invicti

DevSecOps with Invicti

Why do you need it?

What is DevSecOps?

DevSecOps means including security early in the software development and operations lifecycle. When you use a DevSecOps approach, you treat security testing just like unit testing and you include it in CI/CD pipelines. This way, most security vulnerabilities are discovered as early as possible.
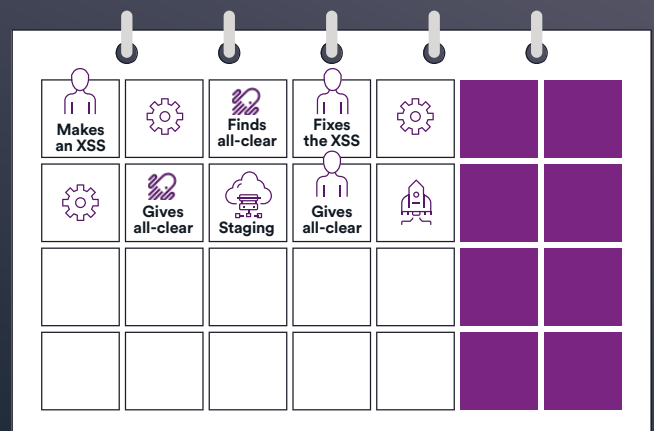
DevSecOps saves you time

With DevSecOps, developers don't waste time fixing someone else's mistakes and releases don't get delayed because a high-severity vulnerability was only found in staging.

Without DevSecOps
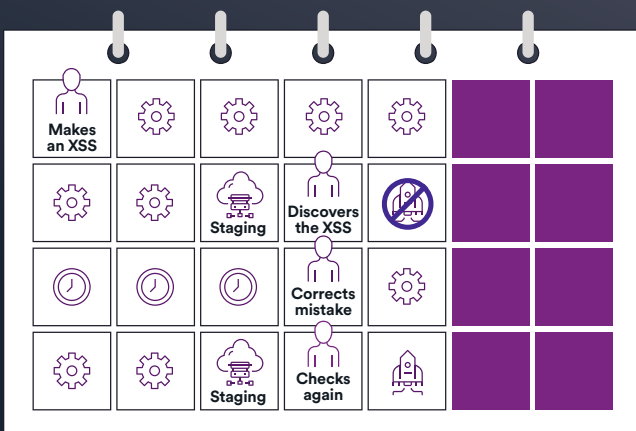
With DevSecOps

DevSecOps improves working relations

Without DevSecOps:

- Developers usually don't see themselves as responsible for security.

- Security analysts are perceived as "the bad guys" and associated with additional workloads and delays.

- Developers and security analysts often don't collaborate at all.

With DevSecOps:

- Developers learn to be responsible for security from the first line of code.

- Security-related bugs don't increase the overall workload and there are very few surprises caused by last-minute blockers.

- Security analysts are perceived as "the good guys" and have more time to help developers better understand security.

Problem:
Developers find it difficult to fix security bugs introduced by other developers.

Solution:
With DevSecOps, a developer won't be able to merge their new or updated code while it contains a security vulnerability. That way, developers only ever need to fix their own code and their own security bugs. They also get to correct their mistakes right after a commit fails rather than weeks later, so they still remember the code and can quickly fix the issue.

Problem:
Developers often don't know enough about avoiding web vulnerabilities.

Solution:
With Invicti as part of DevSecOps, developers get detailed vulnerability reports with all the information they need to fix the issue. Each report also shows how the vulnerability was safely exploited by the scanner, what impact it could have, how it can be fixed, and how to avoid it in the future.

Why choose Invicti as your DAST for DevSecOps?

- Rapid deployment and measurable security benefits in any web application environment
- Industry-leading accuracy and test coverage for modern web applications
- Proprietary vulnerability confirmation technology enables confident and efficient workflow automation
- Over a decade of dedicated security research and development in one solution
- Tried and trusted by customers worldwide

Testimonials

"We have it included in our continuous integration process through TeamCity. Upon every check-in, it will not only deploy to our development environment, but will run the security scan on the site and give us updates/reports on the OWASP threats to ensure we are maintaining a secure site. We love the product!"

Paul Johnson
Software Engineering Manager,
Kansas City University

"As we are faced with perpetual evolving security threats and vulnerabilities, Invicti brings a level of assurance to our business as it is included as part of our development lifecycle to help identify and mitigate such threats prior to deployment. With Invicti being able to provide near zero false positives, it ensures that time is not wasted deciphering whether a vulnerability is legitimate or not."

Chris Evans
Security and Compliance Manager
at ISACA

"We integrate Invicti into our clients' DevOps process to identify security issues early in the development cycle."

Alexander Chaveriat
Chief Security Innovation Officer
at Project Mariana

Out-of-the-box integrations with leading issue trackers and CI/CD tools >>

invicti

FIND US

in linkedin.com/company/invicti-security
twitter.com/invictisecurity
f facebook.com/invicti-security

invicti.com
invicti.com/contact/