Training Course on Supply Chain Integrity and Software Bill of Materials Forensics

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's interconnected global economy, **supply chain integrity** has become a paramount concern for businesses and governments alike. The increasing reliance on complex, multi-tiered supply chains, coupled with the rise of sophisticated cyber threats, necessitates a proactive approach to securing the entire software development lifecycle. This comprehensive training course delves into the critical intersection of supply chain security and **Software Bill of Materials (SBOM) forensics**, equipping professionals with the essential knowledge and practical skills to identify, mitigate, and respond to vulnerabilities and attacks across the software supply chain. Participants will gain deep insights into emerging threats, regulatory compliance, and best practices for ensuring **software transparency** and resilience.

The proliferation of open-source components and third-party software in modern applications has introduced a new frontier of **cyber risk** within the **software supply chain**. A single compromised component can have a ripple effect, impacting numerous organizations and critical infrastructure. Training Course on Supply Chain Integrity and Software Bill of Materials Forensics emphasizes the importance of **SBOM** as a fundamental tool for achieving **software assurance** and enabling effective **vulnerability management**. Through hands-on exercises and real-world **case studies**, attendees will learn to leverage SBOMs for forensic analysis, incident response, and proactive risk mitigation, ultimately strengthening their organization's overall **cybersecurity posture** and fostering **digital trust**.

Programme Curriculum

Training Course on Supply Chain Integrity and Software Bill of Materials Forensics

Introduction

In today's interconnected global economy, **supply chain integrity** has become a paramount concern for businesses and governments alike. The increasing reliance on complex, multi-tiered supply chains, coupled with the rise of sophisticated cyber threats, necessitates a proactive approach to securing the entire software development lifecycle. This comprehensive training course delves into the critical intersection of supply chain security and **Software Bill of Materials (SBOM) forensics**, equipping professionals with the essential knowledge and practical skills to identify, mitigate, and respond to vulnerabilities and attacks across the software supply chain. Participants will gain deep insights into emerging threats, regulatory compliance, and best practices for ensuring **software transparency** and resilience.

The proliferation of open-source components and third-party software in modern applications has introduced a new frontier of **cyber risk** within the **software supply chain**. A single compromised component can have a ripple effect, impacting numerous organizations and critical infrastructure. Training Course on Supply Chain Integrity and Software Bill of Materials Forensics emphasizes the importance of **SBOM** as a fundamental tool for achieving **software assurance** and enabling effective **vulnerability management**. Through hands-on exercises and real-world **case studies**, attendees will learn to leverage SBOMs for forensic analysis, incident response, and proactive risk mitigation, ultimately strengthening their organization's overall **cybersecurity posture** and fostering **digital trust**.

Course Duration

5 days

Course Objectives

Upon completion of this training, participants will be able to:

1. Master the principles of secure software supply chain management and cyber resilience.
2. Analyze and mitigate emerging supply chain attack vectors and threat intelligence.
3. Generate, consume, and verify robust Software Bill of Materials (SBOMs) using industry-standard formats (e.g., SPDX, CycloneDX).
4. Perform deep dive forensic analysis of compromised software components leveraging SBOM data.
5. Identify and remediate zero-day vulnerabilities and known exploits within software dependencies.
6. Implement DevSecOps practices to embed security throughout the software development lifecycle (SDLC).
7. Understand and comply with evolving software supply chain security regulations and compliance frameworks (e.g., NIST, ISO 27001, CRA).
8. Develop robust incident response plans and digital forensics methodologies specific to supply chain breaches.
9. Utilize Software Composition Analysis (SCA) tools and Application Security Testing (AST) techniques for proactive risk identification.
10. Assess and manage third-party vendor risk and establish secure procurement practices.
11. Leverage blockchain for supply chain transparency and immutable audit trails.
12. Apply AI and machine learning in threat detection and vulnerability prioritization within the software supply chain.
13. Build a culture of security by design within their organizations, promoting secure coding practices.

Organizational Benefits

- Proactively identifies and mitigates risks, reducing the likelihood and impact of supply chain attacks.
- Gains deep visibility into software components, ensuring authenticity and integrity.
- Meets evolving governmental and industry mandates for software supply chain security.
- Minimizes downtime and recovery efforts associated with security incidents.
- Builds confidence among customers, partners, and stakeholders in the security of their software products.
- Equips teams with the skills to rapidly detect, analyze, and contain supply chain breaches.
- Demonstrates a commitment to advanced cybersecurity practices in a rapidly evolving threat landscape.
- Enables more effective prioritization of security efforts based on comprehensive risk assessments.

Target Audience

1. Cybersecurity Analysts and Engineers.
2. Software Developers and Architects
3. DevSecOps Engineers
4. Incident Response Teams
5. IT and Security Managers
6. Procurement and Supply Chain Managers.
7. Quality Assurance and Compliance Officers
8. Digital Forensics Investigators

Course Outline

Module 1: Fundamentals of Supply Chain Security and Cyber Risk

- Understanding the modern software supply chain ecosystem and its complexities.
- Identifying key **threat actors** and their motivations in supply chain attacks.
- Exploring historical **supply chain attack case studies** and their impact.
- Introduction to **supply chain risk management (SCRM)** frameworks and best practices.
- The evolving regulatory landscape and its implications for software supply chain security
- **Case Study:** Analysis of the SolarWinds attack, focusing on how compromised software updates cascaded through numerous organizations, and lessons learned for supply chain defense.

