Faster Cyber Security for DevOps

Author:

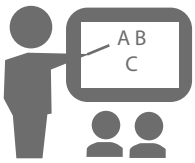
Vinod Vasudevan,
CTO, Paladion Networks

PALADION
HIGH SPEED CYBER DEFENSE

DevOps blends agile methodologies for development with a high level of automation for IT operations. The big question for product owners, product managers, and CISOs is the relevance of traditional information security practices in the world of DevOps. They worry about whether developers will have the time to build non-functional features (specifically, security), when they are iterating at high speed through different versions of software. They question the feasibility of the older model of security for data protection, when deployment happens quickly in a cloud environment. So, what does it take to integrate security in the DevOps world and make it DevSecOps?

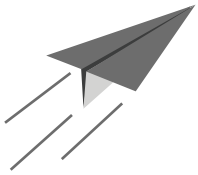
"The big question is the relevance of traditional information security practices in DevOps."

In our experience of working with leading DevOps organizations, the three principles discussed below drive success in DevSecOps.



Security fundamentals remain the same

DevSecOps requires the same fundamental practices we followed for waterfall methodology. We need threat modeling of the application, security code reviews, and dynamic testing of the application in pre-production. The production environment needs to be monitored for attacks and periodically scanned for vulnerabilities. DevSecOps does not mean scaled down security. The key requirement is to adapt these practices to make them effective at the speed of the DevSecOps world.



How to secure at the speed of DevOps

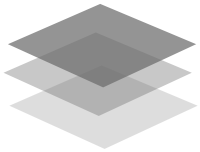
Take the security review of code (SAST – Static Application Security Testing) as an example, builds and releases could be as frequent as every week.

The time available for security code reviews is a fraction of the time available in the waterfall model. This calls for intensive automation of processes involved in security code review, but without diluting the quality of review. Examples include the automation of the initiation of a scan via triggers from the build server, the detection of incremental code, and the publication of results quickly with integration to the bug tracker: all without manual intervention. People resources should be focused on the verification of tool output results and on executing necessary manual test cases, not on the other activities of preparing and conducting tests.

> "DevSecOps does not mean scaled down security."

Another example is threat modeling. In the waterfall world, this is usually a one-time activity carried out during the design phase and updated upon major version changes. In DevOps, the requirements are incremental and continuously changing. Threat modeling is integrated into product grooming/sprint planning discussions with the product management team. Instead of preparing lengthy documentation, threat modeling is carried out with quick design tools for each short sprint.

In the "Ops" part of DevOps, security practices need similar speed. Most DevOps organizations use the cloud for operations. Current security technologies like SIEM, vulnerability scanning, configuration auditing, and traffic monitoring struggle to keep up with the pace of operations and dynamic workloads. A different architecture must be built to natively collect data, events, and configurations from the cloud and orchestrate the response through tools like Chef or Puppet to ensure speed in security.



