How to deploy a comprehensive DevSecOps solution

Red Hat DevSecOps framework lays a solid foundation for a highly scalable, end-to-end DevSecOps solution.

Making DevOps secure is a complicated proposition

Securing DevOps is a complex undertaking because DevOps tools grow and change quickly. Containers and Kubernetes add more complexity and open up new attack vectors and security risks. Development and operations teams must make security an integral part of the entire application lifecycle to safeguard critical IT infrastructure, protect confidential data, and keep pace with change.

Red Hat and our security ecosystem partners created a framework that provides a solid foundation and blueprint for delivering DevSecOps solutions that deploy and scale more efficiently. The Red Hat® DevSecOps framework addresses key security requirements throughout the DevOps life cycle as part of a comprehensive defense-in-depth security strategy. Red Hat and our security partners help you reduce risk by simplifying DevOps security and accelerating DevSecOps adoption.

Security partners like Anchore, Aqua, CyberArk, Lacework, NeuVector, Palo Alto Networks, Portshift, Snyk, StackRox, Synopsys, Sysdig, Thales, Tigera, Trend Micro, and Tufin augment Red Hat native security capabilities, providing end-to-end DevSecOps solutions that improve your security posture and make the most of your Red Hat investments.

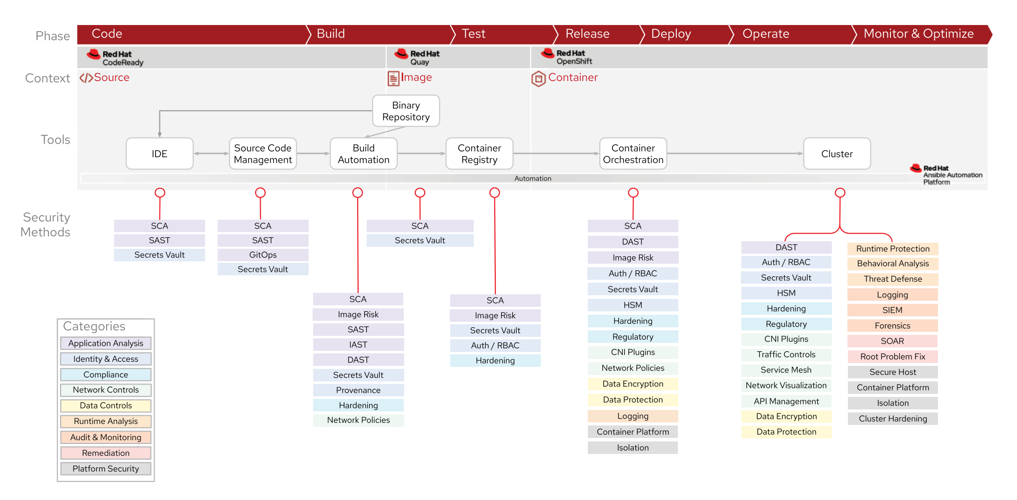

Figure 1. DevSecOps framework

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

Complete framework addresses a range of security methods

The Red Hat DevSecOps framework identifies nine security categories and 32 methods and technologies that address the entire application life cycle. The framework places Red Hat built-in capabilities, DevOps toolchains, and security partner solutions at key integration points in the pipeline. You can implement some or all the methods and technologies within a category depending on the scope of your DevOps environment and your specific requirements.

Platform security

Securing your Kubernetes platform is fundamental. Preparing it to support business-critical applications in a secure, reliable, and scalable manner can be a challenge. In fact, deployment and management of Kubernetes continue to be the top two challenges for enterprises.[1] Red Hat OpenShift® is an enterprise-ready Kubernetes container platform that eliminates complexity, removes adoption barriers, and includes a variety of built-in platform security features.

The Red Hat DevSecOps framework provides foundational features for securing the underlying container host (Red Hat Enterprise Linux® and Red Hat CoreOS) as well the container platform. Most Red Hat security features are enabled by default to simplify deployment and minimize risk. These features help you secure containers at their boundaries and protect the host from container escapes.

Platform security methods

- Host security: Provides mandatory access controls with SELinux, kernel facilities for controlling system calls with secure computing mode (seccomp), and kernel features for isolating CPU, memory, and other resources with CGroups.
- Container platform security: Provides a lightweight container runtime with CRI-O and a secure container image registry with Quay.
- Linux namespaces: Isolate applications across teams, groups, and departments.
- Kubernetes and container hardening: Apply standards like NIST 800-190 and CIS Benchmarks.

Application analysis

Application analysis functions help you identify application vulnerabilities and other security issues early in the life cycle. By shifting security remaining from the DevOps lifecycle, you can identify and address vulnerabilities early and avoid repeated work later on.

