Scribe Use Case:

Gaining SDLC Visibility & Control in an M&A Deal with Scribe Security

INVINCIBLE PRODUCT SECURITY

Additional information is available at https://scribesecurity.com/

Use Case: Gaining SDLC Visibility & Control in an M&A Deal with Scribe Security

Background:

In today's fast-evolving threat landscape, mergers and acquisitions in the tech sector come with significant challenges—especially when it comes to understanding and managing the security posture of the acquired company's software supply chain. Recent incidents, such as the supply chain hack detailed in "Hack Supply Chain for 50k," underscore the risks of unmonitored development pipelines and vulnerable SDLC practices.

The Challenge:

When an acquiring company brings in a new business, it must quickly assess and integrate the target's software development lifecycle (SDLC) without disrupting operations. Key challenges include:

- **Limited Visibility:** Manual audits and legacy reporting often fail to capture real-time details of the acquired company's development processes.
- **Unverified Security Practices:** Without a systematic approach, verifying the integrity of build processes and dependency management is cumbersome and error-prone.
- **Compliance Uncertainty:** Ensuring that the acquired company meets industry standards (such as NIST 800-218, OWASP, etc.) and regulatory mandates is critical yet complex under traditional methods.

Scribe Security's Approach:

Scribe Security's attestation-based platform is designed to address these challenges by delivering continuous, automated oversight of the entire SDLC. Here's how Scribe Security can empower an acquirer:

- **Seamless Integration into CI/CD Pipelines:**
  Scribe integrates directly with source control, CI/CD systems, container registries,

and build tools. It continuously collects evidence across every stage of the SDLC—from static code analysis to automated tests and dependency checks.

- **Automated, Machine-Readable Attestations:**
  The platform generates cryptographically signed attestations for each build and release. These immutable records provide a verifiable chain of custody, ensuring that every software component's provenance is tracked and secured.
- **Comprehensive Compliance & Risk Reporting:**
  Scribe produces real-time dashboards and detailed compliance reports that highlight adherence to secure development standards. These insights enable acquirers to quickly pinpoint vulnerabilities, assess risk, and verify that the acquired company's practices meet both internal and regulatory requirements.
- **Enhanced Due Diligence and Integration:**
  With Scribe, the acquiring company gains immediate, actionable insights into the target's SDLC. This visibility not only facilitates a thorough due diligence process but also supports a smooth integration by aligning the acquired company's security practices with the acquirer's governance framework.

Benefits for the Acquirer:

- **Immediate Visibility & Control:** Gain real-time insight into the acquired company's software security practices, enabling swift identification and remediation of risks.
- **Streamlined Compliance:** Leverage automated attestations and detailed compliance reports to satisfy regulatory and internal audit requirements effortlessly.
- **Risk Mitigation:** Reduce exposure to supply chain vulnerabilities by enforcing continuous monitoring and automated policy checks throughout the SDLC.
- **Smooth Post-Merger Integration:** Seamlessly merge the acquired company's development processes into your own security framework, ensuring consistent, organization-wide security standards.

Conclusion:

In an M&A scenario, ensuring the security and integrity of the acquired company's SDLC is paramount. Scribe Security's platform provides the tools needed to gain complete visibility and control over every phase of the software supply chain—from development to deployment. By automating compliance, enhancing due diligence, and streamlining integration, Scribe empowers acquirers to secure their investment and confidently manage risk in a rapidly changing digital landscape.