Training Course on Hunting for Adversary Lateral Movement

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's volatile **cybersecurity landscape**, **adversary lateral movement** stands as a critical and pervasive threat tactic. Post-initial compromise, sophisticated **threat actors** exploit vulnerabilities and misconfigurations to **traverse networks**, escalating privileges and establishing **persistence** to reach high-value assets. Training Course on Hunting for Adversary Lateral Movement provides **blue teams**, **security analysts**, and **incident responders** with the **proactive defense** strategies and **detection engineering** skills necessary to identify, analyze, and neutralize lateral movement, effectively diminishing **dwell time** and mitigating **breach impact**.

This comprehensive program delves into the intricate methodologies employed by **Advanced Persistent Threats (APTs)**, equipping participants with **actionable intelligence** and **hands-on experience** in leveraging **endpoint detection and response (EDR)**, **security information and event management (SIEM)**, and **threat hunting** techniques. By understanding attacker **TTPs (Tactics, Techniques, and Procedures)**, organizations can significantly enhance their **cyber resilience**, moving beyond reactive defenses to implement **proactive security measures** and fortify their **defensive posture** against evolving **cyber threats**.

Programme Curriculum

Training Course on Hunting for Adversary Lateral Movement

Introduction

In today's volatile **cybersecurity landscape**, **adversary lateral movement** stands as a critical and pervasive threat tactic. Post-initial compromise, sophisticated **threat actors** exploit vulnerabilities and misconfigurations to **traverse networks**, escalating privileges and establishing **persistence** to reach high-value assets. Training Course on Hunting for Adversary Lateral Movement provides **blue teams**, **security analysts**, and **incident responders** with the **proactive defense** strategies and **detection engineering** skills necessary to identify, analyze, and neutralize lateral movement,

effectively diminishing **dwell time** and mitigating **breach impact**.

This comprehensive program delves into the intricate methodologies employed by **Advanced Persistent Threats (APTs)**, equipping participants with **actionable intelligence** and **hands-on experience** in leveraging **endpoint detection and response (EDR)**, **security information and event management (SIEM)**, and **threat hunting** techniques. By understanding attacker **TTPs (Tactics, Techniques, and Procedures)**, organizations can significantly enhance their **cyber resilience**, moving beyond reactive defenses to implement **proactive security measures** and fortify their **defensive posture** against evolving **cyber threats**.

Course Duration

10 days

Course Objectives

1. Gain in-depth proficiency in mapping and analyzing **adversary TTPs** related to **lateral movement**.
2. Develop skills for **proactive threat hunting** to identify anomalous activities indicative of lateral movement.
3. Learn to build and optimize **detection rules** and **use cases** within **SIEM** and **EDR** platforms.
4. Understand and implement robust strategies to counter **credential dumping**, **Pass-the-Hash (PtH)**, and **Pass-the-Ticket (PtT)** attacks.
5. Design and deploy effective **network segmentation** and **microsegmentation** to restrict lateral movement paths.
6. Fortify **IAM solutions** and enforce **least privilege access** to minimize attack surfaces.
7. Identify and defend against common lateral movement methods across **Windows** and **Linux** environments.
8. Utilize **breach and attack simulation (BAS)** and **continuous automated red teaming (CART)** for validating lateral movement defenses.
9. Develop and refine **incident response playbooks** specifically for lateral movement detection and containment.
10. Apply lateral movement detection and prevention strategies within **cloud environments** and **SaaS applications**.
11. Leverage **User and Entity Behavior Analytics (UEBA)** to detect subtle indicators of compromise (IOCs).
12. Understand how lateral movement can originate from **supply chain attacks** and implement preventative measures.
13. Explore the application of **Artificial Intelligence (AI)** and **Machine Learning (ML)** in enhancing lateral movement detection capabilities.

Organizational Benefits

- Significantly decrease the time adversaries remain undetected within the network, minimizing potential damage.
- Strengthen overall cybersecurity posture against advanced threats and sophisticated attack campaigns.
- Enable faster, more efficient, and effective responses to active lateral movement attempts.
- Shift from reactive defense to proactive threat hunting and prevention, identifying weaknesses before exploitation.
- Maximize the effectiveness of existing security tools (SIEM, EDR) through specialized knowledge.

