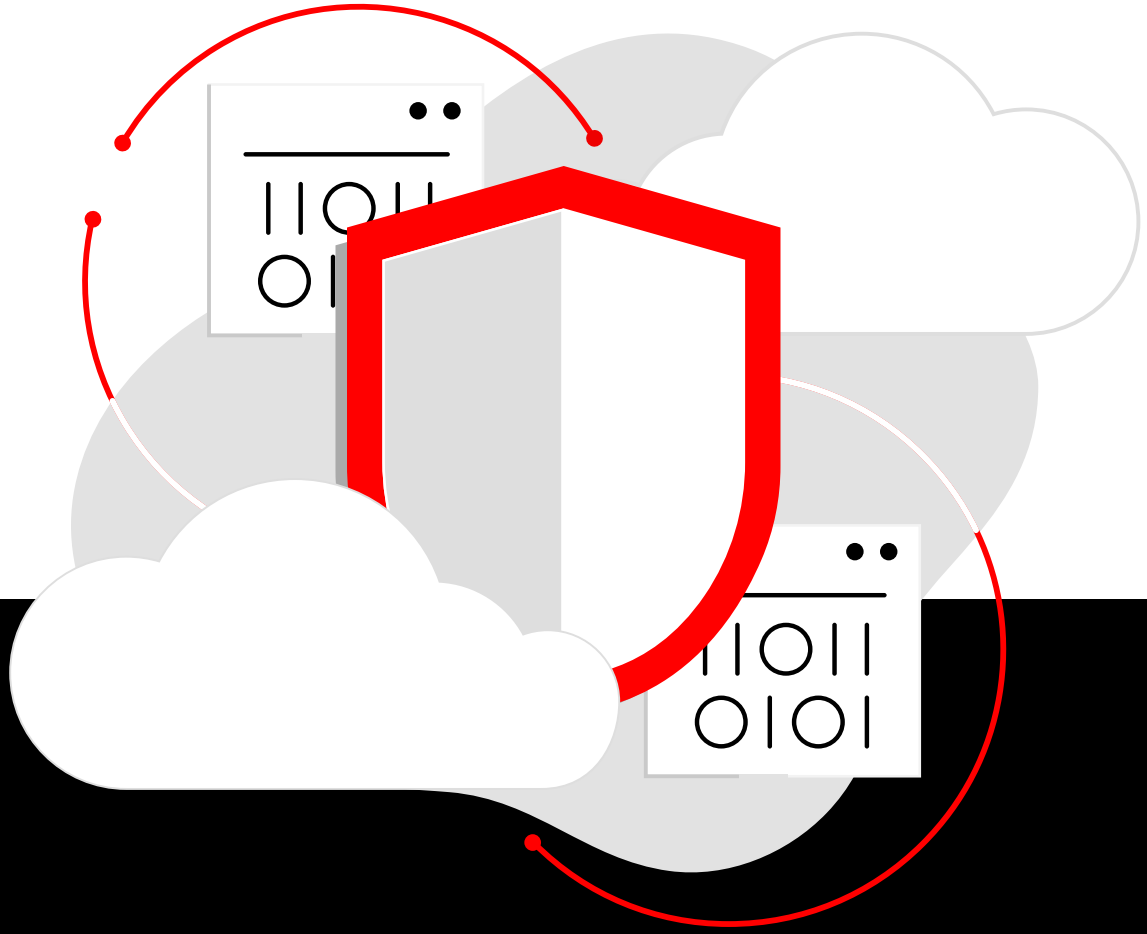
Red Hat



Modernize e proteja os ciclos de vida de aplicações com o DevSecOps

Sumário

Introdução

A segurança de aplicações é essencial em um mundo digital

Com cada vez mais organizações adotando tecnologias de nuvem, container e microsserviços para competir em um mundo digital, a segurança continua sendo uma preocupação principal. De fato, 50% dos líderes de TI sênior em empresas citam a cibersegurança como uma das três principais prioridades em iniciativas de tecnologia.[1] Ao mesmo tempo, 86% esperam que o ritmo de suas organizações na transformação digital acelere em 2021.[1]

Essas novas tecnologias exigem uma abordagem diferente à segurança, já que abordagens tradicionais e baseadas em perímetro não são eficazes em ambientes distribuídos. Além disso, a velocidade de desenvolvimento e a flexibilidade de implantação aumentam com as metodologias nativas em nuvem e de DevOps. Dessa forma, a segurança deve ser considerada no início do processo. Aplicar medidas de segurança somente no fim dos ciclos de desenvolvimento pode resultar em atrasos na entrega e menor proteção.

Adotar abordagens e práticas de **DevSecOps** ajuda a proteger melhor seu ambiente de aplicações e sua empresa.

