DevSecOps

Redefine Security, Redefine Speed:
Accelerate with Confidence through DevSecOps Mastery.

Why DevSecOps ?

Executive Summary 2023

source: GitLab

Organizations say they are incorporating security earlier in the software development lifecycle — and we're seeing real results in terms of the number of vulnerabilities discovered by developers and the use of new technologies such as artificial intelligence and machine learning for security testing and code checks. However, friction remains in the form of unclear responsibilities and expanding toolchains.

DevOps and DevSecOps are taking over

56% of respondents reported using DevOps or DevSecOps methodologies, up from 47% in 2022.

The shift left is getting real

74% of security professionals said they have either shifted left or plan to in the next three years.

71% of security professionals said at least a quarter of all security vulnerabilities are being spotted by developers, up from 53% in 2022.

Driving efficiencies with AI

65% of developers said they are using artificial intelligence and machine learning in testing efforts or will be in the next three years.

Too many security tools

57% of security respondents said they use six or more tools, compared to 48% of developers and 50% of operations professionals.

Better security was one of the top benefits of a DevSecOps platform, according to respondents, along with a more **efficient DevOps practice**, **easier automation**, **cost and time savings**, and **better collaboration**. We define a DevSecOps platform as a single application with one user interface, a unified data store, and security embedded within the DevOps lifecycle.

Challenges Faced By Organizations

Complexity in cloud environments

As stated in the 2021 Flexera State of the Cloud Report, a staggering **92%** of enterprises are employing multiple public clouds. These multi-cloud setups commonly incorporate diverse arrays of cloud services and extensively employ automation. However, these practices also introduce challenges for maintaining robust security measures. Ensuring uninterrupted infrastructure security, compliance adherence, and safeguarding data integrity all emerge as significant hurdles in this context.

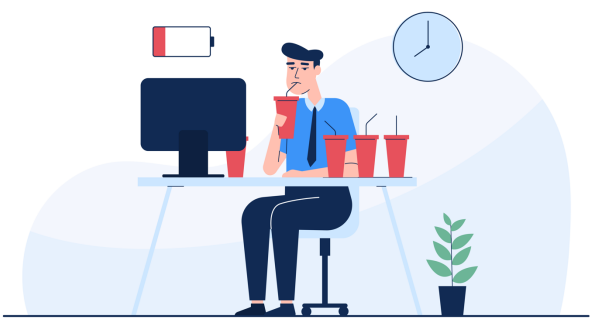
Spotting and rectifying vulnerabilities

According to findings presented in a Security Boulevard report, organizations that haven't embraced DevSecOps practices have a concerning **50%** of their applications consistently exposed to potential attacks. This stands in contrast to the 22% vulnerability rate observed in organizations that have embraced a well-established DevSecOps approach. In cases where security testing traditionally occurs toward the conclusion of the development lifecycle, developers often find themselves making critical code fixes or rewrites during the latter stages, leading to substantial expenses and project slowdowns.

Scarcity of resources and a knowledge gap

According to the stats, **70%** of organizations lack sufficient operational expertise of DevSecOps practices. Bridging the knowledge gap is another difficulty with limited employees, resources, and budget constraints. One of the most typical DevSecOps difficulties is a developer's lack of security and compliance competence. Security and operations personnel, likewise, are unfamiliar with both infrastructure and software development environments. The knowledge gap and the lack of a single platform for knowledge sharing are impediments to successful DevSecOps implementation.

As outlined by Gartner, "*71% of CISOs say their DevOps stakeholders still view security as an impediment to speed-to-market.*" A prevailing misconception within Dev and DevOps circles is that security measures introduce deceleration. Security evaluations are often perceived as a constraint to progress.



Why Choose Us?

Choosing our company for your DevSecOps requirements means adopting a partner who is entirely committed to providing excellent value. Our track record speaks for itself: we stand out from others thanks to our unique approach and extensive offerings.

Holistic Approach

We recognize that DevSecOps is about more than just combining development, security, and operations practices; it is also about cultivating a collaborative culture. Our methodology covers the entire spectrum, from process optimization to mindset adaptation, ensuring that all aspects are in sync for success.

Proven Expertise

Our team consists of seasoned individuals with extensive experience in development, security, and operations. This cross-functional understanding enables us to effortlessly bridge gaps, reduce risks, and drive efficiency throughout your pipeline.

Tailored Solutions

We don't believe in one-size-fits-all solutions because we recognize that every organization is unique. We work together with you to understand your specific challenges and objectives before developing customized DevSecOps strategies that properly correspond with your objectives.

Continuous Learning

Staying ahead in the continually changing field of technology and security is critical. We are dedicated to continuous learning and progress, ensuring that our actions are always in line with the most recent best practices and industry trends.

Advanced Tooling

We improve the efficiency and accuracy of your DevSecOps practices by leveraging cutting-edge tools and technology. Our toolkit has been carefully designed to equip your team with the ability to solve challenges with precision and speed.

Collaborative Partnerships

Beyond just a client-vendor relationship, we strive to build enduring partnerships. We foster open communication, sharing insights and knowledge that empower your team to become proficient in DevSecOps practices over time.

Don't Hesitate, Innovate!

Take Your DevSecOps to New Heights

Contact Us