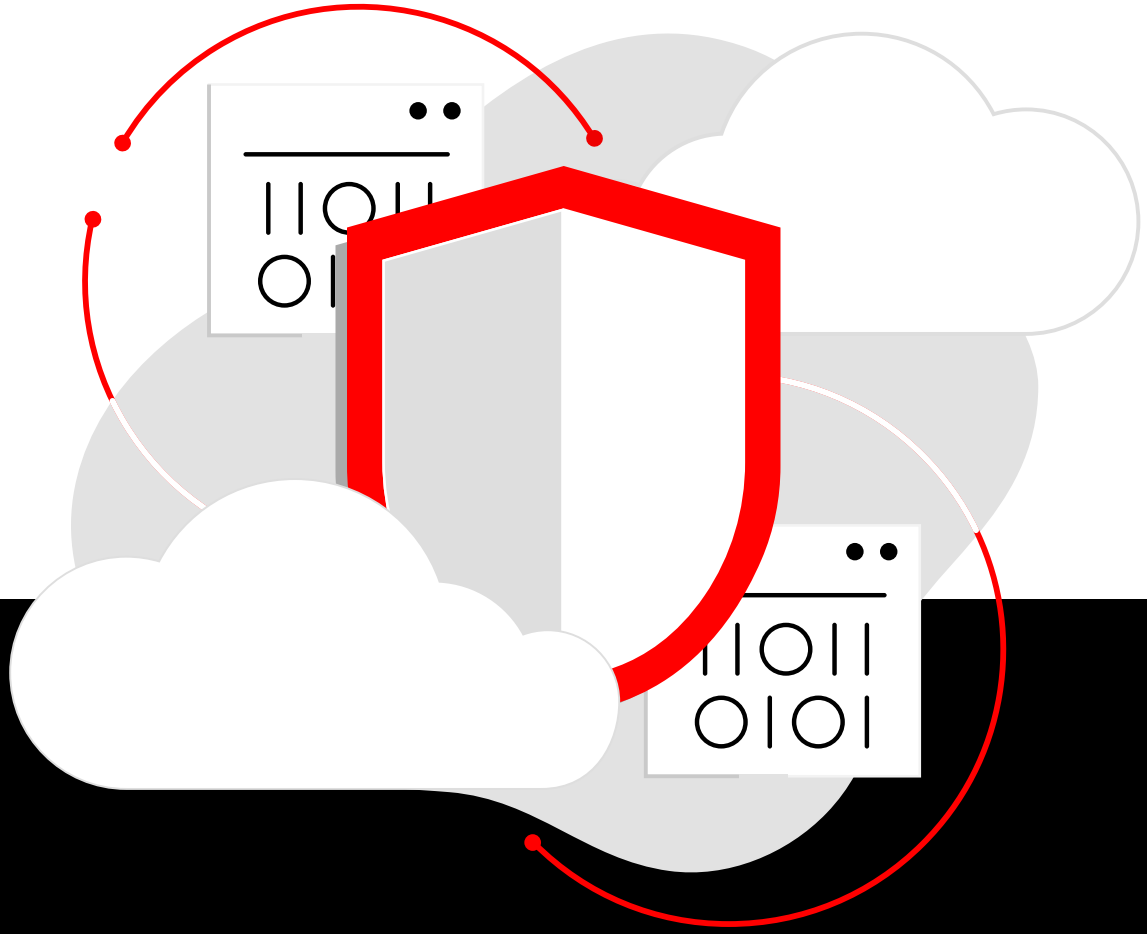
Red Hat



Modernice y proteja los ciclos de vida de las aplicaciones con DevSecOps

Contenido

Introducción

La seguridad de las aplicaciones es importante para el mundo digital

A medida que más empresas adoptan las tecnologías de nube, contenedores y microservicios para competir en un mundo digital, la seguridad sigue siendo una prioridad. De hecho, el 50 % de los líderes de TI sénior de las empresas incluyen a la ciberseguridad como una de las tres prioridades de sus iniciativas tecnológicas[1] y, al mismo tiempo, el 86 % espera que aumente el ritmo de la transformación digital en 2021[1].

Estas tecnologías nuevas requieren un enfoque distinto para la seguridad, ya que los tradicionales que se basan en el perímetro no son eficientes en los entornos distribuidos. Además, la velocidad del desarrollo y la flexibilidad de la implementación aumentan con las metodologías de DevOps y las desarrolladas en la nube, lo cual significa que es importante tener en cuenta la seguridad al principio del proceso. Si se aplican las medidas al final de los ciclos de desarrollo, puede haber demoras en la distribución y menor protección.

Con los enfoques y las prácticas de **DevSecOps** podrá mejorar la protección de los entornos de aplicación y su empresa.

¿Qué es DevSecOps?

DevSecOps amplía la cultura de colaboración de DevOps e incorpora la seguridad en todos los ciclos de vida de las aplicaciones. Incluye a las personas, los procesos y la tecnología para que la seguridad se siga extendiendo en los entornos distribuidos.