O que é DevSecOps?

O DevSecOps estende a cultura colaborativa do DevOps para incorporar a segurança por meio dos ciclos de vida das aplicações. Além disso, ele engloba pessoas, processos e tecnologias para tornar a segurança mais abrangente em ambientes distribuídos.

Por meio do DevSecOps, a segurança se torna uma responsabilidade compartilhada entre equipes, em vez de um conjunto de tarefas de uma equipe só e aplicada ao fim do processo de desenvolvimento e implantação. Equipes de segurança, desenvolvimento e operações trabalham juntas, têm visibilidade dos mesmos recursos e compartilham feedbacks, lições aprendidas e insights. Nesse tipo de abordagem, a segurança é integrada desde o início do desenvolvimento da aplicação e da implantação da infraestrutura, aumentando a proteção e reduzindo riscos.

Benefícios do DevSecOps

Melhore a segurança e reduza riscos.

Lide com problemas de segurança durante o desenvolvimento, e não na produção, para proteger mais suas aplicações e reduzir o número de implantações atrasadas ou interrompidas devido a falha nas verificações da política.

Corrija problemas de segurança com mais rapidez.

Adote práticas e ferramentas de segurança modernas, que incentivam a colaboração e incorporam a automação para acelerar ciclos de lançamento, reduzir o tempo necessário para corrigir problemas de segurança durante a produção e economizar tempo e dinheiro.

Aumente a conformidade e a visibilidade.

Adote processos e ferramentas automatizados que reduzem o risco de erros manuais e aumentam a previsibilidade e repetitividade para melhorar a conformidade e simplificar processos de auditoria.

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

Desafios na implementação de DevSecOps

Embora as abordagens de DevSecOps ofereçam diversos benefícios, muitos fatores podem dificultar sua implementação.

- **Cenário de segurança em evolução:** as regulamentações e ameaças de segurança, incluindo requisitos empresariais, técnicos e geográficos, mudam em ritmo acelerado, o que dificulta se manter atualizado.
- **Complexidade do ambiente de aplicação:** pode ser difícil entender as conexões e implicações de segurança de todas as tecnologias diferentes (como containers, microsserviços e serviços de nuvem) que compõem os complicados ambientes de aplicações em larga escala.
- **Ferramentas e processos atuais ineficientes:** muitas equipes começam aplicando as ferramentas e processos existentes em iniciativas de DevSecOps e descobrem que, com o tempo, essa abordagem não é compatível com seus objetivos.
- **Múltiplas ferramentas de segurança:** escolher, testar, integrar e manter a seleção certa de ferramentas de segurança para sua empresa exige tempo, pesquisa e esforço contínuo.

Um DevSecOps de sucesso depende de cultura, processo e tecnologia

Proteger os ciclos de vida da aplicação com DevSecOps exige mudança e alinhamento em três áreas: cultura, processo e tecnologia.

Cultura

Promova colaboração e objetivos compartilhados em suas equipes de desenvolvimento, operações e segurança. Ajude cada equipe a entender os motivos e métodos para criar segurança nos ciclos de vida da aplicação.

Processo

Padronize, documente e automatize seus processos e fluxos de trabalho para melhorar a eficiência e a segurança por todos os ciclos de vida da aplicação.

Tecnologia

Integre seus processos, ferramentas e plataformas de operações, implantação e desenvolvimento de aplicações em um único sistema coeso.

