Training Course on MITRE ATT and CK Framework for Threat Hunting

Professional Development Training Course Outline

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

Course Introduction

Training Course on MITRE ATT and CK Framework for Threat Hunting provides cybersecurity professionals with the essential knowledge and practical skills to leverage the **MITRE ATT&CK Framework** for advanced **threat hunting**. Participants will gain a deep understanding of adversarial **tactics, techniques, and procedures (TTPs)**, enabling them to proactively detect, analyze, and respond to sophisticated cyber threats. Through hands-on exercises, real-world **case studies**, and **adversary emulation**, this program cultivates a **threat-informed defense** mindset, empowering security teams to enhance their **cyber resilience** and optimize **security operations**.

The curriculum emphasizes practical application, moving beyond theoretical concepts to equip attendees with actionable strategies for **proactive threat detection** and **incident response**. We will explore how to integrate ATT&CK into existing **security tools** and workflows, improve **threat intelligence analysis**, and conduct effective **security posture assessments**. This course is crucial for organizations seeking to mature their **cybersecurity capabilities** and build a robust defense against ever-evolving **advanced persistent threats (APTs)**.

Programme Curriculum

Training Course on MITRE ATT and CK Framework for Threat Hunting

Introduction

Training Course on MITRE ATT and CK Framework for Threat Hunting provides cybersecurity professionals with the essential knowledge and practical skills to leverage the **MITRE ATT&CK Framework** for advanced **threat hunting**. Participants will gain a deep understanding of adversarial **tactics, techniques, and procedures (TTPs)**, enabling them to proactively detect, analyze, and respond to sophisticated cyber threats. Through hands-on exercises, real-world **case studies**, and **adversary emulation**, this program cultivates a **threat-informed defense** mindset, empowering security teams to enhance their **cyber resilience** and optimize **security operations**.

The curriculum emphasizes practical application, moving beyond theoretical concepts to equip attendees with actionable strategies for **proactive threat detection** and **incident response**. We will explore how to integrate ATT&CK into existing **security tools** and workflows, improve **threat intelligence analysis**, and conduct effective **security posture assessments**. This course is crucial for organizations seeking to mature their **cybersecurity capabilities** and build a robust defense against ever-evolving **advanced persistent threats (APTs)**.

Course Duration

10 days

Course Objectives

1. Comprehend the fundamental structure, matrices (Enterprise, Mobile, ICS), and underlying philosophy of the MITRE ATT&CK Framework.
2. Analyze and categorize real-world **adversary TTPs** to understand attacker motivations and methodologies.
3. Integrate **ATT&CK-mapped threat intelligence** into security operations for enhanced situational awareness.
4. Develop and execute effective **threat hunting methodologies** utilizing ATT&CK as a guiding framework.
5. Engineer robust **detection rules** and **security controls** mapped directly to specific ATT&CK techniques.
6. Improve **incident response playbooks** and procedures by correlating security incidents with ATT&CK techniques.
7. Conduct comprehensive **security assessments** to identify gaps in defensive capabilities against known adversary behaviors.
8. Utilize ATT&CK for planning and executing realistic **adversary emulation** and **red team exercises**.
9. Facilitate **purple teaming** engagements to bridge the gap between offensive and defensive security teams.
10. Explore tools and techniques for **automating threat detection** and analysis based on ATT&CK.
11. Identify and mitigate **lateral movement techniques** commonly employed by sophisticated threat actors.
12. Understand and implement effective **privilege escalation** prevention and detection mechanisms.
13. Analyze and investigate **data exfiltration** techniques using the ATT&CK framework for comprehensive forensic analysis.

Organizational Benefits

- Proactively defend against sophisticated attacks by understanding and anticipating adversary behavior.
- Reduce false positives and accelerate incident triage through ATT&CK-informed detections.
- Expedite incident containment and recovery by mapping attack activities to known TTPs.
- Prioritize security tool investments and resource allocation based on real-world threat intelligence.
- Foster a common language for security discussions across different teams (SOC, CTI, Red Team).
- Shift from a reactive to a **proactive defense** strategy, staying ahead of emerging threats.
- Demonstrate robust security practices aligned with industry best practices and compliance frameworks.

- Identify and mitigate vulnerabilities by understanding how adversaries exploit weaknesses.
- Clearly articulate cyber risks and security posture to executive management using a standardized framework.