Con DevSecOps, las tareas en materia de seguridad son responsabilidad de todos los equipos, no de uno solo que debe encargarse de completarlas y aplicarlas al final del proceso de desarrollo e implementación. Los integrantes de los equipos de seguridad, desarrollo y operaciones trabajan en conjunto y comparten los comentarios, el conocimiento adquirido y la información valiosa. Este enfoque permite incorporar la seguridad al comienzo del desarrollo de aplicaciones y de la implementación de infraestructuras, lo cual aumenta la protección y reduce los riesgos.

Ventajas de DevSecOps

Mejore la seguridad y reduzca el riesgo.

Aborde los problemas de seguridad en la etapa de desarrollo, en vez de en la de producción, para proteger mejor las aplicaciones y reducir la cantidad de implementaciones que se demoran o se detienen por las verificaciones de políticas fallidas.

Solucione los problemas de seguridad más rápido.

Aplique prácticas y herramientas de seguridad modernas que fomenten la colaboración e incorporen la automatización para agilizar el lanzamiento de los ciclos, reducir el tiempo que se necesita para solucionar los problemas de seguridad en la etapa de producción y ahorrar tiempo y dinero.

Aumente el cumplimiento normativo y el control.

Adopte procesos y herramientas automatizadas para reducir el riesgo de cometer errores manuales y aumentar la capacidad de predicción y repetición para mejorar el cumplimiento y simplificar los procesos de auditoría.

1 *Flexera. "2021 Flexera State of Tech Spend Report", enero de 2021.*

Desafíos de la implementación de DevSecOps

Si bien los enfoques de DevSecOps ofrecen muchas ventajas, existen varios factores que dificultan su implementación.

- **Panorama de la seguridad en evolución.** Las amenazas a la seguridad y las normas (incluidos los requisitos empresariales, técnicos y geográficos) cambian a un ritmo acelerado, lo cual dificulta mantenerse actualizado.
- **Complejidad del entorno de la aplicación.** Puede ser un desafío comprender las conexiones y las implicaciones de seguridad de las distintas tecnologías, como contenedores, microservicios y servicios de nube, ya que forman parte de entornos complejos de las aplicaciones a gran escala.
- **Procesos y herramientas actuales ineficientes.** Muchos equipos empiezan por aplicar sus herramientas y procesos actuales a las iniciativas de DevSecOps, pero descubren que este enfoque no es compatible con sus metas a largo plazo.
- **Herramientas de seguridad múltiples.** Las pruebas, la integración, el mantenimiento y la elección de las herramientas de seguridad adecuadas para su empresa toman tiempo y requieren investigación y esfuerzos permanentes.

La aplicación exitosa de DevSecOps depende de la cultura, el proceso y la tecnología

El uso de DevSecOps para proteger los ciclos de vida de las aplicaciones requiere modificaciones y alineación en tres áreas: la cultura, el proceso y la tecnología.

Cultura

Fomente la colaboración y las metas compartidas entre los equipos de desarrollo, operaciones y seguridad. Ayude a que cada equipo comprenda los fundamentos y los métodos para incorporar la seguridad dentro de los ciclos de vida de las aplicaciones.

Proceso

Estandarice, documente y automatice los procesos y las cargas de trabajo para mejorar la eficiencia y la seguridad en los ciclos de vida de las aplicaciones.

Tecnología

Integre el desarrollo e implementación de las aplicaciones y las plataformas, herramientas y procesos de operaciones en un solo sistema uniforme.

