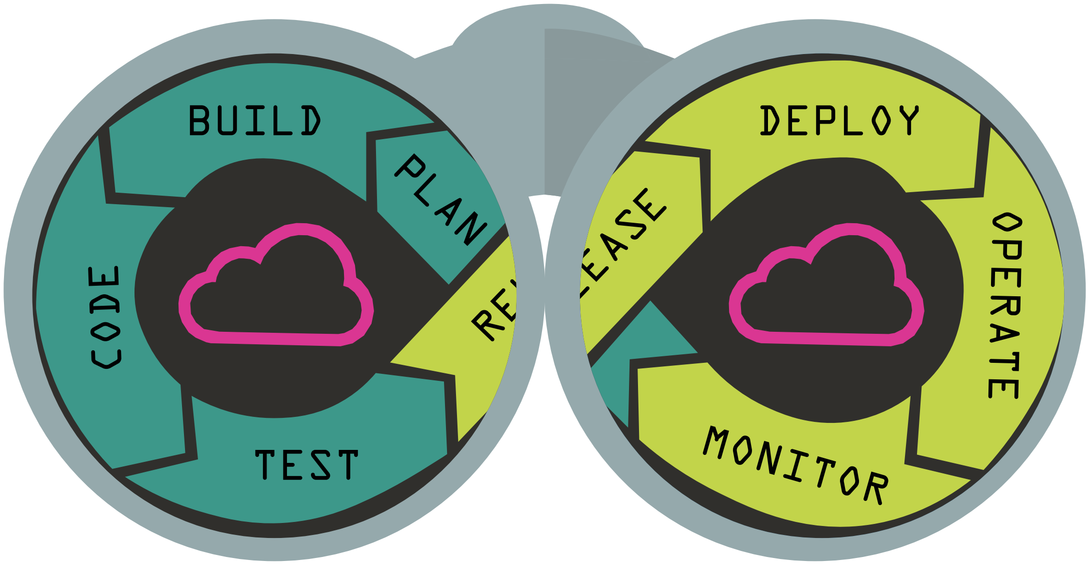
kiuwan

Improving The DevSecOps Process



IMPROVING THE DEVSECOPS PROCESS

The increasing pace at which new software is released nowadays has traditional application security (AppSec) teams struggling to ensure all products meet the necessary security standards while still keeping up with their launching schedule. Consequently, there's a growing need to continuously implement security across the SLDC (Secure Development Life Cycle). Doing so allows teams to identify security weaknesses and vulnerabilities earlier in the pipeline and optimize efficiency when delivering more secure, high-quality applications.

DevSecOps (development, security, and operations) is a relatively new term regarding culture, automation, and platform design in the AppSec space. It spans the entire SDLC, incorporating security testing from the planning and design phases to the software release stage. The primary goal of DevSecOps is to deliver better software faster. Through this approach, businesses can seamlessly incorporate security into their CI/CD (continuous integration and continuous delivery) systems, allowing for increased efficacy throughout the whole SDLC.

The DevSecOps model integrates security as a shared responsibility among development and operations teams, promoting closer collaboration between the core functional teams involved in all stages of SDLC. It adopts **the "shift-left" philosophy**, which encourages finding and preventing defects early in the software development process, enabling organizations to fix security flaws in their code in real-time rather than waiting until the last minute.

According to **the Gartner Hype Cycle for Agile and DevOps**, DevSecOps is becoming a mainstream practice. As of 2020, it had a 20-50% market penetration among its target audience. However, it's estimated that only 15% of solution adopters consider their implementation of DevSecOps mature enough. It is vital to understand how to incorporate this process optimization approach in the AppSec space in order to make the most out of it. Here's a more in-depth look into DevSecOps and the best practices to improve its implementation in business.

DISSECTING THE TRIFECTA: DEVSECOPS EXPLAINED

In practice, DevSecOps combines the three disciplines involved in the SDLC to integrate security throughout the CI/DC pipeline. This process optimization measure observes both the pre-production and the production environments. This is a closer look at each discipline's roles in the fast delivery of better, safer software.

