Improving AppSec while building DevSecOps pipeline

Suresh Chandra Bose, Ganesh Bose
SureshChandra.GaneshBose@cognizant.com

Abstract

More than 85% of the applications from public App store like Apple Store and Google Play violate one or more of the top 10 risks and vulnerabilities identified by OWASP. That clearly shows the current state of our insecure apps and hence the importance of DevSecOps is even more prominent today with the need for transformational shift to improve the AppSec.

By integrating application security principles and practices into software development and operations, teams can deliver with more agility but at the same time not compromising application security. The paper will articulate how to apply the DevSecOps best practices from Gartner across the different pillars of Continuous Delivery Pipeline. Threat Modeling as a service (TMaaS) is carried out to help discover the vulnerabilities and plug any gaps in security controls by identifying the threats and build the necessary protection into your DevSecOps workflows. With 60%-80% of today’s typical application is open source code, the primary focus is to identify and removing Known Open-Source vulnerabilities.

The effective outcomes are measured by tracking 6 key metrics to validate if DevSecOps is successfully implemented. When done right, DevSecOps goes well beyond “shifting security left” (getting involved early) to “shifting security everywhere”, ensuring application is secure in development, delivery and in production. When security is integrated in the DevOps pipeline, it comes with faster delivery and improved security posture enabling greater overall business success.

This paper will discuss real-world scenarios and answer the following questions:

- How Developers, Testers and Ops team work together to protect security?
- How can DevSecOps be adopted for Digital applications?
- How is Pen Testing different from SAST and DAST?
- What are the top 6 metrics every CISO must implement?

Biography

Suresh Chandra Bose, Ganesh Bose is a Senior Manager - Consulting at Cognizant Business Consulting practice. Suresh is an accredited Lead Assessor from TMiMi Foundation and has been in the IT Industry for more than 23 years with vast consulting experience in various industries. He has executed strategic initiatives for many Fortune 100 companies in the areas of PMO, PPM, Process Consulting, Program Management, TMiMi Assessment/ Implementation, Organization Strategy, Test Consulting and CIO/Governance Dashboard/Metrics across the globe.
Suresh holds 21 International certifications in IT and a speaker in 15+ international conferences, such as American Society for Quality (ASQ) Innovation Conference, American Software Testing Qualifications Board (ASTQB), 8.8 Computer Security Conference, DevOps Days Austin, DevOps Days Medellin, DevOps Days Rio de Janeiro, DevOps Days Tampa Bay, DevOps Days Berlin, Docker Community with JFrog, HUSTEF Hungary and the Pacific Northwest Software Quality Conference (PNSQC). Suresh has been part of the selection and review panel for a leading Software Conference.

Copyright Suresh Chandra Bose, Ganesh Bose

1 Background

According to Gartner research, by 2022, 90% of all software development projects will be following DevSecOps practices (up from 40% in 2019). From the recently released 'state of the DevOps report - 2021', our IT industry needed an explicit call to action to start including security from the beginning of the software development lifecycle. For many organizations, the relationship between the security function and the design part of software development was even more distant than that between development and operations.

2 What is DevSecOps?

A simple DevSecOps definition would be having development, security and operations team working collaboratively integrating security in every phase of the software development lifecycle as depicted in figure 1. By having application security practices built into the software development lifecycle, application team can deliver at speed without compromising security.

It is a mindset and a way of working that ensures everyone is responsible for security in the organization.

Figure 1: DevSecOps overview
3 Why DevSecOps?

The below figure 2 on the security tools usage by team across organizations is from the result of a recent survey conducted by Synopsis who is a leader in Gartner’s Magic Quadrant for Application Security Testing. The results display the low usage of security tools to protect vulnerabilities. With limited focus given to the DevSecOps tool adoption, the need is huge to increase investments in various tool set to have a Secured product.