Obtenga más información sobre los aspectos básicos de DevSecOps

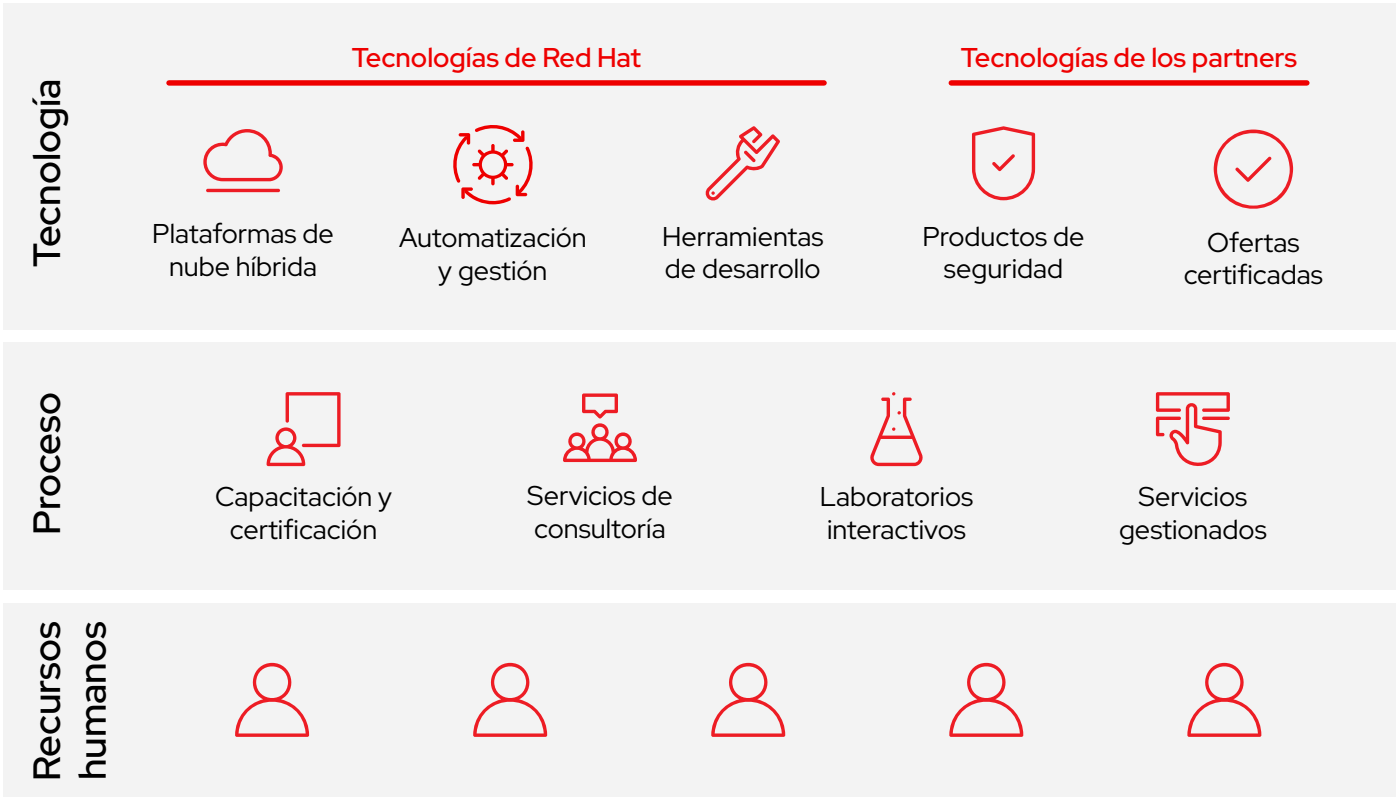
Lea la **publicación del blog Why your DevSecOps practice may be falling short** para obtener más información sobre los cambios que se necesitan para implementar DevSecOps con éxito. Lea el **ebook Aumente la seguridad de la nube híbrida** y descubra las formas para proteger su empresa con enfoques de seguridad desarrollados en la nube.

La estrategia de Red Hat DevSecOps

Red Hat cuenta con un ecosistema de partners certificados, una amplia experiencia y plataformas innovadoras para diseñar, proteger e implementar aplicaciones en entornos de nube híbrida. Esta combinación le permite implementar soluciones de DevSecOps integrales para mejorar la seguridad de las aplicaciones, reducir los riesgos, aumentar el rendimiento y maximizar el valor de sus inversiones.

Las plataformas de Red Hat® proporcionan una base ideal para las soluciones de DevSecOps gracias a una cadena de suministro de contenido de confianza, el respaldo de un equipo de seguridad exclusivo y características de seguridad clave de las versiones anteriores. Nuestros partners amplían y mejoran esta base con productos innovadores e integrados para que se implementen la seguridad y la automatización en todos los ciclos de vida de las aplicaciones. También ofrecemos **cursos de capacitación y certificación**, **laboratorios interactivos**, **servicios de consultoría** y **ofertas gestionadas** para ayudarlo a implementar DevSecOps con éxito.

Podemos ayudarlo en cualquier etapa del proceso de adopción de DevSecOps en la que se encuentre. Con las soluciones expandibles y modulares y los servicios de especialistas que ofrecemos, puede implementar lo que necesite hoy, adaptarse a los cambios del futuro y aprender los métodos y los enfoques necesarios para adoptar DevSecOps de manera eficiente y eficaz.



Diseñe una base de DevSecOps abierta con los productos de Red Hat

Red Hat OpenShift

Red Hat OpenShift® es una plataforma de nube híbrida lista para empresas y centrada en la seguridad que incluye herramientas de DevOps y funciones de seguridad que se habilitan de forma predeterminada. Esta plataforma funciona con las tecnologías y las herramientas de seguridad de terceros y de partners para aumentar la seguridad e implementar soluciones DevSecOps sólidas. Lea **Red Hat OpenShift security guide** y descubra de qué forma se aborda la seguridad en toda la stack de tecnología.

Pruébelo gratis

Características de seguridad clave

- Security-Enhanced Linux (SELinux)
- Restricciones del contexto de seguridad (SCC)
- Gestión de identidades y de acceso
- Cifrado de los datos
- Modo Estándares Federales de Procesamiento de la Información (FIPS)

Red Hat Ansible Automation Platform

Red Hat Ansible® Automation Platform es una plataforma potente y flexible que automatiza e integra las soluciones de seguridad y proporciona un lenguaje común para sus herramientas. Obtenga información sobre los **casos prácticos de automatización**.

