Considerations for implementing DevSecOps practices

1 Build a DevSecOps team

DevSecOps teams need to have security, development, and operations skills and expertise. Whether the team is virtual or led by one manager, their actions need to align with the project goals. Security staff need to work with developers and operators early in the implementation process to make sure the team delivers a successful project. A culture of ownership needs to be instilled.

DevSecOps tools for container-based applications are continually changing. To prepare the team for success, make sure they are familiar with the most current technologies and threat landscapes. Investigate which training and certifications are available to further develop their expertise and confidence. Technical consultants, who are familiar with industry best practices, can help implement a new DevSecOps initiative more effectively.

2 Manage security controls for the entire life cycle

Reacting to each security requirement that arises can make implementing effective security solutions difficult. To implement a more effective security strategy, consider what the needs are throughout development, testing, operations, and monitoring. Increased security controls may be needed for application analysis and testing, identity and access management, data protection, network controls, monitoring, threat detection, auditing, and remediation.

To help understand and evaluate the fundamentals of the entire application life cycle, Red Hat developed a comprehensive DevSecOps security framework.

The framework provides an integrated view of the security technologies and techniques that apply to each stage. The framework evaluates tools and processes to see how they fit into the overall landscape. If needed, use a combination of tools to address the comprehensive security requirements for all life-cycle stages.

3 Use reliable platforms

The foundation of your DevSecOps practices must be stable and reliable. With the move to container-based delivery, organizations have encountered challenges safeguarding Kubernetes for production. A solid foundation needs a trusted source for operating systems, container platforms, container base images, and middleware. Ideally, these components have reliable, hardened, default configurations that meet enterprise-grade requirements.

The same level of controls used for hardening the system should be in place early in the development cycle to avoid problems in later stages.

There are several advantages to using a container platform early in the development stages of a project. A container platform provides space for building continuous integration and continuous delivery (CI/CD) pipelines, in addition to developer self service. These pipelines are an ideal place to add application testing security tools, code, and dependency analysis. Building code into containers during integration helps scan containers for vulnerabilities. Implementing security checks like these into early development stages allows potential vulnerabilities to be addressed before they impact project delivery schedules.

4 Safeguard supply chain and delivery pipelines

Recent security incidents have underscored the need to safeguard your entire software supply chain. Tools can verify that your software components are free from known vulnerabilities and have open source licenses that are appropriate.

It is critical that software components you download have not been modified by third parties. The software you produce also needs to reach production without unauthorized or unintentional changes. Use code and image signing to verify software provenance.

Tools like source code management systems, container registries, and binary repositories need to be reliable and enforce your policies. Container registries and tools should have rich capabilities for working with signed images. The signatures of downloaded codes and images should be verified before they are stored and allowed to run in production.

The controls that are applied to code and software artifacts should be applied to software and infrastructure configuration. Container platforms allow configurations to be expressed in files and treated like source code, using Git-based source code management practices. Using version control for code and configuration allows changes to be traced and audited, fosters automation, and provides opportunities to integrate security throughout the entire life cycle.

5 Weave security throughout the application life cycle

The goal of agile methodologies and DevOps practices is more frequent releases, therefore, security processes need to be ongoing and reiterative. DevSecOps yields the most benefits when security is integrated throughout the entire application life cycle. Instead of forming a barrier, keep your security processes transparent and automatic.

As you weave security technologies and processes throughout development, testing, deployment, and production operations, consider that security needs to be a part of every stage. Multiple tools are needed to address a full set of security requirements, integrated into your platforms, and to each other. Red Hat, along with its partner ecosystem, offers integrated security solutions to address the entire application life cycle.

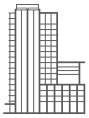
Red Hat has extensive experience delivering reliable platforms starting with Red Hat® Enterprise Linux®. Red Hat OpenShift® is an enterprise-ready Kubernetes platform focused on increasing security at every level of the container stack. Through the open nature of these platforms, Red Hat and its partners create an ecosystem with a comprehensive view of DevSecOps security. In this ecosystem, you can find ways to address the security requirements identified in the Red Hat DevSecOps security framework.

Red Hat DevSecOps framework

Get a comprehensive view of the DevSecOps life cycle and security use cases with the Red Hat DevSecOps framework.

DevSecOps webinars

Watch webinars from Red Hat and Red Hat security partners to see how you can make your application life cycle safer and more reliable.



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

redhat.com
O-F29681