PLURALSIGHT

FIVE STEPS FOR IMPLEMENTING DEVSECOPS IN YOUR AGENCY

Whether your agency is already a well-oiled DevOps machine, or whether you're just in the beginning stages of adopting a new software development methodology, one thing is certain: the security of your product is a top-of-mind concern. And with more public, highly-visible security breaches than ever, you may be evaluating how you can embed a security mindset throughout your organization without sacrificing agility or compromising release schedules.

Responding to security simply as point-in-time, one-off issues—or worse, only taking after you've actually been compromised—is no longer a viable or defensible position. You need to be considering how you can create a model for sustainable security. The key to this comes by embedding security in your software development process itself.

And that's where a DevSecOps strategy comes in.

WHAT IS DEVSECOPS?

In short, DevSecOps is a culture and mindset built on the idea that everyone is responsible for security, with the goal of distributing security decisions at speed and scale within an agile DevOps model to those who hold the highest level of context—without sacrificing the safety required.

Much in the same way that DevOps merges coding, building and testing with the ops functions of releasing, deployment and system monitoring of systems, DevSecOps layers on risk assessment, threat modeling, penetration testing, code review and compliance validation to ensure security is tightly aligned with agency processes and objectives. It makes security practices repeatable, consistent and embedded in development from start to finish.

In an ideal scenario, a perfectly functioning DevSecOps-minded organization would be transparent, aligned, high-performing and have quick releases. But in practice, aligning these three organizations can be difficult. Traditionally, most dev, ops or DevOps see security teams as a hurdle—a delay to getting code out the door. And on the flip side, many security organizations are understaffed relative to development teams or utilizing severely outdated methodologies that focus prioritize reactivity over proactivity. The result is that when these two or three organizations come together, they can lack context about each other's priorities, which can lead to miscommunication.

Luckily, DevSecOps is a better way, but it'll take buy-in.

To that end, here are five critical steps for embedding DevSecOps into your organization, with helpful tips—which combine to make a "DevSecOps Manifesto" of sorts—along the way.

LEANING IN

VS.

~~ALWAYS SAYING "NO"~~

AGENCY DRIVEN SECURITY

VS.

~~RUBBER STAMP SECURITY~~

OPEN COLLABORATION

VS.

~~MANDATED SECURITY CONTROLS~~

1. Understand that DevSecOps is a cultural change

Adopting a DevSecOps approach would (and will) be a huge undertaking for most agencies, so be empathetic to how big of a culture shift it is. Open a dialogue, be bold and be the one to take the first step toward change. If you engage using a clear and simple approach that highlights the efficiency and security benefits for each organization, it'll be easier to find common ground and have a shared mindset going in.

2. Align your security practices with your development workflow—not the other way around

It's important that when you enter discussions with the development teams, you do not bring your current security practices over to the development team and expect them to change how they develop code.

Obviously, you shouldn't ignore what your security requirements are in terms of monitoring, risk assessment and so on, but you need to be willing to change your security practice to align with the development workflow. If you tried to orient your DevSecOps approach around the way you traditionally approach security instead, the entire speed and cadence of your production releases would stall out. So be flexible, and make the priority producing clear value together.

3. Demonstrate that security can keep pace with velocity

As mentioned earlier, there will probably be a natural hesitancy from your dev, ops or DevOps teams to welcome your security teams or professionals into its "way of doing things." You can counter this hesitancy by offering to providing visibility and monitoring services, and working together to map your processes together and find opportunities to support agility.

Early on, you should be less interested in enforcement, blocking activities and slowing down the pipeline, and more investing in demonstrating that security can keep pace with the velocity with which your development teams are building so much product on, to ensure that the pipeline works smoothly.

24/7 PROACTIVE MONITORING

vs.

~~REACTING TO INCIDENTS~~

SHARED INTELLIGENCE

vs.

~~KEEPING INFO TO OURSELVES~~

4. Expand from prevention into vulnerability identification

Once security has found its footing in the development workflow, you can then consider expanding from a monitoring and visibility role into using your expertise to proactively identifying vulnerabilities in code. This is where the security team can become the development team's best friend.

5. Redirect security budget to support the development workflow pipeline

Finally, take a look at your own security budget. As you change your practices to align with the development workflow, are there places you can redirect some security budget to that workflow pipeline? Doing so will show your commitment to the sustainability of security in every release, but you're also going to be seen to be a rockstar for bringing additional budget to the CI/CD pipeline.

Security is everyone's responsibility

It can seem overwhelming to steer toward a cultural shift like DevSecOps, but it's important to remember that cultural shifts don't happen in a day, or even a month or year. Just by starting the conversation, you're already well on your way to a more nimble, sustainable security future.

(Learn more about DevSecOps in depth with Richard's on-demand webinar DevSecOps: The Holy Grail of Sustainable Security.)

Protecting your agency—and your agility—starts with tech skills. Talk to us about starting a pilot.

sales@pluralsight.com
+1 888-368-1240 | +1 801-784-9007

Richard Harpur is a Pluralsight author and highly experienced technology leader with a remarkable career ranging from software development and project management to roles as CEO, CIO and CISO.

You can follow Richard on Twitter at @rharpur.