STACKHAWK

HAWKSOME CUSTOMER

Planetly Selects StackHawk Over Building Internal Service

BACKGROUND

With important customer data and publicly available applications and APIs, Planetly is focused on building secure applications. With both internal mandates and an enterprise customer base that has strong security requirements for their vendors, the team needed a reliable solution.

The engineering team at Planetly, had both static analysis and container analysis in place. As developers commit code, it's first checked with a static analysis security testing tool for any identifiable security risk patterns in the code and then container images are scanned for potential vulnerabilities.

While this was a great foundation, the organization wanted to improve security testing across their running applications. Without testing on their running applications, they lacked a full view of potential vulnerabilities from real life scenarios and an attacker's point of view. Planetly prioritized the ability to find and fix these kinds of vulnerabilities (such as SQL injection) before software deployments. Given this and the requirements from their Enterprise customers, they decided that a dynamic application and API security testing tool was the best path to address these challenges.

.planetly

Company
Planetly

Industry
Internet Software and Services

Location
Berlin, Germany

Use Case
Manage risk and improve security posture

Planetly is a climate tech company based in Berlin that provides software to help companies monitor and track their carbon emissions while also recommending potential carbon reduction strategies.

THE PROBLEM

Lacked a full view of potential vulnerabilities from an attacker's point of few and wanted to improve security testing across their running applications.

THE SOLUTION

Automating application security testing for new services was made simple with StackHawk regardless of running in CI/CD or testing on a local machine.

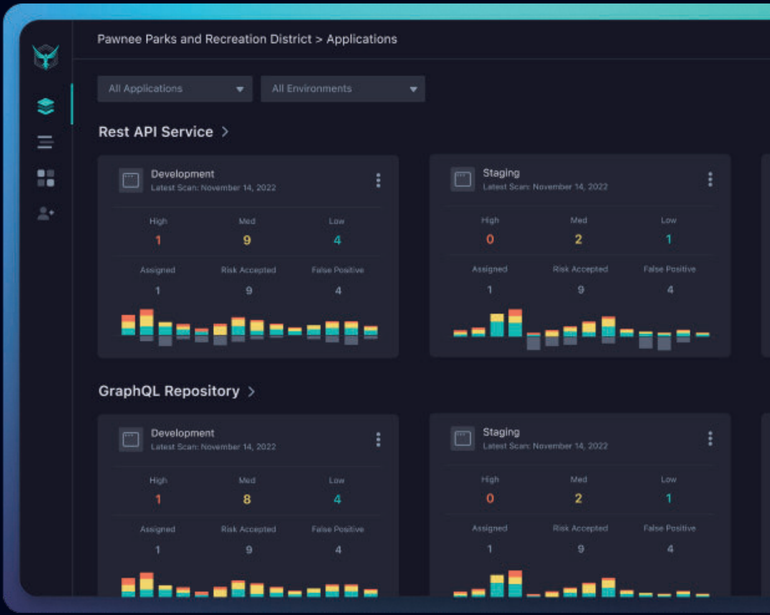
THE RESULT

Scaling application security testing across engineering made simple with shared findings and evidence to inform developers of what to fix.

CHOOSING A SOLUTION

When it came time to seting up a dynamic application security testing tool, Planetly first turned to ZAP, the popular open source vulnerability scanner. As a fast moving engineering team, they explored delivering Zap-as-a-Service.

As the team began to scope and test the work associated with this, they recognized that building ZAP-as-a-Service would require a lot of upfront work and ongoing maintenance. That is when they discovered StackHawk. After spending a week testing ZAP, it took Planetly less than an hour to get StackHawk configured and running authenticated scans against his applications and APIs.



Pawnee Parks and Recreation District > Applications

All Applications ▾ | All Environments ▾

Rest API Service >

Development
Latest Scan: November 14, 2022

High	Med	Low
1	9	4

Assigned	Risk Accepted	False Positive
1	9	4

Staging
Latest Scan: November 14, 2022

High	Med	Low
0	2	1

Assigned	Risk Accepted	False Positive
1	9	4

GraphQL Repository >

Development
Latest Scan: November 14, 2022

High	Med	Low
1	8	4

Assigned	Risk Accepted	False Positive
1	9	4

Staging
Latest Scan: November 14, 2022

High	Med	Low
0	2	1

Assigned	Risk Accepted	False Positive
1	9	4

EXPERIENCE WITH STACKHAWK

With StackHawk, the Planetly team saw several benefits for its application security testing tool:

- **Trusted ZAP Scanner:** ZAP is the industry standard when it comes to web application security testing.
- **Simple Configuration:** With YAML based configuration files, config is managed in code using existing version control systems.
- **Docker Deployment:** With StackHawk's container based deployment of scans, automating application security testing is simple.
- **Developer Fix Features:** cURL based recreation feature allows a developer to recreate the same request to debug the issue.
- **Integrations:** With StackHawk's Jira integration, findings are easily passed into Jira to create new tickets.

WIth StackHawk, Planetly has application security coverage for its applications and is able to distribute testing across engineering, hitting its quarterly OKR within weeks. After testing StackHawk, the team cited productivity gains as one of the biggest benefits and the ability to ensure secure deployments while focusing efforts on other high value work.

STACKHAWK

Learn how to Ship Secure Software Faster at **www.stackhawk.com**