Scribe Security Empowers AI Companies to Safeguard Their AI Models and MLOps Pipelines

Scribe now generates and validates AI attestations and ML-BOMs, signs and verifies AI models and datasets, and enforces AI policy.

TEL AVIV, ISRAEL, January 17, 2024 /EINPresswire.com/ -- Scribe Security, a renowned software supply chain security leader, proudly announces the newest addition to its software supply chain platform. This new capability marks an important milestone in software supply chain protection, granting users the ability to fortify MLOps pipelines and AI models against potential threats and vulnerabilities.

Attack Stage	Attack Techniques	Scribe's Solution
Attacker Resource Development	Publish Poisoned Datasets Poison Training Data	**Data integrity:** Attest to datasets consumed and verify datasets' source and content. Attest to training data and verify training data content and source.
Initial Access	ML Supply Chain Compromise	**Data and code integrity:** Attest to ML pipeline's data, models, software, and configurations. **ML Pipeline Policy enforcement:** Attest to actions and verify policies accordingly (e.g., release process kit, tests, access patterns).
Initial Access, Impact	Evade ML Model (e.g., crafted requests)	**Accurate pipeline tracking:** Track resources and detect anomalies in ML pipeline access patterns.
Execution	Command and Scripting Interpreter	**Accurate pipeline tracking:** Track resources and detect anomalies in ML pipeline access patterns.
Persistence	Poison Training Data	**Data integrity:** Attest to training data and verify training data content and source.
Persistence, ML Attack Staging	Backdoor ML Model	**Data integrity:** Attest to the ML model lifecycle and verify it.
Impact	System Misuse for External Effect	**System Level Policies:** Attest to system behavior and characteristics and apply policies accordingly (e.g., compute costs, access patterns).

Attack stages table

Scribe Logo

MLOps and AI models are becoming increasingly integral to today's technology landscape, but they are not immune to cyber-attack risks. Scribe Security recognizes the unique challenges that MLOps and AI models present and has developed robust solutions to address them. Attack vectors for MLOps can exploit the distinctive nature of AI model generation, including tactics like inserting biases into models or manipulating them to produce exploitative outcomes.

A first step in addressing the new risks introduced by AI technologies is to have an AI assets inventory - which can be done utilizing ML-BOMs (Machine Learning Bill of Materials). A typical ML-BOM documents the models and datasets used within an AI product, service, or system.

Automating ML-BOM generation is the way to create and maintain an AI asset inventory.

Scribe-Security enables automated ML-BOM management and allows the organization to enforce policies, reducing AI risks.

“Just as in traditional cybersecurity domains, regulations in AI and MLOps are evolving to ensure the trustworthiness and provenance of data, tools, and final outputs. Organizations must now provide assurances about the integrity and impartiality of their AI models.” Daniel Nebenzahl, Scribe's Co-Founder and CTO, explains, "We are now harnessing the power of our omnipotent Valint tool to serve as a policy and integrity verification instrument for MLOps and AI models. Enforcing policy compliance on AI models is a pivotal risk management and reduction strategy."

Scribe Security is aligning its new AI security capabilities with the recent security model introduced by MITRE for MLOps protection. This alignment underlines the company's commitment to staying at the forefront of software supply chain security by ensuring the security of MLOps and AI models on top of its existing protection capabilities of CI/CD pipelines. Scribe's comprehensive suite of tools and technologies is poised to comprehensively protect the evolving landscape of software supply chains.

About Scribe Security
Scribe was established by seasoned cyber security and cryptography veterans who share a common mission: to develop and offer the ultimate, all-encompassing solution for software supply chain security. Drawing on their extensive expertise, they created an innovative platform that harnesses cutting-edge concepts and modern frameworks. The result is a security solution that safeguards the software factory and products at every stage of their lifecycle, from source to delivery. For more information, visit https://scribesecurity.com/

Lilach bartal
G2MTeam
544975368398
lilachbartal@gmail.com
Visit us on social media:
Twitter
LinkedIn
YouTube