SHIELDX

ShieldX Solution Approach to Accelerate security at the speed of DevOps

DevOps is a business-driven approach to deliver solutions using agile methods, collaboration and automation. While the main goal of DevOps is to automate and deliver things faster and implement a higher level of integration between teams in an organization, implementing proper security controls can be challenging and therefore security can become an after thought in the evolution of operational paradigm shift to DevOps. Let's take a look at some of the challenges that DevOps pose to security.

CHALLENGE 1:

SECURITY TEAM IS UNAWARE OF NEW APPLICATIONS THAT ARE DEPLOYED BY DEVOPS

Consider an organization just started the journey of micro-segmentation and has to implement simple policies and nothing complex in terms of blocking new applications when are deployed. Micro-segmentation policies are not fully developed or rather loosely in place, DevOps team might spin up new workloads and applications. After all, DevOps is meant to automate things at a faster pace, deploy things often. When DevOps brings up a new application, in this case, the applications might just work fine and connects to all the required services and tiers without issues.

While the security team wants to know about the application to apply policies, there might be some collaborative gaps between both the teams and security team might be blinded in some cases in this scenario and not be fully aware of New Applications and its tiers to properly secure them.

The ShieldX Solution

Graph miner component of ShieldX discover/detect all the new applications/workloads DevOps team might spin up that the security team might not be aware of. The fact that the rules are a little bit loose and that when new applications come online, they might work just fine, however now security teams can fully get a view of what new applications that are being bought up and properly go about securing them.

CHALLENGE 2:

SECURITY TEAM GETS IN THE WAY OF DEVOPS TEAM

Consider another organization implemented complete micro-segmentation with a tight set of rules in place and when DevOps spins up new applications, they need to have "Access Control" rules in place for the new applications to work, because "Access Control" by definition is a whitelisting process of application to allow it to communicate. In this case, unless the DevOps team collaborates with security, the new applications will not be able to communicate.

When the DevOps team spins up new applications, they might not communicate or might not even work at all as the security is completely locked down all the communications to the new applications. The DevOps team has to notify the security team about the new workloads or applications that are being deployed so that the security team can allow the communication for these new workloads.

What we notice in this scenario is DevOps wants to automate as much as possible and security can get in its way and slow down the process of automation, because provisioning and crafting security policies can be time-consuming in general.

The ShieldX Solution

ShieldX solves this is by facilitating a collaborative framework by which the DevOps team can tag the workloads with a predetermined tag of application tiers and as and when these application tiers come up with the right naming convention and tags ShieldX will automagically secure them, that way both the DevOps team can accelerate the deployments of applications and security can also get their wish fulfed of securing the new applications as and when they are deployed.

CHALLENGE 3:
TRANSLATE THREAT MODELING OUTCOME INTO MICRO-SEGMENTATION RULES

In a scenario where an organization wishes that DevOps and Software development team work hand in hand and relevant secure development practices like Threat modeling outcomes can be translated to appropriate micro-segmentation rules and passed on to security teams to refine the security policies. This is bridging the gaps between the development teams, infrastructure teams and the security teams.

The ShieldX Solution

ShieldX solution can take the top-level application requirements that run on the underlying operating system or infrastructure and further refine the security policies based on the threat modeling outputs and align with software development teams on few security-related items that are relevant from securing these applications on the network. In fact, based on the threat modeling output the security intent of the application can be staged and instantiated with appropriate “Access-Control” and security policy sets.

SUMMARY

ShieldX solution brings higher level of automation to the DevOps and Security processes. with API-first modeling that supports integration with development processes in the cloud. This, in turn, can reduce and/or close the gaps between various teams and operational processes.

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

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

November 2018