Red Hat Enterprise Linux CoreOS

Red Hat Enterprise Linux® CoreOS es un sistema operativo ligero, inmutable y optimizado para los contenedores que se basa en el enfoque centrado en la seguridad de Red Hat Enterprise Linux y se usa en Red Hat OpenShift.

Red Hat Quay

Red Hat Quay es un registro para imágenes distribuido y con alta disponibilidad que le permite diseñar, distribuir e implementar contenedores.

Red Hat CodeReady Workspaces

Red Hat CodeReady Workspaces es una herramienta que les permite a los desarrolladores diseñar, llevar a cabo pruebas y crear códigos en los contenedores que se ejecutan en Red Hat OpenShift.

Red Hat Advanced Cluster Security for Kubernetes

Red Hat Advanced Cluster Security for Kubernetes proporciona una arquitectura desarrollada en la nube para la seguridad de los contenedores que protege a las aplicaciones desde el diseño hasta el tiempo de ejecución.

Red Hat Advanced Cluster Management for Kubernetes

Red Hat Advanced Cluster Management for Kubernetes controla los clústeres y las aplicaciones desde una misma consola, con políticas de seguridad integradas.

Obtenga flexibilidad y confiabilidad con un ecosistema de partners de seguridad certificado

Ningún proveedor ofrece todas las funciones que se necesitan para implementar por completo DevSecOps de manera efectiva. Además, cada empresa es distinta y requiere una combinación única de productos y tecnologías para satisfacer sus necesidades.

Red Hat colabora con **partners de seguridad innovadores y líderes del sector** para ofrecer soluciones completas que se basan en integraciones certificadas, imágenes de contenedores y **operadores de Red Hat OpenShift**. Puede seleccionar los partners, los productos y las tecnologías que mejor se ajusten a sus necesidades en el momento en que lo requiera, con la seguridad de que funcionarán en conjunto de manera confiable y uniforme. Los servicios de los expertos, el soporte y las capacitaciones son el respaldo de estas soluciones que le permiten implementar la cultura, los procesos y las herramientas de DevSecOps con éxito.

Ventajas del ecosistema de partners de seguridad de Red Hat

Opciones

Elija los productos y proveedores que mejor satisfagan las necesidades de su empresa en todo momento.

Certificación

Diseñe sus soluciones con la seguridad de que todos los elementos están certificados para trabajar en conjunto de manera confiable.

Experiencia

Aproveche la combinación del conocimiento y la experiencia de Red Hat y los partners sobre DevSecOps.

Servicios

Obtenga ayuda para implementar la cultura, los procesos y las herramientas de DevSecOps dentro de su empresa.

Capacitación

Aprenda sobre las prácticas recomendadas y obtenga las habilidades que se necesitan para adoptar los enfoques de DevSecOps.

Red Hat Vulnerability Scanner Certification

Red Hat Vulnerability Scanner Certification reduce las diferencias entre los resultados del análisis de los puntos vulnerables. Red Hat trabaja con partners de seguridad certificados para ofrecer resultados de este análisis más precisos y confiables para las imágenes y los paquetes publicados de la empresa.

