DEVSECOPS IS JUST THE BEGINNING

Why modern security teams need a transformation (and how they can do it)

snyk | CYBERSECURITY DIVE

Custom content for Snyk by studioID

As companies push for digital transformation, rapid changes are sweeping across all industries, but possibly none more than in the world of software development. Today, every company's business is software, with skyrocketing demand for more advanced applications to meet the needs of mobile and tech-savvy customers.

Developers strive to improve technology for faster delivery, eye-catching features, and cutting-edge functionality. Modern software developers create more applications with faster workflows in more complex environments than ever.

But where has the digital explosion left security in the software development process?

Digital transformation has empowered development while overwhelming security teams with modern development workflows' speed, volume, and complexity. Security must address many unfamiliar risks and protect new endpoints while attempting to integrate often outdated tools into the rapid workflows favored by development–sadly, it's just not happening.

Many security professionals also need to develop an awareness of development. Since 2008, with the birth of DevSecOps, the software development world agreed security must shift left, and developers began to learn about security practices. Unfortunately, many security teams haven't received similar training, often lacking the necessary understanding of development to help break down silos, foster collaboration, and successfully integrate security solutions throughout the software development life cycle (SDLC).

This playbook will explore the current inequities between development and security, why modern security teams must shift their role and approach to security integration, and, most importantly, how they can accomplish this transformation.

Digital disruption and development's head start

Digital transformation created a massive need for software across all industries, with today's consumers demanding the optimum customer experience—service where, when, and how they choose. This demand creates a landscape where all organizations must become software companies, building websites and mobile applications to meet the expanding expectations of consumers. Today, the popular joke is that even banks are software companies that happen to manage people's money.

This business demand for software and the explosion of advancing tech empowers developers who push for faster application and update delivery, advanced features, and superior functionality in every release. Automated processes with streamlined components, fast-changing agile methodology, and cloud-native environments support rapid development workflows.

Advanced digital tools give today's development teams a leg up, empowering them in a position with little security oversight or control. Also, the explosion of new applications, interactions, and touchpoints creates many new, unfamiliar risks for security teams, who often struggle to keep up.

Successful DevSecOps application requires the unification of the two often seemingly at-odds cultures of development and security. Many organizations have dedicated significant internal resources for initiatives like Security Champions or CISO Guidebooks to help developers familiarize themselves with security practices. Sadly, the reverse isn't true–security teams often get overlooked regarding education on the development process.

Today, the emphasis on software development, along with the traditional secondary status of security, results in a huge disparity between the number of developers and security personnel. GitHub Security Lab estimates the ratio of software developers to security professionals to be around 500:1.

> **"The roles in application security are newer for average mainstream companies, not the true tech companies where security roles are more defined."**
>
> **JANET HEINS**
> CISSP award-winning security expert, global IT leader, and advisor at iHeartMedia

Why such a disparity between developers and security pros?

According to Janet Heins, CISSP award-winning security expert, global IT leader, and advisor currently at iHeartMedia, DevSecOps is still new for many organizations, and this could be responsible for the existing imbalance between development and security.

"DevSecOps is still relatively new and in the early stages. What are the roles in the security space? The roles in application security are newer for average mainstream companies, not the true tech companies where security roles are more defined. Still being in the earlier stages of security teams is a possible cause for this imbalance."

Separate cultures with unique challenges

The result of today's digital transformation push is clear—and doesn't favor software security teams. There are far more security-aware developers managing faster workflows with advanced tech tools than the fewer, less informed, and supported security personnel attempting to integrate traditional security solutions into the SDLC. Security teams can't keep up with the volume and speed of modern development workflows, facing the nearly impossible task of integrating security solutions while battling many significant challenges, including:

Diverse responsibility and corporate politics

In security's defense, the usually understaffed team shoulders many other responsibilities besides application security, often suffers atrophy from internal politics, and must compete for scarce resources within the political hierarchy.

Outdated tools and practices

Security teams are often hamstrung by outdated tools and approaches and security planning that fails to account for current code development. Many traditional security tools are built to fit a monolithic code base and don't fit a fast, segmented development process. Worse yet, most of these tools were designed for security teams and usually aren't developer friendly. Also, numerous traditional security approaches don't map to modern development processes, failing to manage the speed and volume required by current development workflows.