Descubra mais sobre os princípios básicos do DevSecOps

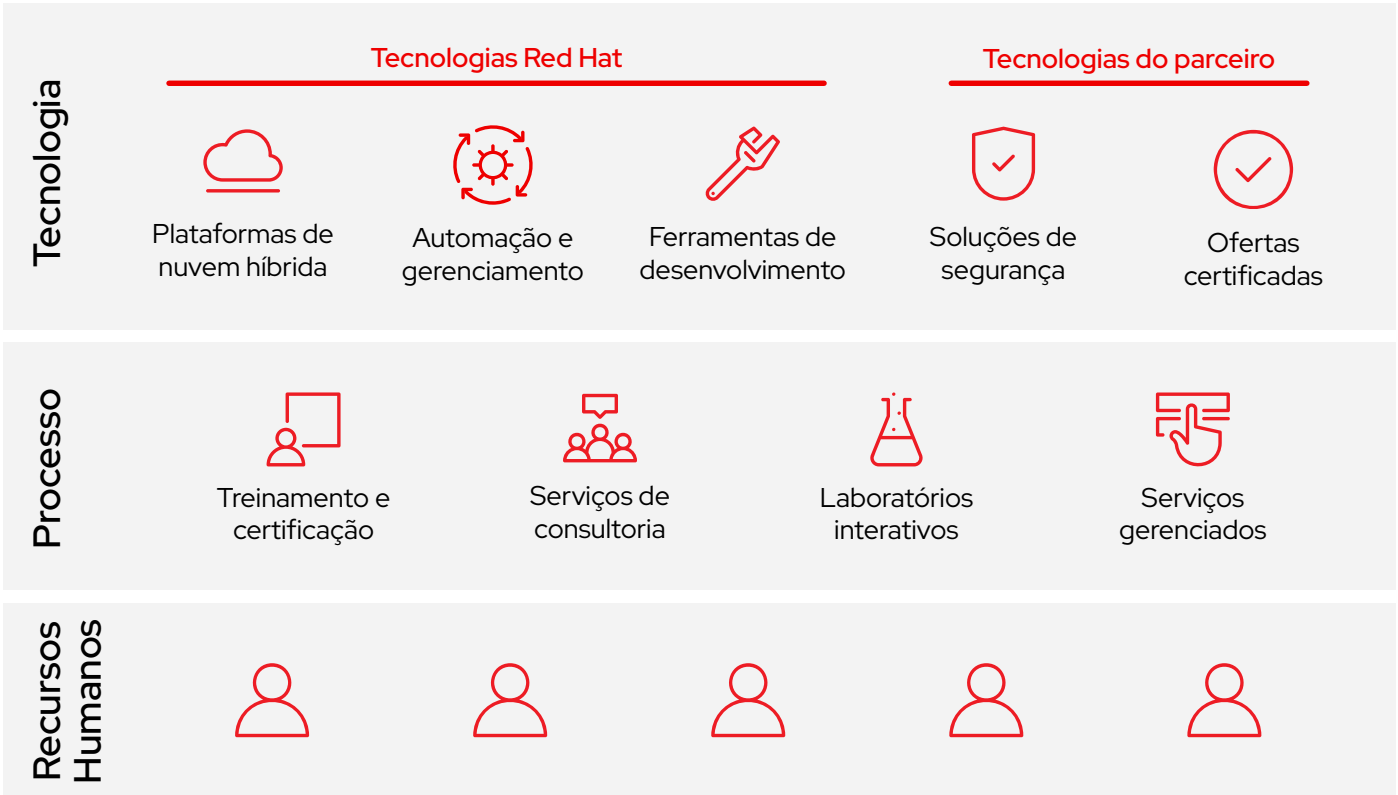
Leia o post do blog **Por que sua prática de DevSecOps pode não estar sendo suficiente?** para entender as mudanças necessárias para implementar o DevSecOps com sucesso.
Leia o ebook **Aumente a segurança na nuvem híbrida** para ver como proteger seus negócios com abordagens de segurança nativas em nuvem.

Estratégia de DevSecOps da Red Hat

A Red Hat une um ecossistema de parceiros certificados, conhecimento abrangente e plataformas inovadoras para criar, proteger e implantar aplicações nos ambientes de nuvem híbrida. Essa combinação permite implementar soluções abrangentes de DevSecOps para melhorar a segurança das aplicações, reduzir riscos, melhorar o desempenho e maximizar o valor dos seus investimentos.

Com uma cadeia de suprimentos de conteúdo confiável, apoio de uma equipe de segurança dedicada e transferência de funcionalidades de segurança cruciais da versão upstream para a versão mais recente, as plataformas da Red Hat® oferecem uma base ideal para soluções de DevSecOps. Nossos parceiros ampliam e melhoram essa base com soluções inovadoras e integradas para aplicar a segurança e a automação nos ciclos de vida da aplicação. Também oferecemos **cursos de treinamento e certificações**, **laboratórios interativos**, **contratos de consultoria** e **ofertas gerenciadas** para ajudar você a implementar o DevSecOps com sucesso.

Juntos, acompanhamos você onde estiver na sua jornada com DevSecOps. Com nossos serviços especializados e soluções expansíveis e modulares, você pode implantar o que precisa hoje, adaptar-se a mudanças futuras e aprender os métodos e abordagens necessários para uma adoção de DevSecOps eficiente e efetiva.



Crie uma base de DevSecOps open source com soluções Red Hat

Red Hat OpenShift

O **Red Hat OpenShift®** é uma plataforma de nuvem híbrida focada na segurança e pronta para as empresas que inclui ferramentas integradas de DevOps e recursos de segurança habilitados por padrão. A plataforma funciona com ferramentas e tecnologias de segurança de parceiros e terceiros para melhorar a segurança e implementar DevSecOps forte. Leia o **guia de segurança do Red Hat OpenShift** para ver como a segurança é abordada em todo o stack de tecnologia.