![Survey Results]

Figure 2: Synopsys Survey – DevSecOps practices and Open Source Management in 2020

4 Continuous Delivery Pipeline

The Continuous Delivery Pipeline contains four aspects as shown in figure 3 as per Scaled Agile Framework® (SAFe®) methodology. They are as follows:

- Continuous exploration
- Continuous integration
- Continuous deployment
- Release on demand
Continuous Exploration (CE) is the initial phase of continually exploring Customer and market needs, fostering innovation and trying to build alignment on the Vision, Roadmap, and Feature set for a Solution. Continuous Integration (CI) is the process of developing, testing, integrating, and validating Features in a staging environment where they are ready for deployment and release. Continuous Deployment (CD) is the process that takes validated functionalities or features in a staging environment and deploy them to production through automated deployments, where they are ready for release. Release on Demand is the process by which functionalities or features deployed into production are released immediately or incrementally based on market needs. CALMR represents Culture, Automation, Lean flow, Measurement, and Recovery.

Let us see how security is injected into all these different aspects.

4.1 Continuous Exploration

Threat modeling is a key practice in Continuous Exploration to identify and prioritize potential threats to protect the entire system. By continuously applying threat modeling techniques, vulnerabilities and threats can be mitigated enhancing the security of the applications across the Organization.
4.1.1 Threat Modeling as a service (TMaaS)

Threat Modeling helps in the followings ways:

- To identify the security requirements,
- To pinpoint security threats and potential vulnerabilities,
- To quantify threat and vulnerability criticality, and
- To prioritize remediation methods to mitigate

Many Organizations started using Threat Modeling as a service (TMaaS) to protect their Enterprise and remediate with end-to-end security strategy and threat intelligence methods. The strategy involves 4 key steps:

Step 1-> what are we building?
Step 2-> what can go wrong?
Step 3-> what are we doing to defend against threats?
Step 4-> have we acted on each of the previous steps?
4.2 Security in Continuous Integration

As the core design and development is implemented in the Continuous Integration, there is a huge need for security measures to be built. The following are the CI practices to build security:

Security is heavily built in the Continuous Integration as the core design and development is implemented. The following are the CI practices to build security:

**Security IDE plug-ins:** Security is highly managed using Integrated Development Environment (IDE) plugins which help developers check for security flaws dynamically while they write their code. These plug-ins provide direct feedback while code is written. Some popular plug-ins are Eclipse, VSCode and IntelliJ.

**Code reviews:** A secure code review identify security threats, vulnerabilities and weaknesses that might go undetected if not reviewed. Code review can be manual and/or automated review of an application's source code done by the developers to identify security-related weaknesses (flaws) in the code component.

**Pair work:** Security subject matter experts are paired temporarily with developers providing real-time feedback directly during design or coding. Pair work also enhances the skill level of the development team on the security practices.

**Static code analysis:** It is called SAST or Static Application Security Testing, also known as, “white box testing”. The source code and code components are analyzed using SAST tools to identify sources of vulnerabilities. The Static analysis tools can detect 50% of existing security vulnerabilities based on the analysis report and is an important element of DevSecOps. Veracode, Synopsys, Checkmarx, and MicroFocus are the leaders in “The Forrester Wave Static Application Security Testing report” published in Q1 2021.

**Third party scans:** This is similar to static code analysis for third part code or code component, which must be scanned to identify vulnerabilities.

**Fuzz testing** is an automated quality assurance technique where you provide invalid, unexpected, or random data in an attempt to make it crash.

**Code signing:** It is a digital signature added to the application to validate that the code is not tampered enhancing the user confidence and trust.
Infrastructure scans are performed to assess the security level of your infrastructure, which includes application servers, databases, ports, as well as outdated components. Infrastructure-as-Code (IaC) scans are also performed on the infrastructure. Terraform, Ansible, AWS CloudFormation, Puppet and Chef are prominent IaC tools.

Malware scans should be used for SaaS infrastructure and before packaging any component.

Dynamic scans: It is called as DAST or Dynamic Application Security Testing, also known as “black box” testing, can find security vulnerabilities in a running application. Unlike SAST, DAST do not have access to the source code. Threats missed by Static application security testing are captured by dynamic scans.

