What is DevSecOps? A Comprehensive Guide

No comments

In software development, DevSecOps refers to the integration of security measures at every stage of the software development lifecycle in order to deliver robust and secure software. In this article, you learned about the Importance of DevSecOps, its implementation, its benefits and etc.

DevSecOps Overview

According to the DevSecOps definition, it is a strategy of engineering that eliminates silos and allows development, security, and operations teams to collaborate. Its goal is to automate the delivery of secure software and infrastructure to production. In other words, DevSecOps is an extension of DevOps that emphasizes security. As a result, security becomes a shared burden among all team members. Vulnerability assessments are often done at the end of development. Consequently, there is more back-and-forth between teams, more expensive solutions, and resource waste. DevSecOps can be integrated into your development pipeline to build a cyclical process for testing apps throughout the development phase. The result will be fewer app vulnerabilities, reduced team friction, and reduced compliance and security costs.

The Importance of DevSecOps

DevSecOps enables "shifting left" security protocols. This means identifying bugs and issues at earlier stages of the development pipeline to make it easier and less expensive to apply security fixes. The goal is a "blanket security" wherein you improve the coverage and effectiveness of security checks, increase software quality, and decrease downtime and number of vulnerabilities.It's simple. The earlier you find a bug, the faster you can address it. The more automated the process, the more time your security teams can save and focus on more critical, challenging issues. And DevSecOps combines all of this to offer you a streamlined, flexible, and secure application development lifecycle.

DevSecOps vs. DevOps

What is the difference between the old way of DevOps versus the new model of DevSecOps? First, let's focus on the similarities. Both methodologies value the concept of teamwork and recognize how this can speed up the release of important new software. They both utilize the agile framework to emphasize a work culture driven by dynamic and continuous work processes, and communication and collaboration are emphasized at all levels.

Both DevOps and DevSecOps use some degree of automation for simple tasks, freeing up time for developers to focus on more important aspects of the software. The concept of continuous processes applies to both practices, ensuring that the main objectives of development, operation, or security are met at each stage. This prevents bottlenecks in the pipeline and allows teams and technologies to work in unison.

By working together, development, operational or security experts can write new applications and software updates in a timely fashion, monitor, log, and assess the codebase and security perimeter as well as roll out new and improved codebase with a central repository. The main difference between DevOps and DevSecOps is quite clear. The latter incorporates a renewed focus on security that was previously overlooked by other methodologies and frameworks. In the past, the speed at which a new application could be created and released was emphasized, only to be stuck in a frustrating silo as cybersecurity experts reviewed the code and pointed out security vulnerabilities.

This former practice, which encouraged the creation of bottlenecks in the software development cycle, would put a lot of pressure on cybersecurity experts and developers to quickly fix glitches and bugs and glitches with the software. This often came at the price of the software's functionality and security.

How to implement DevSecOps

Here is a workflow to implement DevSecOps in your SDLC:

Training

A new approach to working means empowering your engineers with the best knowledge; providing security-specific coding training. Invest in organizing virtual events with industry leaders and seasoned DevSecOps professionals. Incentivize security certifications to make the adoption process faster and more efficient.

IDE Scanning

IDE scanning offers focused, real-time security feedback to developers as they code. Given that these tools generate results within a few seconds, developers can instantly remediate security issues faster. More sophisticated IDE scanning tools offer command-line variants as well, which means the security functionality of an application directs that command-line, even without direct support in the IDE.

Source Code Scanning

In today's fast-moving software development landscape, developers are relying on a large set of open-source integrations such as libraries, source code, components, plugins, frameworks, and more to reduce development time and release faster. It's critical to test open-source code from early on in the development phase, and this is where source code scanning comes in.Source code scanning is a code analysis framework that helps developers create secure applications and software by analyzing security bottlenecks or potential bugs quickly. It identifies a range of security issues against industry test cases for your application to detect open source code issues.

Static Code Analysis

Static code analysis or static application security testing (SAST) is the process of analyzing the source code for common security issues and vulnerabilities while it's not running. Since SAST doesn't require your application to be running, it's a highly effective method of identifying security vulnerabilities in just about every stage of the development pipeline.SAST is a white box testing process that allows the code to be tested before execution. SAST tools evaluate the code line-by-line, offer remediation advice on the discovery of issues, and also ensure that developers conform to the development standards.

Dynamic Code Analysis

Dynamic code analysis or dynamic application security testing (DAST) is a security method to identify security issues and vulnerabilities in a running application. This is often known as black-box testing.DAST takes a more holistic approach and checks the running application from outside to discover flaws or threats by attacking it. So, it doesn't require access to source code or binaries to analyze the application.

