EINPRESSWIRE

Scribe Security Launches Advanced Capabilities to Secure AI/ML-Ops with Continuous Assurance and Guardrails-as-Code Tech

TEL AVIV, ISRAEL, November 12, 2024 /EINPresswire.com/ -- In response to the rapidly growing security needs of the AI/ML industry, Scribe Security, a leader in software supply chain security, has announced new features tailored specifically to protect AI/ML-Ops pipelines. Building on its continuous assurance framework, Scribe now offers, on top of its AI/ML-focused software bill of materials (ML-BOMs), also continuous signing, integrity and provenance verification, and advanced gating capabilities based on its “guardrails-as-code” approach. These features address the unique challenges AI/ML workflows face, including safeguarding complex datasets and models from tampering and ensuring compliance with evolving AI governance standards.

The complexity and value of AI models and datasets make them prime targets for attacks. As companies rapidly adopt AI/ML technologies, they must manage not only security and compliance but also the risks associated with model integrity and provenance. Scribe already provides ML-BOMs—extensions of traditional SBOMs—to provide transparency into AI-specific assets, tracking dependencies, datasets, model architectures, and configurations. This visibility is now bolstered by continuous assurance capabilities, including automated code and model signing, and continuous provenance verification for the datasets and models which ensures that every component in the pipeline is verified for authenticity and integrity.

Guardrails-as-code adds an additional layer of security by embedding policies directly within development workflows. This feature enforces secure AI practices and prevents unauthorized changes to AI/ML pipelines, allowing organizations to automatically detect and block risky alterations in real time.

“Incorporating Scribe’s continuous assurance capabilities and guardrails-as-code into AI/ML-Ops workflows brings an essential level of protection that goes beyond traditional security measures,” said Danny Nebenzahl, Scribe’s CTO. “Companies using our platform can confidently protect their AI models and datasets, ensuring they remain untampered with and compliant from data collection to production. By making ML-BOMs a standard for transparency and trust, we're giving organizations a powerful way to both secure and demonstrate the required transparency of their AI/ML assets."

Scribe's advanced features come at a critical time, as organizations across industries increasingly adopt AI/ML-driven solutions that rely on complex, data-intensive pipelines. These new capabilities empower companies to better manage risks in AI/ML-Ops, providing comprehensive insight and security that scales with the sophistication of their AI models and infrastructure.

With Scribe's new offerings, companies can maintain high levels of security and compliance while reducing the operational burden traditionally associated with AI/ML-Ops protection. This enables secure innovation, protecting the models and data that drive business success in today's AI-powered world.

Lilach BarTal
Scribe Security
544975368398
email us here
Visit us on social media:
LinkedIn
