

splunk >



Red Hat



Securing Complexity: DevSecOps in the Age of Containers



Securing Complexity: DevSecOps in the Age of Containers

Introduction

Acceleration to the cloud is affecting all industries as organizations take advantage of the flexibility, efficiencies and security benefits of being able to hyperscale their abilities to elastically spin up large-scale environments in seconds. But these new cloud-native and hybrid cloud environments, which use containers and serverless applications, result in immense operational complexity, opening up new cyberattack vectors and security risks.

Bad actors use this complexity to exploit unforeseen vulnerabilities and hide their activity from those responsible for monitoring applications, networks and systems. Where DevOps and Security teams are siloed, there are even more opportunities for security blind spots to occur, which attackers can leverage and where their anomalous behavior may go unnoticed.

To reduce the opportunities for attackers, DevOps teams need visibility across their entire tech stack – from on-premises infrastructure to cloud environments. This will ensure high performance, prevent outages and help identify and resolve incidents quickly, before they affect the organization and its customers. Some organizations achieve this by centralizing, aggregating and correlating the logging and systems data from all their different DevOps and security tooling, or tech stack, to reduce the apparent complexity.

A culture change is also needed when integrating DevOps and SecOps in line with the

“shift left” concept of including security early in software design. Traditionally, businesses prioritize speed to market, requiring DevOps to move fast to create apps. Then security teams are called in to review them just before they go out the door – which could often hold up the process when security concerns were identified and then took far longer to fix retrospectively. Security now needs to be more at the center of DevOps to form a refocused culture called DevSecOps, ensuring security is embedded from the outset. But DevSecOps goes beyond building more secure apps; it must also encompass securing the software’s working environment and applications in production.

Another aspect to be addressed is the speed of change. With DevOps tools increasing and changing at a fast pace, security needs to support this “go faster” mentality without being overwhelmed by the addition of new tools. Combining agility with security is achieved by integrating with approaches such as continuous integration with continuous deployment, or CI/CD, to bridge the gaps between development and operation activities and teams, which enforces automation in the building, testing and deployment of applications.

The ability to manage this complexity and execute cloud transformation in a sustainable and efficient way differentiates success from failure. 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.

Problems and Challenges

Increased Complexity With Hybrid Cloud Environments

DevSecOps needs to achieve the speed and agility of DevOps, while incorporating security as part of the entire life cycle process. In particular, it needs to overcome the issues of complexity, especially in hybrid cloud environments where on-premises infrastructure combines with cloud-hosted infrastructure – often from multiple hosting giants such as Microsoft, Amazon or Google, each with their own capabilities and configurations. This can make ensuring efficient resource deployment with visibility and asset identification a significant challenge.

One of the most consistent concerns in the cloud-native journey is the increasing complexity and lack of repeatability in the DevOps life cycle. An essential step is to ensure that in all stages of the delivery cycle, DevSecOps retains visibility and control over ever-more-complex systems.

Coherent Application Visibility and Management


DevSecOps needs visibility over the entire tech stack to identify weaknesses such as insecure

coding practices and to avoid inconsistent access control management when integrating components. Integration of tools and data sources used by separate teams is required so that all teams have situational and operational awareness of their interactions.

In organizations without formalized security programs or systems, implementation of distributed cloud systems can potentially be expensive and require heavy resourcing hours to manage large security processes. In the absence of a formal program, teams are free to choose their own tools, making the task of securing the full software development life cycle manual and extremely difficult. The absence of a data-driven analytics platform leaves organizations with poor operational visibility, which contributes to time-consuming manual processes. These are often highly skilled manual processes, and there is currently an acute shortage of cybersecurity skills.

It is no longer appropriate to silo knowledge, skills and tools, given the rise of containers, Kubernetes platforms and security tools that provide value across teams. Container security tools, such as Red Hat Advanced Cluster Management for Kubernetes, Aqua and Prisma Cloud, provide functionality for Ops, Security





and developers. Hence a platform is required that is suitable for both Developers and Ops, such as Red Hat OpenShift Container Platform. A fragmented approach to authorized access and control, without securing the toolchain in the software development life cycle, or SDLC, can increase the likelihood of intrusions, secrets disclosure and unauthorized access. This puts valuable assets, such as personally identifiable information, or PII, and intellectual property at risk and exposes vulnerabilities.