Faça uma avaliação gratuita

Principais funcionalidades de segurança

- Linux com segurança aprimorada (SELinux)
- Restrições de contexto de segurança (SCC)
- Gerenciamento de identidade e acesso
- Criptografia de dados
- Modo Padrões de processamento de informações federais (FIPS)

Red Hat Ansible Automation Platform

O **Red Hat Ansible® Automation Platform** é uma plataforma poderosa e flexível, capaz de automatizar e integrar soluções de segurança, que oferece uma linguagem comum entre suas ferramentas de segurança. Conheça os **casos de uso de automação**.

Red Hat Enterprise Linux CoreOS

O **Red Hat Enterprise Linux® CoreOS** é um sistema operacional lightweight, imutável e otimizado para containers que tem como foco a segurança do Red Hat Enterprise Linux e é usado dentro do Red Hat OpenShift.

Red Hat Quay

O **Red Hat Quay** é um registro de imagens de container distribuído e altamente disponível que permite criar, distribuir e implantar containers.

Red Hat CodeReady Workspaces

O **Red Hat CodeReady Workspaces** é uma ferramenta em que desenvolvedores podem codificar, criar e testar em containers em execução no Red Hat OpenShift.

Red Hat Advanced Cluster Security for Kubernetes

O **Red Hat Advanced Cluster Security for Kubernetes** oferece uma arquitetura nativa em nuvem para segurança de containers que protege aplicações da criação ao ambiente de execução.

Red Hat Advanced Cluster Management for Kubernetes

O **Red Hat Advanced Cluster Management for Kubernetes** controla clusters e aplicações a partir de um único console com políticas de segurança incorporadas.

Ganhe flexibilidade e confiabilidade com um ecossistema de parceiros de segurança certificados

Nenhum fornecedor sozinho oferece todos os recursos necessários para implementar DevSecOps eficiente. Além disso, cada organização é diferente e exige uma combinação exclusiva de soluções e tecnologias para atender às suas necessidades.

A Red Hat colabora com **parceiros de segurança inovadores e líderes do setor** para entregar soluções completas baseadas em integrações certificadas, imagens de container e **operadores Red Hat OpenShift**. Escolha com confiança os parceiros, soluções e tecnologias mais adequados às suas necessidades sempre, sabendo que vão funcionar de maneira confiável e consistente juntas. Essas soluções também contam com o apoio de serviços especializados, suporte e treinamento para ajudar você a implementar cultura, processos e ferramentas de DevSecOps com sucesso.

Benefícios do ecossistema de parceiros de segurança da Red Hat

Opções

Escolha as soluções e fornecedores que atendam melhor às necessidades da organização em todos os momentos.

Certificação

Crie sua solução com a confiança de que todos os componentes são certificados para trabalharem juntos com segurança.

Conhecimento

Aproveite a experiência e o conhecimento de DevSecOps combinados da Red Hat e parceiros.

Serviços

Receba ajuda na implementação de cultura, processos e ferramentas de DevSecOps na sua empresa.

Treinamento

Conheça as práticas recomendadas e adquira as habilidades necessárias para adotar abordagens de DevSecOps.

Red Hat Vulnerability Scanner Certification

O Red Hat Vulnerability Scanner Certification minimiza as discrepâncias entre resultados do verificador de vulnerabilidades. A Red Hat trabalha com parceiros de segurança certificados para entregar resultados de verificação de vulnerabilidades em containers com mais precisão e confiança para pacotes e imagens publicados pela Red Hat.