Application analysis methods

- Static application security testing (SAST): Analyzes code under development for vulnerabilities and quality issues.
- Software composition analysis (SCA): Examines dependent packages included with applications, looking for known vulnerabilities and licensing issues.
- Interactive application security testing (IAST) tools and dynamic application security testing (DAST) tools: Analyze running applications to find execution vulnerabilities.

[1] Vizard, Mike. "Survey Sees Kubernetes Enterprise Adoption Gains." Container Journal, March 2020.

Application analysis also includes security methods like GitOps configuration management and container image risk management capabilities like malware, embedded secrets, and configuration defect detection functionality.

Identity and access management

Identity and access management (IAM) methods control access to on-premises and cloud assets, applications, and data based on user or application identity and administratively defined policies. They are found in every stage of the DevOps lifecycle and can help protect against unauthorized system access and lateral movement.

IAM methods

- Authentication and authorization controls: Verify the identity of users and applications and grant them access to specific resources and functions.
- Role-based access controls (RBACs): Grant collections of users access to resources or functions based on their job responsibilities, simplify administration and onboarding, and reduce privilege creep.
- Identity providers, secrets vaults, and hardware security modules (HSMs): Manage and safeguard security credentials, keys, certificates, and secrets while at rest and in transit.

Additional IAM methods include container image provenance and image signing functions to validate container image authenticity and establish trust.

Compliance

Compliance methods and technologies help you adhere to industry and government regulations and corporate policies. They automate compliance validation and reporting throughout the DevOps pipeline, helping you simplify audits and avoid costly regulatory fines and lawsuits.

These methods improve compliance with a variety of data privacy and information security mandates, including:

- Payment Card Industry Data Security Standard (PCI-DSS).
- ISO 27001 information security management standard.
- U.S. Health Insurance Portability and Accountability Act (HIPAA).
- EU General Data Protection Regulation (GDPR).

Network controls and segmentation

Network controls and segmentation methods let you control, segregate, and visualize Kubernetes traffic. They help you isolate tenants and secure communications flows between containerized applications and microservices.

Network controls and segmentation methods

- Kubernetes network security policies: Control traffic flows at the IP address or port level and can be enhanced with cluster ingress and egress traffic controls, logging, and network visualization.
- Software-defined networking (SDN): Provides a programmable, adaptable network fabric that is provisioned in real time to support dynamic security requirements and evolving business demands.
- Service mesh: Provides network segmentation, network visualization, authentication, and authorization for containerized applications and microservices.

Data controls

Data control methods and technologies help protect data integrity and prevent unauthorized data disclosure. They protect data at rest and in motion, helping you safeguard intellectual property and confidential customer information.

Data control methods

- Data encryption: Provides data cryptography, tokenization, data masking, and key management capabilities to help prevent unauthorized disclosure of data in databases, files, and containers.
- Data protection: Discovers and classifies data and monitors and audits activity to help protect sensitive data and improve compliance.

Runtime analysis and protection

Production runtime methods help maintain cluster hygiene by identifying and mitigating suspicious and malicious activity in real-time.

Runtime analysis and protection methods

- Admission controller: Functions as a Kubernetes gatekeeper that governs and enforces what is allowed to run on the cluster.
- Runtime application behavioral analysis: Examines system activity and intelligently detects suspicious or malicious actions in real time.
- Runtime application self protection (RASP): Detects and blocks cyberattacks in real time.
- API management: Controls access to APIs and secures API traffic.

Audit and monitoring

Audit and monitoring methods provide information about security incidents in your production environment. They describe when the event occured and provide probable cause and impact information, helping you improve visibility and accelerate incident response.

Audit and monitoring methods include:

- Security information and event management (SIEM): Centralizes events reporting by consolidating logs and network flow data from distributed devices, endpoints, and applications.
- Forensics: Provides insights into security breaches, provides evidence to support compliance audits, and accelerates recovery efforts.

Remediation

Remediation methods automatically take corrective actions when security incidents occur in production. They help you improve uptime and avoid data loss.

Remediation methods

- Security orchestration, automation, and response (SOAR) platforms: Respond to security incidents by automating actions and integrating with other security tools.
- Root problem fix: Automatically resolves issues related to Kubernetes configuration errors and policy infractions.

Conclusion

The Red Hat DevSecOps framework lays a reliable and scalable foundation to help you expand DevOps security and reduce risk. Red Hat and our security partners have the technology you need to simplify and accelerate your DevSecOps implementation. Contact us for more information.

About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com

Copyright © 2020 Red Hat, Inc. Red Hat, the Red Hat logo, and OpenShift are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries