LEGIT

SOLUTION BRIEF

Legit Application Security Posture Management

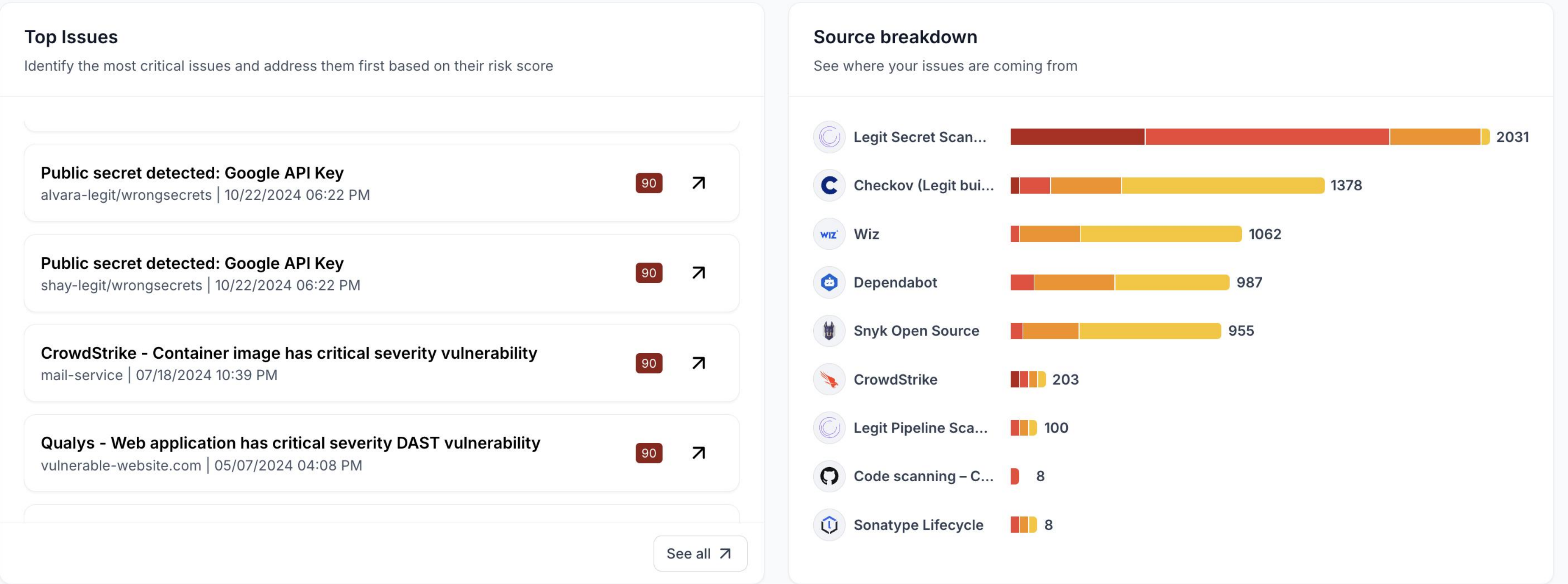
Secure the modern software factory, everywhere

Building a sustainable, scalable AppSec program

The speed and complexity of modern software development have skyrocketed in recent years. Agile, DevOps, and CI/CD methodologies are now the norm, while developer toolchains grow increasingly distributed, spread across sprawling cloud infrastructures and microservices. In turn, today's attack surface has expanded exponentially, rendering legacy scanners and siloed testing tools entirely obsolete.

Legit Security delivers a new, unified solution to see and secure the entire software development lifecycle (SDLC) from one unified ASPM platform. With Legit, not only do security teams gain deep, end-to-end visibility of all their development assets, pipelines, repositories, and cloud services, but they also add granular governance controls, embedding automated guardrails directly into the tools and processes their developers use on a daily basis.

With the Legit ASPM platform, security teams take back control of their software factories with consolidated security signals, AI-powered correlation and prioritization, and seamless, no-code automation and orchestration to proactively prevent emerging threats and surgically remediate the most severe, business-critical issues first.



