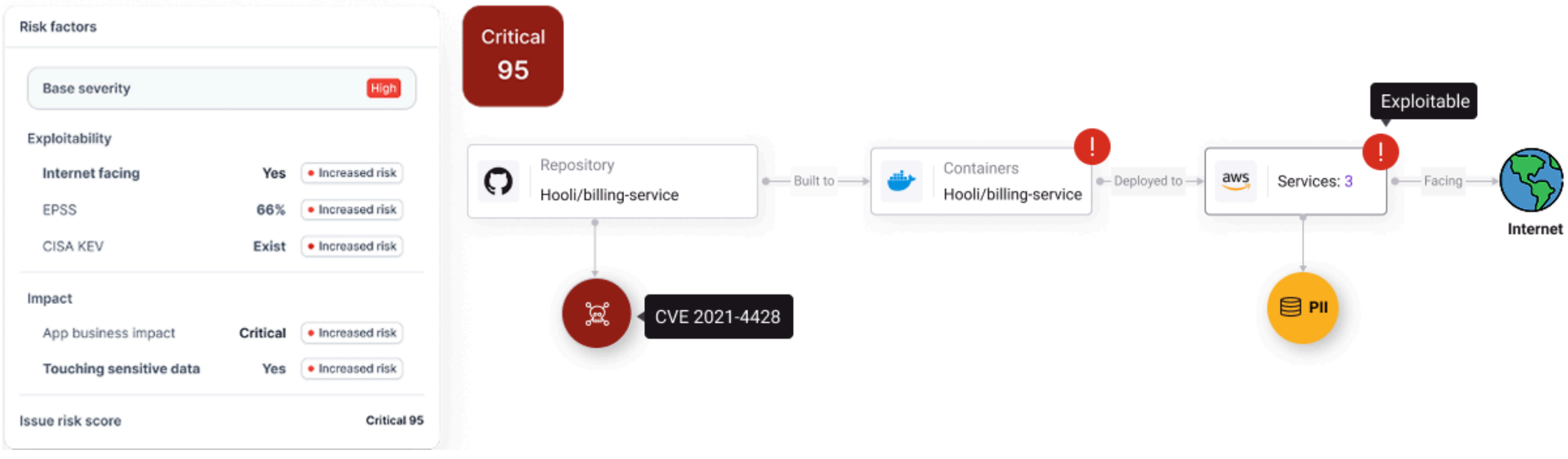
SOLUTION BRIEF

Legit Context

Get deep, insightful visibility into your SDLC and applications, helping you quickly understand risks, prioritize effectively, and drive smarter remediation