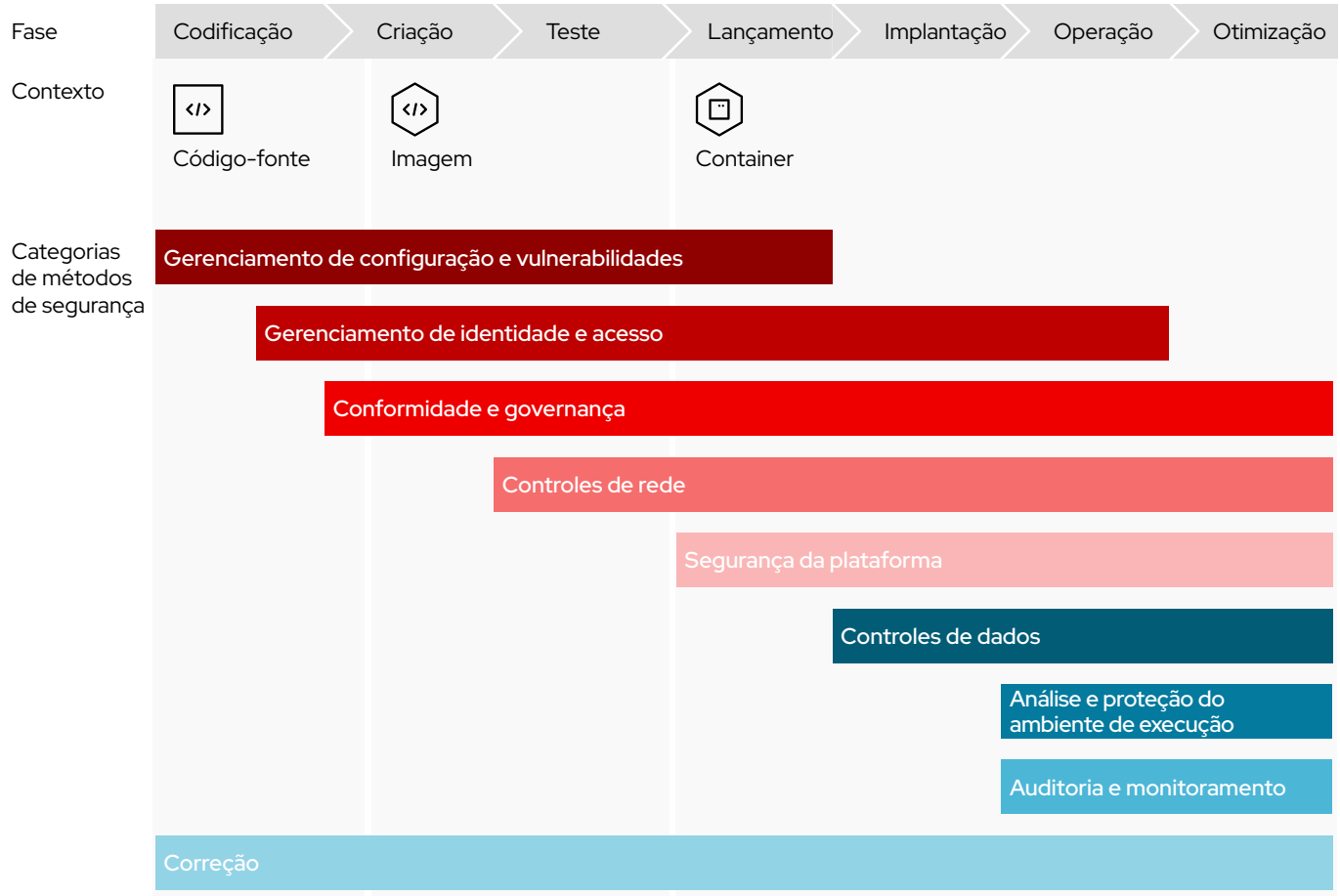
- Minimize falsos positivos e outras discrepâncias.
- Libere tempo e orçamento para projetos e iniciativas estratégicos.
- Conquiste níveis maiores de garantia.
- Melhore a precisão com dados centralizados para imagens publicadas pela Red Hat.
- Simplifique o gerenciamento de vulnerabilidades.

Encontre soluções certificadas

Crie soluções completas de DevSecOps

A Red Hat oferece um framework para criar soluções altamente escaláveis e abrangentes de DevSecOps que atendem os requisitos de segurança por todos os ciclos de vida das aplicações. Criado com os parceiros de segurança da Red Hat, esse framework pode ajudar você a implementar DevSecOps na sua empresa de acordo com suas necessidades atuais e esperadas.

O framework de DevSecOps da Red Hat mapeia um conjunto abrangente de ferramentas e métodos de segurança, categorizados por função, no ciclo de vida de desenvolvimento da aplicação.



Leia a visão geral

Escolha os métodos de segurança e as soluções que atendam às suas necessidades

O framework de DevSecOps da Red Hat organiza 34 métodos principais em nove categorias. Tecnologias da Red Hat e de parceiros certificados se alinham com um ou mais desses métodos para ajudar você a criar uma solução completa de DevSecOps que atenda às necessidades da sua organização e se adapte a mudanças futuras.

Gerenciamento de configuração e vulnerabilidades

- Teste estático de segurança de aplicações (SAST)
- Análise de código estático (SCA)
- Teste interativo de segurança de aplicações (IAST)
- Teste dinâmico de segurança de aplicações (DAST)
- Gerenciamento de configuração
- Riscos em imagens

Gerenciamento de identidade e acesso

- Autenticação
- Autorização
- Cofres de segredos
- Módulos de segurança de hardware (HSM)
- Procedência

Conformidade e governança

- Auditoria de conformidade normativa
- Correção e controle de conformidade

Controles de rede

- Plug-ins da interface de rede do container (CNI)
- Políticas de rede
- Controle de tráfego
- Service mesh
- Visualização
- Análise de pacote
- Gerenciamento das interfaces de programação de aplicações (API)

Segurança da plataforma

- Host seguro
- Plataforma de aplicações em container
- Namespace
- Isolamento
- Fortalecimento de containers e Kubernetes

