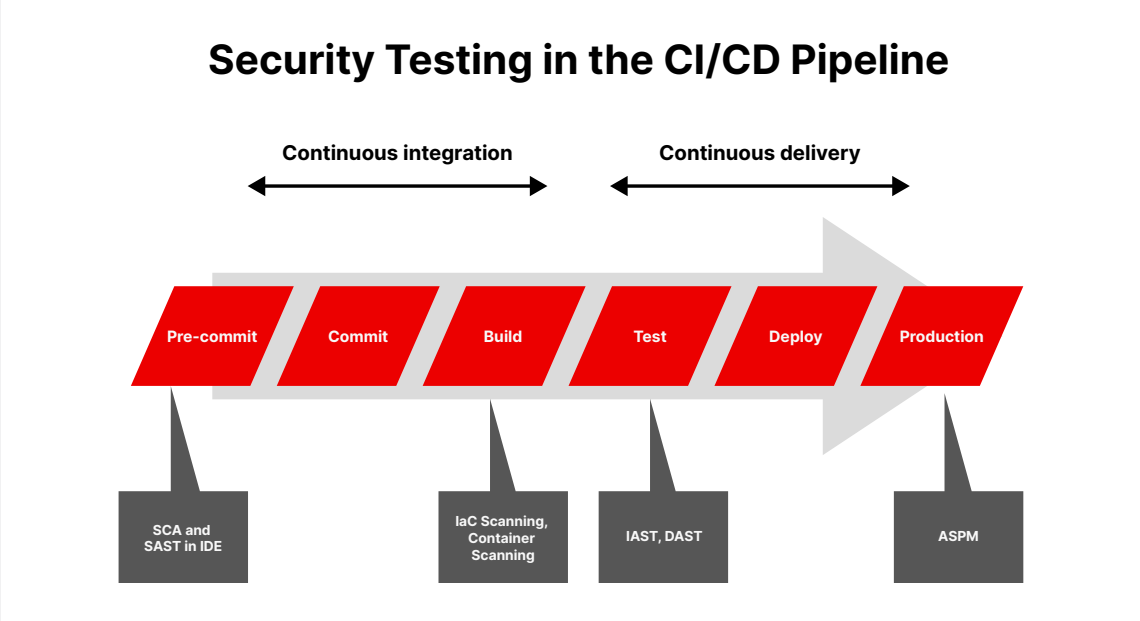
Las empresas deberían invertir en programas de formación y educación continuos para promover la codificación segura entre sus desarrolladores. La competición "Capture the flag" (CTF) y el programa "Security Champions" son iniciativas interesantes para hacer que el aprendizaje en materia de seguridad resulte práctico y entretenido. En los eventos CTF se les pide a los participantes que resuelvan acertijos o rompecabezas relacionados con la seguridad, lo que les permite comprender mejor las amenazas y las correspondientes técnicas de defensa. De manera similar, en los programas "Security Champions" se designa a ciertos miembros del equipo como defensores de la seguridad cuyo propósito es orientar a sus compañeros para garantizar que la seguridad sea la prioridad durante el proceso de desarrollo. Estas estrategias formativas no solo fomentan una cultura de seguridad consolidada, sino que también ayudan a los desarrolladores a diseñar software más seguro y fiable.

Además de estas iniciativas, las prácticas de codificación segura se verán reforzadas al adoptar estándares y directrices de codificación centrados en la seguridad. Las revisiones periódicas del código y las sesiones de programación con otros compañeros también contribuyen a la detección temprana de problemas de seguridad. Esto además favorece la colaboración del equipo de desarrollo en lo que respecta a la seguridad. Con todas estas estrategias, las empresas pueden establecer los cimientos para desarrollar aplicaciones seguras. Esto nos lleva a concluir que las empresas que adopten un enfoque integrado DevSecOps conseguirán diseñar aplicaciones más seguras a una mayor velocidad, especialmente cuando se combine con herramientas comunes y la visibilidad de los recursos.

Práctica recomendada n.º 2: Integrar en la canalización de DevOps

Antes de DevOps, el software se creaba, se probaba y se implementaba manualmente. Este proceso manual era lento y propenso a errores. Además, los cambios de código aparentemente seguros realizados en el entorno de desarrollo interrumpían con frecuencia el funcionamiento del entorno de producción. La transición hacia la canalización de integración continua y entrega continua (IC/EC) automatizada fue un avance significativo, ya que hizo posible diseñar software de manera más rápida y fiable. La canalización de IC/EC es ahora el estándar de los equipos de desarrollo de todo el mundo.