- Bolster compliance with industry regulations and data protection standards by demonstrating robust security controls.
- Safeguard sensitive data, intellectual property, and critical infrastructure from unauthorized access and exfiltration.
- Minimize the financial costs and reputational impact associated with successful cyber breaches.

Target Audience

1. Security Analysts
2. Incident Responders
3. SOC Analysts
4. Threat Hunters
5. Red Team / Blue Team Members
6. Cybersecurity Engineers
7. Network Administrators with Security Responsibilities
8. IT Security Managers seeking technical depth

Course Outline

Module 1: Introduction to Adversary Lateral Movement & the Kill Chain

- Defining lateral movement: Why it's critical post-initial compromise.
- Understanding the role of lateral movement in the Cyber Kill Chain and MITRE ATT&CK Framework.
- Common motivations and objectives of adversaries moving laterally (e.g., data exfiltration, privilege escalation).
- Overview of **attacker methodologies** and common tools.
- **Case Study:** Analyzing a high-profile **ransomware attack** where lateral movement was key to encrypting widespread systems.

Module 2: Reconnaissance & Initial Foothold from a Lateral Perspective

- Internal network reconnaissance techniques (e.g., network scanning, host discovery, service enumeration).
- Identifying misconfigurations and vulnerable services ripe for lateral movement.
- Understanding initial access vectors that facilitate lateral movement (e.g., phishing, exploit kits).
- Mapping network topology and identifying critical assets.
- **Case Study:** How initial compromise of a single workstation led to full domain compromise through inadequate network segmentation.

Module 3: Credential Access & Abuse

- Techniques for **credential dumping** (e.g., Mimikatz, LSASS dumping).
- **Pass-the-Hash (PtH)** and **Pass-the-Ticket (PtT)** attacks: theory and practical exploitation.
- Kerberoasting and other Active Directory-focused credential attacks.
- Detecting and preventing credential theft on endpoints and in memory.
- **Case Study:** The NotPetya attack and its reliance on stolen credentials for rapid lateral propagation.

Module 4: Remote Services & Protocols for Lateral Movement

- Exploiting **Remote Desktop Protocol (RDP)** for lateral movement.

- Leveraging **Server Message Block (SMB)** and shared drives.
- Attacks against **SSH** and other remote administration protocols.
- Misusing legitimate administrative tools (e.g., PsExec, WinRM, WMI).
- **Case Study:** An attacker using stolen RDP credentials to access a critical server, then pivoting to other systems.

Module 5: Persistence Mechanisms for Lateral Movement

- Establishing **backdoors** and **webshells** for continued access.
- Scheduled tasks, services, and run keys for persistence.
- Modifying legitimate software for persistent access.
- Detecting and removing various persistence mechanisms.
- **Case Study:** A threat actor maintaining long-term access to a network by implanting hidden persistence mechanisms across multiple systems.

Module 6: Lateral Movement in Windows Environments

- Detailed exploration of Windows-specific techniques.
- Group Policy Object (GPO) abuse and rogue domain controllers.
- Exploiting common Windows services and misconfigurations.
- Windows event logging and forensic artifacts for lateral movement.
- **Case Study:** An attack leveraging default administrative shares and weak local administrator passwords for widespread Windows lateral movement.

Module 7: Lateral Movement in Linux Environments

- SSH key exploitation and privilege escalation.
- Linux service misconfigurations and vulnerable daemons.
- Container escape techniques for lateral movement in cloud-native environments.
- Linux logging and forensic artifacts for lateral movement.
- **Case Study:** Compromise of a Linux web server leading to lateral movement into a database server via exposed SSH keys.

Module 8: Network Segmentation & Microsegmentation

- Principles of **network segmentation** and its role in limiting lateral movement.
- Implementing **microsegmentation** with firewalls and SDN.
- Designing security zones and access controls.
- Challenges and best practices for effective segmentation.
- **Case Study:** A company's successful containment of a breach within a segmented network, preventing broader impact.