Target Audience

1. Security Operations Center (SOC) Analysts.
2. Threat Hunters
3. Incident Responders
4. Cyber Threat Intelligence (CTI) Analysts
5. Red Team / Penetration Testers
6. Security Architects & Engineers.
7. Security Managers & CISOs.
8. Digital Forensics Professionals

Course Outline

Module 1: Introduction to MITRE ATT&CK Framework

- What is MITRE ATT&CK? History, purpose, and its role in modern cybersecurity.
- Understanding the ATT&CK Matrix: Tactics, Techniques, and Procedures (TTPs).
- Navigating the ATT&CK website and resources (e.g., ATT&CK Navigator).
- ATT&CK vs. Cyber Kill Chain: Similarities, differences, and complementary usage.
- **Case Study:** Analyzing a basic malware attack (e.g., Emotet) and mapping its observed behaviors to initial ATT&CK tactics (e.g., Initial Access, Execution).

Module 2: Core Concepts of Threat Hunting

- Defining Threat Hunting: Proactive vs. Reactive security, hypothesis-driven approach.
- The Threat Hunting Loop: Hypothesis generation, investigation, and enrichment.
- Key enablers for effective threat hunting: Data sources, tools, and skilled analysts.
- Developing threat hunting hypotheses based on threat intelligence and ATT&CK.
- **Case Study:** Formulating a hypothesis to hunt for suspicious PowerShell execution (T1059.001) given recent intelligence on a specific threat actor.

Module 3: Initial Access & Execution Tactics

- Deep dive into Initial Access (TA0001): Phishing, Exploit Public-Facing Application, Valid Accounts.
- Understanding Execution (TA0002): Command and Scripting Interpreter, Scheduled Task/Job, PowerShell.
- Common techniques and sub-techniques within these tactics.
- Detection opportunities and mitigation strategies for initial compromise.
- **Case Study:** Investigating a simulated phishing campaign that leads to malicious macro execution (T1204.002) via a crafted document (T1566.001).

Module 4: Persistence & Privilege Escalation

- Exploring Persistence (TA0003): Boot or Logon Autostart Execution, Create Account, Registry Run Keys.
- Understanding Privilege Escalation (TA0004): Exploitation for Privilege Escalation, Abuse Elevation Control, Scheduled Task.
- How adversaries maintain access and gain higher privileges post-initial access.
- Techniques for detecting and preventing persistent footholds and escalation attempts.

- **Case Study:** Analyzing a scenario where an attacker establishes persistence via a new service (T1543.003) and then escalates privileges using a vulnerable kernel driver (T1068).

Module 5: Defense Evasion & Credential Access

- Deep dive into Defense Evasion (TA0005): Obfuscated Files or Information, Deobfuscate/Decode Files or Information, Disable or Modify Tools.
- Understanding Credential Access (TA0006): OS Credential Dumping, Brute Force, Steal or Forge Kerberos Tickets.
- Adversary methods for bypassing security controls and stealing credentials.
- Strategies for detecting evasion techniques and protecting credentials.
- **Case Study:** Simulating an attacker using a legitimate tool like Mimikatz (T1003) to dump LSASS credentials after disabling antivirus (T1562.001).

Module 6: Discovery & Lateral Movement

- Exploring Discovery (TA0007): System Information Discovery, Network Share Discovery, Remote System Discovery.
- Understanding Lateral Movement (TA0008): Remote Services, Pass the Hash, Remote Desktop Protocol.
- How attackers map the network and move between systems.
- Techniques for identifying and preventing lateral movement within the network.
- **Case Study:** Tracking an attacker's lateral movement from an infected workstation to a domain controller using PsExec (T1021.002) and stolen administrative credentials (T1078).

Module 7: Collection & Exfiltration

- Deep dive into Collection (TA0009): Data from Local System, Archive Collected Data, Screen Capture.
- Understanding Exfiltration (TA0010): Exfiltration Over C2 Channel, Exfiltration Over Other Network Medium, Data Compressed.
- Adversary methods for gathering target data and extracting it from the network.
- Strategies for detecting data collection and preventing exfiltration.
- **Case Study:** Investigating a breach where sensitive documents were collected (T1005), archived into a password-protected zip file (T1560.001), and then exfiltrated over HTTPS (T1041).

Module 8: Command and Control (C2) & Impact

- Exploring Command and Control (TA0011): Standard Application Layer Protocol, Custom Command and Control Protocol, Web Shell.
- Understanding Impact (TA0012): Data Destruction, Data Encrypted for Impact, Service Stop.
- How adversaries maintain communication and achieve their ultimate objectives.
- Detection and mitigation for C2 channels and destructive impact actions.
- **Case Study:** Analyzing a ransomware attack (T1486) where an established C2 channel (T1071.001) was used to encrypt critical files after disabling system restore (T1490).

