How to deploy a comprehensive DevSecOps solution

Deploy a comprehensive DevSecOps solution from Red Hat and security partners

Securing DevOps is a complex undertaking; DevOps tools grow and change at a fast pace. 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 life cycle to safeguard critical IT infrastructure, protect confidential data, and keep pace with change.

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

Red Hat and our security ecosystem partners created a framework that provides a solid foundation and blueprint for delivering DevSecOps solutions that are easy to deploy and easy to scale. The Red Hat® DevSecOps framework addresses key security requirements throughout the DevOps lifecycle 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, JFrog, GitLab, NeuVector, Palo Alto Networks, Portshift, Snyk, Splunk, Synopsys, Sysdig, Thales, Tigera, Trend Micro, and Zettaset augment native security capabilities in Red Hat's portfolio, providing end-to-end DevSecOps solutions that improve your security posture and make the most of your Red Hat investments.

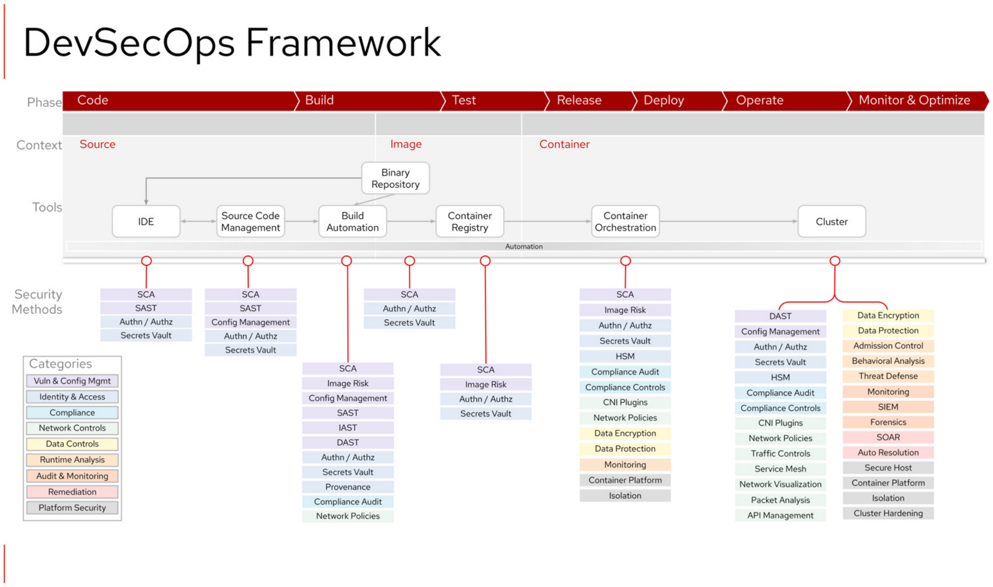

Figure 1. Red Hat's DevSecOps framework.

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

Complete framework addresses a range of security methods

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

Platform security

Securing your Kubernetes platform is fundamental. Downloading and installing Kubernetes is easy. But getting it ready 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 help simplify deployment and minimize risk. These features help secure containers at their boundaries and protect the host from container escapes.

Platform Security security methods include:

- **Host security** provides mandatory access controls with SELinux, kernel facilities for controlling system calls with seccomp (secure computing mode), 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.

Vulnerability and configuration management

Vulnerability and configuration management functions help improve, identify, classify, and resolve application, configuration, and container image security defects. These methods help to incorporate security into the DevOps life cycle early, which saves time and money.

Vulnerability and configuration management methods include:

- **Static application security testing (SAST)**, which analyzes code under development for vulnerabilities and quality issues.
- **Software composition analysis (SCA)**, which examines dependent packages included with applications, looking for known vulnerabilities and licensing issues.
- **Interactive application security testing (IAST)** and **dynamic application security testing (DAST)** tools, which analyze running applications to find execution vulnerabilities.
- **Configuration management** with analysis and management of application and infrastructure configurations in DevOps. Traditionally this was not used as a way to improve security. But properly managing configurations in a GitOps process can strengthen security by improving change controls, identifying configuration defects that can reduce the attack surface, and signing and tracking authorship for better accountability and opportunities to improve.
- **Image risk** is any risk associated with a container image. This includes vulnerable dependencies, embedded secrets, bad configurations, malware, or images that are not trusted.

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

Identity and access management

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

IAM methods include:

- **Authentication**, verifying the identity of users, services, and applications.
- **Authorization**, granting the authenticated users access to specific resources or functions. In Kubernetes context, this is commonly referred to as role-based access controls (RBACs), which 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)**, allowing DevOps teams to manage and safeguard security credentials, keys, certificates, and secrets, while at rest and in transit.
- **Provenance**, the ability to verify the identity or authenticity of code or an image typically through some type of digital signature or attestation record.

Compliance

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

Compliance methods include:

- **Compliance audits**, a function which typically scans a config, container, cluster, or system to report if the object in question is in compliance or not.
- **Compliance controls**, which incorporate automation with technical controls. This can help automate and enable proper actions, or prevent actions that would result in noncompliance.

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

- 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

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

Network controls and segmentation methods include:

- **Kubernetes network security policies**, which 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)**, which provides a programmable, adaptable network fabric that is provisioned in real-time to support dynamic networking security requirements and is typically implemented with a container networking interface (CNI).

- **A hardened service mesh**, which provides network segmentation, network visualization, authentication, and authorization for containerized applications and microservices.
- **Packet analysis**, capturing live pod network traffic to typically debug issues in the communication between services.
- **API management**, controlling access to APIs and securing API traffic.

Data controls

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

Data controls include:

- **Data encryption**, which provides data cryptography, tokenization, data masking, and key management capabilities to help prevent unauthorized disclosure of data in databases, files, and containers.
- **Data protection**, discovering and classifying data—as well as monitoring and auditing activity—to help protect sensitive data and improve compliance.

Runtime analysis

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

Runtime analysis and protection methods include:

- **Admission controller**, which functions as a Kubernetes gatekeeper that governs and enforces what is allowed to run on the cluster.
- **Runtime application behavioral analysis**, which examines system activity and intelligently detects suspicious or malicious actions in real-time.
- **Threat defense and runtime application self protection (RASP)**, which detects and blocks cyberattacks in real-time.

Audit and monitoring

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

Audit and monitoring methods include:

- **Monitoring** Kubernetes and pod processes for malicious activity, and providing visibility into the platform logs.
- **Security information and event management (SIEM)**, which centralizes events reporting by consolidating logs and network flow data from distributed devices, endpoints, and applications.
- **Forensics**, deep data collection which 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 include:

- **Security orchestration, automation, and response (SOAR)** platforms, which automate actions in response to security incidents and integrate with other security tools.
- **Automated resolution** to issues related to Kubernetes configuration errors and policy infractions.

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.

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

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

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 develop cloud-native applications, integrate existing and new IT applications, and automate and manage complex environments. A trusted adviser to the Fortune 500, Red Hat provides award-winning support, training, and consulting services that bring the benefits of open innovation to any industry. Red Hat is a connective hub in a global network of enterprises, partners, and communities, helping organizations grow, transform, and prepare for the digital future.