Context is key to scaling AppSec programs

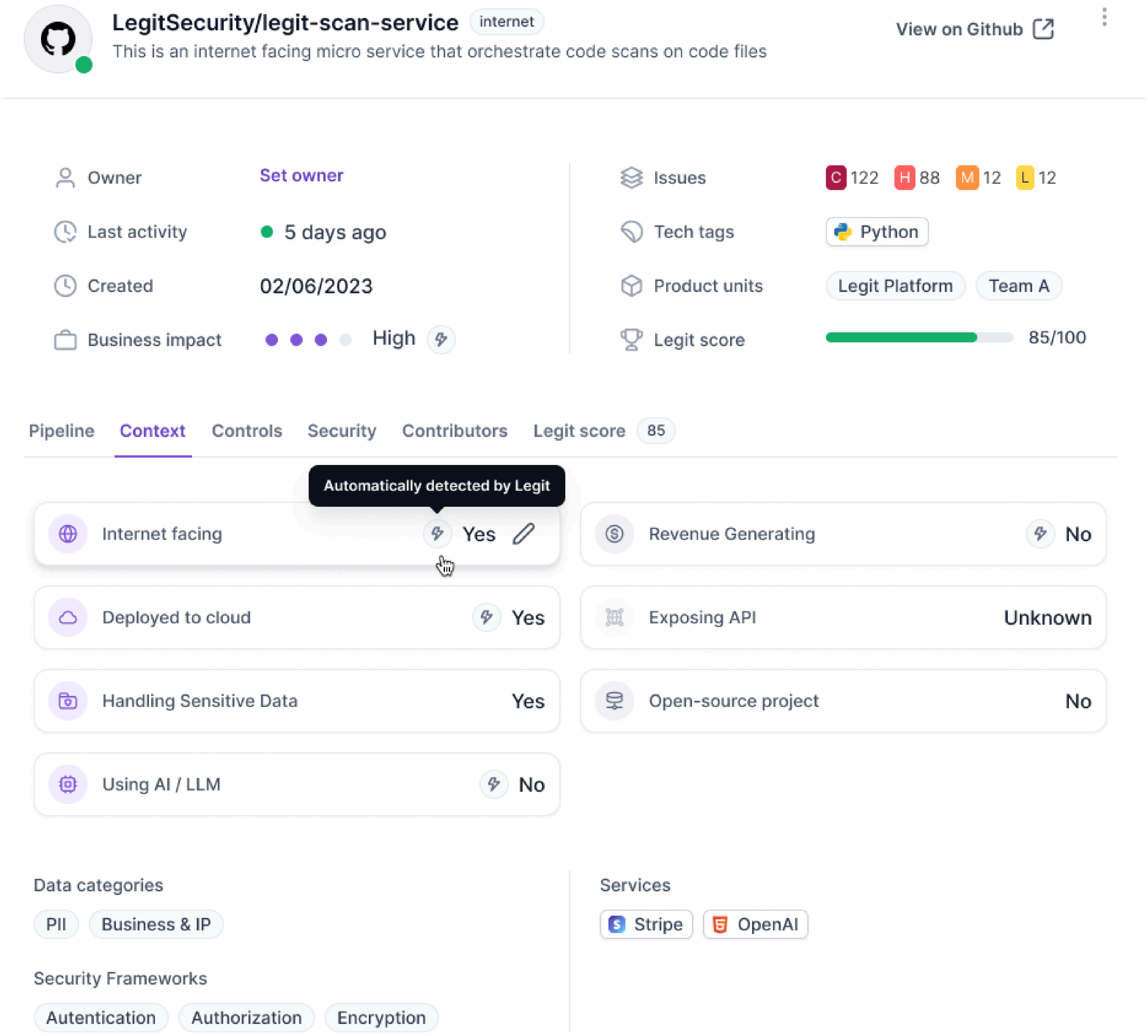
When it comes to securing software, context is key. In modern, cloud-native development, security teams are flooded with AppSec findings, but often lack the insights to determine what to fix and how to fix it effectively. AppSec programs become nothing more than unscalable, siloed backlogs of security risks, leaving security teams with their hands tied.

Relying solely on CVSS scores, for example, can lead to false prioritization, as it fails to reflect an application's true exposure – whether it handles sensitive data, serves as an Internet-facing core customer interface, is protected by a compensating web application firewall (WAF), or perhaps runs in an isolated sandbox with minimal business risk.

Without context, teams struggle to make risk- and business-driven decisions, often fixing the issues that pose little to no real risk, while critical threats remain unaddressed.

Getting the full picture with Legit context

Consider this scenario: You identify a critical vulnerability in your application. At first glance, it seems urgent and requires immediate remediation. But zooming out, you realize the application is not Internet-facing, contains no sensitive data, and is only deployed in a test environment. With this context, you can confidently accept the risk and focus remediation efforts on risks that actually impact the business.



Legit context gives security teams the full picture, connecting the dots to prioritize remediation based on real business impact.

Here's how:

Automatic context detection

Legit now analyzes repositories and applications from code to cloud to automatically assign business impact ratings, from low to critical. By evaluating impact factors such as whether an application is Internet facing, handling sensitive data, leveraging AI, or exposing APIs, Legit sets a baseline risk level that can be adjusted by the user as needed.

Rich, evidence-linked context parameters

Every impact factor is backed by clear, linked evidence. For example, if an application is flagged for handling sensitive data, you can dive directly into the data models or services that triggered the alert.

