Pros and Cons of DevSecOps

Security architects are an essential presence in every IT department. But, if any firm hasn’t embraced it so far, it’s the right time to adopt the DevSecOps culture in their workflow. **DevSecOps** is a trending software development methodology that involves DevOps and security. Similar to SecOps or DevOps, DevSecOps is a concept that combines two separate teams into a unified environment. It is responsible for providing conditions for continuous secure software development.

DevSecOps was created to emphasize the security automation and IT operations in the SDLC as a new concept in the IT field. It includes security as a part of the DevOps foundation and is involved in every phase of the **SDLC**. It emphasizes software security throughout the whole software delivery process while delivering products at a high speed than the traditional process.

DevSecOps model is a new approach for creating a software product that uses agility, CI, and CD. Unlike the traditional process of the software development model, where a security team only joins after a product is going to finish. It combines security while the software is being produced.

According to the report by the GitLab ‘2021, Global DevSecOps Survey’ found that there are dramatic advances in automation, security postures, continuous deployments, and release cadences. Nearly 4300 professionals shared their opinions that 25% of respondents were willing to have complete test automation. 60% of developers release code 2x higher performance and speed than ever.

Before delving deep into topic, let’s explore what DevSecOps is, how it works, and the pros and cons of DevSecOps.

About DevSecOps Services

The DevSecOps movement started in 1976 and continues to rise on the IT industry’s radar. The SDLC process has experienced a significant makeover in the last two decades. It mainly aims to deliver quality software in less time. This radical overhaul includes the adoption of tools, techniques, and DevOps principles. But rapid software development comes with a higher risk of developing insecure code, so it further develops the DevOps principles to include security in their process, i.e., DevSecOps.

DevOps applications have stormed head in terms of size and speed. They are lacking in compliance and strong security. For this reason, the DevSecOps concept was introduced into the SDLC in order to combine development, operations, and security under one roof. Similar to DevOps and its security is much about automation, culture, and shared responsibility. The security operation aims to release better software quickly and detect software problems in production.

The main reason for involving security in the DevOps approach is to ease security issues in the last stages of the SDLC. **DevSecOps boosts automation** and involves security in the design, test, plan, development, and monitoring. A few years back, a security team would add security to software towards the end of the development cycle, and a quality assurance team would test it.

Useful link: All You Need to Know About DevSecOps and its Implementation

DevSecOps Engineer is responsible for securing software development and identifying security threats.

Their job is similar to IT security professional roles. The top skills required for engineers are:

- Good communication skills
- Strong collaborating skills
- Good understanding of DevOps tools
- The person should be aware of threats, compliance laws, and threat modeling tools.
- IT pro should have knowledge of automated code analysis to detect threats and fix vulnerabilities.
- The IT pro should be familiar with Ansible tools, deployment systems tools such as Hibernates, and developer tools such as GitHub. He is also familiar with the programming languages like Java and PHP.

Adoption of DevSecOps

The following principles are adopted by DevSecOps engineers as follows:

- The first phase is planning, where engineers strategically prepare and aim for successful adoption.
- The next is the development phase, where the team's engineer gathers valuable resources to provide guidance and set up a code review procedure to improve uniformity.
- The next step is the building phase; the source code involves machine code through tools.
- Then in the testing phase, the automated testing framework is then subjected to multiple testing practices in the pipeline.
- In the following phase, engineers run IaC tools to increase the pace of software delivery by automating the process.
- The following phase is operation, one of the essential processes, and operation teams frequently engage in periodic maintenance.
- The scaling phase is one of the crucial steps where IT engineers make sure that companies do not have to waste their resources to preserve big data centers.

Useful link: DevSecOps – For Bankers With Futuristic Vision

How does DevSecOps work?

DevSecOps workflow follows the following steps:

- First, the version control system is used for development.
- Team member assesses the application changes. The employee does this by regarding the changes in the security faults, code quality, and potential flaws. The application is then deployed within security configurations.
- By using test automation, the application is then tested in the integration, user interface, back end, and security.
- The application moves to production if it successfully passes the test.
- Security software and multiple monitoring programs monitor the application in the production.

Pros of DevSecOps

Pros of DevSecOps

- ✓ Better communication and collaboration between teams
- ✓ Improve the agility and speed of development teams
- ✓ Improves better-quality control and threat exposure
- ✓ Enables early detection of software flaws
- ✓ Provides better and quick response to changing client requirements

It can make sure that an application will be pretty stable and less vulnerable to malicious attacks. The two most essential benefits of this concept are security and speed. In addition, there are numerous features for DevSecOps services that are beneficial to businesses of all sizes.

Better communication and collaboration between teams

This security solutions culture promotes collaboration and teamwork among **IT professionals** with multiple skills and competencies in order to accomplish one goal. One of **DevSecOps'** primary goals is to integrate teams.

Improve the agility and speed of development teams

Team members are under pressure to respond quickly, review, fix vulnerabilities, and other software issues while in the ongoing development process.

Improves better-quality control and threat exposure

Although the security team may be seen as a source of delay by the **DevOps team**, this shouldn’t be the case. Issues are detected and finished immediately before the entire project is completed. This strategy ultimately leads to better quality control procedures and shorter time projects.

Useful link: DevSecOps – A DevOps Savior to ‘Cybersecurity’ Challenge!