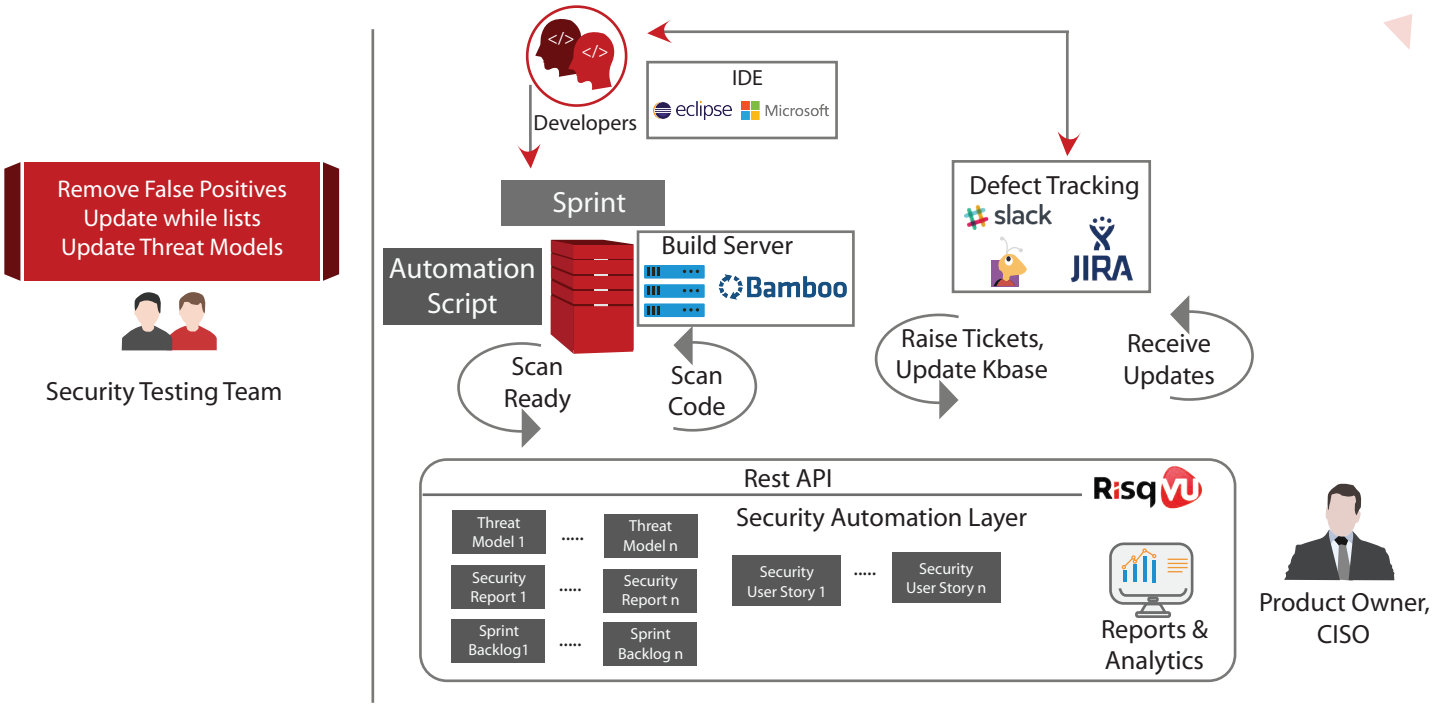
Security should be an invisible layer

The next requirement for DevSecOps is that security controls should be seamlessly integrated in the CICD (Continuous Integration, Continuous Delivery) cycle for the development and operations team.

"A different architecture must be built to collect data and orchestrate responses for speed in security."

Continuous Integration

Developers should do what they do well, which is coding. Security processes including security code reviews should not distract developers from their coding activities. As an example, if we force a developer to upload code after every build for a security code review, download a PDF report, read through it, and raise defect tickets based on the report, this is bound to lead to errors. Instead, there should be a security automation layer that integrates with the build servers to silently push code once a build is complete, and to raise security vulnerabilities as defects in the bug tracking system that the developer is using for his functional defects. Security requirements should translate to security user stories for the developer, similar to functional user stories.