Controles de dados

- Proteção e criptografia de dados

Análise e proteção do ambiente de execução

- Controlador de admissões
- Análise do comportamento de aplicações
- Defesa contra ameaças

Auditoria e monitoramento

- Monitoramento de clusters
- Gerenciamento de eventos e informações de segurança (SIEM)
- Análises forenses

Correção

- Plataformas de orquestração, automação e resposta de segurança (SOAR)
- Resolução automática

Encontre parceiros certificados

Destaque do parceiro

Sysdig

A **Sysdig** ajuda as empresas a executar com confiança cargas de trabalho na nuvem com tecnologias de DevOps focadas na segurança. Os produtos da Sysdig para monitorar e proteger aplicações, cargas de trabalho e containers ajudam centenas de empresas a entregar aplicações nativas em nuvem com mais rapidez.

Juntas, a Red Hat e a Sysdig ajudam empresas a adotar rapidamente abordagens nativas em nuvem. O **Sysdig Secure DevOps Platform**, **Sysdig Secure** e **Sysdig Monitor** usam o Red Hat OpenShift e o **Red Hat Advanced Cluster Management for Kubernetes** para oferecer segurança, conformidade e monitoramento unificados para ambientes privados, híbridos e de multicloud. Essas soluções ajudam você a proteger pipelines de compilação, detectar e responder a ameaças, validar continuamente a postura e a conformidade com a nuvem e monitorar o desempenho. Baseados em um stack open source, os recursos forenses, de segurança e monitoramento nativos em nuvem da Sysdig oferecem o insight e o controle necessários para migrar para a nuvem com menos riscos.

2020
Red Hat eleita a Parceira do Ano do setor público[2]

As soluções da Red Hat e da Sysdig ajudam você a:

- Verificar imagens diretamente dos pipelines de integração/implantação contínuas (CI/CD).
- Monitorar desempenho e disponibilidade em escala da nuvem.
- Implementar conformidade contínua e segurança no ambiente de execução.
- Validar configurações de infraestrutura do Red Hat OpenShift.
- Solucionar e responder a problemas com mais facilidade.

Gerencie riscos de segurança.

Identifique e corrija vulnerabilidades em todos os pipelines. Detecte e bloqueie ameaças no ambiente de execução com políticas e controles automatizados. Responda e investigue incidentes, mesmo após a descontinuação de containers.

Aumente o desempenho e a disponibilidade.

Pesquise e retenha milhões de métricas. Monitore a integridade e o desempenho no seu ambiente para encontrar e corrigir problemas com proatividade. Solucione problemas dentro de clusters, pods e containers com mais facilidade.

Valide a conformidade da nuvem.

Valide a conformidade do ambiente do Red Hat OpenShift com normas comuns. Audite clusters, nós e containers por meio de relatórios detalhados de atividades. Implemente monitoramento de integridade de arquivos nos ciclos de vida do container.

Acesse as integrações

2 Blog da Red Hat. "**Red Hat premia parceiros norte-americanos pelo compromisso com a inovação open source**", 23 de abril de 2020.

Destaque do parceiro

Synopsys

A **Synopsys** oferece composição de software estática e soluções de análise dinâmicas para criar software de segurança com rapidez. Com uma combinação de conhecimento, serviços e ferramentas líderes do setor, a Synopsys ajuda empresas a aplicar DevSecOps para otimizar a segurança e a qualidade nos ciclos de vida de desenvolvimento do software.

A Red Hat e a Synopsys ajudam você a criar um código seguro de alta qualidade para minimizar os riscos e maximizar velocidade e produtividade. A **análise de composição de software (SCA) do Synopsys Black Duck** se integra com o Red Hat OpenShift para aumentar a visibilidade e controle das vulnerabilidades de segurança e violações da política no código open source dentro de seus containers. O **Black Duck for OpenShift** automaticamente identifica, verifica, monitora e inspeciona todas as imagens de container nos clusters do Red Hat OpenShift para detectar riscos de conformidade e segurança open source em qualquer fase da construção do container. O software também ajuda a garantir que containers vulneráveis não sejam enviados para a produção e a responder rapidamente a novas vulnerabilidades que afetem containers em execução.

A solução Black Duck for OpenShift:

- Fornece uma lista completa de todo o código open source externo em cada imagem de container, além de anotar seus pods com metadados de política e vulnerabilidade.
- Alerta imediatamente sobre novas vulnerabilidades que afetam seus containers e identifica quais imagens e containers foram afetados.
- Entende ramificações open source e transferência de recursos da versão upstream para a versão mais recente, além de marcar vulnerabilidades como com patches aplicados quando apropriado, reduzindo o número de vulnerabilidades que exigem investigação.
- **Integra-se** com o Red Hat Advanced Cluster Management for Kubernetes para garantir implantação consistente em todos os clusters.