Actualmente, los equipos de software más sofisticados integran la seguridad directamente en su canalización de IC/EC. Este sistema ofrece de manera inmediata a los desarrolladores comentarios sobre problemas de seguridad, por lo que pueden evitar los cambios de contexto e impedir que las vulnerabilidades lleguen a los entornos de producción. Todas las herramientas que se muestran a continuación son ampliamente utilizadas y ofrecen beneficios únicos al integrarlas en la canalización de IC/EC:



Análisis de composición de software (SCA): Las herramientas SCA detectan las vulnerabilidades de las bibliotecas. Dado que los desarrolladores importan código de proveedores comerciales o de código abierto, SCA manda alertas sobre las vulnerabilidades conocidas que haya detectado en esas bibliotecas.

SAST: Las herramientas SAST proporcionan comentarios de manera inmediata sobre el código que no es seguro. Cuando los desarrolladores diseñan funciones, las herramientas SAST impiden que las vulnerabilidades comunes (como la inyección) se incluyan en tu repositorio de código.

Escaneo de infraestructura como código (IaC): Los análisis de IaC evitan las vulnerabilidades en la infraestructura. A medida que los equipos crean archivos de infraestructura codificados para garantizar que el software se aloje en un entorno aprobado, los análisis de IaC impiden que las vulnerabilidades (como el acceso público) se filtren en tu infraestructura.

Escaneo de contenedores: Los análisis de contenedores detectan las vulnerabilidades de la biblioteca del sistema operativo y mitigan los riesgos.

Pruebas dinámicas de seguridad de aplicaciones (DAST): Las herramientas DAST detectan las vulnerabilidades de las aplicaciones recopiladas. Una vez que las aplicaciones ya están creadas, las herramientas DAST buscan vulnerabilidades que son difíciles de localizar en el código fuente (como los fallos de autenticación).

Pruebas interactivas de seguridad de aplicaciones (IAST): Las herramientas IAST se utilizan para identificar vulnerabilidades en aplicaciones que ya están en funcionamiento.

Gestión de la posición de seguridad de las aplicaciones (ASPM): Las herramientas ASPM (como CrowdStrike Falcon® Cloud Security) detectan las vulnerabilidades y los riesgos de las aplicaciones cuando estas ya están instaladas.

Al incluir estas herramientas en la canalización de IC/EC, los controles de seguridad pasan a ser una parte integral del proceso de desarrollo. Este enfoque preventivo garantiza que se realice una supervisión continua de la seguridad, lo que reduce en gran medida la probabilidad de que las vulnerabilidades se cuelen en la etapa de producción.

Práctica recomendada n.° 3: Aprovechar los marcos y compartir el conocimiento

Modelado de amenazas en ciberseguridad para desarrollar software de forma segura

El modelado de amenazas es un enfoque de ciberseguridad preventivo centrado en identificar y evaluar posibles amenazas dirigidas a las aplicaciones de software durante la fase de desarrollo. Este proceso ayuda a los desarrolladores a anticipar y mitigar riesgos de seguridad antes de que los ciberdelincuentes puedan aprovechar las vulnerabilidades. Al analizar sistemáticamente la arquitectura, los flujos de datos y los posibles perfiles de los ciberdelincuentes, los desarrolladores pueden asegurarse de que las medidas de seguridad se implementan en las primeras fases del ciclo de vida del software. Los equipos también pueden utilizar los marcos de modelos de amenazas como STRIDE, DREAD y PASTA, así como los esquemas de amenazas, a modo de referencia. Este enfoque no solo mejora la posición de seguridad general de la aplicación, sino que además evita la complejidad y los gastos adicionales de abordar las vulnerabilidades después de la implementación.

Revisiones de la arquitectura de las aplicaciones

Asegúrate de realizar revisiones de la arquitectura, ya que son fundamentales para garantizar la resiliencia y eficiencia de las aplicaciones de software. El objetivo es comprobar lo antes posible si existen riesgos técnicos antes de seguir avanzando. En estas revisiones debe examinarse de manera exhaustiva el diseño estructural de una aplicación, incluidos sus componentes, interfaces y estrategias de gestión de datos. Dado que el propósito de una revisión de la arquitectura es reconocer posibles puntos débiles, ineficiencias o problemas de escalabilidad que puedan afectar al rendimiento y la seguridad, resulta útil saber cuál es el mejor punto de partida. La primera recomendación es adoptar marcos como TOGAF e ISO/IEC270001. Por otro lado, herramientas como SCA ayudan a los equipos a encontrar buenas referencias y asistencia para realizar revisiones de la arquitectura y garantizar que se lleven a cabo correctamente. Además, al realizar este tipo de revisiones de manera periódica, los equipos de desarrollo pueden estar seguros de que sus aplicaciones se sustentan en unos cimientos consolidados y son capaces de satisfacer necesidades actuales y futuras. Por si fuera poco, esta práctica también facilita el cumplimiento de los estándares y las prácticas recomendadas del sector.

