CONTEGIX®

How DevSecOps Solves the Top 4 Software Security Challenges

ATLASSIAN

Platinum
Solution Partner
ENTERPRISE

contegix.com   877.289.0395   sales@contegix.com

Table of Contents

Increasingly disruptive cyberattacks have put confidential data at risk, often with record breaking associated costs. To help customers maintain trust in organizations and their applications, development teams have had to uplevel approaches to software security. Although the majority of organizations have identified improving security as a top priority this year, developers still struggle to properly address application security while maintaining desired productivity levels. This eBook will share how IT teams can use DevSecOps to solve the most pressing security challenges, by implementing security policies and following specific approaches during coding, testing, monitoring and controlling phases of the DevOps lifecycle.

Writing Security As Code to Eliminate Sloppy Coding Practices

Modern developers juggle competing projects and long to-do lists that are only compounded by an existing talent shortage: By 2026 the shortage of software engineers in the U.S. will exceed 1.2 million, meaning more developers will have to carry a larger workload in order for organizations to respond to changing customer demands and business priorities.

Strapped teams can lead developers to resort to sloppy coding habits, such as using copied code without checking for vulnerabilities, sourcing code from outdated libraries that haven't been monitored by trusted developers or hastily writing error messages that go undetected—providing information about how the code works to potential hackers. Each of these insecure coding practices gives hackers an entry point and information needed to perform a security attack, such as a data breach. Last year, over 25 billion records were leaked or stolen in data breaches, and by October 2021, there were 1,291 recorded breaches (a 17% increase from 2020).

THE EVOLUTION OF DEVSECOPS

Now that organizations have adopted DevOps to bring together developers and IT teams for faster, more efficient software releases, DevSecOps has emerged as the next progression in software development to ensure releases are both fast and secure. DevSecOps is a security-first approach to agile software dev that ensures security is addressed throughout the entire software development process, instead of only at the end during testing.

DevSecOps adds three basic tenets to well-established agile and DevOps principles:

- **Security-first mindset**: Using development tools, processes and strategies that identify—and address—risks as early as possible in the development process
- **Keeping data safe**: Ensuring that data is secure, while also minimizing inconvenience for users to access data
- **Security as a shared responsibility**: Positioning developers to recognize and escalate security threats as identified during coding and automated testing

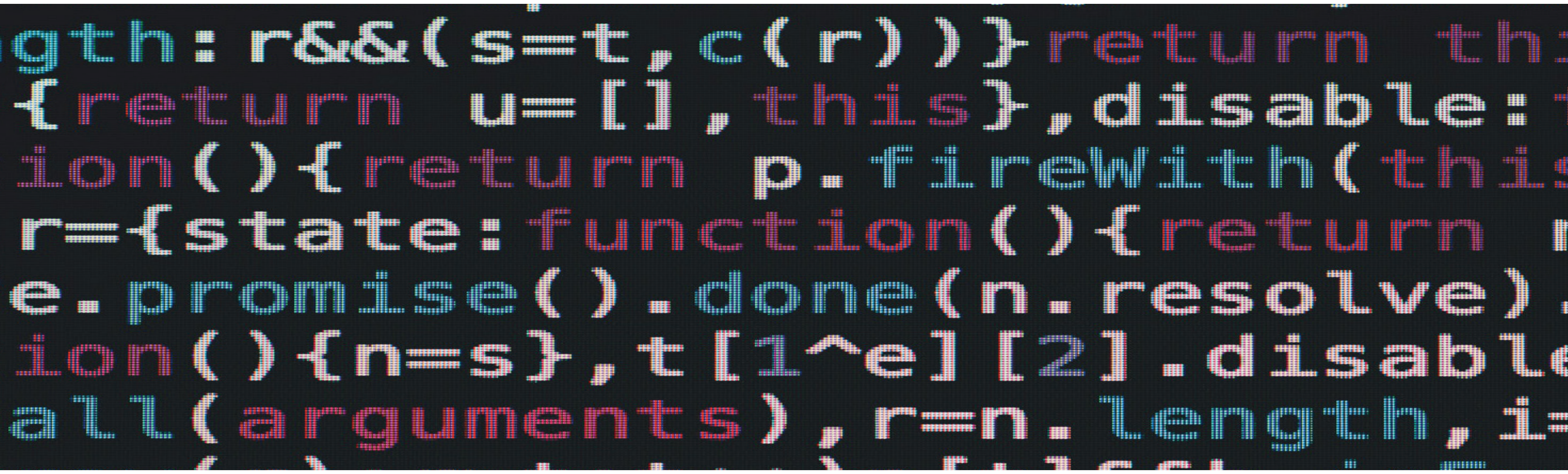
Writing Security As Code to Eliminate Sloppy Coding Practices