Among the most fundamental issues to be tackled is securing Kubernetes platforms. Kubernetes is an open-source container orchestration platform that automates many of the manual processes involved in deploying, managing and scaling containerized applications.

While downloading and installing Kubernetes is relatively easy, getting it ready to support business-critical applications in a secure, reliable and scalable manner can be a challenge. In fact, deployment, security and management of Kubernetes continue to be among the

key challenges for enterprises as they move applications to a containerized environment.

Additionally, to achieve a comprehensive approach for enterprise DevOps in a Kubernetes deployment, it takes culture, processes and additional technical capabilities above and beyond those provided by Kubernetes.

In many environments, creating visibility across the software delivery chain requires changing business structures, practices and even culture. Resistance to change is not uncommon. Staff may resist adding security professionals to a group they feel is working well already.

Other problems include traditional security practices operating after the fact, running their assessment manually once the app is complete and before it is released. In an agile world, where applications are released potentially every week or every day, that approach does not scale. Hence there is a need for automation. Similarly, security professionals will have to master development-centric tools.

Potential Steps on the Journey to DevSecOps

Automated security tools play an important part in coping with the speed of development and helping overcome the shortage of skilled staff. These enable integration of security into the DevOps CI/CD process, providing “continuous security.”

When these tools are created separately by each team, compatibility management issues can be introduced along with approaches to managing additions, and any resulting inconsistency provides a potential security flaw. These potential problems can be overcome by standardizing on an enterprise-ready Kubernetes platform and tools.

Using DevSecOps methodology will help deliver a centralized understanding across the entire team development environment – QE, DevOps, SRE and security – giving teams the ability to align on work processes and objectives without having any disruption in the flow.

Key elements to providing an entire software development life cycle approach, including recommendations explained by Domnick Eger in a Splunk blog, comprise:

- **Planning and Code Review.** DevOps teams can document changes and tasks and provide visibility to all teams, with automated correlation of a task or change request.
- **Build Pipeline Automation.** Tools that scan dependencies and test for vulnerabilities automatically check signatures and CVE mappings to determine how risky code is before it’s released to the company.
- **Release and Monitoring.** Correlating data from planning, source code management, build and testing systems ensures configuration catalogs are consistent.
- **Embrace Continuous Delivery.** Delivery processes should be revamped to focus on smaller, more frequent release cycles, setting the stage for the required operational shifts to migrate to DevSecOps.
- **Align and Integrate Security With the DevOps Workflow.** The goal is to incorporate security tools, including automated security testing, directly into the development process.
- **Implement Continuous Security Monitoring Tools.** Once code is deployed, applications must still be actively monitored to ensure their security over time.
- **Train Staff Appropriately.** Align the skills of your DevSecOps team members. Focus on ensuring developers have access to security training to keep up to date on security practices while also immersing security professionals in DevOps methodology.
- **Focus on Data.** Ensure data is collected from across all siloed data sources to provide a complete integrated picture and ensure visibility.



Splunk/Red Hat Partnership Overview

Splunk and Red Hat, partner together to deliver real-time insights across all stages of the application and software delivery life cycle from the data center to the cloud, with full-stack visibility into private, hybrid and public cloud environments. Splunk's ability to aggregate and correlate data from Red Hat OpenShift and partner technologies provides enterprises the opportunity to improve their DevSecOps metrics.

One example is the ability to decrease the time it takes to resolve a production security incident. When security incidents occur, knowing what apps are affected, insights into the fixes, and who can apply the fixes are critical to restoring service and remediating the application. Using Splunk and Red Hat OpenShift Container Platform and their respective partner ecosystems, data can be gathered and correlated throughout the DevSecOps pipeline to provide this key information proactively, allowing the right people to work on the right fixes right away.

Splunk's ability to aggregate and correlate data from Red Hat OpenShift and Red Hat's partner technology and then aggregate it and put it into context on a single platform enables better understanding of threats and incidents, with automation enabling a faster response, and as a result, threats can be averted and downtime reduced.


Red Hat OpenShift Container Platform

A foundational tool is Red Hat OpenShift Container Platform, an enterprise-ready Kubernetes container platform used by developers and operations teams to easily build, secure and deploy application containers by providing a comprehensive platform that can automate application, container and infrastructure management.

Red Hat OpenShift is available as a fully managed cloud service on leading public clouds or as a self-managed software offering for organizations requiring more customization.

