Case Study

ACV Auctions Uses Legit Security to Deliver Secure, Continuous Software Innovation

Digital transformation is nothing new to ACV Auctions. In fact, one of their stated goals is to *"fundamentally change the wholesale automotive industry, by providing a level of trust and transparency that was once unimaginable."* Becoming the industry's premier wholesale automobile auction site requires rapid innovation and software development lifecycles (SDLC) with continuous integration/continuous delivery (CI/CD) pipelines.

Erik Bataller, Vice President of Information Security for ACV Auctions is the person responsible for securing their applications and software supply chains. He manages a team of 15 people, who are responsible for organization wide cyber security, including maintaining trusted corporate identity, delivering security awareness and training for the entire company, and running vulnerability management and application security programs for roughly 250 developers. When malicious activity takes place, Erik's team takes point on identifying problems, remediating risk, and ensuring that existing controls are effective.

Challenges of secure application delivery in an agile, digital business

Erik and his team are tasked with protecting the software factory that drives ACV Auctions' digital business. Protecting the business means creating and maintaining a secure and sustainable process for developing new and innovative software, which is why they view the SDLC as a critical attack surface to protect, under the responsibility of the attack surface management (ASM) team.

In order to do that, the ASM team needs to analyze what's happening at each stage of the SDLC so that they can truly understand their risk exposure. That means an inventory of the SDLC systems and infrastructure in place, a deep awareness of operational security controls, understanding which regulatory requirements are being adhered to, and which may be drifting out of compliance. That starts with observability, which is one of the key reasons that Erik brought Legit Security into the mix.

Case Study

The Business Imperative to Modernize AppSec

Prior to implementing Legit, the ASM team struggled to efficiently and cost effectively secure their SDLC. While the team had a wealth of talent, they were overly dependent on time consuming, manual processes for auditing and evaluating the pipeline, relying on individual surveys and lengthy documentation reviews to ensure that the proper controls were in place and being followed by the software development teams. The security team was spending too much time on slow, repetitive work that didn't leverage their broader skillsets and training.

They needed a solution that would not only give them critical observability into their SDLC but would also identify their software supply chain vulnerabilities, streamline remediation, provide valuable insights and relevant context to enhance collaboration with developers, and better assess their ability to meet numerous regulatory requirements. And they needed it to be easy to implement, simple to operate, and to automate as much of the process as possible to minimize the drain on time and resources.

Legit Value

- Provide end-to-end observability across CI/CD pipelines and the SDLC
- Automated, real time SDLC security monitoring
- Deeper insights into security issues to improve developer collaboration
- Continuous assurance and risk management for audit and compliance

The Legit Security Solution

Erik and his team selected Legit Security after a platform evaluation that demonstrated all their primary requirements including observability and security of their SDLC pipelines along with real-time auditing and monitoring. Legit was able to immediately provide a broad range of capabilities that delivered what the ASM team needed—at a fraction of the cost that adding staff would have required.

From the beginning, Legit has been able to integrate quickly with ACV's existing systems, tools, and technology stack. For example, Legit can continuously evaluate the security posture and configuration of SDLC systems like GitHub code repositories or Jenkins build servers so that the ASM team can perform security monitoring and audit compliance in real-time. Any time there is change, the Legit platform is immediately aware. If it's degrading the level of security or service, the platform can immediately trigger a response and automate an alert to all relevant parties to make a change or adjustment.

> **"Legit gives us direct, strategic visibility over all of our pipelines in the SDLC to ensure that we are able to develop software securely in a sustainable fashion."**
>
> *Erik Bataller, Vice President of Information Security, ACV Auctions*

Benefits Built on the Foundation of a Secure SDLC

When asked which organizations could benefit from a Legit Security implementation, Erik was quick to list numerous groups. Legit provides a powerful tool for the product security team, who can use it for SDLC oversight to provide an informed and ongoing advisory perspective. Likewise, the software development organization can leverage data generated by Legit internally to manage their own SDLC and to enrich key stakeholders and other interested parties with that data. And the compliance teams can use Legit to continuously monitor drift and report on continuous compliance.

- ✓ **More collaborative application security**
  In addition to the direct value that Legit provides to the ASM team, they are also able to use the platform's risk scoring and deeper contextual information around vulnerabilities to foster more productive and collaborative conversations with their development teams to jointly secure their SDLC.

- ✓ **Smarter vulnerability management**
  Understanding which vulnerabilities to prioritize is critical for efficient risk management and remediation. This can be difficult to accomplish in the SDLC without deep observability and context across end-to-end stages. With Legit in place, the product security team is able to partner with both ASM and development teams to triage security vulnerabilities faster and more effectively.

- ✓ **Continuous assurance and risk management**
  Quickly identifying, prioritizing and remediating security vulnerabilities in the SDLC pipeline is critical for ongoing risk management, protecting the core business, and meeting compliance requirements. Legit allows ACV Auctions to continuously track the state of their SDLC and CI/CD pipelines so the ASM team can understand where and how risk is being introduced and communicate that information to key stake holders not only for remediation but also for reporting and audit purposes.

- ✓ **Improving the bottom line**
  Justifying the cost of a Legit implementation was a simple process for Erik. The platform delivers operational efficiencies for the ASM team and has been proven to be more economically feasible than using people to perform the same mission critical security tasks. In addition, auditing and monitoring requirements are automated to operate in a continuous fashion, which is significantly cheaper and more efficient than allocating highly trained SMEs for periodic manual assessments.

Learn More
Visit our website to book a demo and learn more about the Legit Security Platform: **legitsecurity.com**
Get best practices on software supply chain security from our blog: **legitsecurity.com/blog**
Follow us on LinkedIn for the latest news, events, and content.