Conocimiento compartido: prácticas recomendadas sobre la infraestructura

Compartir adecuadamente las prácticas recomendadas sobre la infraestructura es esencial para mantener la resiliencia y eficiencia del entorno de TI. Los marcos como CIS Benchmark, las prácticas recomendadas de los proveedores de servicios en la nube (ej.: una revisión bien diseñada), el NIST, la guía ITIL y el Cloud Security Alliance Cloud Control Matrix son recursos excelentes para empezar. El hecho de compartir las prácticas recomendadas sobre la infraestructura implica difundir información, estrategias y directrices fundamentales relacionadas con la gestión de la infraestructura, como la configuración de las redes, la gestión de los servidores y la implementación en la nube. Es necesario que las empresas promuevan una cultura de aprendizaje y colaboración constantes a fin de garantizar que sus equipos estén preparados para diseñar y mantener soluciones de infraestructura consolidadas. Pueden organizar talleres e implementar la elaboración de documentos y revisiones entre compañeros de manera periódica para fomentar el intercambio de información y mejorar la gestión de la infraestructura.

Revisiones de seguridad

Las revisiones de seguridad son fundamentales para favorecer la integridad y seguridad de las aplicaciones de software y los sistemas de TI. En estas revisiones se realiza una evaluación exhaustiva de los controles de seguridad, políticas y procedimientos de una aplicación para identificar vulnerabilidades y garantizar el cumplimiento de los estándares de seguridad. Suelen incluirse revisiones del código, pruebas de penetración y evaluaciones de la configuración. Al realizar este tipo de revisiones con regularidad, las empresas pueden detectar y abordar los fallos de seguridad que puedan surgir antes de que los ciberdelincuentes puedan aprovecharse de estas vulnerabilidades. Algunos recursos como el OWASP Software Assurance Maturity Model, el NIST 800-53 y los Controles CIS pueden resultar útiles, ya que abarcan cuestiones de cumplimiento y vulnerabilidades. Este enfoque preventivo no solo sirve para proteger datos y recursos confidenciales, sino que también aumenta la confianza depositada en la posición de seguridad de la empresa.

Práctica recomendada n.° 4: Evaluar la posición de seguridad para mejorar los resultados

Medir el éxito de los desarrolladores y equipos de seguridad puede ser todo un reto. Lo que puede ser todo un éxito para los desarrolladores (ej.: número de aplicaciones que pasan a la fase de producción y rapidez con la que esto ocurre) no tiene por qué serlo también para los equipos de seguridad (ej.: número de vulnerabilidades que se han abordado o cantidad de amenazas que se han detenido). En la práctica, para medir la posición de seguridad es necesario evaluar la eficacia de los controles de seguridad de la empresa, así como su capacidad para proteger aplicaciones, entornos de nube y endpoints. Todos estos elementos están interconectados, por eso es fundamental comprender el entorno en su totalidad. Las aplicaciones, ya estén alojadas en entornos locales o en la nube, suelen ser el principal objetivo de los ciberdelincuentes. Por ello, es necesario incluir medidas de seguridad sólidas y realizar una supervisión continua. De manera similar, y debido a su naturaleza dinámica y escalable, los entornos de la nube precisan de prácticas de seguridad preventivas para evitar errores de configuración y el acceso no autorizado.

Lo primordial es comprender la posición de seguridad del entorno de producción. Para ello, es necesario supervisar continuamente las aplicaciones y la infraestructura. El objetivo es detectar las amenazas y responder en tiempo real. La implementación de sistemas de gestión de eventos e información de seguridad (SIEM) y la respuesta automática ante incidentes resulta útil para identificar y mitigar brechas rápidamente, lo que garantiza la protección de los datos confidenciales y la continuidad del negocio.

Los endpoints y las cargas de trabajo en la nube, incluidas las estaciones de trabajo, los dispositivos móviles y los dispositivos del Internet de las cosas (IoT), son posibles puntos de entrada de ciberamenazas. Para garantizar que estas cargas de trabajo y endpoints son seguros es necesario implementar soluciones de detección y respuesta para endpoints (EDR) y un proceso periódico de gestión de parches. Las empresas pueden conseguir una posición de seguridad integral para mitigar todo tipo de riesgos al integrar las medidas de seguridad en las aplicaciones, la infraestructura de la nube y los endpoints.

Para poder prevenir brechas en entornos reales es necesario adoptar un enfoque preventivo en el que se incluyan evaluaciones de seguridad habituales, pruebas de penetración y garantías de cumplimiento de las prácticas recomendadas en materia de seguridad. Las empresas reducirán las vulnerabilidades, facilitarán el cumplimiento de los estándares de seguridad y se harán más fuertes frente a las ciberamenazas al evaluar y mejorar la posición de seguridad. Por si fuera poco, protegerán sus recursos digitales y su reputación.