In traditional DevOps processes, vulnerabilities resulting from sloppy coding are only detected late in the development process, sometimes requiring teams to start writing new code from scratch. This is a time-consuming fix for busy software teams that also slows down the deployment process. And if security teams miss vulnerabilities during later testing and monitoring stages, security risks can be deployed with the release, putting businesses' customer data in danger.

However, with DevSecOps, developers build continuous security checks into each stage of their coding workflow. Code is automatically scanned for threats, and if detected, developers can immediately relay vulnerabilities to security team members to review. Writing security as code allows teams to catch threats before they're implemented to the main program or repository, enabling dev teams to avoid costly, time intensive patch work later on. This fundamental approach to security protects businesses proactively with minimal work for developers.

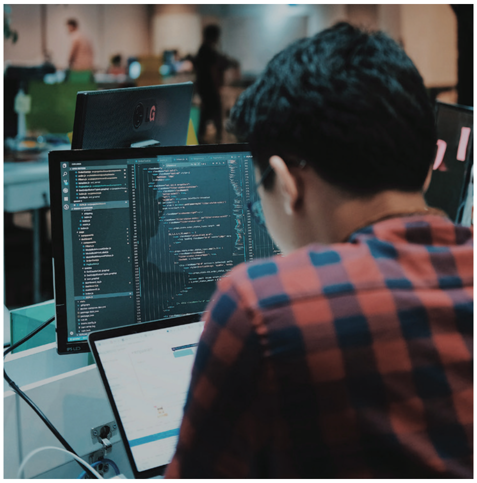
To get started, developers can leverage DevSecOps tools including code repositories from Atlassian (Bitbucket) or GitLab (Github or GitLab) that serve as a single source of truth for project code. Additional recommended tools such as Gerrit, Phabricator and SpotBugs, among others, plug directly into developers' existing Git workflow and trigger a security test or review automatically after every commit and merge.

Contegix can assist an organization during their DevSecOps tool vetting process and help teams implement and optimize their toolset.



```
gth:r&&(s=t,c(r))}return thi
{return u=[],this},disable:
ion(){return p.fireWith(this
r={state:function(){return r
e.promise().done(n.resolve).
ion(){n=s},t[1^e][2].disable
all(arguments),r=n.length,i=
```

Implementing Continuous Testing So Vulnerabilities Don’t Go Undetected



After developers write and build code, the team’s next responsibility is running functionality and performance tests to uphold functional and nonfunctional requirements and scan the software for vulnerabilities. But current DevOps processes often leave little time to conduct necessary tests, as project schedules favor moving a software release quickly through development.

But even with little time dedicated toward testing, 84% of surveyed developers say they struggle to produce frequent code deployments, with testing and quality assurance cited as their top reasons for delays. Traditional DevOps processes magnify current challenges: By waiting to test for security vulnerabilities until the end of the software lifecycle, or by avoiding testing altogether due to limited time, teams risk finding threats too late—or not at all.

If security threats are detected during the testing phase, developers have to allocate more valuable time rebuilding code. If a project moves through development and a bug is identified later on in the life cycle, developers have to start building back at square one, which can impede on other project timelines that command their attention.

Teams can expunge these testing challenges with DevSecOps, which introduces continuous testing through processes that are repeatable and automated. By adopting DevSecOps, developers can implement security testing measures efficiently once, then move on with the rest of the software dev cycle with confidence.

Developers can solve their testing challenges with continuous integration and deployment tools from Atlassian, which are used to catch bugs early in the development cycle through automated testing. By harnessing these capabilities, developers can eliminate time consuming delays and ensure security early on.

