Shifting Your Organization's Security Mindset to Work Well with Developers

By Ashley Ward, Cloud CTO, Palo Alto Networks

In a socially distanced world, having separate silos is important—but the same is not true when it comes to modern software development.

Silos within organizations hinder the digital transformation that is an absolute existential necessity today. Developers once commonly operated in their own silos, but that has changed in recent years with the onset of DevOps.

With DevOps, the barriers between developers and IT operations have been somewhat diminished, but the same isn't necessarily true when it comes to security. More often than not, developers and security are still two separate siloed teams. But that shouldn't be the case. Security shouldn't be its own silo. In fact, breaking down those traditional barriers can help to empower developers and help organizations accelerate their development efforts overall.

Changing up the relationship between DevOps and security isn't just some altruistic dream. It's a concept that is referred to today by multiple terms including 'shifting left' and 'DevSecOps'.

What Are Shifting Left and DevSecOps All About?

The idea of 'shifting left' is about moving security from the end of the software development lifecycle to an earlier point in the process. By employing security tools as part of the development pipeline, the nightmare developers typically face in trying to fix flaws at the end of a development process can be mitigated.

DevSecOps is the next step on the DevOps journey. With DevSecOps, teams building applications shouldn't just be aware of how code is developed and deployed but also how it is secured in operations. DevSecOps is about embedding security in everything. Any and all touch points across the software development lifecycle should have some sort of security element in there.

DevSecOps isn't about making the development process more cumbersome. It's about making the process more efficient and identifying potential issues early. And that's good business.

Breaking Down Barriers Communication Barriers

A critical element for the success of DevSecOps and shifting left is breaking down the barriers that exist across development and security teams.

Some organizations will choose to embed a security person in a development team. Another approach is to train developers directly on security best practices. While either of those approaches can be useful, the first thing that must happen in either case is that communication barriers need to be broken down.

There is a common perception in many organizations that security is only about saying no—to any request—in the name of reducing risk. On the other side, there is a misconception that developers only care about delivering code, and security is not a priority. Neither sentiment is fundamentally true.

Security people are people the same as anyone else in the organization; they want to see the company succeed, and they want to see cool stuff happen. Developers also care about more than just delivery of code; they know that if something bad happens, there are significant implications that they want to avoid.

The Critical Role of Tools on the Path to DevSecOps

Beyond open lines of communication, you need a toolset that is integrated and is going to be able to cope with the changes that might be happening in your organization. Whether those changes are in cloud providers, the deployment stack, or otherwise, there is a clear need to have a platform that will work where you are—in the cloud or on-premises.

Thankfully, cloud native development approaches also unlock new ways of delivering security. The technology now exists to enable scanning for security issues from the developer's code screen right through to automatically scanning production environments. Overlaying the foundation of good security awareness and visibility is a need for user entity and behavioral analytics that can further help to minimize risk.

Overcoming Challenges and Enabling Secure Development

While tools are an essential part of shifting left and enabling DevSecOps, there are still challenges that organizations will face. There are always the 'unknown unknowns' as organizations accelerate digital transformation efforts to do more with less.

Far and away, the biggest problem organizations encounter when trying to bake security into development is that more often than not, everyone just wants the easy answer. They want good enough security—when that's not good enough. So, the biggest challenge about shifting your organization's security mindset to work well with developers is accepting that there's going to be some work on everybody's part. There is no easy button.

Take the time to invest in tools that can help to enable developers and security teams to work together. But also take the time to help break down communication barriers and establish processes that enable developers and security professionals to work together for common purpose.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

© 2022 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.
parent_a_shifting-your-organizations-security-mindset_061622