Top Issues

Identify the most critical issues and address them first based on their risk score

Public secret detected: Google API Key
alvara-legit/wrongsecrets | 10/22/2024 06:22 PM — 90

Public secret detected: Google API Key
shay-legit/wrongsecrets | 10/22/2024 06:22 PM — 90

CrowdStrike - Container image has critical severity vulnerability
mail-service | 07/18/2024 10:39 PM — 90

Qualys - Web application has critical severity DAST vulnerability
vulnerable-website.com | 05/07/2024 04:08 PM — 90

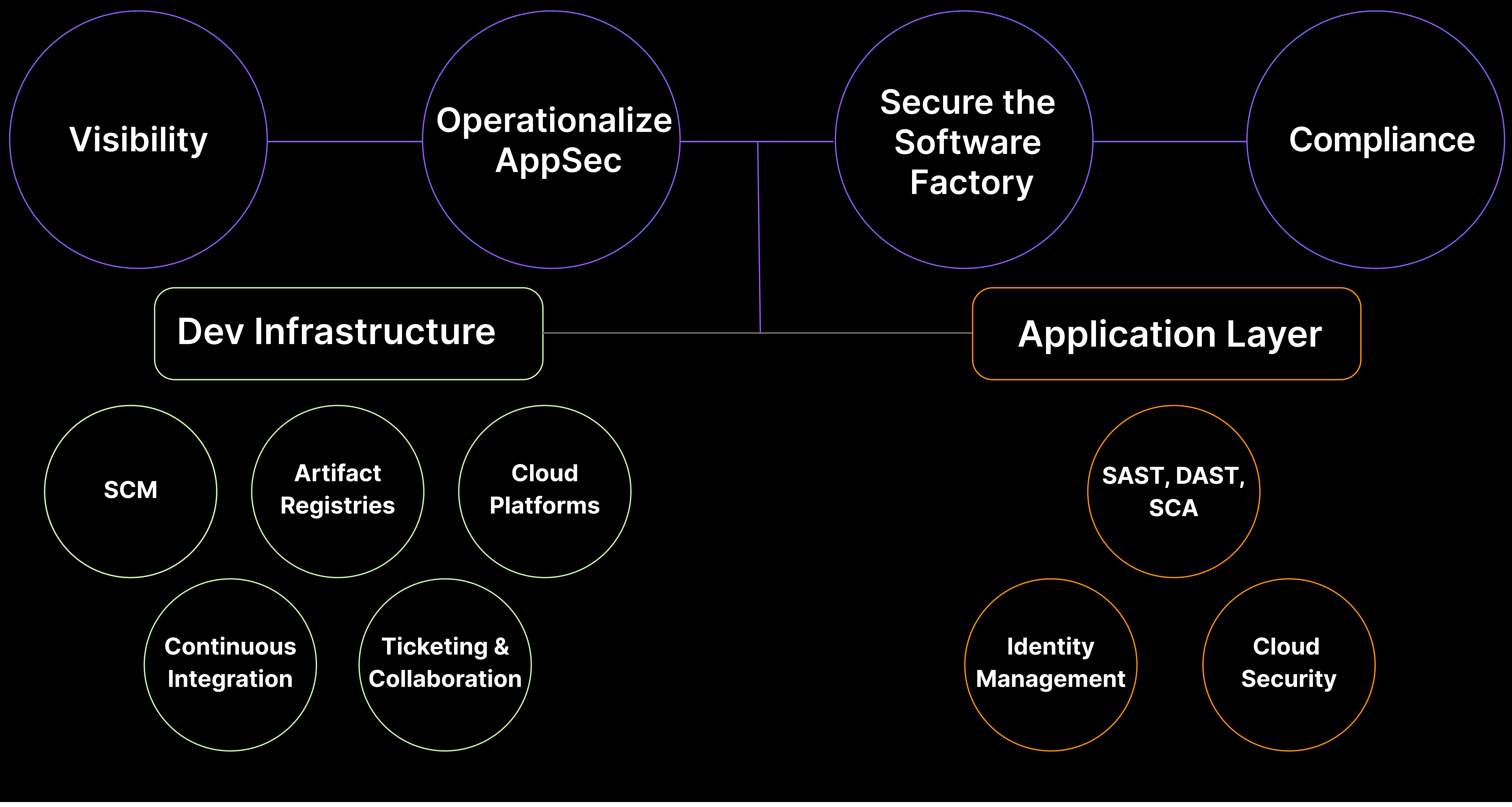
Source breakdown

See where your issues are coming from

Key Features

- Unified AST and AppSec governance
- SDLC and infrastructure-as-code (IaC) security
- Next-gen secrets and source code protection
- Secure-by-design developer guardrails
- Continuous vulnerability and threat exposure management
- DevSecOps automation and remediation
- AI security posture management (AI-SPM)