Maintaining Long-Term Security Measures Through Monitoring and Controlling

Secure development is necessary to bring a safe product to market, but it's equally important to make sure applications remain secure once live. This is why after developers write code, test for security risks and deploy a software release, teams must also monitor the application to detect potential security threats as it's used. However, as an organization's IT infrastructure scales with new software releases, more applications, systems and devices need monitoring. Developers need an effective method to analyze large amounts of data, which can be a time-consuming feat for IT teams if done manually, who already manage a long list of responsibilities.

Part of this process means knowing how teams will build monitoring techniques into the application itself and selecting tools to evaluate the application's foot and web traffic across the entire system. Without an effective method for application monitoring empowered by technology, teams risk failing to identify preventable security threats, like a hacker connecting to internal accounts. When teams have full visibility into how their application is performing and who is using the software, they are better positioned to defend attacks and prevent data loss.

Organizations also need to apply controls for the application to operate in compliance with functional or global standards like International Organization for Standardization (ISO) requirements or General Data Protection Regulation (GDPR). But industry-specific regulations, such as those for healthcare or finance can be difficult to understand and time consuming to translate.

Maintaining Long-Term Security Measures Through Monitoring and Controlling

With DevSecOps, continuous monitoring and controlling provides ongoing security throughout the software lifecycle ensuring threats don't go undetected as the application is used. With the right tools (such as: Splunk, New Relic, Anchor and Twistlock) the live application is automatically observed for attacks or leaks without constant oversight and required legwork from individual team members. Teams who adopt DevSecOps can assure compliance without having to dedicate hours of their time and work.

How do organizations select the right tools to incorporate into their DevSecOps framework to conduct application monitoring and controlling? With so much available technology on the market, it can be overwhelming to research and vet tools for consideration, especially as teams learn new processes. IT teams can find solace by adopting a holistic DevSecOps platform like Jira Software, which offers a centralized platform that integrates Atlassian and other tools needed to follow DevSecOps.

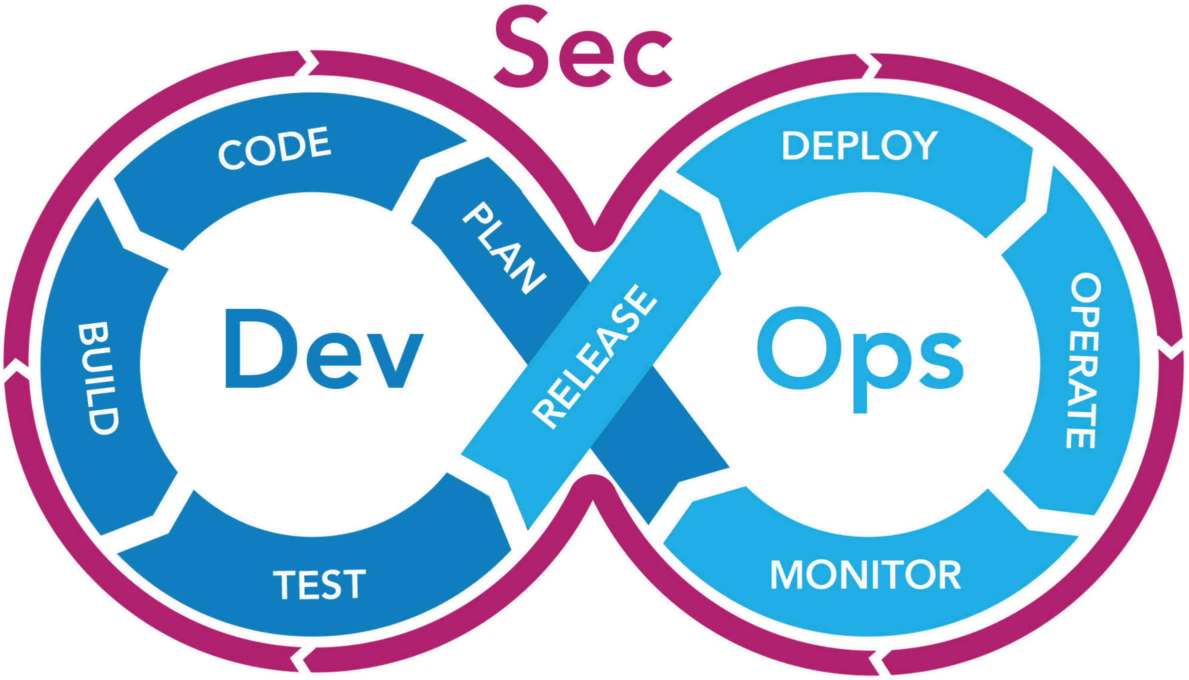
Translating Security Policies Throughout the Dev Life Cycle

While DevSecOps ensures a continuous, automated approach toward security in each stage of the software development cycle—from coding, to testing and monitoring, to controlling—one aspect of security that's woven throughout each stage of development is translating security policies into existing processes. Security policies can cover everything from how a software application sends information elsewhere, to password protection and data privacy.

