LEGIT SECURITY

Cybersecurity Vendor Streamlines Software Security With Legit

A large cybersecurity vendor became a Legit customer because maintaining their hard-earned reputation as one of the most trusted cybersecurity vendors naturally extends to the integrity and security of their own software products, which are used by enterprises globally.

One of the CISO's core responsibilities is to ensure that their customer-facing products, internal applications, and software supply chains are not the source of a breach that could jeopardize their customers, brand reputation or business operations. To prevent this from happening, the CISO and his team rely on Legit Security.

Creating a culture that promotes secure software development without slowing innovation is one of the biggest challenges that the CISO has to overcome and is one of the key drivers for engaging with Legit Security. Legit Security helps them achieve this goal by delivering deep visibility and security into their SDLC assets, pipelines, teams and application releases.

This allows the application security and software engineering teams to better understand where they have risk—with valuable relevant context—and how to prioritize their efforts. Enforcing customizable security guardrails with streamlined remediation and collaboration between teams helps this cybersecurity vendor achieve fast and secure software development.

But what were the criteria that convinced the CISO to choose Legit Security?

Why the cybersecurity vendor selected Legit Security

The cybersecurity vendor needed a solution that delivered the visibility and security to rapidly prioritize and remediate vulnerabilities across the SDLC based on their actual risk, as well as fostered better communication and collaboration between application security and software engineering teams.

The solution needed to integrate with all the SDLC tools they already had, along with the flexibility to allow different resources to work within Legit's UI or to access the data they need within their own preferred tools. And to top it off, the solution had to reduce overall AppSec complexity and security issue noise.

Integration with existing tools

Legit Security's ability to integrate with the vendor's existing tools, teams and processes allowed them to simplify vulnerability and risk mitigation and expedite mean time to resolution (MTTR). When an issue is discovered in their SDLC or a specific application release, integration with their Jira deployment automatically opens a trouble ticket that notifies the right resources with the context they need to remediate fast. This includes risk ratings specific to their environment that allows them to prioritize based on factors like production status and issue severity.

How collaborative application security drives better business outcomes

The cybersecurity vendor CISO uses a real-world example to highlight the efficacy of this AppSec driven, collaborative approach, in a situation where one of his team's security tools identified nearly 160 issues related to a cross site scripting error.

This was difficult for software engineers to detect because it's the type of issue that traditional code scanning tools like SAST will frequently miss. Instead, one of his application security engineers researched the issue and identified the cause, which was related to the same 2 lines of code in every instance and was able to pass all relevant details and context to the software engineering team to remediate. Armed with this information, the assigned software engineer was able to fix all of these downstream vulnerabilities in 15 minutes rather than being charged with tracking down 160 individual vulnerabilities across multiple apps to find the source of the problem at the expense of accomplishing their future application development objectives.

Visibility and security across the SDLC

The cybersecurity vendor's use of Legit Security isn't limited to helping consolidate application vulnerability data, tracing root causes, reducing information overload or improving collaboration between teams. According to the CISO, the most critical capability that Legit Security delivers is deep visibility and security across the SDLC.

This allows the vendor's application security team to see vulnerabilities and risk throughout the software supply chain faster, and with greater context. Armed with that information, the application security team can send relevant details to the software engineers for fast, effective mitigation—without wasting their time or getting in the way of meeting their primary business

---

Legit Value

- End-to-end visibility across CI/CD pipelines and the SDLC

- Automated, real time SDLC security monitoring

- Deeper insights into security issues to improve developer collaboration

- Better prioritization to focus remediation efforts and lower MTTR

objectives of delivering new product functionality fast. And when new applications are introduced, Legit Security automatically discovers and analyzes any new SDLC infrastructure and pipelines, immediately rolling them into the AppSec team's security policies and processes.

"Visibility is the most important aspect of security. You can't defend what you don't know about," says the CISO. However, visibility in the SDLC isn't limited to faster threat detection and finding things that you otherwise wouldn't—it also helps create a collaborative culture of secure software development and innovation. "Visibility gives engineers the ability to implement great ideas quickly with guardrails in place. Everyone acts and feels as part of the same team by meeting software engineers where they need to be to feel successful."

Securing the cybesecurity vendor's software supply chain: a closer look

In addition to improving collaborative processes and operational efficiency for secure software development, the vendor uses Legit Security to secure their end-to-end software supply chain. As the CISO points out, "Nobody wants to ship insecure code, but shipping secure code is incredibly difficult." One of those underlying challenges is taking a comprehensive approach to securing the software supply chain.

Securing the software supply chain

Effectively securing the software supply chain remains a challenge for most enterprises today. Engineering teams are primarily focused on meeting business objectives for rapid innovation through agile development and continuous integration/continuous delivery processes, with only a small percentage of software engineers having any formal cybersecurity training.

Conversely, cybercriminals have a significantly easier task finding and exploiting vulnerabilities across a sprawling pre-production development environment attack surface. A common response to address this is to deploy additional traditional code scanning tools and checkpoints, which are not designed to address modern supply chain attacks on SDLC infrastructure and pipelines. Unfortunately, the placement of these redundant traditional tools often ends up hindering more than they help in the cybersecurity vendor CISO's experience.

It's the CISO's philosophy that an effective cyber security program needs to defend the entire organization while simultaneously helping engineers securely ship code at the speed that they need to hit their objectives. To do so, security organizations need to understand how engineering organizations operate and partner better with them to better embed security as an integral part of their development processes. As the CISO emphasizes, the wrong approach is to simply buy more overlapping tools and flood engineers with a bunch of issues. Ideally the application security team and their tools should do the majority of the work up-front to analyze and evaluate vulnerabilities and risk, waiting to engage the engineering team when all relevant detail and event context is collected, minimizing the time and effort expected of the software engineers responsible for remediating the issue.

Visibility in the SDLC isn't limited to faster threat detection and finding things that you otherwise wouldn't—it also helps create a collaborative culture of secure software development and innovation.

Application security guardrails

By implementing clearly defined application security guardrails and security policies across the software supply chain with real-time visibility and consolidated vulnerability management, Security can take the lead in improving communication and collaboration with Engineering and make secure software development more automated, efficient and effective.

The Legit Security platform reduces tool and alert fatigue by consolidating application security data from across the SDLC, analyzing and prioritizing vulnerabilities, and automating processes for collaboration and remediation. This gets the right information into the hands of the software engineers faster, telling them where critical vulnerabilities have been introduced into the software supply chain and how to fix them, without getting in the way of their primary objectives.

The bottom line

Legit Security helps organizations like this vendor secure their software supply chains and ensure the integrity of application releases, while improving security team efficiency and streamlining engineering collaboration. This leads to better security outcomes without impacting the rapid innovation and continuous delivery that is the lifeblood of modern software development today.

Learn More About Legit Security

Visit our website and Book a Demo

About Legit Security

Legit Security provides an application security posture management platform that secures application delivery from code to cloud and protects an organization's software supply chain from attacks. The platform's unified application security control plane and automated SDLC discovery and analysis capabilities provide visibility and security control over rapidly changing environments and prioritize security issues based on context and business criticality to improve security team efficiency and effectiveness.