Impact factors include:

- Internet facing: Verified through CSPM products, build logs, or cloud asset correlations
- Deployed to cloud: Identified through cloud deployment metadata and CSPM tools
- Handling sensitive data: Insights from code-based data models
- Exposing APIs: Direct links to API endpoints and relevant code locations
- Using AI: Detected AI components and services within the application

New inventory items for full visibility

To complete the picture, Legit tracks and manages essential inventory items that shape your application's risk profile:

- Services: Identify third-party services like Stripe or OpenAI through direct code references or dependency analysis
- Data models: Uncover and link to critical data elements in your code
- Frameworks: Understand the security frameworks in play, such as encryption or authentication libraries
- APIs: Detail API endpoints, versions, protocols, and authentication methods

Customizable application catalog for tailor-made risk management

Every organization has unique needs, and Legit lets you tailor your application catalog with custom fields. Whether a "Revenue" field, "Application Tier" indicator, release version, or threat modeling due date, you can define what needs to be considered for your risk assessments.

Additionally, you can assign external users to key roles, such as Security Champion, seamlessly integrating with your workflows and SLA rules.

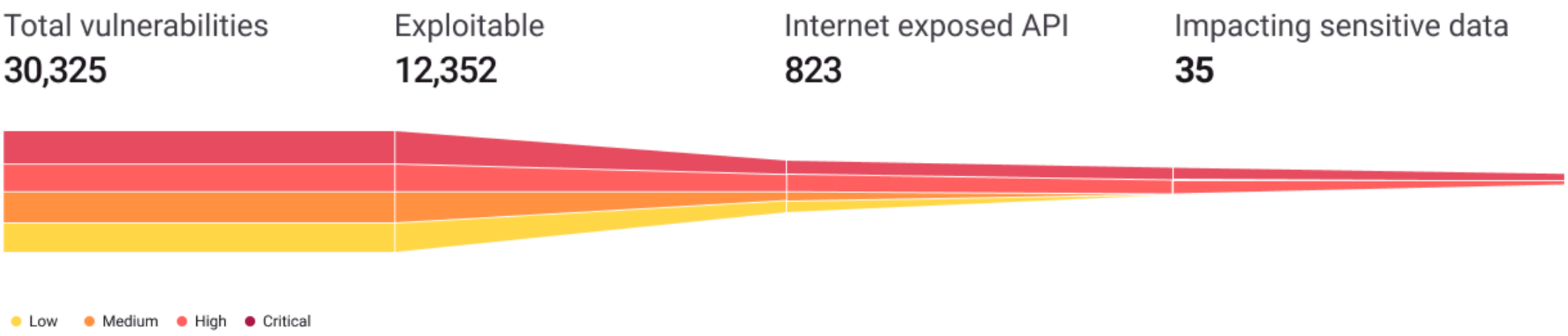
The power of Legit context: Smarter security, faster remediation

Legit context turns raw data into actionable insights, enabling organizations to move from reactive firefighting to proactive security management. By connecting risk-based prioritization and deep contextual awareness, it helps security teams cut through the noise and focus on what truly matters.

Reduce business risk: Focus efforts on vulnerabilities that pose the highest business risk.
Reduce noise and manual investigation with automated context detection and linked evidence.

Prioritize, easily: Reduce noise and manual investigation with smart prioritization, powered by Legit's automated context detection and linked evidence.

Fix faster: Eliminate uncertainty with clear, evidence-backed insights, helping teams fix the right issues without unnecessary delays.



Get more details on ASPM. Contact us to get more information or Request a demo.

Learn More About Legit Security

Visit our website and Book a Demo

About Legit Security

The Legit Security ASPM platform is a new way to manage application security in a world of AI-first development, providing a cleaner way to manage and scale AppSec and address risks. Fast to implement, easy to use, and AI-native, Legit has an unmatched ability to discover and visualize the entire software factory attack surface, including a prioritized view of AppSec data from siloed scanning tools. As a result, organizations have the visibility, context, and automation they need to quickly find, fix, and prevent the application risk that matters most. Spend less time chasing low-risk findings, more time innovating.