Sometimes translating security policies means following specific guidelines that are part of an organizations' industry—such as FedRAMP if the application is part of a government agency, or HIPAA if software is within the healthcare industry. Even more highly regulated industries like finance or insurance require IT teams to adopt specific security policies in order to operate under compliance.

Industry-specific security policies can be an additional feat for teams who already have to adopt standard security measures such as implementing two-factor authentication, securing connections with HTTPS, building firewalls, introducing robust password requirements and restricting application access to unauthorized users.

While understanding what security policies an organization has to follow as well as translating those policies into the software development workflow can be time consuming for IT teams, if organizations don't implement industry best practices when it comes to translating security policies, teams risk introducing serious security threats.



Translating Security Policies Throughout the Dev Life Cycle

With DevSecOps, teams are required to account for these policies upfront by building test scripts in their code. Once policies are implemented, the necessary measures are accounted for and developers don't have to spend any additional time on building security into their workflow, and teams can focus on building code.

Especially within highly regulated industries, security policies can evolve and change. New amendments get built onto existing standards and additional requirements create more policies for IT teams to stay compliant with. Working with partners who are FedRAMP or HIPAA certified can help organizations know which security policies to code against and build applications on a secure framework.

PREPARE FOR YOUR TRANSITION TO DEVSECOPS

Successfully executing a change initiative like adopting DevSecOps requires thoughtful planning to prepare for two key eventualities:

1. Organizations must **prepare for a culture shift** that replaces siloed working conditions with a collaborative environment. Leaders initiating the transition to DevSecOps should provide a motivating vision statement that outlines measurable goals for success and offers clear implementation guidelines. This way, dev, IT ops, security and leadership are aligned on upcoming changes and can see the benefits of DevSecOps adoption.
2. As part of the planning phase, teams adopting DevSecOps should **conduct a security analysis** to evaluate the maturity of existing coding practices. A security analysis helps teams identify areas within their code that could become entry points for malicious activity and impact other parts of their IT infrastructure where the code is replicated.

Bolster Your Application Security by Adopting DevSecOps

Without a secure environment and approach to software development, organizations risk having their employees' and customers' information leaked or distributed illegally, which could lead to reduced trust in the application and potential legal action for the organization.

The most advanced organizations follow DevSecOps to address top security challenges in today's cybersecurity climate. In fact, by next year, 90% of software development projects will aim to follow DevSecOps.

For organizations looking to adopt or master their DevSecOps framework, a DevSecOps partner like Contegix can provide invaluable assistance across multiple touchpoints depending on an organizations' needs:

- **DevSecOps assessment**: Contegix can help software teams identify their unique pain points, the specific elements they'll need in order to build security into their dev processes and then recommend the methods and tools to achieve their goals.
- **Coaching DevSecOps adoptions and implementation**: Contegix's team of expert project managers and agile specialists will coach software teams through the entirety of the DevSecOps adoption process, enabling team-wide collaboration around security steps. Whether an organization requires consultation for DevSecOps tools, or a partner to build out their workflows and toolchains in their entirety, Contegix provides support at every level to ensure DevSecOps implementations are successful.
- **Ongoing support and governance**: As security challenges evolve, Contegix not only designs and tailors custom DevSecOps instances for customers, but also will optimize and fine-tune those solutions for customers as their security needs grow or change.
- **DevSecOps training for teams**: Contegix's certified trainers can teach software teams DevSecOps principles, as well as how to most effectively use DevSecOps tools to meet their dev and security needs across their unique software pipelines.

By guiding teams in their DevSecOps adoption, Contegix helps organizations hit their benchmarks while keeping their customers' data protected.

Visit contegix.com | Call 877.289.0395 | E-mail sales@contegix.com