ACL Digital
an ALTEN group company

DEVSECOPS

Industry best practices for software application development and operations through the lens of security and privacy compliance

Phase 05 of Software Lifecycle Management

Digital Product Engineering Services

Table of contents

Introduction

DevSecOps has become a very developer friendly term in the past couple of years. This is so because, all this while, the manpower strength of developers to operations to security used to be very poorly managed in software application development teams. As security personnel were engaged only towards the end of the software development cycle, the overall project delivery timelines used to be prolonged to remediate the findings. With a large adoption of advanced technology frameworks over the past decade, software applications have transitioned from software development to software assembly, thereby increasing the dependency on third-party software frameworks and libraries.

To deal with the onslaught of multiple vulnerabilities across dependent resources and reduced engagement of security teams early in the application development lifecycle, it is imperative for all organizations to reorganize their software development processes and include security gates at every stage. As Gartner suggests[1], software developers can double up as security coaches and security advisors by possessing pi-skills (broad domain skills, secondary security coaching skill in addition to a primary deep development skill) instead of T-skills (broad domain skills and one deep primary development skill). One way of reaching scalable heights of security integration is by following the DevOps evolution model[2] as proposed by Puppet.

Key principles of DevSecOps

During the QCOn 2019, Guy Podjarny, CEO of Snyk, gave a talk on "The Three Faces of DevSecOps"[3] and for him the three essential pillars on which DevSecOps stands are stated as below:

1 Securing DevOps methodologies

Adding continuous security to the continuous integration, continuous delivery (CI/CD) pipeline is what makes DevSecOps a reliable approach to ensure secure application development, deployment and release. It mandates quick turn-around-time for which DevOps emerged scalable over agile methodologies and emphasizes the need to 'shift left' security gates into the Software Lifecycle Management (SLM) process.

2 Securing DevOps technologies

There are many tools and technologies that you can take advantage of, in order to setup the DevSecOps pipeline following 'secure by design' principles. It is not recommended to setup a completely new suite of tools and discard what already exists in your organization. However, the key here is to let your tools adapt to the changing needs of the application development lifecycle and to verify if the existing tools can comply with the increasing demands from a security standpoint.

3 Include security in DevOps shared ownership

John Allspaw and Paul Hammond from Flikr, in their seminar on "10 deploys a day"[4] concluded that IT operators could work in an agile mode very similar to that of the developers and demonstrated the same through Flikr's automated infrastructure for continuous integration and deployment.

DevSecOps evolved from DevOps as an extension and, in 2012, gained center stage when Shannon Lietz published the DevSecOps manifesto. The objective was to bring development and operations out of closed silos and merge them both into a unified cycle to infuse secure practices from the very beginning. In short, DevSecOps needs to fit into the overall culture of the organization, and they should allow it to mature over time so that it attains a more stable baseline in the future.

Secure coding, secure code-repository management, automated application security testing (AST), persisting keys, secrets and credentials in secure vaults, managing application configuration in the cloud, utilizing multi-factor authentication, setting up security groups for cloud infrastructure resources, securing buckets and datastore, performing software composition analysis (SCA) for open source software, performing cloud audit (network and credential scan), setting up web application firewall (WAF), setting up cloud workload protection (CWP), enforcing container hardening, setting up microservices security monitoring are the key junctures at which appropriate tool-chains need to be established.

Conclusion

Establishing secure practices for every-day software development is more of a mindset change than following a set of security principles, practices, and policies. Secure by default needs to be inculcated into the very DNA of your organization, and slowly over time, its maturity can be seen rising with a big dip in privacy and security-related issues. Every member of your organization should always be an avid practitioner of these security princi-ples. It is then that the actual value of 'secure by design' will be realized and put into real and active use.

Recommended Reading

Software Lifecycle Management Infographic

Phase-01: Requirement Lifecycle Management

Phase-02: Secure Architecture and Solution Design

Phase-03: Continuous Integration, Continuous Delivery (CI/CD)

Phase-04: Verification and Validation

References

- [1]Gartner Report: DevOps Security Coaches Help Organizations Gain Leverage Without Training Everyone, May 2022
- [2]https://puppet.com/resources/report/2020-state-of-devops-report
- [3]https://www.youtube.com/watch?v=eC_Y74sfFrI
- [4]https://www.youtube.com/watch?v=LdOe18KhtT4
- [5]http://www.devsecops.org/
- Gartner Market Guide for Operational Technology Security, January 2021
- Gartner Critical capabilities for application security testing, April 2022
- International Institute of Business Analysis: https://www.iiba.org/knowledgehub/business-analysis-body-of-knowledge-babok-guide
- Open Web Application Security Project® (OWASP) Top 10: https://owasp.org/Top10/A00_2021_How_to_use_the_OWASP_Top_10_as_a_standard/
- General Data Protection Regulation, Europe: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
- Privacy enhancing technologies: https://en.wikipedia.org/wiki/Privacy-enhancing_technologies
- NITS Cybersecurity Framework: https://www.nist.gov/cyberframework/online-learning/components-framework
- HITRUST CSF Framework: https://hitrustalliance.net/product-tool/hitrust-csf/
- https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest
- https://docs.microsoft.com/en-us/azure/architecture/patterns/sidecar
- Gartner Report: Predicts 2022: APIs Demand Improved Security and Management
- Gartner Report: Top Strategic Technology Trends for 2022
- OWASP Top 10: https://owasp.org/Top10/
- Gartner report: 2021-2023 Emerging Technology Roadmap for Large Enterprises
- OWASP Top 10 Low-code/no-code security risks