> **"I hand over my code to someone to tell me what security flaws I have, then I go onto something else, and two days later they come back, and I'm not even in that code anymore, and they list the flaws that I need to go find, fix, and resubmit—it's just super disruptive."**
>
> **JANET HEINS**
> CISSP award-winning security expert, global IT leader, and advisor at iHeartMedia

Lack of development awareness

Security's most significant challenge today may be its need for development awareness. Many security professionals lack an understanding of modern development processes, systems, components, workflows, goals, and needs. Security's lack of awareness and empathy for development can become an obstacle when trying to communicate and collaborate with developers on security integration.

Different and siloed cultures

Unwelcoming developers don't always make it easy on security teams as the two separate cultures often seem to hold conflicting goals destined to clash. Developers fear production slowdowns and often act like security isn't their problem. They're frustrated by unfamiliar, hard-to-use tools and inconvenient problem alerts, overwhelming and burdening them during production while failing to offer solutions.

Heins explains a developer's frustration, "I hand over my code to someone to tell me what security flaws I have, then I go onto something else, and two days later they come back, and I'm not even in that code anymore, and they list the flaws that I need to go find, fix, and resubmit—it's just super disruptive."

Application security needs a transformation

Most can agree that the DevSecOps shift left principle of incorporating security into software development early on should no longer be optional. How that's best accomplished is where the debate arises, but one thing is sure—security's role as the vulnerability-testing police, struggling to keep pace and regulate over a gaping culture disconnect, is over. So too, is dropping security tools in developers' laps while encouraging them to figure it out on their own, as this misses what needs to happen for successful security integration.

Today's DevSecOps demands transformative change–and it needs to come from security. The security pro's role must transform into an aware, knowledgeable, supportive partner with the teaching skills capable of empowering developers to make security decisions independently. Simon Maple, Field CTO at Snyk, explains, "The security team's role isn't so much to keep up with development but to create awareness, making sure the development teams become educated in knowing the best things to do, the right policies and steps so that they can deliver secure code by themselves. Security teams are on a journey, changing how they work to help and enable the developers, so they're empowered to do the correct work within their sprints."

Getting security up to speed

Helping your security team transform into its new role will require a dedicated effort from all departments across your organization. Here are some helpful suggestions to get your security team up to speed:

Increase awareness

Security's first step should be increasing awareness of development priorities, processes, systems, workflows, and goals. Security must put in the time and do the work to better understand and empathize with developers—only then can they be seen and trusted as true partners throughout the development process. From this foundation of understanding can grow a trusted relationship of communication and collaboration, with both departments working toward the shared goal of more secure software.

Don't assume an understanding of all developers because your security team sat with one group. Just because development teams practice the same agile methodology doesn't mean they use the same tools similarly. Security teams should invite themselves to each development team's meetings, knowledge shares, and scrums. Sit down, ask questions, and be curious to learn their unique processes.

Select the right tools

It's critical to select developer-friendly security solutions—easily learned and used by developers and, most importantly, seamlessly integrating into workflows while offering solutions rather than just identifying problems. According to Heins, offering developers a quick code fix is key to increasing developer buy-in, "Traditional methods say 'here's this flaw our tool discovered, now go fix it, and good luck figuring out how.' Better for security to say, 'here's this tool that will show you real time what needs to be fixed and how — I'm gonna give you this tool that will show you how to make it better quickly, so you can move on to the next thing you want to do.'"

Ask the right questions

Security teams must bring a comprehensive understanding of their solutions to the table. This knowledge and an educated awareness of the development process will help security work alongside developers to select and integrate the most appropriate tools. Here are some questions all security teams should ask:

- What are the best ways to seamlessly integrate our solutions into the development team's workflows without impeding their cadence?
- How can our solutions deliver the most relevant, problem-solving, actionable results for developers?
- How will the developers best receive the results?
- What is the minimum set of actionable results to be delivered?

Initiate effective internal practices

Modern security teams should fill their ranks with as many personnel with development backgrounds as possible. Hiring those with prior development experience can bring a valuable perspective to your team and add credibility in developers' eyes.