Module 9: Endpoint Detection and Response (EDR) for Lateral Movement Hunting

- Leveraging **EDR solutions** for real-time visibility and threat detection.
- Analyzing EDR alerts related to lateral movement TTPs.
- Proactive hunting using EDR queries and behavioral analytics.
- Automated response and containment capabilities of EDR.
- **Case Study:** Using EDR to identify and terminate a lateral movement chain initiated by a suspicious PowerShell script.

Module 10: Security Information and Event Management (SIEM) for Lateral Movement Detection

- Correlating logs from various sources to detect lateral movement.

- Developing **SIEM use cases** and alerts for known lateral movement indicators.
- Leveraging **UEBA** within SIEM for anomalous behavior detection.
- Building effective dashboards and reports for lateral movement insights.
- **Case Study:** A SIEM system flagging unusual login patterns and failed authentication attempts across multiple systems, indicating lateral movement.

Module 11: Active Directory Security & Lateral Movement

- Common Active Directory vulnerabilities exploited for lateral movement.
- Securing Active Directory against credential theft and privilege escalation.
- Group Policy hardening and effective user management.
- Monitoring Active Directory for signs of compromise.
- **Case Study:** A Golden Ticket attack allowing an attacker to impersonate any user in an Active Directory domain, highlighting the critical need for AD security.

Module 12: Cloud-Specific Lateral Movement Techniques

- Lateral movement within IaaS (AWS, Azure, GCP) environments.
- Exploiting misconfigured cloud services and IAM roles.
- Container and Kubernetes security challenges for lateral movement.
- Cloud logging and monitoring for lateral movement indicators.
- **Case Study:** An attacker exploiting an over-privileged IAM role in AWS to pivot between different cloud resources and exfiltrate data.

Module 13: Threat Intelligence and Adversary Emulation

- Integrating **threat intelligence** into lateral movement hunting strategies.
- Understanding **adversary profiles** and their preferred lateral movement TTPs.
- Conducting **adversary emulation** to test defensive capabilities.
- Utilizing frameworks like MITRE ATT&CK for red team and blue team collaboration.
- **Case Study:** Applying intelligence from a recent APT campaign to simulate their lateral movement techniques and validate existing detections.

Module 14: Incident Response & Remediation of Lateral Movement

- Developing **incident response plans** specifically for lateral movement.
- Containment strategies for active lateral movement.
- Eradication and recovery procedures.
- Post-incident analysis and lessons learned.
- **Case Study:** A rapid incident response effort that successfully contained a lateral movement incident by isolating compromised hosts and rotating credentials.

Module 15: Advanced Lateral Movement Techniques & Future Trends

- Living Off The Land (LotL) techniques and their challenges for detection.
- Advanced persistent threats (APTs) and their evolving lateral movement TTPs.
- Supply chain attacks and their impact on lateral movement.
- The role of AI and automation in both attacking and defending against lateral movement.
- **Case Study:** An analysis of a sophisticated **zero-day exploit** combined with novel lateral movement techniques that bypassed traditional security controls.

Training Methodology

- **Instructor-Led Sessions**: Expert-led discussions of concepts, theories, and real-world examples.

- **Hands-on Labs & Workshops**: Extensive practical exercises in a simulated environment, allowing participants to apply learned techniques.
- **Case Study Analysis**: Deep dives into real-world breaches and lateral movement scenarios to understand attacker motivations and defensive failures.
- **Red Team / Blue Team Drills**: Simulated attack and defense scenarios to build practical skills in detecting and responding to lateral movement.
- **Tool Demonstrations**: Live demonstrations and usage of industry-standard cybersecurity tools (SIEM, EDR, network forensic tools).
- **Interactive Discussions & Q&A**: Encouraging peer-to-peer learning and problem-solving.
- **Scenario-Based Training**: Solving realistic cybersecurity challenges to reinforce learning.
- **Gamified Learning**: Incorporating challenges and competitive elements to enhance engagement.

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.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 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