It is official, cybercrime has become the world's third-biggest economy. What is more, the con artists' activity shows no signs of slowing down as more and more sophisticated attacks are being conducted. Keeping up with cybercrimes and implementing appropriate cybersecurity from the start of the software development process is now more important than ever. That is why today's article answers the question of how to ensure the security of the software using DevSecOps.

What is DevOps?

Let me start with a brief answer to the question: what is DevOps. DevOps is a combination of two words: development and operations. What does DevOps mean? It is simply an array of tools, philosophies, or practices that ensure the delivery of the product on time. This is achieved by combining the work of development and operations teams. Those teams are frequently merged into one, resulting in even faster development and implementation of the software.

What does DevOps do?

In short, DevOps helps to build software faster. What are the biggest advantages? Increased efficiency and speed are indeed among the most frequently listed features. However, security is also something we must mention. Hence, DevSecOps is often distinguished. The whole package of fast, efficient, and secure development and delivery serves as the main principle of DevSecOps. It gives a competitive advantage to businesses and their clients compared to traditional development.

DevOps vs DevSecOps – what is the difference?

There is no clear distinction between what is DevOps and what is DevSecOps. Some say that the key is the greater stress placed on the security feature in the latter. Others claim that security should be a self-explanatory and ever-present feature that need not be mentioned in the acronym. Who is right? To my understanding, placing security in the middle of processes should be natural and go without saying. However, if some need to be reminded of its importance, or the client needs to be ensured about the security features involved, there is no harm in using the terms interchangeably. The most crucial part is not the detail, like the name. The team's understanding of the security and compliance importance from the very beginning is what DecSecOps focuses on. This ensures the protection of software integrity.

What is more, DevSecOps ensures a smooth and seamless integration. It allows for sufficient control and visibility of the organization, which can conduct insightful and complex security processes with ease at every step.

It is worth mentioning that many environments can benefit from DevSecOps implementation. No matter if it is on-premises, cloud-native, or hybrid, the use of DevSecOps ensures maximum control over the entire software development lifecycle.

8 areas of DevSecOps improved security

What does DevOps mean? DevOps improves the development lifecycle. It means that it is implemented within crucial areas of software development but also at every lifecycle stage. These stages are:

Planning

Before work starts, it is crucial to discuss and organize it. The planning stage involves such steps as recognizing the work that needs completion, organizing it with the use of prioritization, and securely planning tracking and completion from start to finish.

Creation

The development team writes, designs, and develops through the secure management of the code and all data involved.

Verification

Testing the code and verifying its correctness is an essential part of software development. After all, if it is faulty, the whole project ceases to function. Quality checks and automated testing are also important in ensuring the security of the software.

Packaging

To package means to build containers and artifacts and securely manage them.

Security

Testing of software focuses heavily on security. Checking for vulnerabilities is conducted through dynamic and static tests as well as dependency scanning and fuzz testing.

Deployment (Release)

Releasing the software to the users.

Monitoring

The monitoring phase consists of tracking the performance of the released software and reducing the number of incidents as well as their severity.

Governing (Configuration)

This phase consists of managing the flaws and errors in security, policies, and compliance across the software.

Why do we use DevSecOps?

There are several benefits of implementing DevSecOps within the created software. These advantages can be divided depending on the three main areas: Development, Security, and Operations.

Benefits for Developers

- one application- using such tools as GitLab keeps all DevSecOps functionalities in one place
- boost in productivity – a single application improves cycle time and prevents context switching
- automation in crucial areas – rich-in-features automated tools help remove unnecessary work.

Security Advantages

- built-in security- buzz testing, API screening, DAST, and more are integrated into the software, not added on

- adequate compliance – precise separation of duties between teams is no longer a problem thanks to DevSecOps; vast customization solutions are available including, tailored approval rules, which significantly reduce risks
- automation – automatic scanning of code for vulnerabilities ensures speedy development and accurate testing results.

Operational Advantages

- scaling- DevSecOps helps to scale businesses with almost no downtime
- metrics visibility – all data regarding software development lifecycle stored in one place (no need for extra integrations!)
- no provider ties- the GitLab tool we use is not restricted to one cloud vendor so there is no cloud lock-in.

Automated security checks and seamless deployment of your software with Sailing Byte

Any reputable software house knows that security is the key to all software creation. Sailing Byte not only implements security but we also make sure to use the most cutting-edge tools and solutions. All that to ensure two features crucial for us (and our clients): ease and time-saving. Thanks to GitLab we can not only ensure the highest standard of security but also its automation, which allows us to devote more time to creating top-notch pieces of software. Improved efficiency, security, and reduced coding time? A heaven to all modern developers and their Clients! Add scalability and compliance to the mix and you can make substantial savings and generate profits for your enterprise. After all, one wise man once said, time is money. We take it to heart and save it as much as we can. Put your trust in us and we will deliver a secure and flawless product in the shortest time possible. Book a call today to discuss your idea and speed up the process even more.