Container Security Management

Another security practice that you need to embed in your software development lifecycle is container security. It's the process of using security tools and policies to assure that all your containers are working as intended, including infrastructure, system tools, software supply chain, system libraries, and runtime against cyber security threats.Container security management helps you ensure that the environment's configuration is secure. Since containers heavily use third-party components, they need to be evaluated for any potential weaknesses or threats. Vulnerability assessment in container security management helps ensure that software teams are not deploying insecure code with known security exploits integrated into the DevOps pipeline.

Secrets Management or Vault

These tools are specifically used to securely store and manage secrets like API keys, database credentials, encryption keys, sensitive configuration settings (usernames, email addresses, debug flags, etc), and passwords. Choose a secret management tool or a vault that helps you maintain tight access control and provides comprehensive audit logs.

Benefits of DevSecOps

1- Support from multiple vendors

DevSecOps provides a framework for integrating workflows that enable a multi-vendor, multi-cloud technology environment. Even when multiple vendors support the network, DevSecOps automation provides an application-centric view of the infrastructure.

2- Recognition of vulnerabilities

The team of DevSecOps can speed up the detection and resolution of open-source concerns. Developers gain access to real-time analytics to detect vulnerabilities and compliance problems before they result in significant data loss or application harm. Regardless of waiting until the end of development to implement security, DevSecOps permits it to be integrated into the developer's workflow.

3- Assured compliance

Eventually, DevSecOps is about improving and standardizing security considerations. Compliance is considered one of the most significant factors in this area. Compliance targets assist organizations in protecting client data and support them to avoid hefty fines and public criticism.

4- Reliable security methods

Hearing about how DevSecOps increases security quicker may trigger some red flags regarding reliability. Regardless, DevSecOps' pace does not necessitate cutting corners. DevSecOps engineers can improve the reliability of critical security operations by investing in automation and reducing the chance of human error.

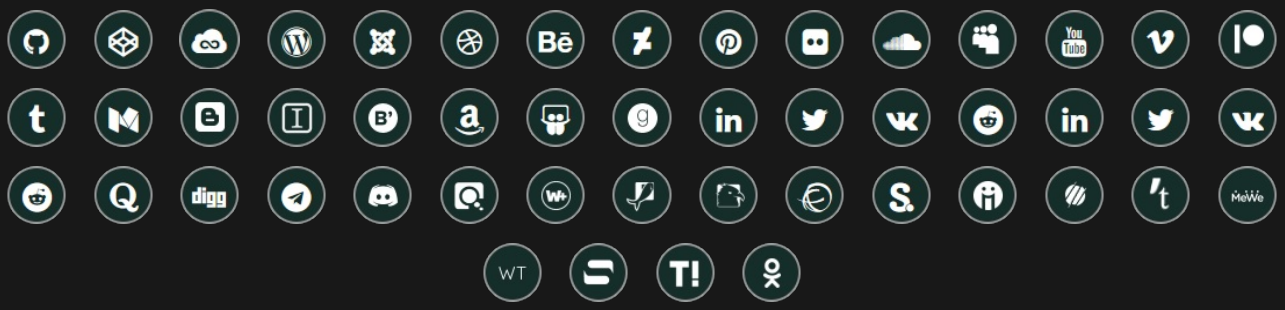
Conclusion

DevSecOps is undoubtedly changing the way businesses manage security. However, many mid-level and low-level businesses are still apprehensive about moving to DevSecOps for various reasons. Some of these issues include a lack of awareness of DevSecOps, a cultural shift that is unwelcome for employees, and sometimes ambiguity in the phrase itself. As a result of using DevSecOps, organizations can benefit both technically and financially; Although there will undoubtedly be some setbacks, DevSecOps has the potential to offer your organization long-term benefits.

Join Arashtad Community

Follow Arashtad on Social Media

We provide variety of content, products, services, tools, tutorials, etc. Each social profile according to its features and purpose can cover only one or few parts of our updates. We can not upload our videos on SoundCloud or provide our eBooks on Youtube. So, for not missing any high quality original content that we provide on various social networks, make sure you follow us on as many social networks as you're active in. You can find out Arashtad's profiles on different social media services.



Get Even Closer!

Did you know that only one universal Arashtad account makes you able to log into all Arashtad network at once? Creating an Arashtad account is free. Why not to try it? Also, we have regular updates on our newsletter and feed entries. Use all these benefitial free features to get more involved with the community and enjoy the many products, services, tools, tutorials, etc. that we provide frequently.

SIGN UP | NEWSLETTER | RSS FEED