DEVELOPMENT

The developers' team is responsible for creating new software applications and iterating on them. Their job is generating custom apps designed for a specific purpose, building API-driven connections between legacy systems and new products, and leveraging open-source code to expedite the whole programming and coding process.

Traditional development practices tend to prioritize sequential steps (**waterfall approach**), while in DevSecOps, the goal is implementing **agile models.** Working along with the operation and security teams from the beginning of the process helps prevent operational issues and security vulnerabilities in the later stages of the pipeline.

OPERATIONS

The operations team is in charge of managing software functionality. They monitor system performance, repair defects, and take care of testing after any updates and changes have been implemented. This allows them to polish the release system of new software.

Isolating the operations and development stages creates a complex road map rather than enhancing the workflow, as it requires a constant back and forth between both teams whenever issues are found. Most organizations are now fully aware that these two processes must coexist to increase production efficiency and identify and address potential problems in a timely manner. Implementing both development and operations in parallel reduces deployment time and streamlines the workflow.

SECURITY

The security team creates tools and techniques that help design less vulnerable software that resists cyber attacks. Their job is to detect and respond to intrusions and handle security breaches. Traditionally, application security has been left to the last stages of the SDLC, initiated only when development is completed. However, this approach is less than helpful when attempting to expedite software development, testing, and release. By unifying all three teams in the DevSecOps process, organizations have a better chance of accelerating the workflow.

KEY COMPONENTS IN DEVSECOPS

Adopting the DevSecOps approach aligns three different areas into one seamless unit that can focus on several key components while instituting a "shift-left" mentality. The essential elements that fuel this methodology are:

- **Security training** — Ensuring all personnel know the guidelines and how to implement them
- **Compliance monitoring** — Guaranteeing all parts of the trifecta are mindful of compliance at all times
- **Code analysis** — Securing the early detection of vulnerabilities by developing and reviewing code in small batches
- **Automation** — Using automatic security protocols to maintain prompt code delivery in a CI/CD environment

BENEFITS OF DEVSECOPS

DevSecOps provides numerous advantages, but the two most important ones are perhaps speed and security. When software is produced in a traditional environment, it's more likely to present security issues resulting in significant delays. This can become time-consuming and costly since fixing security flaws in the code takes additional work. When all teams involved work together, the delivery is faster and, therefore, more cost-effective. The need to repeat tasks is reduced and security issues are addressed in real-time.

Introducing cybersecurity measures from the beginning of the development phases allows for the code to be scanned and tested for vulnerabilities and issues. The unit is able to resolve problems sooner rather than later. Having all teams working together enhances a company's ability to respond in a timely and organized fashion when incidents occur.

DevSecOps allows for most cybersecurity testing tasks to be integrated into an automated system. It is a repeatable process that adapts to ever-changing industry needs and evolves along with software organizations. This approach warrants security is applied consistently throughout all departments and provides a robust infrastructure for the AppSec environment.

CHALLENGES IN IMPLEMENTING DEVSECOPS

Implementing DevSecOps may incur some difficulties. It entails a shift in culture and a learning curve. Businesses might need to retrain their DevOps team members to ensure they fully understand security best practices. Otherwise, they won't know how to use the new security tools and will have a harder time adopting the "shift-left" mindset. It's imperative to onboard all parties involved. After all, they're as responsible for the security of the apps they're building as they are for other technical aspects.

Finding **the right tools** to implement security in all stages of the SDLC might be another challenge for some companies to overcome. Automation is essential to expedite the onboarding process and cut down the learning curve. The more integrated the security tools are with an organization's CI/CD pipeline, the less culture-shifting and training will be required.

As an industry leader, Kiuwan is designed to guard development operations at every stage of the pipeline. We offer tools that maximize the advantages of static application security testing (SAST) and source code analysis (SCA). Our resources help organizations across all industries identify vulnerabilities and provide efficient code-enhancing solutions.