Verifique automaticamente imagens de container.

Monitore código open source continuamente.

Identifique vulnerabilidades de segurança.

"A Synopsys e a Red Hat compartilham uma visão muito semelhante para o futuro do desenvolvimento e implantação de aplicações e, juntas, estamos felizes em ajudar organizações a criar confiança em suas aplicações em containers."

Vatsal Sonecha
Vice-presidente de desenvolvimento de negócios, Synopsys

Acesse as integrações

Destaque do parceiro

Palo Alto Networks

A **Palo Alto Networks** entrega inovação para dar suporte à transformação digital segura, mesmo com a aceleração das mudanças. A empresa oferece um portfólio de soluções de segurança que ajudam mais de 60 mil clientes do mundo todo a proteger seus negócios.

A Red Hat e a Palo Alto Networks ajudam você a proteger seu ambiente com conformidade e segurança nativa em nuvem por todo o ciclo de vida de desenvolvimento. O **Prisma Cloud, da Palo Alto Networks**, usa o Red Hat OpenShift para oferecer gerenciamento de postura de segurança em nuvem (CSPM) abrangente e proteção da carga de trabalho na nuvem (CWO) para suas implantações. Essa solução oferece segurança em todo o ciclo de vida para hosts, containers e serverless, além de visibilidade e governança da sua postura de segurança.

Parceiro Red Hat desde

2017

Principais funcionalidades e benefícios

Gerenciamento de vulnerabilidades

Incorpore segurança do desenvolvimento à produção com detecção, compreensão e prevenção de vulnerabilidades em cada etapa do ciclo de vida da aplicação.

Conformidade

Implemente e mantenha a conformidade com facilidade para Center for Internet Security (CIS) benchmarks, regimes de conformidade externa e requisitos personalizados.

Segurança de CI/CD

Integre segurança diretamente em seus processos de integração contínua (CI) para encontrar e corrigir problemas antes que sejam implantados na produção.

Defesa do ambiente de execução

Aplique segurança em escala com machine learning que cria automaticamente modelos de ambiente de execução baseados na lista de permissões com privilégios mínimos para todas as versões da aplicação.

Segurança de interface e aplicações web

Proteja-se contra ameaças à camada 7 e **Open Web Application Security Project (OWASP) Top Ten** em seus ambientes de nuvem pública e privada.

Controles de acesso

Estabeleça e monitore controles de acesso de cargas de trabalho e aplicações enquanto se integra com ferramentas de gerenciamento de segredos, acessos e identidade existentes.

Acesse as integrações

Destaque do parceiro

CyberArk

A **CyberArk** aplica uma abordagem única que prioriza a segurança para controle de acesso privilegiado baseado em identidade. A empresa entrega soluções completas para proteger segredos e credenciais usadas por pessoas, aplicações, scripts e máquinas em ambientes empresariais, de nuvem e de DevOps.

Juntas, a Red Hat e a CyberArk ajudam você a melhorar a segurança dos ambientes de container e dos scripts de automação. Políticas de segurança com acesso privilegiado em toda a empresa oferecem visibilidade, auditoria, reforço e gerenciamento de segredos para reduzir os riscos dos negócios. As soluções de DevSecOps da CyberArk, incluindo **Conjur Secrets Manager** e **Credential Providers**, integram-se ao Red Hat OpenShift e Red Hat Ansible Automation Platform para proteger, alterar, monitorar e gerenciar credenciais privilegiadas para pessoas, aplicações, scripts e outras identidades não humanas usando uma plataforma centralizada. Com um único ponto de controle em toda a sua organização, é possível unificar o gerenciamento da segurança, reduzir vulnerabilidades, minimizar superfícies de ataque e otimizar operações.

A arquitetura modular permite implantar cada componente de maneira independente para personalizar a proteção em ambientes de nuvem híbrida, multicloud, em containers e de DevOps. Forte autenticação do ambiente de execução e controles de acesso baseados em função asseguram que somente containers e pods autorizados recebam segredos. Com a integração com o Red Hat Ansible Automation Platform, playbooks podem acessar segredos gerenciados e eliminar a necessidade de entrada e troca manuais de segredos. Essa integração também permite automatizar tarefas de correção em resposta a incidentes de segurança detectados.

Unifique a segurança.

Gerencie e proteja segredos e credenciais de acesso privilegiados de maneira central em toda a infraestrutura, de acordo com suas políticas.

Simplifique as operações

Permita que desenvolvedores e engenheiros de automação protejam, gerenciem e façam a rotação de segredos e credenciais que usam com base em suas políticas.

Melhore a consistência.

