DevSecOps
Reference Guide

Tailored DevSecOps Concepts and Practical Application

DOWNLOAD THE FULL REPORT AT SNYK.IO

The DevSecOps culture

Online media and marketing are filled with terms like DevSecOps methodology, DevSecOps model, or DevSecOps techniques. However, in order to be successful, organizations must understand that DevSecOps is first and foremost a culture. DevSecOps focuses on uniting the normally siloed roles of Development, Security, and Operations into a collaborative shared-responsibility paradigm. It seeks to break down barriers of finger pointing and deflection. Instead, it aims to build empathy and common goals among various disciplines within the organization.

There are three key pillars that must be considered when looking to shift the culture of an organization: people, processes, and technologies. DevSecOps principles build on these three intersecting parts, by eliminating the silos and creating a collective focus. This environment of shared responsibility and mutual empathy requires breaking down barriers between teams.

Consequently, people are the starting point and the foundation of any DevSecOps implementation.

Restructuring DevOps and Security teams to establish efficient cooperation between them, as well as offering good quality and targeted training to the wider organization will ensure that security becomes a frame of mind rather than a hindrance.

The next step is to introduce supporting **processes**, with the aim to further improve collaboration between people as well as achieving more secure development processes as a whole. These process changes are designed to span the three functional areas of development, security, and operations providing cohesion and uniformity between them. They establish a common goal of secure and stable software developed at scale.

Last but not least, the DevSecOps approach requires having the right **technologies** in place to enable employees to execute these processes as well as automate them. This, ultimately, reduces the organization's attack surface and enables effective management of the technical security debt.

As best practice, before starting on the journey to DevSecOps, organizations should assess their current development, security, and operations teams. The objective of this assessment is to plan for how DevSecOps approaches can be integrated into the organization. Visibility of the organization's overall readiness to adopt a DevSecOps paradigm should be established with clear action items for addressing any deficiencies.

People: empowering the team

Rather than following the habit of calling humans 'the weakest link' when looking at security-related factors, we can empower them to be the strongest link and an important part of a company's defenses. A modern security culture and mechanisms that work for, rather than against, people are crucial to making security work. Moving to DevSecOps starts by challenging the way traditional security teams integrate with the wider business. But the focus needs to be wide-ranging and not forget operations. Strong links between development, security, and operations teams ensure earlier feedback on the quality, from a security point of view, of the code, software or application, and in turn reduce the costs of implementing fixes.

Traditionally development was responsible for fast delivery, security was responsible for application security, and operations was responsible for stability. DevSecOps destroys those silos, eliminates finger pointing and unites all three roles in a common goal of quickly delivering software that is both secure and stable. Everyone has equal stake in all three objectives and uses their own expertise to support the others. Accountability, empathy, enablement become crucial characteristics of successful teams. To support this, underlying processes must change as well.

Process: supporting the new culture

Changing the mindset of the organization requires that processes are in place to ensure the new culture is adopted with ease.

Looking at organizational processes in DevSecOps requires breaking down traditional barriers of authoritarian policies and workflows. To support the model of shared-responsibility, equity of purpose needs to be established between each of the disciplines.

Gating models have to be removed when shifting to DevSecOps. Traditional security strategies involved setting key milestones at which security activities occurred and not allowing the process to progress past that milestone until an acceptable result was achieved. In some organizations with particularly mature models, operations implemented similar gates before software could be deployed. This gating model creates lengthy feedback loops that slow software delivery and ultimately reinforce silo-based thinking.

Mutual accountability is a concept that must be embraced, as a replacement to gating, and supported by subsequent process changes. Development, security, and operations roles should be working together to ensure all objectives of fast, secure, and stable software are achieved. Processes by which security and operational best practices are implemented throughout the delivery pipeline are crucial in establishing this collaboration and accountability. Of course, to do this also requires the support of proper technologies.

Technology: paving a path to success

While people and processes work together to ensure adoption of this new culture, it can all still fall apart if the underlying technology doesn't accommodate the changes. Technology that can integrate into the delivery pipeline, can be used with relatively low effort (often through automation), and supports the multi-functional needs of a DevSecOps model needs to be adopted.

Often when people think about DevSecOps technologies they get caught up in the automation of delivery processes such as builds, promotions, and deployments. But automation isn't always the correct answer.

Organizations need to look at their technology and automate when necessary and capable, streamline where possible, and eliminate where it's not practical or it is redundant. Minimizing the various technologies through which the pipeline travels is an underrated but effective way to optimize software delivery.

Developer first security to enable DevSecOps

Shifting left is not enough

There's a lot of talk in the security industry about shifting left. About how it's more effective to find vulnerabilities or security problems early in the process. About the need to scale security as digital transformation increases the volume and importance of software to every business. About speeding up the software development lifecycle by merging "Sec" with "DevOps" in the same way "Ops" was merged with "Dev".

But the reality is, to build a truly effective DevSecOps model, you can not just plug a security tool into the development environment and expect it to work. You need an approach that gives developers the ownership for security, and provide developer-first and friendly tools to enable them to successfully implement the security responsibility. And you need to enable security teams to both support and govern the development team to manage security effectively.

Enabling more than 400,000 developers to continuously find and fix vulnerabilities in open source libraries and containers.

SCHEDULE A DEMO

Open Source Security ***Container Security*** ***License Compliance***

Empower both developer and security teams to tackle the application security challenge

Developer-first Security

A frictionless and intuitive security-focused developer tool enables developer adoption

Automated Remediation

Actionable fix advice and automated remediation workflows make it easy to fix, and not just find vulnerabilities.

Security depth

Comprehensive, timely, accurate and enriched vulnerability database ensures issues are found quickly and fixed easily.

Visibility and Control

Reporting and prioritization features enable security teams to monitor security levels, and implement and govern policies.

Protected by snyk

Google mongoDB Skyscanner mastercard salesforce intuit New Relic BBC asos Telstra

Twitter: @snyksec

Web: https://snyk.io

Report author

Alyssa Miller (@AlyssaM_InfoSec)

Report contributors

Simon Maple (@sjmaple)

Guy Podjarny (@guypod)

Patrick Debois (@patrickdebois)

Francois Ouellet

Report design

Growth Labs (@GrowthLabsMKTG)

Office info

London

C/O Wework, 97 Hackney Rd
London E2 8ET

Tel Aviv

40 Yavne st., first floor

Boston

200 Berkeley Street, 24th Floor
Boston, MA 02116