ESSENTIAL APPLICATION SECURITY TOOLS IN DEVSECOPS

When implementing a DevSecOps approach, organizations need to assess numerous AST tools before incorporating them into their CI/CD pipeline. Some of the most common and efficient are:

STATIC APPLICATION SECURITY TESTING (SAST)

These tools are made to scan proprietary or custom code for design flaws and other errors that could mean exploitable weaknesses. They're mainly used throughout the coding, building, and development stages.

Unlike other application security alternatives, Kiuwan offers **SAST tools** for a vast array of coding languages. This allows developers to easily check for vulnerabilities in their code for multiple projects at a time. We constantly add new languages and frameworks, expanding benefit to our customers.

SOFTWARE COMPOSITION ANALYSIS (SCA)

These alternatives scan source code and binaries, allowing developers to identify weaknesses in open-source and third-party components. They give organizations a better understanding of security and license risks, thereby expediting any correction efforts. SCA tools can be integrated into a CI/CD pipeline to detect vulnerabilities from the building stage.

Kiuwan's Insights, our **SCA tool**, helps manage open-source risks and reduce third-party component hazards. It allows for on-demand scans and minimizes dependency, security, and license compatibility issues that are common in open-source solutions. Insights eliminates error-prone complications that can be time-consuming, thus ensuring frictionless use to facilitate all security assessment efforts.

A FIVE-STEP GUIDE TO IMPROVING DEVSECOPS IN BUSINESS

Implementing a DevSecOps approach in business is an excellent way to accelerate the software production pipeline and reduce costs. It also promotes a teamwork mindset in which all parties involved work for a common goal rather than on isolated tasks and processes. When all three teams work as a unit, an organization is more likely to reach its release deadlines and deliver better, more secure apps to its customers.

However, a shift in mindset and culture is not always easy, especially when a company has been working with the same procedures for a long period. Here are some pointers to help ease the execution process or improve DevSecOps for those businesses that have already jumped on the bandwagon.

1 LEARNING HOW TO FOSTER A DEVSECOPS CULTURE

2 UNDERSTANDING HOW TEAMS CAN BUILD IN SECURITY

3 KNOWING WHERE TO ADD SECURITY INTO THE SDLC

4 EMBRACING THE ROLE OF AUTOMATION

5 ACKNOWLEDGING THE THREAT OF VULNERABILITIES

STEP 1

LEARNING HOW TO FOSTER A DEVSECOPS CULTURE

As already mentioned, modern development best practices encourage organizations to connect their three core units: the development team, the operations team, and the security team. This is done primarily to enhance security protocols throughout the entire pipeline while building and releasing code much faster. The "shift-left" strategy promotes frequent communication, collaboration, and engagement to empower the deployment system.

To ease all teams into the adoption of DevSecOps, a shift of culture is essential. DevSecOps is now standard across the industry, and it's meant to replace outdated methodologies and implement more reliable techniques. However, change is never easy, and regardless of how effective a new business approach may be, it takes time for everyone involved to warm up to it. How can organizations achieve this?

Resistance is natural when introducing new tactics. Team members may worry they won't be able to adapt or that their jobs are in danger if they don't keep up. On the other hand, managers may think the new methodology won't work or take an "if it's not broken, don't try to fix it" position. The goal is to increase communication and cohesive work between teams, and it's important to assure all parties involved that DevSecOps will make life easier for everyone and significantly improve operations.

Continuous integration and deployment will dramatically increase the amount of time and effort saved within a company. Although the benefits may seem obvious, getting all stakeholders on board can make the entire difference between staying behind the curve or keeping up with the times. Fostering open collaboration and cultivating shared responsibilities is the way to go. It will help all members of the organization feel more empowered and embrace change much faster.

Incorporating Kiuwan's tools to obtain objective data on the cost, effort, activity, quality maintainability, efficiency, and dependencies of an organization's applications will empower all teams involved. By supporting company growth and customer success, Kiuwan's solutions can give developers the confidence they need to adopt a DevSecOps approach with fewer objections.