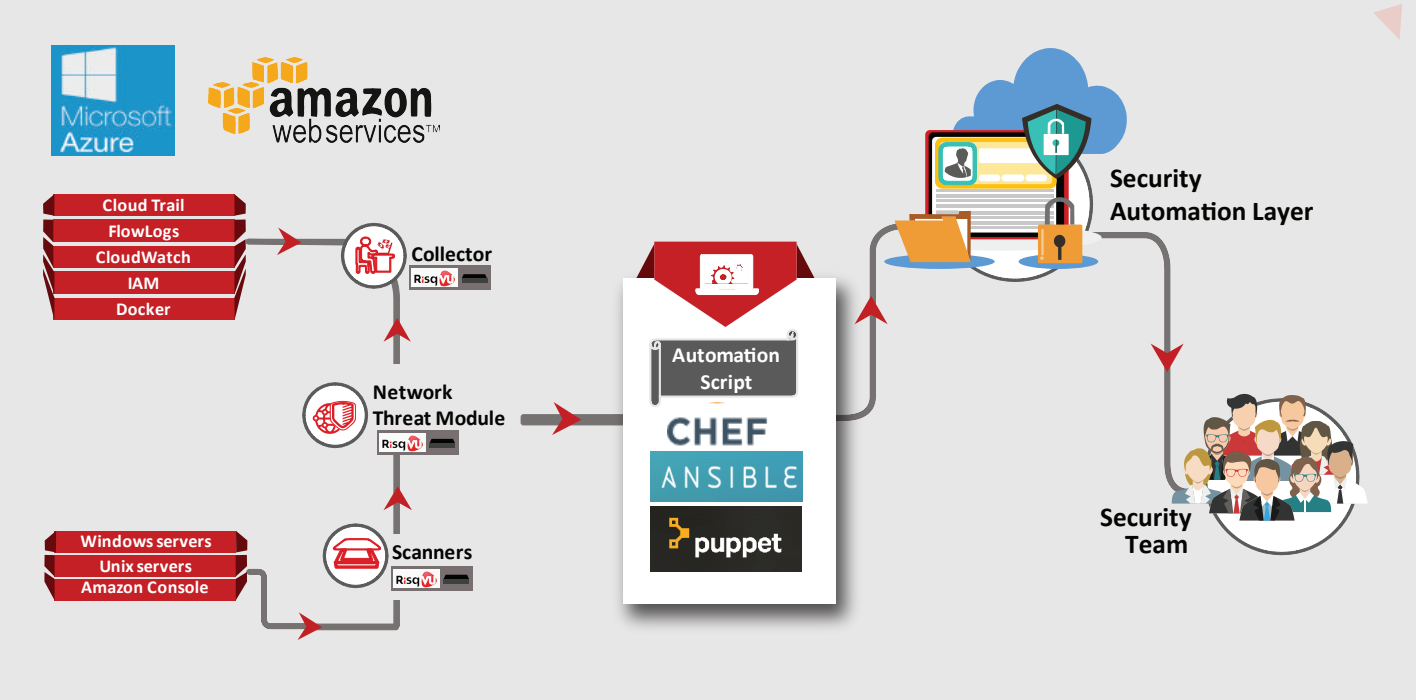


The diagram shows a typical automation flow and architecture for security in the continuous integration model.

"A different architecture must be built to collect data and orchestrate responses for speed in security."

Continuous Delivery/Deployment

Organizations at the higher end of DevOps maturity have a fully automated application deployment process.



Automation is done using a combination of tools available with cloud service providers such as Amazon and Azure and configuration tools including Chef, Puppet, and Ansible.

Security testing and monitoring operations should integrate into this fabric to provide an invisible layer of security controls. For example, configuration assessments of systems should start as soon as a dynamic workload comes up.

There are also new elements that must be secured in the cloud. In particular, the cloud console is effectively the master key for opening all doors and is often a high-risk entry point. Security teams in a DevOps organization must focus on this high-risk component among others, through configuration audits of cloud consoles, and monitoring of console related admin/user activities.

"DevSecOps is still in its infancy, but will evolve very quickly."

DevSecOps is still in its infancy, but we can expect it to evolve very quickly. New risks will also develop, as opportunities become ripe for Cybercrime syndicates to exploit vulnerabilities. Success in this new context is dependent on speed and seamless operation. Security becomes a silent but powerful engine humming in the background and providing desired business outcomes, while the DevOps team continues to move forward at high speed.

PALADION
HIGH SPEED CYBER DEFENSE

ABOUT PALADION

Paladion is a global cyber defense company that provides Managed Detection and Response Services, DevOps Security, Cyber Forensics, Incident Response, and more by tightly bundling its semi-autonomous cyber platform and managed services with leading security technologies. Paladion is consistently rated and recognized by independent analyst firms and awarded by CRN, Asian Banker, Red Herring, amongst others.

For 17 years, Paladion has been actively managing cyber risk for over 700 customers from its six cyber operations centers placed across the globe. It houses 900+ cyber security professionals including security researchers, threat hunters, ethical hackers, incident responders, solution architects, consultants and more. Paladion is also actively involved in several information security research forums such as OWASP, and has authored several books on security monitoring, application security, and more.

WW Headquarters: 11480 Commerce Park Drive, Suite 210, Reston, VA 20191 USA. Ph: +1-844-507-7668

Bangalore: +91-80-42543444, Mumbai: +91-2233655151, Delhi: +91-9910301180, London: +44(0)2071487475, Dubai: +971-4-2595526, Sharjah: +971-50-8344863, Doha: +97433559018, Riyadh: +966(0)114725163, Muscat: +968 99383575, Kuala Lumpur: +60-3-7660-4988, Bangkok: +66 23093650-51, Jalan Kedoya Raya: +62-8111664399.

sales@paladion.net | www.paladion.net