Scribe Use Case:

Empowering Digital Operational Resilience in Financial Services

Software Supply Chain Security in Compliance with DORA

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

Empowering Digital Operational Resilience in Financial Services

How Scribe Security Ensures Secure Software Development Lifecycle Assurance and Software Supply Chain Security in Compliance with DORA

Executive Summary

The Digital Operational Resilience Act (**DORA**) sets a new standard for the financial sector by mandating rigorous operational, cybersecurity, and software supply chain practices. This white paper explains how the Scribe Security platform addresses key DORA requirements—specifically those related to secure software development lifecycle (SDLC) assurance and software supply chain security. Through continuous, automated attestations, integration with DevOps toolchains, and comprehensive evidence generation, Scribe Security enables financial institutions to achieve and maintain digital operational resilience while streamlining compliance.

Introduction

Financial services organizations face increasing pressure to secure their digital ecosystems against rapidly evolving cyber threats. DORA, the Digital Operational Resilience Act, aims to protect these institutions by requiring robust ICT risk management, secure SDLC practices, and enhanced software supply chain security. As financial institutions increasingly rely on digital solutions, ensuring that every software component is developed, tested, and deployed securely is paramount.

Scribe Security offers a holistic solution by automating security controls throughout the SDLC, ensuring that every release meets rigorous security standards, and providing verifiable, machine-readable evidence of compliance. This white paper details how Scribe

Security helps organizations in the financial sector not only comply with DORA but also build a resilient, secure software foundation.

Overview of DORA and Its Relevance to Financial Institutions

DORA Objectives:

- **Resilience Against Cyber Threats:** Ensure that financial entities can withstand and quickly recover from ICT-related incidents.
- **Secure Software Development:** Mandate secure SDLC practices, including continuous risk assessment and proactive vulnerability management.
- **Supply Chain Security:** Require transparency and accountability in the software supply chain to mitigate risks associated with third-party dependencies and integrations.

Key Challenges Addressed by DORA:

- **Fragmented Security Practices:** Traditional security approaches often focus on isolated vulnerabilities, failing to address the entire software lifecycle.
- **Complex Supply Chains:** Financial institutions rely on multiple vendors and open-source components, creating numerous potential entry points for attackers.
- **Compliance and Reporting:** Meeting regulatory standards requires continuous monitoring and evidence-based reporting, which is both resource-intensive and error-prone when done manually.

Scribe Security's Approach to DORA Compliance

Scribe Security's platform is engineered to support the stringent requirements of DORA by embedding security directly into the SDLC and across the software supply chain. Key features include:

1. Automated Attestations Across the SDLC

- **Continuous Evidence Generation:**
  Scribe Security integrates seamlessly with CI/CD pipelines, automatically capturing and signing security evidence at each development stage. For example, every code

commit, build artifact, and dependency update is accompanied by a cryptographically signed attestation—ensuring that no step is overlooked.

- **Machine-Readable Attestations:**
  By converting security and compliance data into machine-readable formats, Scribe enables automated, scalable reviews and audits. This directly supports DORA's requirement for verifiable evidence of secure software practices.

2. Holistic Software Supply Chain Security

- **Comprehensive SBOM Generation:**
  Scribe produces multi-stage Software Bill of Materials (SBOMs) that document all components, dependencies, and third-party integrations. This transparency is critical for identifying and mitigating risks throughout the software supply chain.
- **End-to-End Provenance Tracking:**
  The platform provides continuous code signing and in-toto attestations, ensuring that every software component's origin and integrity are verifiable. This level of detail supports rapid incident response and remediation efforts, in line with DORA's security mandates.

3. Integration of Security into DevOps (Guardrails-as-Code)

- **Embedded Compliance Controls:**
  Scribe's platform automates compliance-as-code guardrails, which enforce mandatory SDLC security controls. For instance, if a code change fails to meet predefined security thresholds, it is automatically halted, preventing non-compliant software from reaching production.
- **Real-Time Risk Mitigation:**
  By continuously monitoring the development pipeline, Scribe helps financial institutions preemptively mitigate risks. Any deviation from secure development practices triggers immediate alerts, ensuring that vulnerabilities are addressed before they become systemic issues.

4. Evidence-Based Reporting for Audits and Compliance

- **Automated Compliance Reports:**
  Scribe generates comprehensive, evidence-based reports that demonstrate adherence to both internal security policies and external regulatory frameworks such as DORA. These reports include detailed logs of security attestations, SBOMs, and vulnerability remediation actions.

- **Audit-Ready Documentation:**
  Financial institutions can easily provide auditors with a complete, immutable trail of security evidence. This not only simplifies the audit process but also builds confidence among regulators regarding the organization's resilience against cyber threats.

Real-World Examples

Example 1: Securing a Financial Institution's Trading Platform
A leading bank integrated Scribe Security into its CI/CD pipeline to secure its primary product. Each software release was accompanied by a multi-stage SBOM and cryptographically signed attestations covering code integrity, provenance, dependency management, and vulnerability management. This approach enabled the bank to meet stringent SDLC requirements for secure software development and provided auditors with clear, machine-readable evidence of compliance.

Example 2: Enhancing Third-Party Risk Management
A multinational F500 financial services firm used Scribe to manage software supply chain risks associated with first-party and third-party vendor components. By automating the generation of comprehensive SBOMs and continuous provenance tracking, the firm was able to quickly identify vulnerabilities, perform impact analysis, and initiate the remediation process, ensuring that all third-party software met strict security criteria.

Benefits for Financial Services Organizations

- **Enhanced Operational Resilience:**
  Continuous monitoring and automated compliance measures ensure that potential vulnerabilities are addressed in real-time, reducing the risk of disruptions.
- **Streamlined Audit Processes:**
  With machine-readable attestations and comprehensive evidence-based reporting, meeting regulatory audit requirements becomes efficient and less resource-intensive.
- **Improved Risk Management:**
  Automated guardrails and real-time alerts empower organizations to proactively mitigate risks, ensuring that only secure, compliant software reaches production.

- **Scalable Compliance:**
  As digital operations expand, Scribe's platform scales with your organization—ensuring consistent security and compliance across all software assets.

Conclusion

DORA mandates that financial institutions adopt robust security practices to protect their digital infrastructures. Scribe Security meets these demands by embedding security into every phase of the SDLC and providing comprehensive software supply chain security. Scribe empowers financial services organizations to achieve digital operational resilience through SBOM generation, collection and management, automated SDLC security signed attestations, continuous software supply chain compliance reporting, and integration of security guardrails into DevOps that allow delivering secure-by-design software. By leveraging Scribe, institutions not only comply with DORA but also build a secure, trustworthy foundation for future innovation.

For further information, see https://scribesecurity.com/