Module 9: Mapping Threat Intelligence to ATT&CK

- Sources of threat intelligence and their relevance to ATT&CK.
- Techniques for parsing raw threat intelligence reports and extracting TTPs.
- Utilizing the ATT&CK framework to contextualize and prioritize threat intelligence.
- Creating ATT&CK Navigator layers for specific threat actors or campaigns.

- **Case Study:** Mapping a public threat intelligence report (e.g., a Mandiant or FireEye report on a specific APT group) to the ATT&CK framework to identify their common TTPs.

Module 10: Building ATT&CK-Driven Detections

- Principles of detection engineering: From Indicators of Compromise (IOCs) to Behaviors.
- Translating ATT&CK techniques into actionable detection rules (e.g., SIEM alerts, EDR queries).
- Developing analytics to identify suspicious behavioral patterns across multiple events.
- Baselines and anomaly detection using ATT&CK for context.
- **Case Study:** Developing detection rules in a SIEM (e.g., Splunk, Elastic) for a specific ATT&CK technique like "Process Injection" (T1055), considering various sub-techniques.

Module 11: Threat Hunting with MITRE ATT&CK Navigator

- Hands-on practical usage of MITRE ATT&CK Navigator for visualization and analysis.
- Creating custom layers to track threat actor TTPs, defensive coverage, and red team engagements.
- Comparing and contrasting different ATT&CK layers to identify gaps and overlaps.
- Using Navigator for communication and reporting within security teams.
- **Case Study:** Using ATT&CK Navigator to visualize the TTPs observed in a recent internal incident and identify areas for improved detection coverage.

Module 12: Adversary Emulation and Red Teaming with ATT&CK

- Planning and executing **adversary emulation** exercises based on ATT&CK.
- Designing realistic red team scenarios aligned with specific threat actor profiles.
- Measuring defensive efficacy against emulated ATT&CK techniques.
- Using tools like Caldera or Infection Monkey for automated adversary emulation.
- **Case Study:** Designing a small-scale adversary emulation exercise focused on a specific ATT&CK technique (e.g., Kerberoasting T1558.003) and evaluating blue team detection capabilities.

Module 13: Purple Teaming and Continuous Improvement

- The role of **purple teaming** in bridging the gap between offensive and defensive security.
- Facilitating collaborative exercises using ATT&CK as a common language.
- Iterative improvement of security controls based on red team findings and ATT&CK.
- Developing a continuous **threat-informed defense** strategy.
- **Case Study:** A simulated purple team exercise where a red team executes specific ATT&CK techniques, and the blue team attempts to detect and respond, followed by a collaborative review and improvement session.

Module 14: Advanced Threat Hunting Techniques & Data Sources

- Hunting for **Living Off The Land (LOTL) binaries** and fileless malware.
- Leveraging Sysmon logs for granular endpoint activity monitoring.
- Network traffic analysis for C2 detection and data exfiltration.
- Cloud environment threat hunting with ATT&CK for Cloud.
- **Case Study:** Hunting for suspicious LOLBIN usage (e.g., cmd.exe or powershell.exe executing unusual commands) using detailed endpoint logs.

Module 15: Operationalizing ATT&CK for Your Organization

- Strategies for integrating ATT&CK into existing security frameworks and processes.

- Building a **threat-informed defense** program tailored to your organization's risk profile.
- Measuring the maturity of your ATT&CK implementation.
- Future trends in MITRE ATT&CK and threat hunting.
- **Case Study:** Developing a roadmap for an organization to adopt and operationalize the MITRE ATT&CK framework across their security functions, including defining key metrics for success.

Training Methodology

This training course employs a **blended learning approach** combining:

- **Interactive Lectures**: Clear explanations of MITRE ATT&CK concepts, tactics, techniques, and procedures.
- **Hands-on Labs**: Practical exercises utilizing realistic scenarios and industry-standard tools (e.g., SIEM, EDR, forensic tools, ATT&CK Navigator, and potentially open-source emulation tools).
- **Real-world Case Studies**: In-depth analysis of actual cyber incidents and how ATT&CK could have been applied for detection and response.
- **Adversary Emulation Exercises**: Controlled simulations of adversary behaviors to test defensive capabilities.
- **Group Discussions & Collaboration**: Fostering peer-to-peer learning and knowledge sharing.
- **Quizzes & Assessments**: To reinforce learning and assess comprehension.
- **Practical Demonstrations**: Live demonstrations of tools and techniques.
- **Resource Sharing**: Providing participants with supplementary materials, templates, and further reading.

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. Upcoming Scheduled Sessions

Start Date	End Date	Location	Price

23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

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

Register Online Now

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