Figure 6: Security in Continuous Integration © Scaled Agile, Inc

4.3 Security in Continuous Deployment

Pen Testing or Penetration Testing is a key security practice in Continuous Deployment. It is also called ethical hacking. The pen testing security experts conduct a series of simulated hacking or attack against the network using different methods. The different types of penetration tests include network services, applications, client side, wireless, social engineering, and physical. A vulnerability scan (SAST or DAST) is automated, while a penetration test is mostly a manual test similar to a product risk assessment performed by a security professional. Qualys and Netsparker is used widely for vulnerability scans.
4.4 Security in Release on Demand

Continuous security monitoring (CSM) is a threat intelligence approach that automates the monitoring of information security controls, vulnerabilities, and other potential threats. CSM empowers companies to oversee their IT assets, both in cloud and on premise. This is done by a security information and event management (SIEM) system that gives organizations with next-generation detection, analytics and response providing real-time analysis of security alerts generated by applications and network hardware. With the data collected, security team can take required actions and generate applicable security compliance and audit data. The leaders of SIEM from Gartner’s 2021 magic quadrant are Exabeam, IBM, Splunk, Securonix, Rapid7 and LogRhythm.

The security response team or CSIRT (Computer Security Incident Response Team) provides information about newly discovered vulnerabilities and feeds this information back to the development and operations teams. CSIRT respond to computer security incidents quickly and efficiently, thus regaining control and minimizing damage. Security Bulletins are used to notify customers about the vulnerabilities for quick remediation.
5 Key Best practices from Gartner and others leading experts

Organizations face more challenges when transforming to DevSecOps, and they can be addressed by employing these DevSecOps best practices. There are many practices adopted by security professionals in the DevSecOps adoption but here are just a few key best practices from Gartner and other leading experts for organizations seeking to run the DevSecOps practices smoothly:

- Automation is good
- Shift Left for efficiency
- Adopt a Security Champion
- Training developers on security
- Carry out threat modeling
- Implement Strong Version Control
- Focus on Known Open-Source Vulnerabilities
6 DevSecOps Metrics

There are many possible measures to track the success of DevSecOps implementation. The decision of which metrics to track is largely based on business need and compliance requirements. The following are key metrics for every CISO (Chief Information Security Officer) to ensure if the DevSecOps practices are effectively working in your Organization:

- Reduction in Total Security Tickets opened
- Reduced Time-to-Deploy
- Discovery of Preproduction Vulnerabilities
- Reduced Time-to-Remediate
- Percentage of Security Audits Passed
- Reducing Failed Security Tests

7 Summary

DevSecOps transforms the way organizations manage security. Integrating security into DevOps to deliver DevSecOps demands changed mindsets, processes and technologies. The most important and obvious benefit of a DevSecOps approach is that organizations can improve your overall security posture with faster delivery. Identifying vulnerabilities and bugs before deployment results in an exponential reduction in risk and operational cost enabling greater overall business success. DevSecOps also ensures meeting compliance with industry-standard regulations. When done right, DevSecOps goes well beyond “shifting security left” to “shifting security everywhere.” It ensures software is secure in development, delivery and in production thereby improving overall AppSec in entire DevSecOps pipeline.
8 References

https://www.amazon.com/Continuous-Testing-DevOps-Professionals-Practical-ebook-dp-B07H8PH7VB/dp/B07H8PH7VB/

Survey Report: DevSecOps Practices and Open Source Management in 2020 by the Synopsys Cybersecurity Research Center (CyRC) and Censusswide, August 2020
https://www.synopsys.com/software-integrity/resources/analyst-reports/devsecops-practices-open-source-management.html


Web Sites: Scaled Agile Framework, version 5.0 Continuous Delivery Pipeline
https://wwwscaledagileframework.com/

https://www.synopsys.com/software-integrity/resources/analyst-reports/forrester-wave-sast.html

Web Sites: Gartner- 12 Things to Get Right for Successful DevSecOps, Published 19 December 2019 - ID G00450792

https://www.synopsys.com/software-integrity/resources/analyst-reports/gartner-magic-quadrant-appsec.html