Lacework

HOW TO BUILD A DEVSECOPS CULTURE

Strategies to successfully integrate security practices in DevOps for better outcomes with your cloud infrastructure.

Security integration is a business necessity

How DevSecOps culture benefits my business

The cloud enables organizations to remain highly responsive to customer and market needs, where velocity, cost, scale, and flexibility are the key differentiators. DevOps practices capitalize on these cloud capabilities to accelerate feature delivery.

The downside of a DevOps-only mindset

DevOps teams are incentivized to build fast, but not necessarily to build securely. Emphasis on feature velocity takes the focus away from security best practices, anomalies, and compliance.

In the cloud era, when security is divested from delivery, vulnerabilities are more likely to escape into deployment. This negatively impacts the overall security posture of the organization.

According to a study by IBM System Science Institute, the cost of fixing a bug increases 6 times at build-time when it escapes development. The cost increases 15 times when detected during customer testing, and 100 times when detected during the production maintenance window. The cost factor is even higher for security flaws. Security incidents not only imply financial losses, they also adversely impact an organization's reputation, customer loyalty, intellectual property, and legal standing.

A shift towards DevSecOps

Security and delivery speed are different games. While speed is visible, security is not unless it fails, and when that happens it's too late. Thus it is not practical for security practices to compete with feature velocity. The solution is to integrate them together. DevSecOps enables just that.

A DevSecOps culture embeds security in your DevOps workflows to speed up delivery speed without compromising security. It encourages more collaboration and less friction between DevOps and SecOps teams. In this culture, security is a shared responsibility that drives productivity, efficiencies, and better quality.

> **2019 State of DevOps Survey Findings:** Implementing security throughout the software delivery cycle improved an organization's overall security posture. Teams were twice as confident of their security posture after integrating security deeply into the software delivery lifecycle.

Five reasons to build a DevSecOps culture

1. Risk Mitigation

Automation is integral to embedding security in all stages of development and delivery. Enterprises with fully integrated security practices employ automation for driving efficiencies to:

- Detect security defects
- Stop a push to production to prevent escapes of critical vulnerabilities into production
- Quickly remediate, and restart the push

These practices reduce risks in production.

2. Better Quality

When delivery teams share the security responsibility with their security peers, security vigilance improves all across the development lifecycle. Security problems are caught early in the cycle lowering the time and cost of remediation, reduces defect density, and improves product quality.

3. Smarter Execution

DevSecOps culture removes the organizational barriers between development and security teams and results in smarter execution with shared goals and responsibility. When the build team is trusted to evaluate the security posture, and when they can autonomously decide whether to stop the build based on technical and business priorities, the overall delivery speed improves without compromising the security context.

4. More than "Shift-left"

A DevSecOps culture is more than just shifting security checks to the left. It enables multiple teams to work together and breaks knowledge silo. This instills more security awareness in the teams, emphasizes cross-team collaboration, and reduces friction in priorities. Everyone involved with software delivery sees security as their responsibility, they diligently address potential security issues, adhere to security policy and best practices, and cooperate if a security concern warrants a halt in deployment.

5. Resilience

Security drives reliability, predictability, measurability, and observability in your deployments. This fosters an intrinsically secure environment, it also improves responsiveness to security issues when they arise by leveraging discipline and automation.

> **2019 State of DevOps Survey Findings:** 22% of the surveyed companies who integrated security at the highest level have reached an advanced stage of DevOps evolution. Doing security well enables you to do DevOps well.

Transitioning to Integrate Security with DevOps

Five Steps to build a strong DevSecOps culture in your organization.

In organizations, usually, there's a dedicated team responsible for security while the development team focuses on feature delivery. A DevSecOps culture changes that dynamic by bringing Dev, Sec, and Ops teams together with shared security responsibility.

Steering this transition successfully can seem like a major undertaking for business leaders, who are faced with the question: **"But how do we integrate security into the software delivery lifecycle?"**

The following five steps can help you establish a game plan to achieve that transition.

Step 1: Training and Awareness

To build a team that secures systems at the speed of DevOps, the first step is to institute cross-team security awareness.

