scribe

SOFTWARE SUPPLY CHAIN CONTINUOUS ASSURANCE

Secure Your Software Products, CI/CD Pipelines, and SDLC Processes

Gain full **VISIBILITY** of your software assets and risk

by **SDLC** auto-discovery, **evidence** collection, and **SBOMs**

MITIGATE risks and **PREVENT** attacks in your software factory

by integrating automated **SDLC guardrails-as-code** into the CI/CD

DETECT and **PREVENT** software tampering

by automating continuous code **signing** and **attestations**

Secure The Software Factory and Products Without Compromising Development Speed

Scribe is a comprehensive software supply chain platform for managing SDLC risk and protecting your software factory and products from development to deployment. We have automated all SDLC security and compliance practices (signing, attestations, risk management, prevention, mitigation, compliance, and trust) into the DevOps toolchains, enabling secure-by-design products and protecting the organization from security and liability risks.
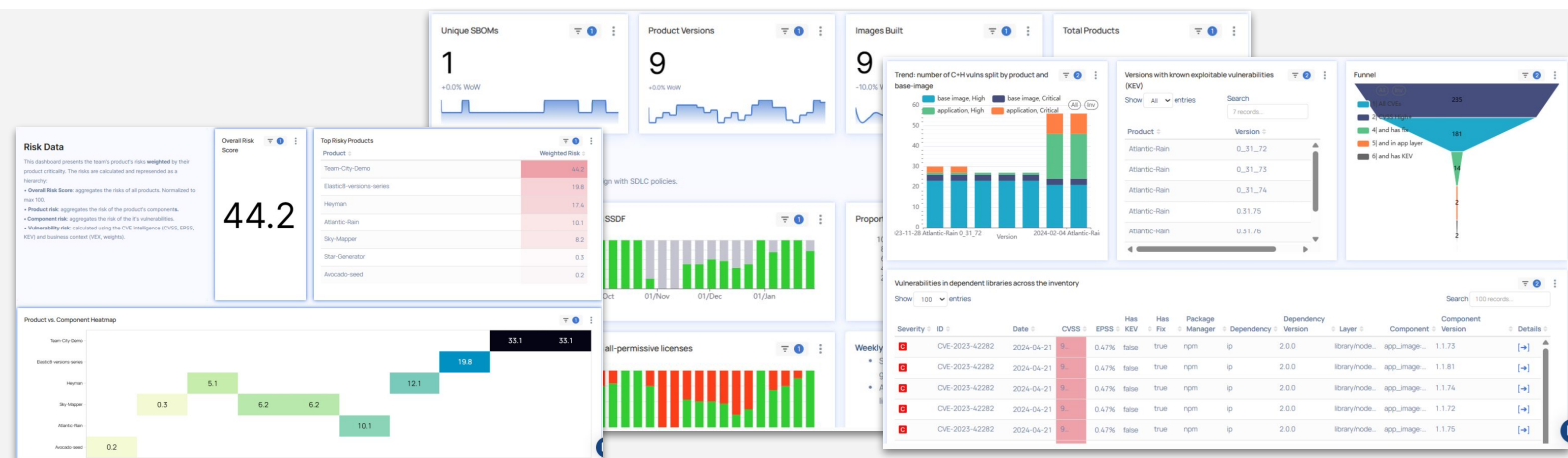
What You Get With Scribe:

✓ **Build & Deploy with Confidence:** Scribe ensures a **secure-by-design** approach, establishing a robust chain-of-custody for your software with seamless code signing and end-to-end verification.

✓ **Proactive SDLC Risk Management** – Scribe detects **vulnerabilities, exploits, and compliance risks**, with AI-driven prioritization, comprehensive analytics and integrations with your entire security ecosystem.

✓ **Centralized SBOM Management** – Scribe auto-generates, ingests, and centralizes **SBOMs** with real-time risk insights. Automate SBOM sharing and vulnerability disclosure to eliminate liability risk.

✓ **Automated Governance & Policy Enforcement**– Scribe enforces **automated guardrails** across your development and deployment pipelines. At build time, deployment, or out-of-band, **policy-as-code framework** ensures SDLC governance that adapts to your security and compliance requirements.

✓ **Effortless Compliance** – Scribe streamlines adherence with industry frameworks like **SLSA, SSDF, and custom security mandates** using prebuilt blueprints and automated evidence collection.

