CISO's Guide to DevOps: Learning to Cooperate with DevOps and Living to Tell the Tale

The DevOps paradigm presents a major dilemma to Chief Information Security Officers (CISOs) and their security teams. DevOps requires agility and, in fact, most areas of IT have become agile by automating in areas like service orchestration and continuous deployment. The problem? The rate of change in security is slow and many IT security processes are still manual. For example, before deploying a new application, a security team may require weeks to analyze new architectures and create, test and deploy new security controls. This inhibits technical and business innovation.

Almost all companies today are trying to adopt DevOps practices. Organizations are moving from traditional, waterfall approaches to iterative development, agile, scaled agile and, finally, DevOps. DevOps moves the focus from development to delivery—a subtle but important distinction.

At ShieldX, we see security teams trying to get around the technical and innovation issues by using an agent-based approach. An agent gets baked into every system image and virtual machine. And that means every time developers test images, they have to also test the agent and every time the vendor updates the agent, they have to test the agent again. The agent-based approach severely constrains DevOps by requiring many additional testing cycles and even more application developers. Bottom line, application developers are often loathe to bake agents into their workloads. And, so the divide continues to grow.

CHECKLIST: HOW ARE SOME WAYS TO BETTER COOPERATE WITH DEVOPS

We think there are ways you can improve how you work with DevOps and survive.

- ☐ Take a service provider approach and figure out how your security team can come to the table as a collaborator. DevOps uniquely enables security to be better by building in the functionality and appropriate processes from the start through its CI/CD (Continuous Integration / Continuous Development) approach.
- ☐ Understand that there is going to have to be a process and a tooling change that closely aligns to the DevOps approach, for example, repeatable, template-driven processes.
- ☐ Look for a security solution that connects at the orchestration layer to offer multi-vendor support. This is a fundamental requirement for visibility and consistent policy across your cloud-extended enterprise.
- ☐ Embed security into the overall developer chain: It not only speeds up the development process, but also makes it more secure.
- ☐ Automate as a way to securely enable CI/CD at the pace that development and the business require. Today there are toolsets that can take security intent and dynamically adjust security policy based on that intent. As DevOps spins up new workloads, security toolsets that leverage machine learning can automatically apply policy regardless of where the workload is housed and regardless of the rate of DevOps change. This not only provides security teams peace of mind and assurances around compliance, it also enables DevOps to spin up workloads faster and without security having to put on the brakes. Where not possible to automate, build in manual system checks into the software development lifecycle.
- ☐ Leverage policy-based security controls—these enable security and developers to collaborate on defining application connectivity policies and bridge the drive without agents. Network policy-based controls also allow for real-time changes based on traffic visibility and in synch

with DevOps spinning up or dialing down workloads. This needs to be a full set of security policy-based controls, spanning access control to anti-malware and Data Loss Prevention (DLP) to threat detection and prevention.

- ☐ Work with developers to ensure the passwords are compliant, that they are being rotated.
- ☐ Apply encryption at rest, in use and in transit.
- ☐ Get involved in open source. Increasingly developers and companies are relying on open source software. However, there's no standard way of documenting security in open source projects so it becomes important to build security into the development process and check and re-check applications for security threats and flaws.
- ☐ Treat security as an ever-evolving practice that one has to stay on top of and alter practices as the landscape changes. Organizations that offer developers and security teams the opportunity to cross-train will find that they develop security-conscious developers and security teams that are business focused. This is an opportunity for security teams to come up to speed with developer tools such as Chef and Puppet while developers get to learn about emerging security toolsets and practices.

Today's CISOs are faced with the dual mandate of securing an organization's assets and enabling agility. This dual mandate means matching the right people with updated processes and automated and orchestrated technologies that reduce the complexity of operations, but without compromising security. For CISOs and their teams to be truly empowered, they have to bridge the divide with DevOps and align with future development and emerging technologies.

SHIELDX MAKES SECURITY THE EASIEST THING ENTERPRISES DO IN THE CLOUD.

Our cloud-native, network security platform elastically delivers a full stack of agentless security controls—IPS, firewall, malware prevention, microsegmentation, and more—to protect data centers, cloud infrastructure, applications, and data. Our driving philosophy is to bring cloud speed, scale, and orchestration into the hands of security professionals worldwide. Based on cloud agnostic microservices technology, ShieldX ensures that security teams understand and maintain vigilance over cloud operations and workflows by continuously translating a security's intention into controls as cloud infrastructure rapidly evolves. Today, customers including Alaska Airlines and IDT have saved millions of dollars by eliminating control sprawl and consolidating security processes to dramatically reduce tactical systems management.

SHIELDX

ShieldX Networks, Inc.
2025 Gateway Place, Suite 400
San Jose, CA 95110 USA

+1 408.758.9400
info@shieldx.com
www.shieldx.com

October 2018