Proteja com consistência segredos e credenciais usadas por aplicações, scripts e pessoas acessando seus consoles de gerenciamento.

Assista ao webinar

Destaque do parceiro

Tigera

A **Tigera** transforma o modo como empresas protegem, observam e solucionam problemas de comunicação de microsserviços e rede Kubernetes.

A Red Hat e a Tigera ajudam organizações a integrar segurança em seus ambientes Kubernetes monitorando, analisando e gerenciando o tráfego de rede. Com certificação do Red Hat OpenShift, a **Tigera Calico Enterprise** ajuda a operar, otimizar e proteger aplicações críticas em container nos ambientes de nuvem. A arquitetura do Kubernetes incorpora a solução ao seu ambiente de aplicações para oferecer controles de segurança detalhados e maior visibilidade entre as camadas de rede e de microsserviços. A solução também se integra a suas ferramentas de segurança, ambientes e centros de operações de segurança (SOCs) para oferecer mais controles e recursos às cargas de trabalho modernas. Melhore a segurança da aplicação nos ambientes de desenvolvimento, teste e produção com redes Zero Trust, controles de acesso de saída, visibilidade de tráfego, proteção e defesa contra ameaças e relatórios de auditoria de conformidade automatizados.

Amplie seus recursos de segurança.

Proteja aplicações por meio de firewalls existentes, segurança com privilégios mínimos e criptografia de tráfego interpods.

Ganhe visibilidade de rede.

Acesse fluxos de rede para depurar conectividade, procurar ameaças e automatizar a geração de relatórios de conformidade.

Garanta a conformidade.

Monitore a conformidade de aplicações e entregue alertas em tempo real sobre cargas de trabalho fora de conformidade.

Acesse o operador

Destaque do parceiro

Aqua Security

A **Aqua Security** ajuda os clientes a inovar e executar seus negócios com o mínimo de atrito. A empresa oferece automação de prevenção, detecção e respostas contra ameaças em todos os ciclos de vida da aplicação para melhorar a segurança em todos os aspectos do seu ambiente.

A Red Hat e a Aqua Security ajudam você a gerenciar e escalar suas cargas de trabalho nativas em nuvem com mais segurança na infraestrutura local, híbrida e em nuvem. O **Aqua Cloud Native Security Platform** integra-se ao Red Hat OpenShift para oferecer gerenciamento de vulnerabilidades com base em riscos, proteção detalhada do ambiente de execução e segurança e conformidade abrangentes da infraestrutura. A solução capacita as equipes de desenvolvimento, segurança e operações para entregar aplicações com mais segurança, proteger contra ameaças no ambiente de execução e avaliar e corrigir configurações de infraestrutura baseadas nas verificações de política.

Principais funcionalidades e benefícios

Dê suporte a abordagens de DevSecOps.

- Analise código, configurações e permissões para imagens de registro do Red Hat OpenShift em escala.
- Priorize vulnerabilidades por risco.
- Automatize processos de construção por meio da integração com pipelines CI/CD.

Proteja aplicações no ambiente de execução.

- Detecte e reduza automaticamente a atividade de container não autorizada sem interromper aplicações.
- Aplique imutabilidade de containers identificando e evitando mudanças não autorizadas de imagens padrão.

Melhore a segurança da cadeia de suprimentos do software.

- Execute e valide imagens em ambientes de teste protegidos de pré-produção.
- Identifique malware avançado que pode não ser identificado por verificadores estáticos antes da implantação.

Mantenha a conformidade da infraestrutura.

- Verifique e valide centenas de políticas de configuração e controle para estar em conformidade com as práticas recomendadas e com Center for Internet Security (CIS) benchmarks.
- Aplique controles de acesso baseados em função (RBAC) por meio de políticas de segurança declarativas baseadas em Open Policy Agent (OPA).

Acesse as integrações

Tudo pronto para iniciar sua jornada de DevSecOps?

A segurança das aplicações é um requisito para empresas digitais. Adotar abordagens de DevSecOps ajuda a proteger melhor seu ambiente de aplicações e sua empresa.

A Red Hat combina uma base tecnológica inovadora com um ecossistema abrangente de DevSecOps e extenso conhecimento para ajudar a implementar DevSecOps em toda a sua organização com sucesso.

- Escolha entre uma variedade de ferramentas e tecnologias certificadas e líderes do setor para ter suas necessidades atendidas agora e no futuro.
- Conheça as práticas recomendadas e adquira habilidades de DevSecOps com recursos de treinamento de especialistas.
- Faça implantações mais rápido com serviços especializados e compromissos de consultoria.

Veja mais informações sobre a implantação de DevSecOps com a Red Hat:
redhat.com/pt-br/partners/devsecops

F29623_0721_KVM

Red Hat