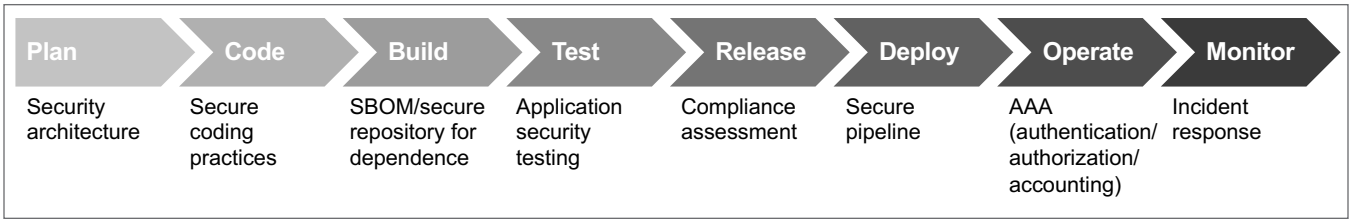
Splunk Elevates DevSecOps Strategy With Visibility and Action

Businesses understand the value of cloud and want to realize its full potential. However, accelerating to the cloud leads to immense operational complexity. The ability to manage the complexity and execute cloud transformation in a sustainable and efficient way differentiates the successes from the failures. Fortunately, data is at the heart of cloud computing and holds the key to sustainable implementations.

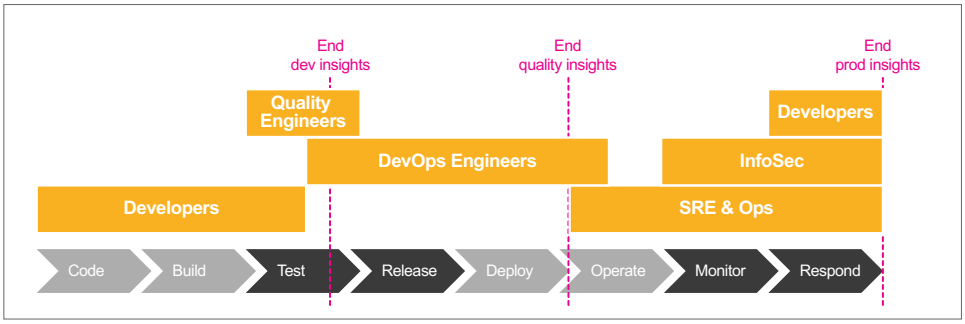
An important part of the cloud journey is changing how you build, manage and deploy services. Engineering and development teams often still exist and operate in siloed structures, and due to policy or politics, are also separated from security teams. Recent shifts in DevOps practices emphasize cloud and automation. As application velocity has increased, enterprises should re-evaluate their organizational structure and how they create visibility across their software delivery chain. While increased delivery velocity has reduced mean time to value for customers, it potentially increases attack vectors and expands attack surfaces.

Enter DevSecOps — the integration of security practices throughout the software development life cycle (SDLC) to ensure that secure services are brought to market. Through implementing DevSecOps practices, it's possible to secure the service delivery chain itself and the software being delivered in it. To be successful, the DevSecOps practice needs to be observable, with actionable insights and incident response capabilities.



Without DevSecOps organizations are exposed to:

- **Increased threat vectors and attack surfaces:** Poor visibility, secure coding practices and integrated, secure build-and-deploy methodologies can lead to potentially more vulnerabilities, configuration and version drift, and lack of consistent access control management.
- **Lack of coherent data visibility and management:** With the lack of sharing and integration of tools and data sources, teams blindly perform their work without situational and operational awareness of their interactions. The absence of a common analysis or visualization capability leads teams to imprecision and inaccuracy when making decisions regarding incident response, resource management and event handling.
- **Less holistic approach to authorized access and control:** Without securing the toolchain in the SDLC you will increase the potentiality for intrusions, secrets disclosure and unauthorized access. This puts development resources and intellectual property at risk and exposes vulnerabilities.



Forward-looking enterprises have embraced DevSecOps practices by incorporating security considerations earlier in development and establishing more visibility into SDLC processes. Analyzing activity across the SDLC allows developers, operations and security teams to be confident they are building the best possible product.

Splunk provides observability across the entire DevSecOps practice and delivers actionable insights for development, operations and security teams.

Secure applications with Splunk Cloud and Splunk Infrastructure Monitoring

- Make vulnerability scans visible: Measure the coverage, effectiveness and activity of your vulnerability scanning processes.
- Visualize measures of success: Establish cross-team KPIs and metrics to measure the success and performance of DevSecOps practices.

Secure delivery chain with Splunk Cloud and Splunk Enterprise Security

- Secure access to tool chain: Identify and alert on suspicious access and activity to your dev/test environments, tools such as CI/CD, secrets management, code repositories and other development resources.
- Ensure toolchain uptime: Support resilience of your critical SDLC infrastructure such as CI/CD, secrets management, code repositories and artifact management.

Secure production apps with Splunk Cloud and the Observability Suite

- Activate continuous verification: Alert on net new production vulnerabilities and activate remediation prior to their exploitation.
- Break visibility silos: Thread production incidents back to originating code with full-stack monitoring. From user activity to infrastructure, Splunk APM and Splunk Infrastructure Monitoring correlate production activity to deployments. Full-stack monitoring delivers valuable context to Splunk's On-Call incident response tool to reduce MTTI and MTTR.

Data guides code-to-cloud visibility

During the cloud journey, Splunk's DevOps and Security solutions provide teams the observability they need to deliver capabilities sooner with more confidence and trust.

The end goal for any organization should be the fulfillment of complete visibility into their SDLC in order to better secure the service delivery process and the services within, from code origination to cloud realization. Splunk is a transformation partner for enterprises developing successful DevSecOps practices.

Ready to Learn More?
Try our cloud-native infrastructure monitoring and get better visibility today.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

21-16935-Splunk Elevates DevSecOps Strategy-101-SG