Para mantener y mejorar la posición de seguridad es fundamental implementar un sistema SIEM. Este sistema incluye funciones de registro y supervisión centralizadas. De este modo, las empresas pueden recopilar y analizar eventos de seguridad, así como responder, en tiempo real. Conseguirás una estrategia de seguridad más cohesionada y preventiva al integrar la telemetría de la canalización de DevSecOps en una solución SIEM.

Las soluciones SIEM reúnen datos de diversas fuentes, como logs de aplicaciones, el tráfico de la red y la telemetría de endpoints. Este enfoque centralizado ofrece a los equipos de seguridad una vista integral de su entorno, por lo que pueden identificar anomalías o posibles amenazas de manera más eficiente. Además, las soluciones SIEM pueden incorporar datos tanto de herramientas propias como de otras externas. Esto ofrece una perspectiva más rica y detallada del panorama de seguridad de una empresa.

Práctica recomendada n.° 5: Utilizar los datos de producción para ajustar los procedimientos en consecuencia durante las primeras etapas de la canalización

El objetivo principal de trasladar la seguridad a la canalización de desarrollo es identificar y resolver problemas antes de que el producto pase a la fase de producción. El propósito de este enfoque preventivo es incluir la seguridad en todas las fases del proceso de desarrollo de software para reducir las vulnerabilidades y mejorar la posición de seguridad en general. El escaneo de IaC y SCA son herramientas esenciales en este proceso. El escaneo de IaC garantiza que las implementaciones en la infraestructura sean seguras y cumplan con la normativa desde el principio. Por su parte, SCA ayuda a identificar y gestionar las vulnerabilidades de dependencias y componentes externos. Las empresas podrán evitar que numerosos problemas lleguen a la fase de producción al integrar estas herramientas con antelación, lo que reduce el riesgo de sufrir brechas de seguridad. Además de recibir comentarios, también es fundamental realizar una supervisión continua. De la supervisión de los entornos de ejecución obtenemos información práctica sobre el funcionamiento de los controles de seguridad en condiciones reales. Gracias a estos comentarios, los equipos pueden determinar la eficacia de la adopción de DevSecOps e identificar áreas de mejora.

No obstante, también es importante utilizar los datos de los entornos de producción para perfeccionar y mejorar continuamente las prácticas de seguridad. De la supervisión de los entornos de ejecución obtenemos información práctica sobre el funcionamiento de los controles de seguridad en condiciones reales. Gracias a estos comentarios, los equipos pueden determinar la eficacia de la adopción de DevSecOps e identificar áreas de mejora. Es necesario que las empresas realicen los cambios necesarios en función de estos datos con regularidad para garantizar que sus medidas de seguridad sigan siendo pertinentes y se adapten en consecuencia. Este ciclo constante de evaluación y ajustes no solo mejora la protección, sino que además permite a los desarrolladores seguir diseñando con agilidad y velocidad sin que esto afecte a la seguridad.

Conclusión

Estas cinco prácticas recomendadas no abarcan absolutamente todos los aspectos en materia de seguridad, pero ofrecen un punto de partida y un enfoque adecuados para que los equipos de DevSecOps puedan diseñar, mejorar y crear aplicaciones. CrowdStrike proporciona las herramientas necesarias para que los equipos puedan seguir estas prácticas recomendadas, con la oferta de productos de seguridad del código a la nube más completa del mercado. Conoce por qué CrowdStrike es considerado líder y descubre cómo puede ayudarte Falcon Cloud Security a garantizar la seguridad y la agilidad de los equipos de DevSecOps.

Consigue gratis una comprobación de la seguridad de tu nube

Acerca de CrowdStrike

CrowdStrike (Nasdaq: CRWD), líder mundial en ciberseguridad, ha redefinido la seguridad moderna con la plataforma nativa en la nube más avanzada del mundo, para proteger aspectos fundamentales del riesgo empresarial: las cargas de trabajo, la identidad y los datos, tanto en los endpoints como en la nube.

Gracias a CrowdStrike Security Cloud y una inteligencia artificial de talla mundial, la plataforma CrowdStrike Falcon® se nutre de indicadores en tiempo real, inteligencia sobre amenazas, información de las herramientas evolutivas de los adversarios y telemetría enriquecida con datos de toda la empresa, para facilitar detecciones hiperprecisas, protección y remediación automatizadas, Threat Hunting de élite y observación de vulnerabilidades por prioridades.

Desarrollada expresamente en la nube con una arquitectura de agente ligero único, la plataforma Falcon ofrece un despliegue rápido y escalable, una protección y un rendimiento superiores, una menor complejidad y una rentabilidad inmediata.

CrowdStrike: **We stop breaches.**

Más información: https://www.crowdstrike.com/es-es/

Síguenos: Blog | X | LinkedIn | Facebook | Instagram

Empieza una prueba gratuita hoy mismo: https://www.crowdstrike.com/free-trial-guide/