Training Cours on Attacker Kill Chain and Defensive Strategies

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 evolving cyber landscape, understanding the attacker’s mindset is crucial to building effective defense mechanisms. The Attacker Kill Chain provides a structured approach to identify, analyze, and mitigate each stage of a cyberattack. Training Course on Attacker Kill Chain and Defensive Strategies equips cybersecurity professionals with advanced defensive strategies to break the attacker’s chain, strengthen incident response, and enhance proactive threat hunting.

This hands-on course emphasizes real-world simulations, tactical defense operations, and strategic threat intelligence to empower blue teams, SOC analysts, and security engineers. By dissecting the kill chain—from reconnaissance to exfiltration—participants gain practical insight into adversary tactics, techniques, and procedures (TTPs), ensuring organizations stay resilient in the face of evolving cyber threats.

Programme Curriculum

Training Course on Attacker Kill Chain and Defensive Strategies

Introduction

In today’s evolving cyber landscape, understanding the attacker’s mindset is crucial to building effective defense mechanisms. The Attacker Kill Chain provides a structured approach to identify, analyze, and mitigate each stage of a cyberattack. Training Course on Attacker Kill Chain and Defensive Strategies equips cybersecurity professionals with advanced defensive strategies to break the attacker’s chain, strengthen incident response, and enhance proactive threat hunting.

This hands-on course emphasizes real-world simulations, tactical defense operations, and strategic threat intelligence to empower blue teams, SOC analysts, and security engineers. By dissecting the kill chain—from reconnaissance to exfiltration—participants gain practical insight into adversary tactics, techniques, and procedures (TTPs), ensuring

organizations stay resilient in the face of evolving cyber threats.

Course Objectives

1. Understand the 7 phases of the cyber kill chain framework.
2. Identify and neutralize initial reconnaissance activities.
3. Detect weaponization and delivery vectors using threat intel.
4. Analyze exploitation and privilege escalation techniques.
5. Monitor command and control (C2) channels in real time.
6. Prevent data exfiltration and lateral movement within networks.
7. Map adversary behavior using MITRE ATT&CK framework.
8. Deploy deception technologies to disrupt attacker tactics.
9. Use endpoint detection and response (EDR) tools effectively.
10. Design resilient defense-in-depth architectures.
11. Integrate security orchestration and automation (SOAR) in incident response.
12. Create actionable cyber threat intelligence (CTI) from attack analysis.
13. Apply zero trust principles to minimize attack surfaces.

Target Audience

1. Cybersecurity Analysts
2. SOC (Security Operations Center) Teams
3. Incident Responders
4. Threat Hunters
5. Penetration Testers
6. IT Security Managers
7. System Administrators
8. Network Engineers

Course Duration: 5 days

Course Modules

Module 1: Introduction to the Attacker Kill Chain

- Understanding Lockheed Martin’s Kill Chain Model
- Phases: Reconnaissance to Actions on Objectives
- Comparing Kill Chain vs. MITRE ATT&CK
- Role in Cyber Defense Strategy
- Limitations and Modern Variants
- **Case Study**: SolarWinds Attack Breakdown

Module 2: Reconnaissance and Intelligence Gathering

- Passive vs. Active Reconnaissance
- OSINT Techniques and Tools
- DNS, WHOIS, and Metadata Analysis
- Detecting Recon Activities
- Building Recon Detection Sensors
- **Case Study**: Target Corp. Data Breach

Module 3: Weaponization and Delivery

- Malware Creation Techniques
- Payload Encoding and Obfuscation

- Social Engineering & Phishing Delivery
- Exploit Kits and Dropper Chains
- Email Security & Sandbox Solutions
- **Case Study**: Emotet Malware Campaign

Module 4: Exploitation and Installation

- Identifying Common Vulnerabilities (CVEs)
- Remote Code Execution and Exploits
- Post-Exploitation Persistence Mechanisms
- Memory-based Attacks
- Host Hardening Techniques
- **Case Study**: Equifax Exploitation Scenario

Module 5: Command and Control (C2) Infrastructure

- Types of C2 Protocols (HTTP, DNS, TLS)
- Detection and Blocking of C2 Channels
- Beaconing Behavior & Frequency Analysis
- Threat Intelligence Integration
- Decoy Traffic & Anomaly Detection
- **Case Study**: APT29 (Cozy Bear) C2 Tactics

Module 6: Actions on Objectives & Data Exfiltration

- Privilege Escalation Techniques
- Data Staging and Compression Methods
- Common Exfiltration Protocols
- Monitoring Data Access Patterns
- Network Segmentation & DLP Strategies
- **Case Study**: Sony Pictures Data Leak

Module 7: Defensive Strategies and Mitigation

- Kill Chain Disruption Points
- SIEM and SOC Alert Tuning
- Threat Hunting Playbooks
- Integrating SOAR with Detection
- Incident Response Readiness
- **Case Study**: Colonial Pipeline Defensive Gaps

Module 8: Proactive Security & Threat Intelligence

- Cyber Threat Intelligence Cycle
- Indicators of Compromise (IOCs) & TTPs
- Red vs. Blue Teaming Exercises
- Threat Modeling & Simulation
- Implementing Threat Feeds in Defense
- **Case Study**: MITRE ATT&CK Defender Workshop

Training Methodology

- Instructor-led lectures and real-world cyber scenarios
- Hands-on lab exercises using live network data
- Red and blue team interactive simulations
- Group-based threat modeling assignments

- Case study walkthroughs and forensic reviews
- Quizzes and assessments to measure knowledge retention

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
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

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

Register Online Now

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