Using ATT&CK for Cyber Threat Intelligence Training Course

Professional Development Training Course Outline

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

Course Introduction

In today’s rapidly evolving digital landscape, cybersecurity remains a top priority for organizations worldwide. Cyber threats are becoming increasingly sophisticated, and the need for a comprehensive and strategic approach to cybersecurity is greater than ever. Using ATT&CK for Cyber Threat Intelligence Training Course equips professionals with the skills to effectively utilize the MITRE ATT&CK framework, one of the most trusted resources for mapping and identifying adversary behaviors in cybersecurity. By learning how to leverage the ATT&CK framework, participants will enhance their ability to conduct threat intelligence analysis and fortify their organization’s defenses against advanced persistent threats (APTs) and other malicious actors.

This training is designed to offer hands-on experience in using the ATT&CK framework for identifying tactics, techniques, and procedures (TTPs) used by cyber adversaries. As cyber-attacks become more complex, it's crucial to stay ahead of the curve by adopting proactive threat intelligence strategies. By the end of this course, participants will understand the full scope of ATT&CK, allowing them to analyze data, detect threats in real time, and contribute to a robust cybersecurity strategy. The course also emphasizes collaboration among security teams and the importance of threat-sharing to improve defense mechanisms. This training ensures that professionals are equipped with the most current tools and techniques in cybersecurity threat intelligence.

Programme Curriculum

Using ATT&CK for Cyber Threat Intelligence Training Course

Introduction:

In today’s rapidly evolving digital landscape, cybersecurity remains a top priority for organizations worldwide. Cyber threats are becoming increasingly sophisticated, and the need for a comprehensive and strategic approach to cybersecurity is greater than ever. Using ATT&CK for Cyber Threat Intelligence Training Course equips professionals with the skills to effectively utilize the MITRE ATT&CK framework, one of the most trusted resources for mapping and identifying adversary behaviors in cybersecurity. By learning how to leverage the ATT&CK framework, participants will enhance their ability to conduct threat intelligence analysis and fortify their organization’s defenses against advanced persistent threats (APTs) and other malicious actors.

This training is designed to offer hands-on experience in using the ATT&CK framework for identifying tactics, techniques, and procedures (TTPs) used by cyber adversaries. As cyber-attacks become more complex, it's crucial to stay ahead of the curve by adopting proactive threat intelligence strategies. By the end of this course, participants will understand the full scope of ATT&CK, allowing them to analyze data, detect threats in real time, and contribute to a robust cybersecurity strategy. The course also emphasizes collaboration among security teams and the importance of threat-sharing to improve defense mechanisms. This training ensures that professionals are equipped with the most current tools and techniques in cybersecurity threat intelligence.

Course Objectives:

- Understand the MITRE ATT&CK framework and its role in cyber threat intelligence.
- Analyze cyber threats using ATT&CK’s tactics, techniques, and procedures (TTPs).
- Learn to map adversary behaviors to ATT&CK matrices.
- Develop effective strategies for incident detection and response using ATT&CK.
- Apply ATT&CK to improve threat-hunting techniques within an organization.
- Gain practical experience in utilizing ATT&CK for incident analysis and forensics.
- Improve skills in cyber defense by understanding adversary tactics and methods.
- Collaborate with teams to build a more comprehensive cybersecurity defense strategy.
- Leverage cyber threat intelligence tools alongside ATT&CK for improved analysis.
- Understand the importance of threat-sharing and collaboration across teams.
- Enhance capabilities in attack simulation and red teaming using ATT&CK.
- Implement ATT&CK in creating detection rules and playbooks for proactive security.
- Interpret and analyze the cyber threat landscape using real-world data and case studies.

Target Audience:

- Cybersecurity Analysts
- Incident Response Teams
- Threat Intelligence Analysts
- Security Operations Center (SOC) Teams
- Red Team Members

- Blue Team Members
- Cybersecurity Engineers
- IT Security Managers

Course Duration:

5 days

Course Modules:

Module 1: Introduction to MITRE ATT&CK

- Overview of the MITRE ATT&CK framework.
- Key concepts: Tactics, Techniques, and Procedures (TTPs).
- Understanding the ATT&CK Matrix.
- ATT&CK's role in cybersecurity.
- Benefits of using ATT&CK for threat intelligence.

Module 2: Threat Intelligence Fundamentals

- What is threat intelligence?
- Types of threat intelligence: tactical, operational, strategic.
- Integrating threat intelligence into cybersecurity.
- Using ATT&CK to analyze threats.
- Threat intelligence lifecycle.

Module 3: Mapping Adversary Behaviors to ATT&CK

- Understanding adversary tactics and techniques.
- Mapping real-world attack scenarios to ATT&CK.
- Identifying gaps in security defenses.
- Using ATT&CK for attack simulation.
- Practical examples of threat analysis.

Module 4: Threat Detection with ATT&CK

- How to detect attacks using ATT&CK.
- Building detection rules.
- Leveraging security tools with ATT&CK.
- Analyzing attack patterns in real-time.

- Best practices for threat detection.

Module 5: Advanced Threat-Hunting Techniques

- Introduction to proactive threat hunting.
- Using ATT&CK for advanced threat detection.
- Creating custom attack scenarios.
- Leveraging automation in threat hunting.
- Best tools for threat hunting.

Module 6: Incident Response and Analysis Using ATT&CK

- How to respond to incidents using ATT&CK.
- Integrating ATT&CK into incident response workflows.
- Conducting forensic analysis with ATT&CK.
- Managing and mitigating cyber incidents.
- Post-incident reporting and lessons learned.

Module 7: Threat Sharing and Collaboration

- The importance of threat intelligence sharing.
- How to collaborate with external and internal teams.
- Using ATT&CK for cross-organizational threat sharing.
- Platforms for threat sharing.
- Best practices for effective collaboration.

Module 8: Practical Applications and Case Studies

- Real-world case studies of using ATT&CK.
- Hands-on exercises with ATT&CK tools.
- Simulating and analyzing real cyber-attacks.
- Improving security posture with ATT&CK insights.
- Discussion and review of case study results.

Training Methodology:

- Blended Learning Approach
- Practical, Scenario-Based Learning
- Hands-On Labs and Simulations

- Group Exercises & Collaborative Projects
- Assessment and Feedback
- Expert Guest Sessions
- Continuous Learning & Resource
- Certification and Recognition

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

Start Date	End Date	Location	Price
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