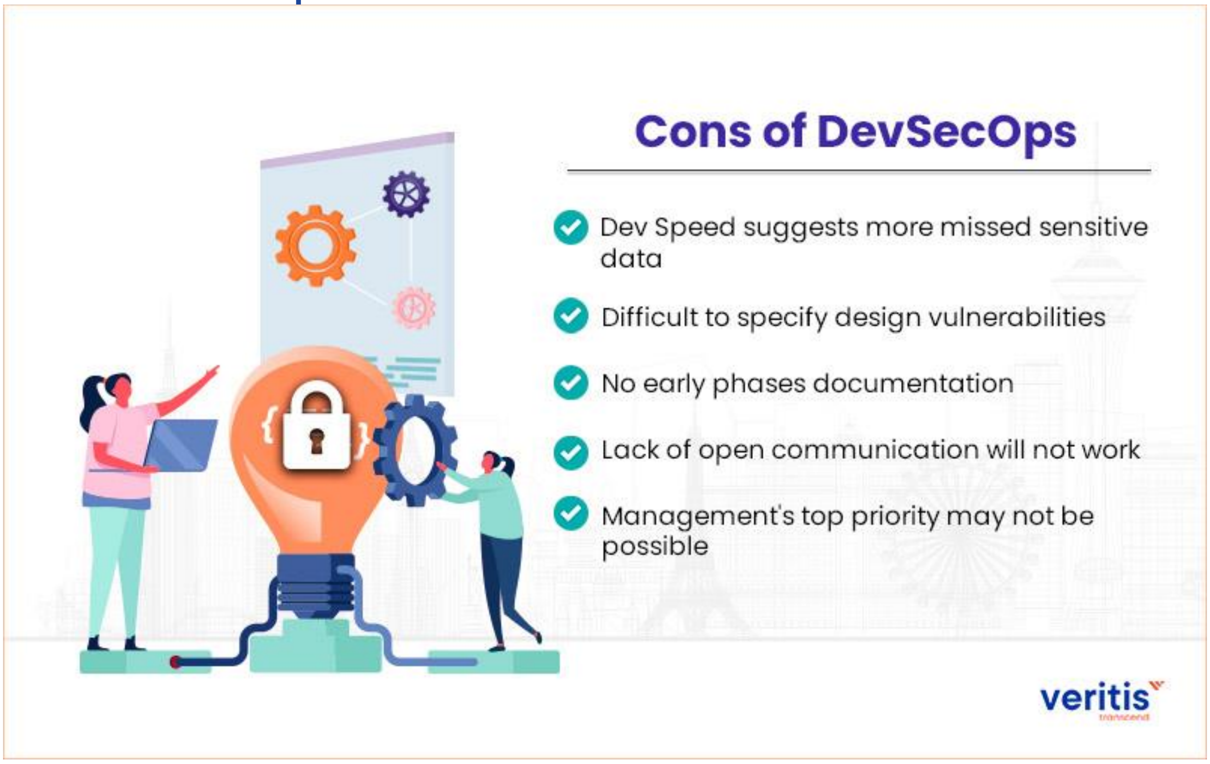
Enables early detection of software flaws

One of the main tasks of the security team is to manage and reduce the risks effectively. It can only improve by including the security team in the DevOps process. Doing this can combine the speed, and reliability of a product in an efficient way.

Provides better and quick response to changing client requirements

Due to the fact that DevSecOps can work faster in reviewing projects, scan vulnerabilities, and integrating changes and applications during the development stage.

Cons of DevSecOps



Cons of DevSecOps

- ✓ Dev Speed suggests more missed sensitive data
- ✓ Difficult to specify design vulnerabilities
- ✓ No early phases documentation
- ✓ Lack of open communication will not work
- ✓ Management's top priority may not be possible

DevSecOps can’t solve all issues related to business. Every organization must evaluate its requirements and needs.

The below mentioned are some of the disadvantages of DevSecOps:

Dev Speed suggests more missed sensitive data

DevSecOps approach has sped the development of the application at the starting stage. However, this speed comes at the price of missing vulnerabilities.

Difficult to specify design vulnerabilities

This model depends on the agile system. It uses multiple techniques to produce the first application as soon as possible. This comes from the fact that it is based on the client feedback to improve the application. So, it becomes hard and time consuming to find design-based exposures.

No early phases documentation

The absence of documentation in the beginning phase of the application development makes identifying exposures, particularly the business logic ones, more complex as the **security experts** will require more time to understand the application logic.

Useful link: Signs of a Failed DevSecOps Strategy Which None Should Ignore

Lack of open communication will not work

Communication and collaboration are the two essential steps from the IT department; software development and security must develop to work. However, if any of these teams withhold crucial information from each other, it may not work correctly.

Management’s top priority may not be possible

Not every executive in a software company views security as a top priority. As a result, an organization executive may not accept with the changes tracked by a manager. As a result, the business may only resume security testing once the software development processes are deemed complete.

Conclusion

DevSecOps is a new model that involves security in the starting stages of software development. It can make sure full functionality, reduce cyber threats, and fast deployment of the software product. Implementing security at every stage of the SDLC allows software products to deliver quickly. This **security solutions** can implement in automotive, healthcare, finance, and retail industries.

It is a management model that involves security, operations, application development, and IaaS in a continuous delivery cycle. DevSecOps’s goal is to apply security at all stages of the SDLC. Using security at each stage of the SDLC allows for continuous integration, reduced cost compliance, and quickly delivering software products. Its main objective is to make everyone responsible for security.

Veritis, the Stevie Award winner, has been a trusted partner from small to large companies, including Fortune 500, for over a decade. We have enough expertise in delivering solutions for IT projects and combining emerging technologies in a dynamic environment. **Veritis** offers multiple technology services for your business with a cost-effective solution. So, get in touch with us to embrace productivity with the best DevSecOps tools.

Services