DevSecOps with Acunetix

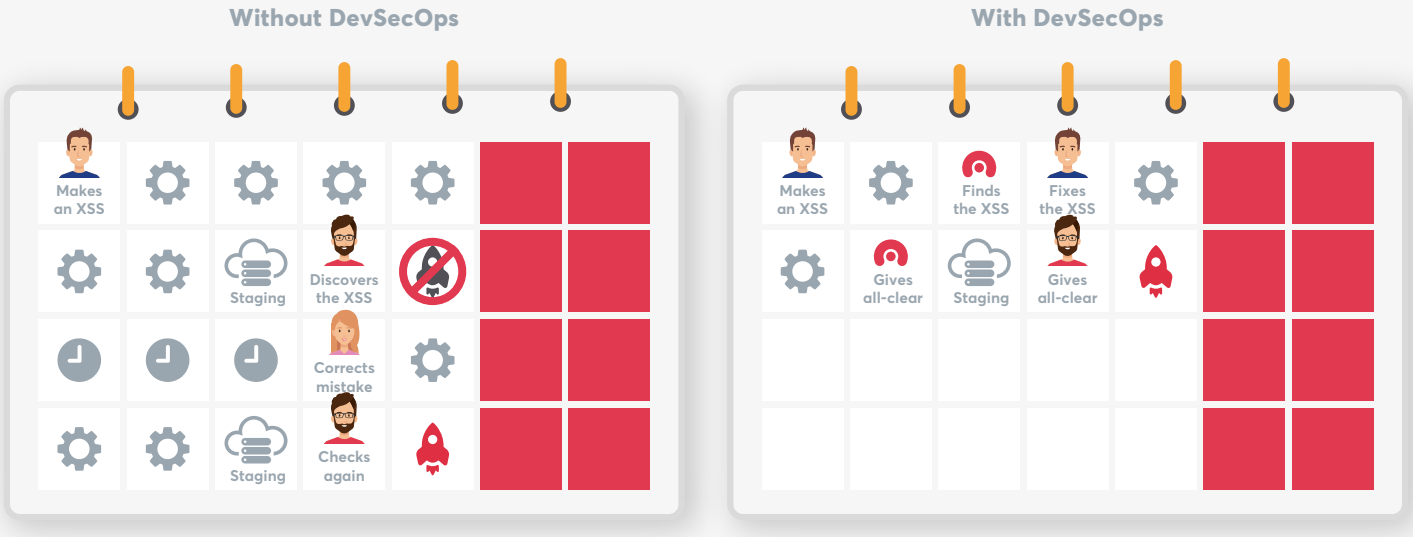
Why Do You Need It?

What Is DevSecOps?

DevSecOps means including security early in the software development 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 mistake and release dates don't have to be pushed back due to high severity vulnerabilities found during staging.



DevSecOps Improves Relationships

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
- Relationships between developers and security analysts often don't exist at all

Developer

He finds insignificant problems, making me work more! No explanation of the problem is given so I don't know how to fix it. I have to correct someone else's code, which is more difficult, causing us significant delays and a chaotic work environment.

He doesn't bother to learn the basics of web security and makes simple mistakes, creating a lot of issues, which makes me work harder to find them. He doesn't understand simple explanations or instructions and whines about having to do his work properly!

Security Analyst

Developer

He has time to talk to me when I have a problem or I don't understand something. I've also been trained on the basics of web security and now I know how to avoid errors.

Acunetix finds most security errors immediately and confirms they are real. It also explains the vulnerabilities and how to fix them. It teaches me about web security.

He knows the basics of web security and makes few security mistakes. He also asks valid technical questions so that I can help him learn.

Security Analyst

With DevSecOps:

- Developers learn to be responsible for security from the ground up
- The workload doesn't increase due to security issues and there are very few "last-moment surprises"
- Security analysts are perceived as "the good guys" and have more time to help developers understand security better

Problem:

Developers find it difficult to correct security bugs introduced by other developers.