The Legit ASPM Platform



Visibility

Operationalize AppSec

Secure the Software Factory

Compliance

Dev Infrastructure

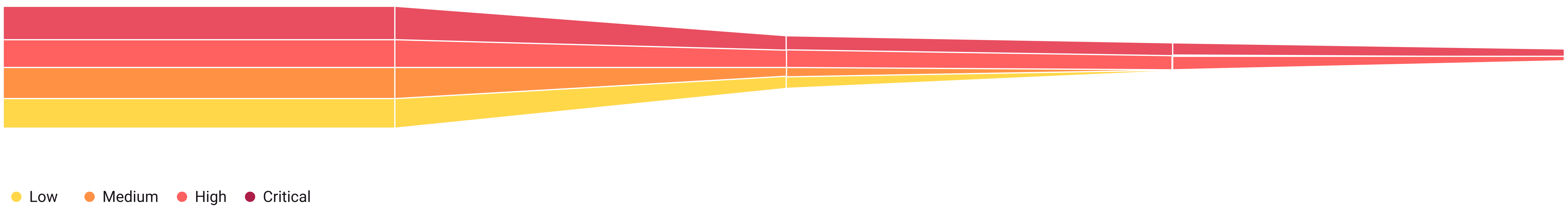
- SCM
- Artifact Registries
- Cloud Platforms
- Continuous Integration
- Ticketing & Collaboration

Application Layer

- SAST, DAST, SCA
- Identity Management
- Cloud Security

Fix what matters most

Total vulnerabilities	Exploitable	API exposed	High business impact
100% (over 1M)	40%	10%	1%



Key Benefits

Protect the entire SDLC

Connect and see everything across your entire developer environment with full visibility, and granular controls and enforcement.

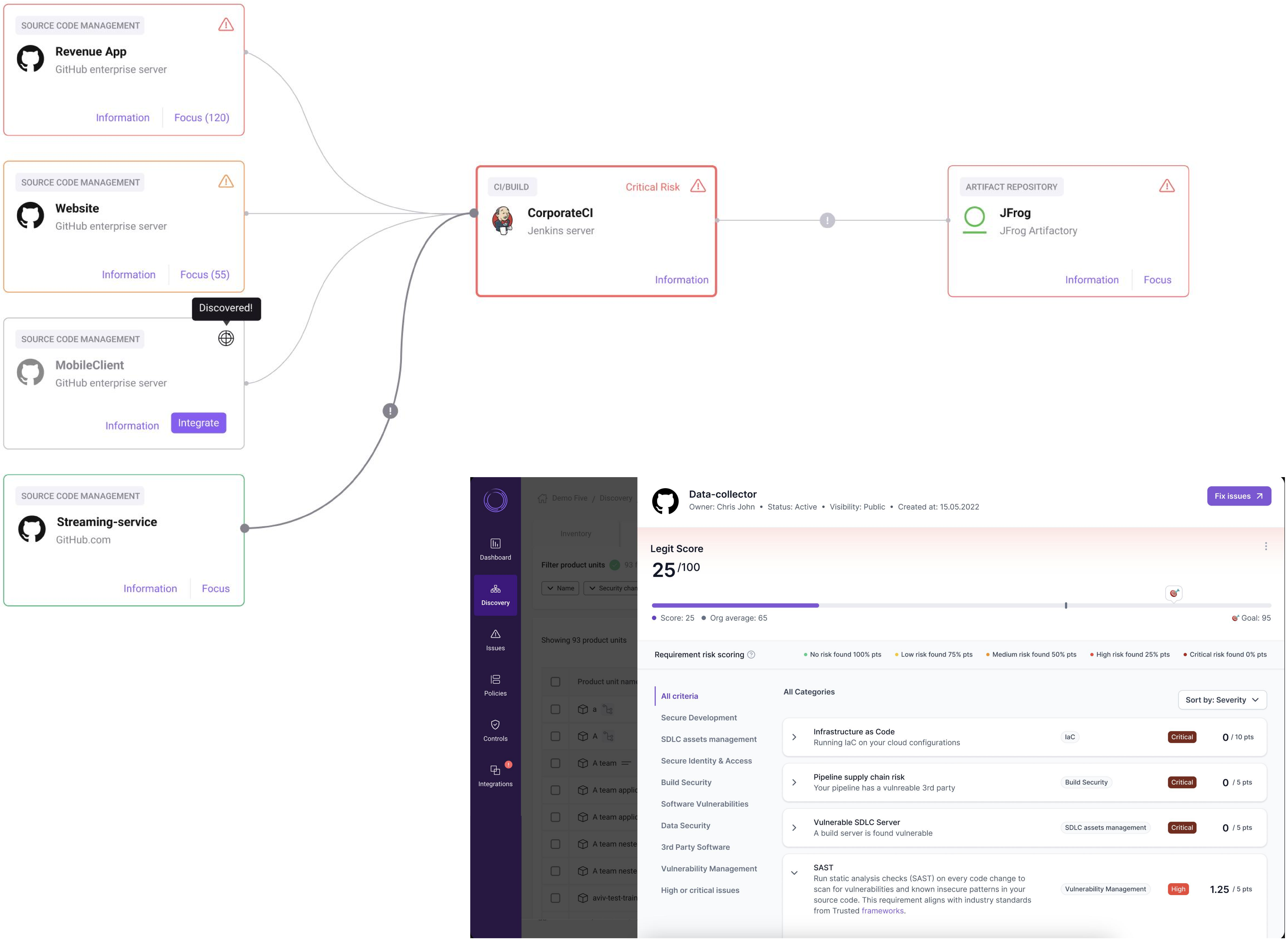
Fix what matters, first

Correlate, prioritize, and surgically remediate the critical risks, vulnerabilities, and misconfigurations that matter most, first.