Module 2: Introduction to Software Bill of Materials (SBOM)

- Definition, purpose, and benefits of a **Software Bill of Materials (SBOM)**.
- Key elements and data points required for a comprehensive SBOM.
- Overview of **SBOM formats** (SPDX, CycloneDX, SWID) and their applications.
- Strategies for **generating and consuming SBOMs** throughout the software lifecycle.
- The role of SBOMs in achieving **software transparency** and **vulnerability disclosure**
- **Case Study:** Examining how an organization could have leveraged an SBOM to quickly identify affected systems and components during a hypothetical open-source library vulnerability disclosure.

Module 3: SBOM Generation and Management Techniques

- Practical tools and techniques for **automated SBOM generation**
- Integrating SBOM generation into **CI/CD pipelines** for continuous security.
- Challenges in SBOM creation, maintenance, and addressing **false positives**.

- Best practices for **version control** and updating SBOMs for dynamic software.
- Leveraging SBOMs for effective **software asset management** and inventory
- **Case Study:** Implementing an automated SBOM generation process in a simulated development environment and analyzing the resulting data for compliance and risk.

Module 4: Software Component Vulnerability Management

- Understanding the lifecycle of **software vulnerabilities** and **Common Vulnerabilities and Exposures (CVEs)**.
- Techniques for **vulnerability scanning** and **Software Composition Analysis (SCA)**.
- Prioritizing and **remediating vulnerabilities** identified through SBOMs.
- Managing **open-source software risks** and license compliance.
- The importance of **security patching** and **supply chain hygiene**.
- **Case Study:** Analyzing a real-world vulnerability found in a popular open-source library and using an SBOM to identify all affected applications within a fictional organization.

Module 5: Digital Forensics in Supply Chain Compromise

- Principles of **digital forensics** applied to software supply chain incidents.
- Techniques for **data acquisition** and **preservation** in compromised environments.
- Tools and methodologies for **malware analysis** and **reverse engineering** of suspicious components.
- Tracing **attack paths** and identifying **indicators of compromise (IOCs)** within the supply chain.
- Reconstructing events and building a **timeline of compromise** for post-incident analysis.
- **Case Study:** A simulated incident response scenario involving a backdoored software update, requiring forensic analysis to determine the origin and extent of the compromise.

Module 6: Advanced SBOM Forensics and Analysis

- Deep dive into **SBOM data analysis** for uncovering hidden dependencies and anomalies.
- Using **graph databases** and **visualization tools** for complex SBOM relationships.
- Identifying **supply chain tampering** and integrity violations through SBOM discrepancies.
- Techniques for **attestation** and verifying the authenticity of software components.
- Developing custom scripts and tools for advanced **SBOM forensic investigations**.
- **Case Study:** Forensic examination of a suspected tampered SBOM, identifying inconsistencies and evidence of malicious modification.

Module 7: Secure Software Development and DevSecOps

- Embedding **security by design** principles throughout the **SDLC**.
- Implementing **DevSecOps** practices for continuous security integration.
- Utilizing **Static Application Security Testing (SAST)** and **Dynamic Application Security Testing (DAST)**.
- Secure coding practices and **threat modeling** for robust software.
- Building a **culture of security awareness** among development teams.
- **Case Study:** Analyzing a fictional software project's DevSecOps pipeline to identify security gaps and propose improvements based on secure coding and testing methodologies.

Module 8: Regulatory Compliance and Future Trends

- In-depth review of key **software supply chain security regulations** (e.g., US Executive Order 14028, EU Cyber Resilience Act).

- Best practices for achieving and demonstrating **compliance**.
- Emerging technologies and trends in **supply chain security** (e.g., **AI/ML for threat detection**, **blockchain for traceability**, **confidential computing**).
- The future of **software assurance** and the evolving role of SBOMs.
- Developing a **long-term strategy** for continuous supply chain integrity.
- **Case Study:** A mock compliance audit, where participants must demonstrate their organization's adherence to specific SBOM and supply chain security regulations.

Training Methodology

This training course will utilize a highly interactive and practical approach, combining:

- **Expert-Led Lectures and Discussions:** Engaging presentations by industry specialists with Q&A sessions.
- **Hands-on Labs and Exercises:** Practical application of tools and techniques in a simulated environment.
- **Real-World Case Studies:** In-depth analysis of actual supply chain security incidents and their resolutions.
- **Group Activities and Debates:** Fostering collaborative learning and diverse perspectives.
- **Interactive Demonstrations:** Showcasing the capabilities of various SBOM, forensic, and security tools.
- **Scenario-Based Simulations:** Putting theoretical knowledge into practice through realistic incident response drills.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com