SDLC Assets Discovery and Management

- **Scan** the organization's source code managers, build systems, container registries, and production clusters, to generate **code-to-cloud lineage** of your pipelines.
- **Automatically generate SBOM**, AI-BOM, and various security attestations for every build, straight from the CI pipeline.
- **Harden your software factory** - Fix misconfigurations and close security gaps in your CI/CD tools and infrastructure.

## Vulnerability Management & Incident Response

- **Intelligence feeds**: CVSS, EPSS, KEV, Scorecard, licences.
- **Define relevancy**: layers separation, dependencies, VEX
- **Prioritize risk** using Scribe risk analytics, vulnerability triage, impact analysis of incidents and AI recommendations.
- **Monitor exposure** to new risks through the product's life cycle.
- **Mitigate incidents** based on the audit trail of all SDLC activities.
- **Remediate risks** with Heyman**,** Scribe's **AI-ASPM agent**

Anti-Tampering Software Assurance

- **Protect from attacks** on your CI/CD by hardening them.
- **Validate the integrity and provenance** of code, algorithms, and AI models by integrating continuous code signing.
- **Alert/ block unallowed modifications** to code & CI/CD tools.

Policy Governance, Enforcement, and Compliance

- Set up SDLC policy-as-code guardrails to **govern policy, prevent breaches and deliver secure-by-design products**.
- **Demonstrate compliance** with SLSA, SSDF, EU-CRA, PCI, FDA, DORA, FedRAMP or any other customized requirement.
- **Comply** with SBOM sharing and vulnerability disclosure requirements to **reduce liability risk and gain a Safe Harbor.**
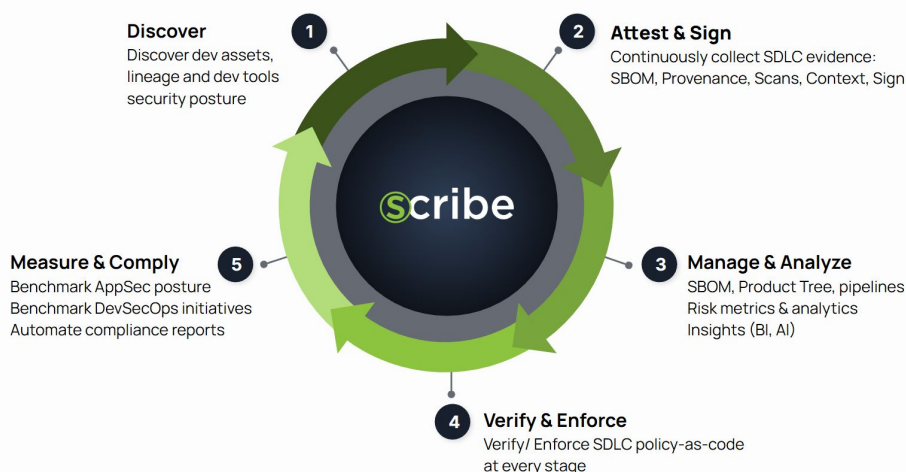
SCRIBE ADVANTAGES:

Full visibility into the assets in the SDLC and their risk posture

Audit trail of all SDLC activities based on machine-readable attestations

Frictionless SDLC governance by automating policy enforcement

Attestation-based compliance with any regulatory requirements and standards

Prevent software tampering by protecting the integrity of software delivery

Share SBOMs, vulnerability disclosures, VEX advisories and security attestations

ABOUT SCRIBE

Scribe was established by seasoned veterans in cyber security and cryptography who shared a vision and mission: a software supply chain security solution that can really protect you.

Recognizing the delicate balance between security and operational efficiency, we understand that every security decision impacts time to market, and ultimately, your revenue. We built a SSCS platform that harnesses modern frameworks and concepts to protect your software factory and secure by design your software products at every stage of their lifecycle, from development to deployment and delivery.

Discover
Discover dev assets, lineage and dev tools security posture

1

2 **Attest & Sign**
Continuously collect SDLC evidence: SBOM, Provenance, Scans, Context, Sign

scribe

Measure & Comply **5**
Benchmark AppSec posture
Benchmark DevSecOps initiatives
Automate compliance reports

3 **Manage & Analyze**
SBOM, Product Tree, pipelines
Risk metrics & analytics
Insights (BI, AI)

4 **Verify & Enforce**
Verify/ Enforce SDLC policy-as-code at every stage