Red Hat OpenShift includes a container-optimized Linux operating system, container runtime, networking, monitoring, registry and authentication and authorization solutions. Its users can automate life cycle management to get increased security, tailored operations solutions, easy-to-manage cluster operations and application portability.

The enterprise-grade container platform also includes Red Hat Enterprise Linux CoreOS foundation support, plus training and consulting where required. This open-source container orchestration platform automates many of the manual processes involved in deploying, managing and scaling containerized applications so users can cluster together groups of hosts running Linux containers, leveraging Kubernetes to manage those clusters.



Beyond app creation, additional functionality is provided by Red Hat OpenShift for common operational tasks required to run applications on a Kubernetes cluster, including:

- Source code management, builds and deployments for developers;
- Management and promotion of container images (moving them through various runtime environments);
- Application management tools;
- Team and user tracking;
- Networking infrastructure for the cluster.

The Red Hat DevSecOps Framework

Red Hat and its security ecosystem have created a DevSecOps framework that provides a blueprint for delivering an enterprise DevSecOps solution. The Red Hat DevSecOps framework identifies nine security categories and 34 security functions and their integration points that should be considered in the DevOps life cycle. These security categories include:

- Platform security, including host and container runtime security features;
- Vulnerability and configuration management, which analyzes applications and images with functions such as SAST, SCA and DAST;
- Identity and Access Management to provide authentication, authorization, secrets management and provenance;
- Compliance audits and controls;
- Network controls, such as network policies, SDNs, service mesh and packet analysis;
- Data encryption and protection;
- Runtime behavioral analysis and threat defense;
- Logging and monitoring;
- Security orchestration and remediation.

Security and Red Hat's Open Hybrid Cloud Strategy

Red Hat provides a resilient, security-focused foundation and trusted technologies so that customers can turn their focus to building, managing, and controlling hybrid environments, implementing an automation strategy, and developing robust applications with DevSecOps practices.

Red Hat's people, processes, and technologies work together to allow customers to mitigate their risk and meet compliance requirements across the application and infrastructure stack and life cycle, for both traditional and cloud-native environments. They are enabled to build an open hybrid cloud that helps them achieve their defense-in-depth objectives and take control of their hybrid cloud security and DevSecOps challenges.

The Splunk Data Platform

Splunk's core data platform enables searching, monitoring and analyzing of machine-generated data to provide visibility and response capabilities throughout the entire CI/CD pipeline, delivering a solid foundation upon which to successfully implement and operate a DevSecOps practice.

Splunk Cloud and Splunk Enterprise provide organizations with a flexible, scalable data platform that combines security and visibility of data from all sources in a single solution.

With so many different tools used throughout the CI/CD pipeline, producing one holistic view requires the flexibility to be able to integrate with whatever combination of tools are currently in practice. Thankfully, Splunk Cloud and Splunk Enterprise both have the flexibility to ingest data from any source. Splunk's Data-to-Everything Platform includes Getting Data Into (GDI) Splunk, facilitating the collection of data – for example, from AWS instances for Splunk deployments.

There is an ecosystem of application development partners on the Splunkbase website that lets users post and share apps and add-ons, enabling Splunk to visualize the results of vulnerability scans and application testing results, map defects and vulnerabilities out to build numbers or application versions

and provide a risk assessment of how many instances of a particular version are currently running in production. Teams responsible for DevSecOps success can view the security and risk of their applications in development as well as the current landscape of threats and attacks in production.

Splunk Enterprise Security and Observability Solutions

Attack data from WAF or RASP solutions can be cross-correlated with the current vulnerability backlog in Splunk Enterprise Security to dynamically raise or lower the priority of vulnerabilities to remediate, as well as trigger security configuration and control changes in production through Splunk SOAR - security orchestration, automation and response for modern SOCs. Splunk SOAR automates repetitive tasks to multiply staff's efforts, enabling them to better focus their attention on mission-critical decisions. Users can respond faster and reduce dwell times with automated investigations using playbooks that execute at machine speed.

