WHAT IS DEVSECOPS? COMBINING DEVELOPMENT, SECURITY & OPERATIONS

DevOps has dramatically increased how quickly you can deliver new features to the market. But with this speed comes new security risks—this is where DevSecOps comes into play.

(This article is part of our DevOps Guide. Use the right-hand menu to navigate.)

Overview of DevOps & SecOps

DevOps and SecOps have some key similarities. For everyone to have a deeper understanding of other aspects of the project they are working on, both DevOps and SecOps:

- Emphasize the importance of collaboration
- Promote the use of cross-discipline teams

This enhanced insight provides team members with a unique perspective that empowers them to:

- Focus on their tasks
- Consider how their work will impact the work of teammates

Operational intelligence is a constant concern for the teams as they look to enhance their understanding of each system and its vulnerabilities.

SecOps tools feed teams constant streams of insightful data that empowers them to maintain security standards while achieving continuous compliance. Yes, this intense focus on security can result in slower deployment rates. But that extra time provides high levels of security for increased

stability and mitigated risks.

What is DevSecOps?

Marrying SecOps and DevOps gives us the tools to go faster—while still maintaining safety. DevSecOps refuses to accept that the speed and safety are mutually exclusive.

DevSecOps is about creating a culture where security is a part of everyone's job, not just the people specifically working in security roles. Security needs to be at the top of every developer's mind as they build, test, and release features to production.

Bill Gates (reportedly) shared this very message in a 2002 Wired article:

> *"When we face a choice between adding features and resolving security issues, we need to choose security".*

The faster we move, the truer this becomes.

When we prioritize code creation above security testing, Parkinson's Law dictates that development work will consume the time up until the release date. Parkinson's Law says:

> *"Work expands to fill the time available for its completion."*

This normally means that less thought than necessary is given to security during the development process. If the release date is to be kept, often there is no time left to fix security issues.

Remediation of security concerns, identified late will see the production release date delayed, displeasing the development team and business owners alike. This can lead to dev teams and line of business owners circumventing the IT security team, shipping code to production with or without security scans, regardless of the results.

We cannot afford for security checks to be the final piece of the development puzzle. When security flaws aren't discovered until the 11th hour or after release, you will have reputational and financial damage—as too many businesses have demonstrated, to their peril.

DevSecOps moves the responsibility for security, ensuring it is fully integrated into every stage of the development journey, continually delivering security throughout the software development process. It achieves this goal through a combination of new tools and processes that enhance security of both the application software and the cloud resources which these apps use.

How DevSecOps works

There aren't steps in some process you need to achieve in order to "be DevSecOps". Instead, you'll want to incorporate two significant practices into your development practice.

1. Run early, frequent security checks

In order to secure the application software itself, run security checks much earlier and more frequently during the software development process. The earlier you catch vulnerabilities, the less dramatic and expensive those violations are to resolve. Waiting until release will just leave you nervous and unprepared.

By continuously delivering security alongside the continuous delivery of software, you'll identify

security problems before they become hopelessly entangled in the application and therefore more difficult, and costly, to resolve.

For example, when an application developer checks-in a new code snippet, a scan can be automatically initiated at build time to check for known vulnerabilities, such as those which might originate from the use of third-party libraries.

Performing early, automatic scans ensures that you're testing both functionality **and** security throughout the development cycle. The continuous delivery of security makes security scans far less disruptive than the old style 'big-bang' security scan at the end of the just prior to delivery. Just as they would have fixed a compile error found during automated testing, the developer can fix a discovered security issue as soon as it is flagged. In this way DevSecOps ensures that far fewer application vulnerabilities find their way into production.

2. Manage cloud resources for security

But security checks do not start and finish here. Most applications are now delivered using cloud services and resources such as:

- Storage
- Serverless compute functions
- Database searches

The number of these options provided by cloud service providers can easily number in the 100s and each of these must be correctly configured, by the customer, in order to be secure.

Gartner predicted that, through 2020, 95% of cloud breaches would result from the customer's action or inaction. For example, misconfiguring permissions of cloud storage. A quick online search of cloud data breaches over the last 12 months proves that prediction accurate.

As developers ship incremental application enhancements at a weekly, daily, or even hourly continuous delivery cadence – and where IT Operations provide self-service resource provisioning and configuration to those developers – they must put mechanisms in place to manage the security and regulatory compliance of all these cloud resources.

Benefits of DevSecOps in your company

Embedding a DevSecOps practice into your product development will:

- Ensure that security and compliance scans are integrated into DevOps processes
- Find and fix security and compliance concerns in cloud services

Best of all, DevSecOps will allow you to achieve these ends at a pace that mirrors DevOps. The business will innovate more quickly because security is integral to the process, not a hindrance to it. The result will be less risk of data breaches, more secure applications, and continuous security monitoring of cloud resources and services.

Implemented well, DevSecOps can deliver a sustainable competitive advantage, minimizing company exposure to the reputational and financial risks delivered by security breaches.

Related reading

- BMC DevOps Blog
- BMC Security & Compliance Blog
- DevOps Guide, a series of DevOps articles
- SecOps vs DevSecOps: What's The Difference?