Drive DevSecOps

Meet developers where they work, embedding security into the tools, ticketing systems, and workflows they use everyday.

The security of your development environment at a glance



Data-collector
Owner: Chris John • Status: Active • Visibility: Public • Created at: 15.05.2022

Legit Score
25 /100

Score: 25 • Org average: 65 • Goal: 95

Requirement risk scoring
● No risk found 100% pts ● Low risk found 75% pts ● Medium risk found 50% pts ● High risk found 25% pts ● Critical risk found 0% pts

All criteria
Secure Development
SDLC assets management
Secure Identity & Access
Build Security
Software Vulnerabilities
Data Security
3rd Party Software
Vulnerability Management
High or critical issues

All Categories
Sort by: Severity

Infrastructure as Code Running IaC on your cloud configurations	IaC	Critical	0 / 10 pts
Pipeline supply chain risk Your pipeline has a vulnreable 3rd party	Build Security	Critical	0 / 5 pts
Vulnerable SDLC Server A build server is found vulnerable	SDLC assets management	Critical	0 / 5 pts
SAST Run static analysis checks (SAST) on every code change to scan for vulnerabilities and known insecure patterns in your source code. This requirement aligns with industry standards from Trusted frameworks.	Vulnerability Management	High	1.25 / 5 pts

The legit foundation of your AppSec program

SDLC Security

- **Granular code-to-cloud context.** Gain end-to-end visibility of the entire developer toolchain to monitor and contextualize risk across repositories, code packages, cloud services, and pipelines throughout the SDLC.
- **Real-time inventory and asset discovery.** Continuously unearth shadow IT and hidden dependencies concealed in your code and running services.
- **IaC security and misconfigurations.** Harden your CI/CD pipelines and preempt posture drift by embedding and enforcing controls earlier in the dev lifecycle before commits are pushed live.

AppSec Governance

- **Dynamic posture management.** Instantly monitor, measure, and score AppSec risks business-wide. Glean critical insights and benchmark posture performance in real-time by user role, team, application, or other segment.
- **Continuous compliance and control mapping.** Expedite reporting and attestation with prebuilt control mapping to important regulations and standards like NIST SSDF, SLSA, SOC II, PCI DSS, FedRAMP, and more.
- **Auto-generated SBOMs in seconds.** Ensure your SBOMs are generated fast and are always up-to-date with granular visibility into every open-source software component.

Secrets Protection

- **Next-gen secrets scanner with 400+ detectors.** Scan everything, everywhere leveraging advanced techniques to continuously unearth hidden and hard-coded secrets far beyond source code across the SDLC.
- **AI-powered detection and noise reduction.** Stop triaging irrelevant alerts, slash your mean-time-to-remediate (MTTR), and eliminate false positives by 86% with Legit's advanced, AI-powered detection and noise reduction.
- **Secure-by-design dev guardrails.** Prevent insecure secrets from leaking and avoid immutable Git history by pre-receiving and pre-pushing your hooks and commits without burdensome controls slowing down dev teams.

Vulnerability Management

- **Prioritize and fix what matters most, first.** Consolidate security findings across all your scanners and tools (i.e., SCA, SAST, DAST, etc.), leveraging AI-driven correlation and risk scoring to fix your most critical issues, first.
- **DevSecOps automation and remediation.** Turn your developers into security champions by equipping them with the tooling, guidance, and automation they need in the systems and workflows they already use.
- **Actionable root-cause and attack path analysis.** Perform complex, multi-variable scenario analyses to anticipate the most likely and easily exploitable attack paths and toxic combinations where your organization could be vulnerable.

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

LEGIT

About Legit Security

Legit is a new way to manage your application security posture for security, product, and compliance teams. With Legit, enterprises get a cleaner, easier way to manage and scale application security and address risks from code to cloud. Built for the modern SDLC, Legit tackles the most challenging problems facing security teams, including GenAI usage, proliferation of secrets, and an uncontrolled dev environment. Fast to implement and easy to use, Legit lets security teams protect their software factory from end to end, gives developers guardrails that let them do their best work safely, and delivers metrics that prove the security program's success. This new approach means teams can control risk across the business – and prove it.