Splunk's technology enables organizations to better understand their own and their customers' environments. The integrated approach includes use of the Splunk Observability Cloud,





incorporating machine learning and IoT along with IT operations and security. This allows users to build and release new digital products faster with a more personalized omnichannel experience for each customer by automating processes while enhancing capabilities. By integrating an organization's existing security infrastructure, each part is actively participating in its defense strategy. An established vulnerability incident handling process, such as vulnerability management, can be set up with Splunk, avoiding a security process that usually involves several teams' system owners. Vulnerability Scan reports from Nessus, Qualys and other well-known vendors can then be fed into Splunk, which breaks them down into a full report of events to ensure every vulnerability in a system can be handled and investigated separately if necessary.

Splunk Mission Control can then unify security data, analytics and operations functionality on a single cloud-based platform to streamline workflows and increase team efficiency.

As a part of Splunk Observability Cloud, Splunk Infrastructure Monitoring is particularly suited for Monitoring of OpenShift, which means gathering metrics about the health and performance of the underlying Kubernetes environment at each of its layers – at the cluster, node and pod level – as well as the application containers running on Kubernetes. This fine-grained resolution and AI-assisted detection and troubleshooting ensures users always know what is happening in their OpenShift environment.

Splunk Observability Cloud is the only full-stack, analytics-powered and OpenTelemetry-based Observability Cloud. Its infrastructure monitoring delivers real-time infrastructure monitoring and troubleshooting for all environments, whether on-prem, hybrid or multi-cloud.

As part of this process, downtime from incidents can be further reduced using Splunk On-Call, or Incident Intelligence, to automate time-sensitive aspects of incident response, including escalations, war room, and post-incident reviews.

And Continuous Security Monitoring, plus K8 for Kubernetes Monitoring, further enhances organizations' ability to get a clear picture of their security posture with comprehensive dashboards and security metrics.

Advanced Threat Detection leverages ready-to-use content from Splunk's Threat Research team for additional context from Splunk User Behavior Analytics.

Rapid Threat Investigation and Response can then aggregate and analyze the context of an organization's data all from one view.

These transformational capabilities give organizations complete visibility into their SDLC to better secure the service delivery process and the services within, from code origination to cloud realization.

Conclusion

Splunk and Red Hat have partnered to enable organizations to overcome some of their most difficult challenges, such as adapting to new ways of delivering production applications and responding to the innate complexity in modern environments.

Combining Splunk’s ability to aggregate, analyze and drive response to all of an organization’s data with Red Hat’s leadership implementing open hybrid cloud infrastructure the focus is on providing a fully integrated solution.

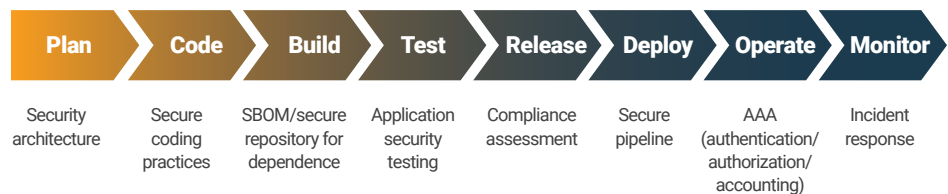
Among Kubernetes solutions, Red Hat OpenShift stands out as a leader with an enterprise grade Kubernetes platform – including built-in security features, a complete portfolio of application development and integration tools with expert training and consulting for those that need further support.

Functionality is provided for common operational tasks required to develop and run applications on a Kubernetes cluster, including source code management, builds and deployments for developers; management and promotion of container images (moving them through various runtime environments); and application management tools.

Splunk Infrastructure Monitoring of OpenShift and Kubernetes environments helps further improve the velocity, quality and business impact of app delivery and improves security by boosting visibility, automation and data use. This is achieved by providing observability across the entire DevSecOps practice and delivering actionable insights for development, operations and security teams.

These tools also facilitate the integration of DevOps and SecOps into a unified DevSecOps team that sees the same information, uses the same metrics, traces the same problems to the same source and is offered the same remediation solutions, in many cases, via automated service.

The result is more efficient use of skilled personnel, more secure development process and production environment, faster identification of issues and faster remediation, less downtime, and a more productive, data-centric operation.



About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

 BANK INFO SECURITY®  Just for Credit Unions CU INFO SECURITY®  GOV INFO SECURITY®  HEALTHCARE INFO SECURITY®

 infoRisk
TODAY

 CAREERS INFO SECURITY®

 Data Breach
Prevention, Response, Notification. TODAY

 CyberEd.io

**iSMG**
INFORMATION SECURITY
MEDIA GROUP