Module 0:
Introducing MITRE ATT&CK® for Cyber Threat Intelligence Training

Adam Pennington

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Lesson 0.1: Introducing ATT&CK® for Cyber Threat Intelligence

Lesson 0.1 Objectives

1. Review the Training Goals for ATT&CK for Cyber Threat Intelligence
2. Review the Training Module Overviews
3. Learn about how ATT&CK can help with Cyber Threat Intelligence

Training Goals

0 Why ATT&CK is useful for cyber threat intelligence (CTI)

1 How to map to ATT&CK from both narrative reporting and raw data

2 How to store and display ATT&CK-mapped data and what you should consider when doing that

3 How to perform CTI analysis using ATT&CK-mapped data

4 How to make defensive recommendations

Training Overview

- Module 0: Introducing ATT&CK for CTI Training
  - Topic introduction and Training Goals
- Module 1: Mapping to ATT&CK from Narrative Reporting
  - Topic introduction
  - Exercise 1: Mapping to ATT&CK from external narrative reporting (Self-administered exercise in the Resources section)
  - Exercise 1 Review
- Module 2: Mapping to ATT&CK from Raw Data
  - Topic introduction
  - Exercise 2: Mapping to ATT&CK from raw data (Self-administered exercise in the Resources section)
  - Exercise 2 Review

Training Overview

- Module 3: Storing and Analyzing ATT&CK-mapped Intelligence
  - Topic introduction
  - Exercise 3: Comparing layers in ATT&CK Navigator
    (Do it yourself with materials in the Resources section and on https://mitre-attack.github.io/attack-navigator/)
  - Going over Exercise 3
- Module 4: Making ATT&CK-mapped Data Actionable with Defensive Recommendations
  - Topic introduction
  - Exercise 4: Making defensive recommendations
    (Do it yourself with materials on attack.mitre.org/training/cti)
  - Going over Exercise 4 and wrap-up

Cyber Threat Intelligence

Threat intelligence is actionable knowledge and insight on adversaries and their malicious activities enabling defenders and their organizations to reduce harm through better security decision-making.

-Sergio Caltagirone

Threat Intelligence – How ATT&CK Can Help

- Use knowledge of adversary behaviors to inform defenders

- Structuring threat intelligence with ATT&CK allows us to…
  - *Compare* behaviors
    - Groups to each other
    - Groups over time
    - Groups to defenses
  - *Communicate* in a common language

Communicate to Defenders

Communicate Across the Community

Lesson 0.1 Summary

1. Reviewed the Training Goals for ATT&CK for Cyber Threat Intelligence
2. Reviewed the Training Module focus areas
3. Examined how ATT&CK can assist with Cyber Threat Intelligence by offering a common language and structure

ATT&CK for CTI

Module 0

ATT&CK®

Understand ATT&CK

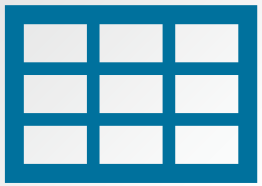
0

Module 01
Module 02

Map Narrative & Raw Data to ATT&CK

1-2

Module 03



Store & Analyze ATT&CK-mapped Data

3

Module 04

Make Defensive Recommendations from ATT&CK-mapped Data

4

Next Up:

Module 1:
Mapping to ATT&CK from Narrative Reports

End of Module 0

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®