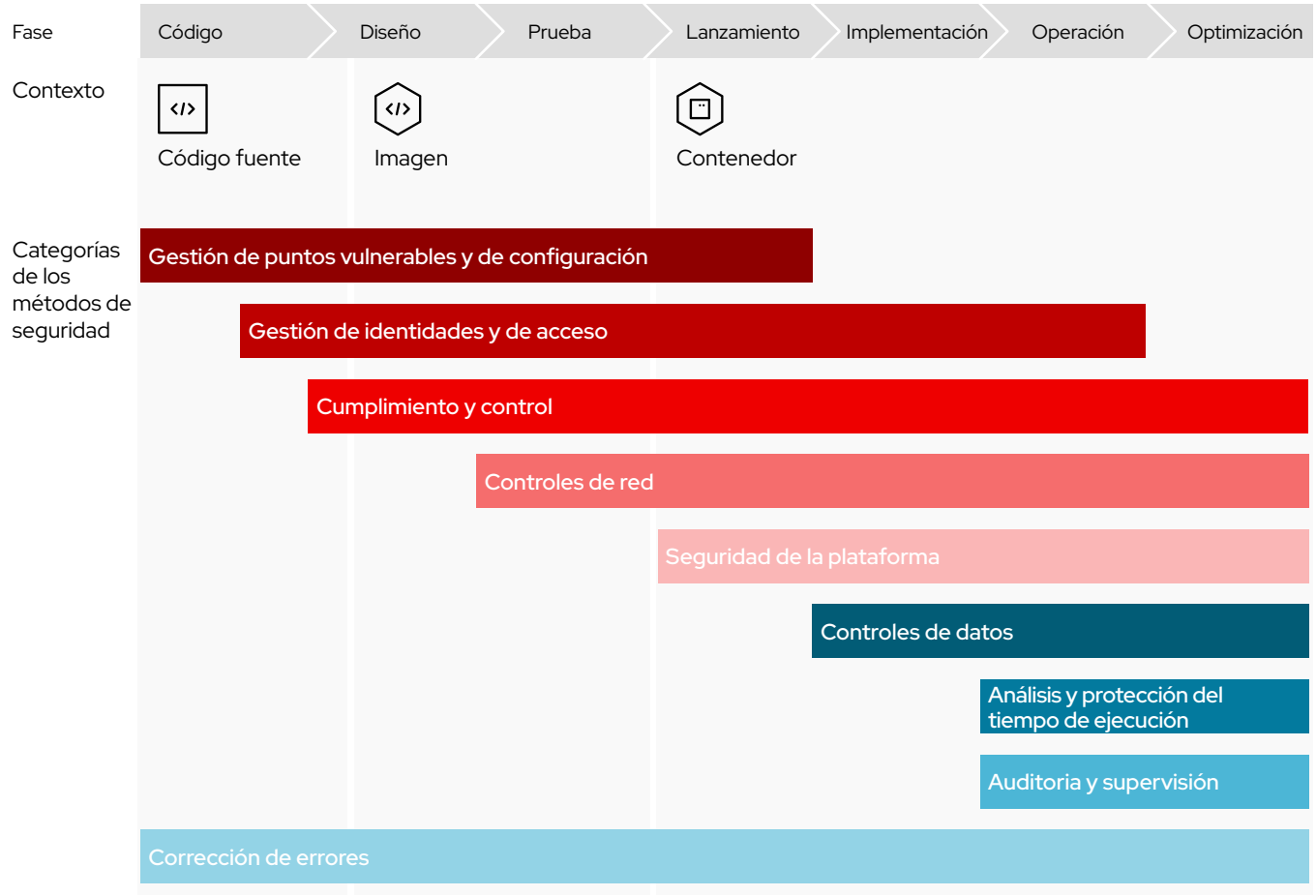
- Reduce la cantidad de falsos positivos y otras discrepancias.
- Libera tiempo y presupuesto que se puede invertir en proyectos e iniciativas estratégicas.
- Alcanza mayores niveles de garantía.
- Mejora la precisión con los datos centralizados para las imágenes publicadas de Red Hat.
- Simplifica la gestión de los puntos vulnerables.

Descubra los productos certificados

Cree soluciones de DevSecOps completas

Red Hat ofrece un marco para diseñar soluciones de DevSecOps integrales y altamente ajustables que abordan los requerimientos de la seguridad en los ciclos de vida de las aplicaciones. Este marco se creó en conjunto con nuestros partners de seguridad y le permite implementar esas soluciones en su empresa según sus necesidades actuales y futuras.

El marco DevSecOps de Red Hat asigna un conjunto completo de herramientas y métodos de seguridad, que se categorizan según su función, dentro del ciclo de vida de desarrollo de las aplicaciones.



Lea la descripción general

Elija los métodos de seguridad y los productos que se adapten a sus necesidades

El marco DevSecOps de Red Hat organiza los 34 métodos de seguridad principales en 9 categorías. Red Hat y las tecnologías de los partners certificados se ajustan con uno o más de estos métodos para que diseñe una solución completa de DevSecOps que satisfaga las necesidades de su empresa y se adapte a los cambios futuros.

Gestión de puntos vulnerables y de configuración

- Pruebas estáticas de la seguridad de las aplicaciones (SAST)
- Análisis estático del código (SCA)
- Pruebas interactivas de la seguridad de las aplicaciones (IAST)
- Pruebas dinámicas de la seguridad de las aplicaciones (DAST)
- Gestión de la configuración
- Análisis de riesgo de las imágenes

Gestión de identidades y de acceso

- Autenticación
- Autorización
- Almacén de secretos
- Módulos de seguridad de hardware (HSM)
- Registros de procedencia

Cumplimiento y control

- Auditorías del cumplimiento normativo
- Controles y resolución de problemas de cumplimiento

Controles de red

- Plugins de la interfaz de red de los contenedores (CNI)
- Políticas de redes
- Control del tráfico
- Malla de servicios
- Visualización
- Análisis de paquetes
- Gestión de interfaces de programación de aplicaciones (API)

Seguridad de la plataforma

- Host seguro
- Plataforma de contenedores
- Espacio de nombres
- Aislamiento
- Fortalecimiento de Kubernetes y los contenedores

Controles de datos

- Protección y cifrado de los datos

Análisis y protección del tiempo de ejecución

- Controlador de admisión
- Análisis del funcionamiento de las aplicaciones
- Defensa ante amenazas

Auditoria y supervisión

- Supervisión de los clústeres
- Gestión de la información y los eventos de seguridad (SIEM)
- Análisis forense

Resolución de problemas

- Plataformas de organización, automatización y respuesta de la seguridad (SOAR)
- Resolución automática de problemas

Encuentre partners certificados

Historias destacadas de los partners

Sysdig

Sysdig ayuda a las empresas a ejecutar las cargas de trabajo en la nube con confianza utilizando las tecnologías de DevOps centradas en la seguridad. Sus productos para controlar y proteger las aplicaciones, las cargas de trabajo y los contenedores permiten que cientos de empresas envíen aplicaciones desarrolladas en la nube más rápido.