Members of the Dev and Ops teams need to understand how security standards and practices impact their functional workflows. This requires regular security awareness training. It is also important to educate on the technical debt and business fallouts of shipping code with security gaps and vulnerabilities. Awareness empowers engineers to integrate security vigilance when they gather project requirements, plan the design, build code, perform static analysis and internal tests, and most importantly when pushing code to production. They begin to recognize the role and relevance of security scanning and automated checks during the CI/CD process. By integrating security into the complete software-development lifecycle teams can better handle the security challenge, instead of having to play catch-up and address critical security issues post-deployment.

Step 2: Embed Security Processes

Processes enforce security practices in the cloud workflows

Tightly managed processes in compliance with security policies and standards are necessary to embed security in your cloud operations. This begins with close teamwork between Dev, Sec, and Ops teams during cloud infrastructure design, network buildout, resource management, access control, threat modeling, etc. Security governance and reviews ensure compliance. Processes to support developers when they seek security guidance improves productivity. For example, a security expert can be part of the daily scrum calls to address concerns. Ticketing systems and collaboration tools can be instituted to provide answers on business risk questions. DevOps can partner with security experts to implement isolated environments for development, staging, and production with secure access hygiene and configurations.

Step 3: Prioritizing Automation

Automation is the cornerstone of security integration in DevOps

Organizations with a strong DevSecOps culture relies on automation. Dynamic DevOps cycles where cloud workloads are provisioned on-demand require a high degree of automation. Automation is essential to integrate continuous assessments and to streamline security management workflows. Integration of security tools and software in the CI/CD pipeline to run vulnerability scans, configuration checks, container hardening, code analysis, compliance checks, attest artifacts, etc. simplifies the collaboration between security and DevOps to confirm security. Automated notifications alert the teams to assess security and reduce escapes. How well the automation tools are instituted determines how effectively you can enforce security practices and facilitate security sign-offs.

Step 4: Include Security Requirements in Reviews

Cross-team security reviews harden the build

There are occasions when the security experts prioritize certain security measures which may adversely impact operations, while the operations team may overlook security holes caused by certain configurations. Pre-deployment reviews provide a platform for the teams to address knowledge gaps and make informed wtrade-offs. This process provides clarity to senior management to gauge the business impact of deploying with a known vulnerability. Reviews create a feedback process to ensure changes have been implemented before deployment and ensure compliance for high-risk areas of code (authentication, cryptography, etc.).

Step 5: Incentivize Collaboration

Incentives communicate the value of DevSecOps culture

Incentives recognize the business-worth of driving a culture of cooperation and collaboration between security and development teams. When teams perceive security as something valuable to the business they are more likely to treat security as a responsibility that's shared within the organization. This fosters a culture where it is more likely that security will be treated with priority across the organization.

Incentives can be instituted across the organizational ladder. While engineers are rewarded for effective security assurance, managers and IT leaders should be recognized for instilling a collaborative environment and for continuously improving it.

The rewards of building a DevSecOps Culture

Enterprise-wide benefits driving better outcomes

The benefits of a strong DevSecOps culture span across the entire organization and yields many positive outcomes:

Reduce the risk of a security incident – Security awareness and concerted actions by teams to prevent security issues reduces the risk of a breach during deployment and improves the overall security posture of the organization.

Quickly response to security issues – Increased security focus, continuous assessments, and informed trade-offs helps to quickly identify and remediate issues found in deployment.

Accelerate feature velocity – DevOps teams can leverage integrated security disciplines to reduce unexpected risks, which accelerates their development cycles.

Lower security budget – A security-savvy organization can streamline resources, tools, and security processes that positively improve the bottom line.

About Lacework

Lacework security platform has been specifically designed to simplify how organizations implement a security-first model in their cloud infrastructure by addressing the challenges of both build-time and run-time operations. It provides the leverage of a unified security solution to integrate security across your entire development lifecycle. By integrating the multiple layers of cloud security in one platform, Lacework provides account protection, automates intrusion detection, secures containers, and ensures configuration compliance across AWS, Azure, GCP, and private clouds. Lacework's comprehensive view across cloud workloads and containers delivers one-click investigation and simplifies cloud compliance. Having these capabilities will not only strengthen your organization's overall security posture, it will also empower your DevSecOps teams with deep visibility and agility to successfully meet the requirements of the cloud era.