Training Course on Supply Chain Attack Incident Response

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 digital ecosystem, supply chain attacks have emerged as one of the most pressing cybersecurity threats. Organizations worldwide are increasingly vulnerable to breaches stemming from third-party vendors, open-source dependencies, and compromised software updates. Training Course on Supply Chain Attack Incident Response equips IT professionals, security analysts, and corporate decision-makers with the strategic knowledge and technical skills required to identify, contain, and recover from such attacks. Through hands-on modules, real-world case studies, and advanced threat intelligence insights, this course fosters robust incident response readiness and compliance with cybersecurity frameworks like NIST and ISO 27001.

By focusing on cybersecurity resilience, vendor risk management, and zero-trust architecture, the course helps organizations proactively reduce attack surfaces and respond to threats before they escalate. Participants will learn how to conduct forensic analysis, assess third-party security postures, and design multi-layered defense mechanisms tailored to the evolving threat landscape. This course is ideal for enterprises seeking to safeguard critical infrastructure and maintain business continuity amid rising cyber threats targeting supply chains.

Programme Curriculum

Training Course on Supply Chain Attack Incident Response

Introduction

In today's interconnected digital ecosystem, supply chain attacks have emerged as one of the most pressing cybersecurity threats. Organizations worldwide are increasingly vulnerable to breaches stemming from third-party vendors, open-source dependencies, and compromised software updates. Training Course on Supply Chain Attack Incident Response equips IT professionals, security analysts, and corporate decision-makers with the strategic knowledge and technical skills required to identify, contain, and recover from such attacks. Through hands-on modules, real-world case studies, and advanced threat intelligence insights, this course fosters robust incident response readiness and compliance with cybersecurity

frameworks like NIST and ISO 27001.

By focusing on cybersecurity resilience, vendor risk management, and zero-trust architecture, the course helps organizations proactively reduce attack surfaces and respond to threats before they escalate. Participants will learn how to conduct forensic analysis, assess third-party security postures, and design multi-layered defense mechanisms tailored to the evolving threat landscape. This course is ideal for enterprises seeking to safeguard critical infrastructure and maintain business continuity amid rising cyber threats targeting supply chains.

Course Objectives

1. Understand the fundamentals of supply chain cybersecurity threats.
2. Identify early indicators of a supply chain compromise.
3. Master incident response frameworks specific to third-party attacks.
4. Apply threat intelligence in identifying malicious vendors and compromised software.
5. Design a vendor risk management strategy aligned with cybersecurity best practices.
6. Implement zero-trust security models to reduce supply chain attack vectors.
7. Conduct effective digital forensics for third-party breach investigations.
8. Establish business continuity plans in response to cyber disruptions.
9. Utilize real-time threat detection tools and automation platforms.
10. Comply with global standards such as NIST CSF, ISO/IEC 27001, and CMMC.
11. Train internal teams in cyber hygiene and phishing resilience for vendor-originated threats.
12. Evaluate the security posture of open-source software and third-party integrations.
13. Learn from real-world case studies involving major supply chain breaches (e.g., SolarWinds, Kaseya).

Target Audiences

1. Cybersecurity Analysts
2. Incident Response Teams
3. IT Security Managers
4. Chief Information Security Officers (CISOs)
5. DevSecOps Engineers
6. Risk and Compliance Officers
7. Government Security Agencies
8. Third-Party Vendor Managers

Course Duration: 5 days

Course Modules

Module 1: Introduction to Supply Chain Threats

- Define supply chain attacks and key vulnerabilities.
- Review high-profile attacks (e.g., SolarWinds, NotPetya).
- Discuss threat actors and motivations.
- Understand stages of the attack lifecycle.
- Identify hidden risks in vendor ecosystems.
- **Case Study:** SolarWinds breach: attack chain and response lessons.

Module 2: Threat Detection and Risk Assessment

- Tools for continuous monitoring.
- Behavioral analysis of compromised applications.
- Vendor risk assessment templates.
- Indicators of compromise (IOCs).
- Risk scoring for third-party tools.

- **Case Study:** Kaseya VSA attack and detection gaps.

Module 3: Incident Response Planning

- Phases of an IR plan tailored to supply chain threats.
- Team roles and communication protocols.
- Creating IR playbooks and escalation procedures.
- Tabletop simulation design.
- Integrating with enterprise BCP (Business Continuity Planning).
- **Case Study:** Target breach via HVAC vendor.

Module 4: Digital Forensics and Evidence Collection

- Identifying malware insertion points.
- Using forensic tools for compromised vendor software.
- Evidence preservation best practices.
- Chain of custody for legal compliance.
- Log analysis for supply chain malware.
- **Case Study:** Codecov Bash Uploader backdoor forensic analysis.

Module 5: Secure Software & Open Source Dependencies

- Vetting open-source packages.
- SBOM (Software Bill of Materials) usage.
- Dependency scanning tools and CI/CD integration.
- Monitoring developer environments.
- Securing build pipelines.
- **Case Study:** Event-Stream npm package compromise.

Module 6: Zero Trust and Segmentation Strategies

- Principles of zero-trust architecture.
- Network segmentation to isolate third-party tools.
- Identity and access management (IAM) controls.
- Role-based access controls (RBAC).
- Micro-segmentation for software access control.
- **Case Study:** Microsoft Exchange attack and role-based segmentation.

Module 7: Regulatory Compliance and Legal Response

- Overview of NIST, ISO, CMMC, GDPR compliance.
- Legal obligations in breach notification.
- Contractual clauses with vendors.
- Working with law enforcement post-breach.
- Ensuring audit readiness.
- **Case Study:** Equifax third-party data breach and legal impact.

Module 8: Building Resilient Ecosystems

- Conducting supply chain penetration testing.
- Implementing continuous vendor audits.
- Fostering internal security culture.
- Resilience metrics and KPIs.
- Cross-team collaboration for proactive defense.
- **Case Study:** DHL logistics chain cyberattack resilience.

Training Methodology

- Instructor-led live virtual or in-person sessions with industry experts.
- Hands-on labs and practical simulations using real-world tools and threat scenarios.
- Interactive discussions and peer-learning forums.
- Downloadable IR templates, checklists, and vendor evaluation forms.
- End-of-module assessments to ensure learning outcomes.
- Capstone project to develop and present a customized incident response plan.

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

Start Date	End Date	Location	Price
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