Juntas, Sysdig y Red Hat permiten que las empresas adopten los enfoques de la nube rápidamente. Los productos **Sysdig Secure DevOps Platform**, **Sysdig Secure** y **Sysdig Monitor** trabajan con Red Hat OpenShift y **Red Hat Advanced Cluster Management for Kubernetes** para brindar seguridad, cumplimiento normativo y supervisión unificados en los entornos privados, híbridos y multicloud. Estas soluciones permiten proteger los canales de compilaciones, detectar amenazas y tomar medidas al respecto, validar permanentemente la estrategia de nube y el cumplimiento normativo, y controlar el rendimiento. Sysdig se diseñó en una stack open source y sus funciones desarrolladas en la nube de supervisión, seguridad y análisis forense brindan la información y el control que necesita para trasladarse a la nube con menos riesgos.

Las soluciones de Sysdig y Red Hat le permiten lo siguiente:

- Analizar las imágenes directamente dentro de sus canales de integración e implementación continuas (CI/CD)
- Supervisar el rendimiento y la disponibilidad en toda la nube
- Implementar permanentemente la seguridad de los tiempos de ejecución y el cumplimiento normativo
- Validar las configuraciones de la infraestructura de Red Hat OpenShift
- Solucionar los problemas de forma más sencilla

2020

Red Hat obtuvo el premio Rising Star Partner of the Year para el sector público[2]

Gestione los riesgos de la seguridad.

Identifique y corrija los puntos vulnerables de todos sus canales. Detecte y bloquee las amenazas en los tiempos de ejecución con políticas y controles automatizados. Solucione los incidentes e investigue las causas incluso luego de haber eliminado los contenedores.

Aumente el rendimiento y la disponibilidad.

Examine y retenga millones de indicadores. Supervise el estado y el rendimiento de todo su entorno para encontrar y solucionar problemas con anticipación. Solucione los problemas dentro de los clústeres, los pods y los contenedores de forma más sencilla.

Verifique el cumplimiento normativo de la nube.

Verifique el cumplimiento del entorno de Red Hat OpenShift con los estándares comunes. Lleve a cabo auditorías de los clústeres, los nodos y los contenedores a través de informes de actividad detallados. Supervise la integridad de los archivos en todos los ciclos de vida de los contenedores.

Acceda a las integraciones

2 Blog de Red Hat. "**Red Hat awards North American partners for commitment to open source innovation**," 23 de abril de 2020.

Historias destacadas de los partners

Synopsys

Synopsys ofrece una composición del software estática y soluciones de análisis dinámicas para diseñar rápidamente sistemas de software seguros. La empresa brinda una combinación de conocimientos, servicios y herramientas líderes del sector que le permite a las empresas aplicar DevSecOps para optimizar la seguridad y la calidad a través de los ciclos de vida del desarrollo del software.

Synopsys y Red Hat lo ayudan a crear códigos de alta calidad que se centren en la seguridad para reducir los riesgos y mejorar la agilidad y la productividad. **El análisis de la composición del software (SCA) de Synopsys Black Duck** se integra a Red Hat OpenShift para aumentar el control y la supervisión de los puntos vulnerables de la seguridad y las infracciones de las políticas en el código open source dentro de los contenedores. La solución **Black Duck for OpenShift** detecta, analiza, supervisa e inspecciona automáticamente todas las imágenes de contenedores en los clústeres de Red Hat OpenShift para identificar riesgos de cumplimiento normativo y seguridad open source en cualquier etapa del desarrollo de los contenedores. Este software también permite garantizar que los contenedores vulnerables no se introduzcan en la producción y corregir rápidamente los puntos vulnerables nuevos que afecten los contenedores que se encuentren en ejecución.

Funciones de la solución Black Duck for OpenShift:

- Proporciona una lista completa de todos los códigos open source de terceros en cada imagen de contenedor y adjunta en los pods los metadatos sobre los puntos vulnerables y las políticas.
- Envía alertas de inmediato cuando detecta nuevos puntos vulnerables e identifica los contenedores y las imágenes afectados.
- Comprende las bifurcaciones y las versiones anteriores open source e indica, cuando es pertinente, en cuáles puntos vulnerables se ejecutaron los parches, lo cual disminuye la necesidad de investigación.
- **Se integra** a Red Hat Advanced Cluster Management for Kubernetes para garantizar la implementación uniforme en todos los clústeres.

Analiza automáticamente las imágenes de contenedores.

Supervisa constantemente el código open source.