STEP 2

UNDERSTANDING HOW TEAMS CAN BUILD IN SECURITY

Having an efficient methodology to ensure security in the SDLC is the cornerstone of DevSecOps. Following these steps will allow for a better implementation of security throughout the pipeline:

SECURE LOCAL DEVELOPMENT

Establishing a secure working environment should always come first. Programmers typically work with open-source technologies when building an app, which is of exceptional value at the early stages of software development. However, they must always ensure that the tools they're using are updated and patch to minimize the risk of vulnerabilities in the code.

SECURITY ANALYSIS

Having multiple people working on the same code, especially when done remotely, is a primary cause of software vulnerability. Performing security analysis and improving collaboration between developers and other team members is a must. Instituting automated tools for **cloud application security** within code dependencies will detect human error and reduce risks significantly.

THREAT MODELING

All members of the organization must ensure security standards during the entire pipeline. Following best practices, developers should use HTTPS protocol that's appropriately secured and equipped for attack mitigation. At the same time, project managers and data engineers are in charge of threat modeling, which intends to detect and manage risks before any harm is done.

DEPLOYMENT SECURITY

Encrypting the code is highly recommended to boost security protocols during the deployment and promotion stages. Encryption will keep all components under the radar to avoid information leakage that could compromise the software.

SECURITY TESTING

Reaching the production stage is not an indicator that the software is fully secure. The DevSecOps unit must stay on top of the situation by continuously testing for any vulnerabilities that could still come up.

Kiuwan's tools are built to be seamlessly integrated into your DevOps environment every step of the way. Our platform supports a wide range of build systems and helps quickly organize source code and manage dependencies. It works with the most common third-party repositories to manage commits, enabling organizations to position their code scanning where it makes the most sense within the software supply chain.

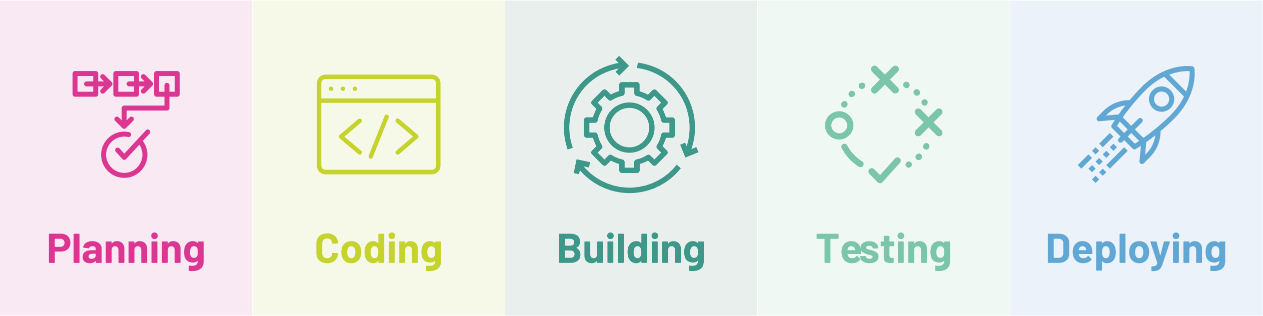
STEP 3

KNOWING WHERE TO ADD SECURITY INTO THE SDLC

Security comprises a blend of compliance and engineering. A company's development, operations, and compliance teams should work together to enforce its security posture and make sure all members of the organization understand it.

Every party involved in the SDLC should acknowledge the organization's security standards and the basic principles of AppSec. Becoming familiar with **the Open Web Application Security Project (OSWAP) top 10** is also a must in AppSec testing. At the same time, developers are responsible for mastering thread models, compliance checks, risk assessment, and security control implementation.

A typical DevSecOps process includes numerous stages in which each piece of work is completed and undergoes security checks. These phases are:



Planning | Coding | Building | Testing | Deploying

Although security is a shared responsibility in DevSecOps, each part of the unit must have different methods to perform tests. For example, the DevSecOps unit outlines a strategy to determine when, how, and where security testing will be performed during the planning stage. Next, in the coding phase, Git controls and linting tools are used to secure all passwords and API keys.

