Software Supply-Chain Risk Management Training Course

Professional Development Training Course Outline

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

Course Introduction

The modern software landscape is defined by its deep reliance on third-party components, particularly vast ecosystems of Open Source Software (OSS). This reliance, while enabling rapid innovation, has fundamentally expanded the attack surface, transforming the Software Supply Chain (SSC) into a primary target for sophisticated threat actors. High-profile incidents like SolarWinds and the XZ Utility Backdoor demonstrate that compromising a single, trusted link whether a third-party vendor, a build environment, or a popular open-source library can lead to catastrophic, cascading breaches across thousands of organizations. The current state demands a shift from reactive vulnerability patching to a proactive, security-by-design approach. Organizations are now struggling with a fundamental lack of visibility into their dependencies, a surge in malicious packages and typosquatting, and the imperative to comply with rapidly evolving mandates for transparency and integrity, notably the generation and consumption of the Software Bill of Materials (SBOM).

Software Supply-Chain Risk Management Training Course is critical for embedding cyber-resilience throughout the entire Software Development Life Cycle (SDLC). It moves beyond traditional perimeter defenses to focus on securing the very process of software creation, integration, and delivery. Participants will master essential security controls, including automated Software Composition Analysis (SCA), Artifact Verification, Code Integrity validation, and the implementation of robust CI/CD pipeline hardening techniques. By adopting a Zero Trust model applied to the supply chain and leveraging continuous Threat Modeling, students will gain the expertise to not only identify and mitigate current risks but also to establish a sustainable, auditable, and secure DevSecOps culture that meets regulatory requirements and safeguards against the inevitable future of AI-generated code vulnerabilities.

Programme Curriculum

Software Supply-Chain Risk Management Training Course

Introduction

The modern software landscape is defined by its deep reliance on third-party components, particularly vast ecosystems of Open Source Software (OSS). This reliance, while enabling rapid innovation, has fundamentally expanded the attack surface, transforming the Software Supply Chain (SSC) into a primary target for sophisticated threat actors. High-profile incidents like SolarWinds and the XZ Utility Backdoor demonstrate that compromising a single, trusted link whether a third-party vendor, a build environment, or a popular open-source library can lead to catastrophic, cascading breaches across thousands of organizations. The current state demands a shift from reactive vulnerability patching to a proactive, security-by-design approach. Organizations are now struggling with a fundamental lack of visibility into their dependencies, a surge in malicious packages and typosquatting, and the imperative to comply with rapidly evolving mandates for transparency and integrity, notably the generation and consumption of the Software Bill of Materials (SBOM).

Software Supply-Chain Risk Management Training Course is critical for embedding cyber-resilience throughout the entire Software Development Life Cycle (SDLC). It moves beyond traditional perimeter defenses to focus on securing the very process of software creation, integration, and delivery. Participants will master essential security controls, including automated Software Composition Analysis (SCA), Artifact Verification, Code Integrity validation, and the implementation of robust CI/CD pipeline hardening techniques. By adopting a Zero Trust model applied to the supply chain and leveraging continuous Threat Modeling, students will gain the expertise to not only identify and mitigate current risks but also to establish a sustainable, auditable, and secure DevSecOps culture that meets regulatory requirements and safeguards against the inevitable future of AI-generated code vulnerabilities.

Course Duration

5 days

Course Objectives

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

1. Map and obtain deep Visibility into multi-tiered software supply chains, including all transitive dependencies.
2. Analyze, generate, and consume Software Bill of Materials in standard formats for Compliance and risk analysis.
3. Implement and enforce Code Integrity controls using digital signatures and secure artifact verification processes.
4. Apply Threat Modeling techniques specifically to the CI/CD Pipeline to identify and mitigate high-impact attack vectors.
5. Differentiate between and secure against various modern attacks: Dependency Confusion, Typosquatting, and Malicious Packages.
6. Harden Build Systems and Source Code Repositories using principles of Least Privilege and secure configuration management.
7. Integrate Software Composition Analysis (SCA) and Static Application Security Testing (SAST) tools early in the SDLC (Shift Left).
8. Design an effective Vulnerability Exploitability eXchange (VEX) program to manage and communicate vulnerability status efficiently.
9. Establish Continuous Monitoring and logging across the supply chain to detect anomalous and suspicious activity in real-time.
10. Implement a supply chain-focused Zero Trust architecture, specifically for developer and system access.