Identifica los puntos vulnerables de la seguridad.

"En Synopsys y Red Hat compartimos una visión para el futuro similar sobre el desarrollo y la implementación seguras de las aplicaciones y esperamos ayudar a que las empresas confíen en sus aplicaciones organizadas en contenedores".

Vatsal Sonecha
Vicepresidente de Desarrollo empresarial de Synopsys

Acceda a las integraciones

Historias destacadas de los partners

Palo Alto Networks

Palo Alto Networks ofrece tecnologías innovadoras para respaldar la transformación digital segura incluso si el ritmo se acelera. La empresa proporciona una cartera de soluciones de seguridad que han ayudado a que más de 60 000 clientes de todo el mundo protejan sus empresas.

Palo Alto Networks y Red Hat le brindan una solución que garantiza el cumplimiento normativo y la seguridad en la nube durante todo el ciclo de vida de desarrollo, para que pueda proteger su entorno. Prisma Cloud de Palo Alto Networks junto con Red Hat OpenShift ofrecen la gestión integral de la estrategia de seguridad de la nube (CSPM) y la protección de las cargas de trabajo de este entorno (CWP) para sus implementaciones. Esta solución proporciona seguridad completa del ciclo de vida para los hosts, los contenedores y la informática sin servidor, además de la supervisión y el control de su estrategia.

Partners de Red Hat desde

2017

Ventajas y características clave

Gestión de puntos vulnerables

Seguridad integrada desde el desarrollo hasta la producción con funciones de prevención, comprensión e identificación de los puntos vulnerables en cada etapa del ciclo de vida de la aplicación.

Cumplimiento normativo

Implemente y mantenga el cumplimiento de forma sencilla de los indicadores del Center for Internet Security (CIS), los regímenes de cumplimiento externos y los requerimientos personalizados.

Seguridad de CI/CD

Integre la seguridad directamente en los procesos de integración continua (CI) para encontrar y solucionar los problemas antes de que se implementen en la producción.

Protección de los tiempos de ejecución

Aplique la seguridad según sea necesario con el aprendizaje automático que crea modelos de tiempos de ejecución con mínimos privilegios y se basan en la lista blanca para todas las versiones de las aplicaciones.

Seguridad de las aplicaciones web y la interfaz

Protéjase de la capa 7 y de las diez amenazas más importantes de Open Web Application Security Project (OWASP) en todos sus entornos de nube pública y privada.

Controles de acceso

Establezca controles de acceso y supervíselos para las cargas de trabajo y las aplicaciones y, al mismo tiempo, intégrelos a las herramientas de identidad, acceso y gestión confidenciales actuales.

Acceda a las integraciones

Historias destacadas de los partners

CyberArk

CyberArk aplica un enfoque único que prioriza la seguridad para el control del acceso con privilegio basado en la identidad. La empresa ofrece soluciones completas para proteger los secretos y las credenciales que utilizan las personas, las aplicaciones, los scripts y las máquinas en las empresas, las nubes y los entornos de DevOps.

Mejore la seguridad de los entornos de contenedores y de los scripts de automatización con el trabajo en conjunto de CyberArk y Red Hat. Las políticas de seguridad que establecen el acceso con privilegios en toda la empresa permiten observar el estado de los sistemas, realizar auditorías, exigir el cumplimiento normativo y gestionar los secretos para reducir los riesgos. Los productos de CyberArk para DevSecOps, como Conjur Secrets Manager y los proveedores de credenciales, se integran a Red Hat OpenShift y Red Hat Ansible Automation Platform para proteger, rotar, supervisar y gestionar las credenciales con privilegios de las personas, las aplicaciones, los scripts y demás identidades no humanas a través de una plataforma centralizada. Puede unificar la gestión de la seguridad, minimizar los puntos vulnerables, reducir la superficie de ataques y optimizar las operaciones mediante un único punto de control para toda su empresa.

La arquitectura modular le permite implementar cada elemento de forma independiente para personalizar la protección en todos los entornos de DevOps, en contenedores, multicloud y de nube híbrida. La autenticación de los tiempos de ejecución sólida y los controles de acceso basados en funciones aseguran que solo los pods y los contenedores autorizados reciban los secretos. La integración con Red Hat Ansible Automation Platform permite que los playbooks accedan a los secretos gestionados y eliminen la necesidad de ingresarlos y rotarlos de forma manual. Además, podrá automatizar las tareas de correcciones que responden a los accidentes de seguridad que se detectan.

Unifique la seguridad.

Gestione y proteja de manera central los secretos y las credenciales de acceso con privilegios en toda su infraestructura, de acuerdo con sus políticas.

Simplifique las operaciones.

Permita que los desarrolladores y los ingenieros de la automatización aseguren, gestionen y roten los secretos y las credenciales que utilizan en función de sus políticas.

Mejore la uniformidad.

Proteja de manera uniforme los secretos y las credenciales que utilizan las aplicaciones, los scripts y las personas con acceso a sus consolas de gestión.