Consider starting a Security Champions program comprised of committed and dedicated developers who can provide a liaison bridge between departments with a sizable portion of their schedule dedicated to security matters.

Be sure to establish and define security and developer roles and monitor with designated metrics to help security integrate and work with development.

"It's about who owns what and who's responsible for what element. What's accountability, and how do you measure it? I think it's helping organizations put some more structure around that, and I think it comes from a combination of communication, collaboration, and technology to help achieve some of these elements," adds Mic McCully, Field CTO at Snyk.

Request developers complete scorecards detailing what they do and create a plan from the results clearly outlining developer roles and responsibilities. Also, include golden images and workflows to provide examples and guardrails around what constitutes a desirable security decision.

Invite security and development teams to collaborative activities like threat modeling exercises that help both learn the other's perspective concerning the SDLC and the risk relationship.

"What's accountability, and how do you measure it? I think it's helping organizations put some more structure around that, and I think it comes from a combination of communication, collaboration, and technology to help achieve some of these elements."

MIC MCCULLY
Field CTO at Snyk

Celebrate success

Recognizing and celebrating the success of either department regarding integrating security into the development process can often get overlooked but that shouldn't be the case, according to Maple.

"Celebrating success is really important to the development team's adoption of security processes. When an engineer does well or when a team achieves something, celebrating that success actually grows other people doing similar things. Engineering leads celebrating their teams doing something well in security is something I believe can also help security teams grow their awareness."

"Celebrating success is really important to the development team's adoption of security processes. When an engineer does well or when a team achieves something, celebrating that success actually grows other people doing similar things. Engineering leads celebrating their teams doing something well in security is something I believe can also help security teams grow their awareness."

SIMON MAPLE
Field CTO at Snyk

Is anyone successfully integrating security solutions into the SDLC today?

Given that DevSecOps is still relatively new for many organizations and security and development teams face significant challenges integrating security into the SDLC, are there any companies currently excelling in the real-world practice of a shift left methodology?

Richard Bird, Chief Security Officer at Traceable, weighs in, “No company I know of is performing at a world-class level in this space. I believe many companies are doing an okay job in balancing the challenges and tensions between security and development teams, but even the higher-performing DevSecOps organizations struggle tremendously with the friction caused by how long it takes security resources to address remediation. Most importantly, being just okay isn’t remotely good enough to defend against, let alone win, against the bad guys.”

Today, the companies experiencing success running progressive DevSecOps programs employ scorecards to help create plans, rely on Security Champion programs supported by Slack group participation, and maintain a strong culture where developers are empowered to answer other developers’ questions.

Others see results from self-healing systems using automated remediation requiring zero-touch from developers for specific vulnerabilities. Metrics now allow certain companies to witness tangible business impact from a productivity perspective and validate future shift left initiatives while helping boost developer buy-in.

Optional no longer an option

The explosion of digital technology created an enormous demand for software while giving developers the advanced toolset to meet that demand. Traditional security tools and practices fell behind, unable to keep pace with modern development workflows.

Security must transform into a new role of knowledgeable, empowering partners, helping developers integrate security solutions on their own. Building awareness of development is a must for modern security teams–only then will they be truly equipped to help select the best tools matching modern workflow requirements.

Viewing security from siloed camps is no longer an option. Developers and security pros must partner around a common goal—quickly and securely creating top-notch software features and functionality. Heins aptly sums it up, “The security and development partnership isn’t optional anymore. When you look at the rate of increasing cybersecurity attacks, a solid partnership between development and security has become necessary to protect a company’s customer base and reputation.”

Snyk is a developer-first security company that helps software-driven businesses develop fast and stay secure. Snyk is the only solution that seamlessly and proactively finds and fixes vulnerabilities and license violations in open source dependencies and container images. Snyk's solution is built on a comprehensive, proprietary vulnerability database, maintained by an expert security research team in Israel and London. With tight integration into existing developer workflows, source control (including Bitbucket, GitLab, Github), and CI/CD pipelines, Snyk enables efficient security workflows and reduces mean-time-to-fix. For more information or to get started with Snyk for free, visit https://snyk.io.

Learn More