11. Interpret and ensure adherence to key regulatory frameworks, including NIST Secure Software Development Framework (SSDF) and Executive Order 14028.
12. Develop and practice a comprehensive Software Supply Chain Incident Response plan using real-world scenarios.
13. Evaluate and manage the security posture of Third-Party Vendors and outsourced development partners.

Target Audience

1. DevSecOps Engineers/Architects
2. Application Security (AppSec) Managers
3. Software Engineers/Developers
4. Cybersecurity Risk Analysts
5. CISO/CTO and Technology Leadership
6. Security Auditors and Compliance Officers
7. Supply Chain/Procurement Managers
8. Cloud Security Engineers

Course Modules

Module 1: Understanding the Software Supply Chain Threat Landscape

- Code, Dependencies, Build Tools, CI/CD, Deployment.
- From direct breaches to supply chain poisoning.
- Malicious Packages, Transitive Dependencies, Typosquatting, CI/CD Pipeline Attacks.
- Case Study: The XZ Utility Backdoor.
- Mapping your critical supply chain assets and identifying the riskiest links.

Module 2: Dependency and Open Source Risk Management

- Fundamentals of Software Composition Analysis (SCA) tooling and its limitations.
- Managing Vulnerability Management for Open Source Software (OSS) at scale.
- Best practices for dependency approval, version pinning, and repository trust.
- Open Source Vulnerabilities (OSV), VEX (Vulnerability Exploitability eXchange), Dependency Management Policy.
- Case Study: Log4j (Log4Shell).

Module 3: Software Bill of Materials (SBOM) and Transparency

- The purpose, utility, and standards of SBOM
- Automating SBOM generation and validation within the build process.
- Consuming and analyzing third-party SBOMs for risk exposure and license compliance.
- SBOM Generation, Attestation, Digital Signature, Data Integrity.
- Case Study: Executive Order 14028 Requirements.

Module 4: CI/CD Pipeline and Build System Hardening

- Reproducible Builds and Immutable Artifacts.
- Implementing Code Signing and artifact verification across environments.
- Hardening the build environment and build secrets management.
- CI/CD Hardening, Code Signing, Artifact Verification, Immutable Infrastructure.
- Case Study: SolarWinds ORION Breach.

Module 5: Code and Developer Environment Security

- Implementing Zero Trust principles for developer workstations and access to source code.
- Best practices for securing Source Code Repositories
- Secret Management and the use of secrets scanning tools early in development.
- Least Privilege, Secrets Scanning, SAST/DAST Integration, Code Review Automation.
- Case Study: Codecov Compromise.

Module 6: Third-Party Risk Management (TPRM)

- Techniques for conducting comprehensive security assessments of software vendors.
- Integrating supply chain security requirements into legal Contracts and SLAs.
- Continuous monitoring of vendor security posture and threat intelligence sharing.
- Vendor Due Diligence, TPRM, Cloud-based Supply Chain, Security Questionnaires
- Case Study: Kaseya VSA Attack.

Module 7: Frameworks, Compliance, and Governance

- Adopting and tailoring the NIST Secure Software Development Framework
- Introduction to the Supply Chain Levels for Software Artifacts framework.
- Developing and maintaining a formal Cybersecurity Supply Chain Risk Management program.
- NIST SSDF, SLSA, C-SCRM, Compliance Automation.
- Case Study: Regulatory Non-Compliance Impact.

Module 8: Monitoring, Incident Response, and Future Trends

- Establishing Continuous Monitoring of logs and artifacts for anomalies and signs of tampering.
- Developing and testing the Software Supply Chain Incident Response plan.
- AI-generated code security and the rise of Post-Quantum Cryptography
- Threat Hunting, Anomaly Detection, Incident Playbook, AI/ML Security.
- Case Study: Mock Attack Simulation.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

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