LEGIT SECURITY

Case Study

Customer Case Study: Noname Security

How Noname Uses Legit Security to Secure Their Own Software Development Life Cycle

Introduction

About Noname Security

Despite the moniker, Noname Security is making a big name for themselves in the world of API security by protecting some of the world's largest organizations from API-based attacks. As a developer of SaaS solutions, they're no strangers to the challenges organizations face maintaining a rapid pace of innovation while continuously enforcing secure software delivery. As Karl Mattson, Noname's CISO, says, "Security begins with us."

"What I needed as a responsible security leader, was to see the whole picture of all our software moving through its development processes. I needed to look at the procedures we were using, the integrity and security of our code repositories and our pipeline, as well as the software itself." Karl engaged with Legit to do exactly that. "We were looking for a holistic view across the entire Noname product set, and Legit was exactly what we needed to get that view, that incorporated all the elements of process, technical standing, and vulnerability management for our product."

"Our software has to be spotless, and we have to be able to prove it."

Karl Mattson

CISO, Noname Security

noname

Background

In order to maintain the trust Noname's customers have in their ability to protect them from API-based attacks, Karl and his team employ a wide range of open-source and off-the-shelf security solutions. While these solutions deliver critical insights to the Noname security team, they are oftentimes difficult to use, noisy, and limited to point in time insights. Karl needed a solution that would cut through the noise and give him and his team better visibility across their entire SDLC.

Key challenges to overcome:

- Lack of visibility
- Noisy and inaccurate vulnerability data
- Poor usability across application security stack
- Missing risk context to deliver to developers
- Slow, manual reporting

Building a collaborative culture of secure software delivery

One of the key goals that Karl had for implementing Legit was to build a culture of collaboration between the application security team, DevOps and Noname's software developers. The developers were the user base that Karl was most concerned with empowering because historically they viewed vulnerability and risk data with a skeptical eye, considering it to be noisy, inaccurate and taking away from time they could better spend on innovation and software development. Karl needed a solution that would deliver high quality, actionable data about critical vulnerabilities, misconfigurations and other risks to the software developers and DevOps engineers, without inundating them with false positives and alerts about expired SLAs.

Meaningful visibility across the SDLC is exactly what Legit Security delivers for Karl and the rest of the Noname team. Legit integrates with Noname's SDLC stack and application security toolset, with the AppSec team setting up policies, alerting and workflows to automatically analyze vulnerability and risk data and prioritize what needs to be addressed first.

This information is delivered to the software development and DevOps teams along with all of the context they need to understand the issue and quickly remediate it. By delivering higher quality vulnerability data, they're able to focus on a handful of security tasks that actually matter. And Karl can use Legit as a true single pane of glass to derive real insights and visibility into their application risk and AppSec progress, rather than being stuck with a dashboard of missed alerts and overdue SLAs. He can then track progress over time to easily evaluate which programs are most effective and where there is room for improvement.

Noname was looking for:

- Deep Visibility
- Ease-of-use and deployment
- Noise reduction
- Improved collaboration
- Faster mean time to remediation
- Demonstrable application security posture management

Demonstrating security to close business

Internal security wasn't the only concern that Karl had when he evaluated Legit. As a security vendor protecting mission critical applications for some of the world's largest organizations, Noname is frequently asked to provide proof of their own internal security and secure application delivery processes. This includes providing customer facing evidence that their application and software supply chain is protected. As Karl says, "Our software has to be spotless and we have to be able to prove it."

The level of detail Noname needs to provide varies by company, like the level of process documentation or whether an SBOM is required, and Karl only sees the bar getting higher. Prior to Legit this would frequently take hours or days to generate and needed to be done on an individual basis. With Legit they can now cut that process down to minutes, delivering continuously updated visibility into their application security posture, including SBOMs when requested. Noname is able to quickly demonstrate product security for prospective customers, freeing up time to stay focused on rapid secure software delivery while maintaining their competitive edge.

Summary

Legit's ability to deliver deep visibility across the entire SDLC benefits Noname Security in many ways, both internal and external. The Noname application security team has a more collaborative risk remediation process with developers and DevOps by delivering higher quality vulnerability detail that reduces noise and accelerates remediation. And Noname can now quickly generate critical information about their application security posture in minutes rather than days. Legit Security gives them the tools they need to improve secure software delivery and help close new business while reducing overhead.

About Us

Visit our website to book a demo and learn more about our platform at legitsecurity.com.
Get best practices on ASPM and software supply chain security from our blog.
Follow us on LinkedIn for the latest news, events, and resources.