Solution:

With DevSecOps, the developer cannot merge their new or updated code if there is a security vulnerability in that code. This way, the developer never needs to correct someone else's mistakes. The developer can also correct the mistake soon after they made it, while they remember and understand their own code very well.

Problem:

Developers often don't know enough about how to avoid web vulnerabilities.

Solution:

With Acunetix as part of DevSecOps, developers receive detailed reports on where they introduced the vulnerability. They can see how it was safely exploited. They also receive several links that explain the vulnerability and teach them how to fix and avoid it.

DevSecOps with Acunetix

Your Best Choice

DAST or SAST for DevSecOps?

SAST

- Works only with selected development languages and environments
- Prone to reporting a lot of false positives
- Does not actually prove any vulnerabilities, just reports that they are possible
- Unable to find issues that only appear during run time

DAST

- Works with any development language and environment
- Much less prone to reporting false positives
- Proves vulnerabilities by safely exploiting them and showing the results
- Able to find issues that only appear during run time

Why Choose Acunetix as Your DAST?

- Most established product on the market
- Developed by web application security specialists, not a generic manufacturer
- Created with an emphasis on efficiency, won't hog your pipelines
- Bundled with a lot of automation and integration options as well as a complete API
- Tested by many customers in various DevSecOps scenarios

What's in It for Me?

Security Analyst

- Thanks to Acunetix, **I have much more time for important tasks** because developers don't make as many security mistakes and I don't have to check for them.
- There is also **no need for me to train developers on security** as much because Acunetix teaches them how to handle security issues.
- I can also **use Acunetix for my own work**. I can, for example, use it to find the most typical vulnerabilities on WordPress websites or other web assets that are not developed in-house. I can also use it to double-check staging sites.
- All-in-all, **Acunetix saves me a lot of time and improves my relationship with developers.**

Developer

- Thanks to Acunetix, **I immediately know when I made a security mistake** and can correct it before merging the code.
- Because I'm using Acunetix, **I almost never have to correct security mistakes made by other developers**, which saves me a lot of time to actually focus on creating valuable code.
- **I learn a lot from Acunetix vulnerability reports** – they contain links to Acunetix articles, which explain vulnerabilities clearly, as well as tell me how to fix and avoid such issues in the future.
- **I develop healthy programming habits thanks to Acunetix** – I care more about security, use more secure constructs when programming, and notice more potential errors.

Testimonials

> Initially we were thrilled to run Acunetix to find and fix some rather large vulnerabilities we had no idea existed. Since then, we have moved to a more comprehensive strategy that includes multiple scan targets running in tandem with our software development lifecycle. When our customers ask us if our software is security tested, Acunetix gives us the confidence to say it is.
>
> **GREG FULLER, VERMONT SYSTEMS**

> Acunetix is a key point in our application's security strategy, it's integrated with the QA process, allowing us a cost effective way of detecting flaws that can be solved early within the development life cycle. After trying many others, we can say that it is the fastest one and has the best relationship between findings and false positives.
>
> **ING DIRECT**

> The use of Acunetix has allowed us to schedule regular automated scans on a host of sites under the Betfair Group umbrella, providing invaluable visibility in capturing vulnerabilities early in the SDLC.
>
> **JAN ETTLES, BETFAIR.COM**

WHERE TO FIND US

Stay up to date with the latest web security news.

Website. www.acunetix.com
Blog. www.acunetix.com/blog
Facebook. www.facebook.com/acunetix
Twitter. twitter.com/acunetix

CONTACT INFORMATION

Acunetix (Europe and ROW)
Tel. +44 (0) 330 202 0190
Fax. +44 (0) 30 202 0191
Email. sales@acunetix.com

Acunetix (USA)
Tel. (+1) 737 241 8773
Fax. (+1) 737 600 8810
Email. salesusa@acunetix.com