DETECTIFY CASE STUDY: AUTH0

How Auth0 scales security to match their growing organization

AN INTERVIEW WITH:

Marcin Hoppe
SENIOR ENGINEERING MANAGER

detectify

auth0

About Auth0

Auth0 provides a platform to authenticate, authorize, and secure access for applications, devices, and users. It safeguards billions of login transactions each month

Auth0's security challenges

- A fast scaling company with a growing product base
- Multiple security tools to maintain and process
- Test for the latest vulnerabilities in Auth0's applications
- Web application security testing at scale

Marcin Hoppe leads the Auth0 security team and is constantly looking to expand its security coverage with tools to grow and keep applications secure. When it comes to web application security, they chose Detectify because of its ability to quickly find the latest vulnerabilities in Auth0's applications.

Industry:	Software
Company size:	501 - 1000 employees
Location:	Headquartered in Bellevue, Washington state, with employees located in 30 countries

Marcin Hoppe

SENIOR ENGINEERING MANAGER

How Auth0 uses Detectify

Securing customer-facing applications

Auth0 utilizes Application Scanning to test the authentication sequences in their customer-facing applications.

By creating an authenticated state, Detectify was able to scan behind login and check for password resets, create form submissions, and dynamically test the actions and API calls made within the application.

This ensured that any customer-facing applications were secure, which is critical for Auth0.

Triaging vulnerabilities

Before Detectify, Auth0 had a broad application-specific focus. For example, team members would add all their tickets from external tools to Jira, creating considerable noise. Using Detectify, they can now create integrations that alert the security team to new vulnerabilities, where they utilize the user interface to triage them.

Due to Auth0's unique environmental setup, vulnerability risk varies from application to application and a predetermined CVSS score doesn't always show the true extent of a vulnerability. Detectify assists Auth0 by delivering a low rate of False Positives to ensure quick visibility and escalation of the highest quality of pre-verified vulnerabilities.

Budgeting for new tools

Auth0 is a rapidly changing company that takes a pragmatic approach when a problem or need arises; they will seek a tool or solution to match their needs. Marcin's team is careful not to overlap with existing tools so that each has its unique purpose.

For example, they identified one lacking area as automatic dynamic application testing. Detectify could fulfill their dynamic testing needs by providing a solution that replicates a hacker's actions while continually updating with the latest techniques.

The power of the latest high-quality results from Crowdsource

Auth0 is confident in the results that Detectify provides and trusts in the continual updates from Crowdsource to ensure consistent, high-level results.

”There are a lot of extremely noisy tools, and they generate a lot of findings, but to get to the true positives, you have to spend a lot of time analyzing the results. So we were very happy with the low rate of Detectify’s false positives,” says Marcin.”

Ease of use and less wasted time

Detectify’s ease of use and clarity in its findings meant Auth0 developers were no longer burdened with irrelevant information. As a result, they now have more time to build products and need less time to focus on results.

Additionally, by having recurring automated scans, Auth0’s developers could scale and test all of the applications they had publicly available whenever they made changes without impacting the application.

Marcin's security tips

Marcin recommends doing a thorough evaluation of your applications and deciding upon a solution that best suits their needs. Looking at open-source solutions is always an option.

However, you must have someone that can maintain and own that tool -having a 3rd party tool that continually updates can save considerable time and hassle by knowing that you are confident with the results it provides.

Applications that require authentication should be configured with the appropriate users in mind and not be publicly exposed unless necessary. There is no reason to reinvent the wheel if there are solutions out there that do the job for you.

You will achieve a far better product if you focus on your strengths rather than trying to create and source externally where possible.

> *"There are a lot of extremely noisy tools, and they generate a lot of findings, but to get to the true positives, you have to spend a lot of time analyzing the results"*

Marcin Hoppe
SENIOR ENGINEERING MANAGER

go hack yourself.