Course Syllabus

MITRE ATT&CK Defender™ (MAD) ATT&CK® Cyber Threat Intelligence Certification Training

Instructor Name: Adam Pennington, Amy Robertson & Jackie Lasky

Instructor Contact: adamp@mitre.org/ arobertson@mitre.org/ jlasky@mitre.org

Course Creation Date: 12/04/2020

Course Description and Goals

Course Description: The ATT&CK® team will help you learn how to leverage ATT&CK® to improve your cyber threat intelligence (CTI) practices. This course provides hands-on instruction in mapping narrative reporting and raw data to ATT&CK®, efficiently storing and expressing the mapped intelligence, and operationalizing the intelligence through actionable recommendations to defenders.

Target audience: ATT&CK® for Cyber Threat Intelligence is an intermediate course that focuses on identifying, developing, analyzing, and applying ATT&CK®-mapped intelligence. Participants should have a solid understanding of the ATT&CK® framework. If you're unfamiliar with ATT&CK®, we suggest that you take MITRE ATT&CK Defender™ (MAD) - ATT&CK® Fundamentals prior to this course.

Prerequisites:

- ❑ An understanding of the ATT&CK® framework through the MITRE ATT&CK Defender™ (MAD) – ATT&CK® Fundamentals course
- ❑ An understanding of security concepts, previous training, or prior CTI field experience

Upon completion of ATT&CK® for Cyber Threat Intelligence, we recommend that you expand your ATT&CK® knowledge and operations with one of the following courses**:**

- ❑ **MITRE ATT&CK Defender™ (MAD) - Detection and Analytics / TTP Hunting**
- ❑ **MITRE ATT&CK Defender™ (MAD)– Threat Emulation**
- ❑ **MITRE ATT&CK Defender™ (MAD) – Adversary Engagement**

Supplementary Materials:

- ❑ ATT&CK® Website
- ❑ MITRE ATT&CK®: Design and Philosophy
- ❑ MITRE ATT&CK Defender™ (MAD) – ATT&CK® Fundamentals
- ❑ Getting Started with ATT&CK®
- ❑ ATT&CK® Blog

Defensive Resources

- ❑ ATT&CK®: https://attack.mitre.org
- ❑ Cyber Analytics Repository: https://car.mitre.org/
- ❑ Threat Hunter Playbook: https://github.com/hunters-forge/ThreatHunter-Playbook

Course Goals: By the end of this course, students should be able to:

- ❑ Map to ATT&CK® from both narrative reporting and raw data
- ❑ Effectively store and display ATT&CK®-mapped data
- ❑ Leverage ATT&CK® Navigator for analysis
- ❑ Perform CTI analysis using ATT&CK®-mapped data
- ❑ Provide actionable defensive recommendations based on ATT&CK®-mapped data

Course Outline

Module 1 | Mapping to ATT&CK® from Narrative Reports

- Lesson 1.1: Challenges, Advantages, and the Process of Mapping to ATT&CK®
- Lesson 1.2: Identify and Research Behaviors
- Lesson 1.3: Translate Behaviors to Tactics, Techniques, and Sub-techniques
- Lesson 1.4: Mapping to a Narrative Report
- Lesson 1.5: Comparing Your Results

Module 2 | Mapping to ATT&CK® from Raw Data

- Lesson 2.1: The Process of Mapping from Raw Data
- Lesson 2.2: Identify and Research Behaviors
- Lesson 2.3: Translate Behaviors to Tactics, Techniques, and Sub-techniques
- Lesson 2.4: Raw Data to Narrative Reporting

Module 3 | Storing and Analyzing ATT&CK®-Mapped Data

- Lesson 3.1: Storing and Displaying ATT&CK®-mapped Data
- Lesson 3.2: Expressing ATT&CK®-mapped Data
- Lesson 3.3: Analyzing ATT&CK®-mapped Data
- Lesson 3.4: Comparing Layers in ATT&CK® Navigator

Module 4 | Making Defensive Recommendations from ATT&CK®-Mapped Data

- Lesson 4.1: The Defensive Recommendation Process
- Lesson 4.2: Research How Techniques and Sub-techniques are Being Used & the Defensive Options
- Lesson 4.3: Research Organizational Capabilities and Constraints & Determine Trade-offs
- Lesson 4.4: Make Defensive Recommendations
- Lesson 4.5: Prioritize and Customize Defensive Recommendations