Applying Kiuwan's SAST solutions during the building stage enables businesses to check for flaws before production begins and until the deploying stage. Our tools are up to OWASP standards and are easy to implement at all phases of SDLC.

STEP 4

EMBRACING THE ROLE OF AUTOMATION WITHIN THE PROCESS

The best AppSec tools run with a high automation level to align with most CI/CD resources. This helps organizations skip custom scripts and other tasks that involve manual steps. Automation is crucial to improve the DevSecOps pipeline so that team members can focus on addressing form and function issues. It's useful to:

- **Detect system vulnerabilities**
- **Automatically build and update the development environment**
- **It Help transition into a continuous deployment system**
- **Manage updates**

Automated testing helps keep all components in the DevSecOps model in synergy. It combines and generates new strengths within the organization and allows for faster delivery throughout the pipeline. This approach offers an optimized platform that enables the team to find errors opportunely and handle cyber attacks.

Moreover, automation provides a more competent strategy to safeguard crucial applications for the company. **A recent study** found that businesses with automated governance and change management processes are thrice more likely to beat their competitors in DevSecOps implementation. Automation helps break barriers in DevOps and makes organizations more confident that their solutions are operating like clockwork.

Employing rules based on AppSec best practices before allowing production is much easier when using automated change management across the pipeline. It instills governance by reaping the benefits of collecting relevant data from the pipeline and implementing it during code scanning tasks.

Kiuwan allows organizations to feel confident that their code and brand are secure against the most common types of cyber attacks. Our approach to AppSec automation enables businesses across all industries to leverage the benefits of DevSecOps.

STEP 5

ACKNOWLEDGING THE THREAT OF VULNERABILITIES IN THE SOFTWARE DEVELOPMENT PROCESS

As previously stated, just because an app is ready for release doesn't mean it's safe from flaws and vulnerabilities that could keep a door open for cyber attacks. That's why there should be continuous testing at all stages of the pipeline. Acknowledging the possibility of threat vulnerabilities helps organizations stay alert and solve issues a lot faster.

According to recent research, there have been a plethora of DDOS and ransomware attacks in the past 12 months. Code vulnerabilities caused by a weak development process help further propagate these threats. It's estimated that roughly **83% of industry leaders in the financial sector** think they're increasingly prioritizing security within their businesses.

Industry data gathered by Kiuwan reveals that **up to 75%** of banking and finance developers have a hard time detecting vulnerabilities across a vast array of development environments. Yet 57% of enterprise-level organizations leveraging software development are implementing software supply chains into their cybersecurity plan. Our platform enables DevOps teams to easily identify flaws in their software so that they can quickly fix them and continuously scan code for security analysis.

About **94% of web apps** contain bugs in some of their essential security features. At the same time, API abuse and code quality problems have multiplied over the past few years. All these factors are solid evidence that there's an increasing need for software development units to make a bigger effort at securing the DevOps process.

THE BOTTOM LINE

Security is an essential part of the DevOps process. Connecting the three core elements of DevSecOps is a robust approach to software development that helps organizations promote teamwork and shared responsibilities while expediting the workflow and increasing application security.

It's common practice to perform a threat modeling and risk assessment before materializing a DevSecOps shift. Doing so may give a business a clearer idea of potential and current threats to their assets, the existing control strategies to protect them, and whether any gaps need to be addressed.

Managing cybersecurity doesn't have to be a headache. Up to **40% of organizations** remain without a framework for evaluating cybersecurity threats and visualizing vulnerabilities. Don't be a part of the statistic. Contact Kiuwan today and have a look at the **security solutions** we have available for you.

REQUEST A TRIAL AT **KIUWAN.COM/REQUEST-A-TRIAL**
LEARN MORE AT **KIUWAN.COM**

GET IN TOUCH

Headquarters
2950 N Loop Freeway W, Ste 700
Houston, TX 77092, USA

United States: **+1 732 895 9870**
Asia-Paciifc, Europe, Middle-East and Africa: **+ 44 1628 684407**

contact@kiuwan.com
Partnerships: **partners@kiuwan.com**