Vea el webinar

Historias destacadas de los partners

Tigera

Tigera transforma la manera en que las empresas aseguran, observan y solucionan los problemas de la comunicación de los microservicios y la red de Kubernetes.

Junto con Red Hat, ayudan a las empresas a integrar la seguridad en sus entornos de Kubernetes supervisando, analizando y gestionando el tráfico de la red. Tigera Calico Enterprise está certificada con Red Hat OpenShift y le permite operar, optimizar y proteger con éxito las aplicaciones organizadas en contenedores más importantes en todos los entornos de nube. Esta arquitectura de Kubernetes incorpora la solución en sus entornos de aplicación para proporcionar controles de seguridad detallados y supervisión mejorada de las capas de microservicios y redes. Además, la solución se integra a sus entornos y herramientas y centros de operaciones de seguridad (SOC) para ofrecer controles y funciones adicionales para las cargas de trabajo modernas. Mejora la seguridad de las aplicaciones en los entornos de desarrollo, prueba y producción con las redes de confianza cero, los controles de acceso de salida, la supervisión del tráfico, la protección y defensa contra amenazas y los informes de auditoría de cumplimiento automatizados.

Amplíe sus funciones de seguridad.

Proteja las aplicaciones a través de los firewalls actuales, la seguridad con privilegios mínimos y el cifrado del tráfico entre los pods.

Aumente la supervisión de las redes.

Acceda a los flujos de las redes para depurar la conectividad, buscar amenazas y automatizar los informes de cumplimiento.

Asegure el cumplimiento normativo.

Controle el cumplimiento de las aplicaciones y ofrezca alertas inmediatas para aquellas cargas de trabajo que no cumplan con las normas.

Acceda al operador

Historias destacadas de los partners

Aqua Security

Aqua Security ayuda a los clientes a innovar y gestionar sus negocios sin problemas. La empresa ofrece funciones de detección y prevención de amenazas y respuestas automatizadas de los ciclos de vida de las aplicaciones para mejorar la seguridad de todos los aspectos de su entorno.

Con Aqua Security y Red Hat, podrá gestionar y ajustar sus cargas de trabajo originales de la nube de forma más segura en las infraestructuras locales, híbridas y de nube. Cloud Native Security Platform de Aqua se combina con Red Hat OpenShift para ofrecer la gestión de los puntos vulnerables basada en los riesgos, la protección minuciosa de los tiempos de ejecución, y el cumplimiento normativo y la protección de toda la infraestructura. Esta solución faculta a los equipos de desarrollo, seguridad y operaciones a proporcionar aplicaciones de forma más segura, protegerlas de las amenazas en los tiempos de ejecución y evaluar las configuraciones de la infraestructura y solucionar los problemas según las verificaciones de las políticas.

Ventajas y características clave

Respalde los enfoques de DevSecOps.

- Analice el código, las configuraciones y los permisos para las imágenes de registro de Red Hat OpenShift según sea necesario.
- Priorice los puntos vulnerables según el nivel de riesgo.
- Automatice los procesos de diseño mediante las integraciones con los canales de CI/CD.

Proteja las aplicaciones en los tiempos de ejecución.

- Detecte y reduzca de manera automática la actividad en los contenedores que no está autorizada sin interrumpir las aplicaciones.
- Aplique la inmutabilidad de los contenedores mediante la identificación y prevención de los cambios que no están autorizados desde las imágenes estándar.

Mejore la seguridad de la cadena de suministros del software.

- Ejecute y valide las imágenes que se encuentran en los entornos de prueba de preproducción protegidos.
- Identifique el malware avanzado que las herramientas de análisis estáticas no llegan a detectar antes de que se implementen.

Mantenga el cumplimiento de la infraestructura.

- Analice y valide cientos de políticas de control y configuración para el cumplimiento con las prácticas recomendadas y los indicadores de Center for Internet Security (CIS).
- Aplique controles de acceso basados en funciones (RBAC) mediante Open Policy Agent (OPA) que se basa en las políticas de garantía declarativas.

Acceda a las integraciones

Comience el proceso de adopción de DevSecOps

La seguridad de las aplicaciones es necesaria para los negocios digitales. Con los enfoques de DevSecOps podrá mejorar la protección de los entornos de las aplicaciones y la empresa.

Red Hat combina una base tecnológica innovadora con un ecosistema de DevSecOps integral y una amplia experiencia que lo ayudará a implementar DevSecOps con éxito en toda su empresa.

- Seleccione una de las distintas tecnologías y herramientas certificadas y líderes del sector que satisfaga sus necesidades actuales y futuras.
- Utilice los recursos de las capacitaciones de especialistas para aprender las prácticas recomendadas y mejorar sus habilidades de DevSecOps
- Utilice los servicios especializados y de consultoría para lograr una implementación más ágil.

Obtenga más información sobre la implementación de DevSecOps con Red Hat: **redhat.com/es/partners/devsecops**

F29623_0721_KVM

Red Hat