Case Study

Scribe

Enhancing Software Supply Chain Security

The company is a global provider of critical information systems for academic institutions. Their software plays a crucial role in managing sensitive academic and administrative data, making security and trust fundamental to their operations.

THE CHALLENGE:

Restoring Trust After a Severe Supply Chain Breach

The organization faced a significant cybersecurity breach caused by a software supply chain attack, leading to the theft of sensitive customer data. Given their reliance on legacy enterprise codebases and on-premise software deployments, they needed to rebuild customer trust by demonstrating the highest levels of software supply chain (SSC) integrity. Their software update process—delivered via self-extracting zip files—needed to be modernized for tamper resilience and compliance with evolving security standards.

THE SCRIBE SECURITY SOLUTION:

Implementing Next-Gen Software Integrity

Following a rapid onboarding analysis with the core DevOps team, Scribe identified three key objectives for the security overhaul:

1. **Enhance software update distribution** to ensure tamper resilience
2. **Increase transparency** in software composition by verifying all components
3. **Provide signed evidence** of a trustworthy build process through SLSA-L2 compliance

Implementation Steps & Achievements

1. **Tamper-Resilient Software Updates**
   - Scribe deployed its Valint CLI tool on the build server, generating signed Software Bills of Materials (SBOMs) at multiple build stages.

- Secure Public Key Infrastructure (PKI) was implemented, with private keys stored safely in an Azure Key Vault.
- Customers were provided with a command-line tool to independently verify software authenticity using a zero-trust model.
- Software updates now included both the updated application files and signed SBOMs, allowing customers to validate integrity before installation.

2 **Full Transparency in Software Composition**

- By collecting SBOMs at different build pipeline stages, full visibility of both direct and indirect dependencies in their software were achieved.
- An Aggregated SBOM and Vulnerability Disclosure Report (VDR) were generated, offering customers a clear view of potential security risks.
- Vulnerability Exploitability Exchange (VEX) advisories enabled the company to assess and communicate the real-world exploitability of security vulnerabilities.

3 **Building Trust Through SLSA-L2 Compliance**

- By collecting SBOMs at different build pipeline stages, full visibility of both direct and indirect dependencies in their software were achieved.
- An Aggregated SBOM and Vulnerability Disclosure Report (VDR) were generated, offering customers a clear view of potential security risks.
- Vulnerability Exploitability Exchange (VEX) advisories enabled the company to assess and communicate the real-world exploitability of security vulnerabilities.

RESULTS:

Restored Customer Confidence & Comprehensive Compliance

- **Customer Confidence:** Client confidence was fully restored by demonstrating transparency and security across its software development lifecycle.
- **Comprehensive Compliance:** The company achieved full SLSA Level 2 compliance, ensuring continuous visibility and control over the integrity of their build process.
- **Improved Security & Efficiencies:** Enabled faster, more secure software updates which reduced the risk of future breaches, while improving operational efficiency.
- **Scalable Framework:** Provided a scalable, tamper-proof software development framework that can be extended to other products and markets.

This case study demonstrates how Scribe's software supply chain security solutions empower software vendors to proactively address supply chain risks, meet compliance standards, differentiate themselves in a security-conscious market, and build client confidence and trust.