Blue Team Level 1 (Standard)
SI4) Correlation
6 Topics | 1 Qu
SI5) Using Splunk
5 Topics | 2 Qu
INCIDENT RESPON
IR1) Introduction
8 Topics | 1 Qu
IR2) Preparation F
10 Topics | 2 C
IR3) Detection an
7 Topics | 4 Qu

Section Introduction, ATT&CK

Blue Team Level 1 Certification (Standard) > IR6) MITRE ATT&CK > Section Introduction, ATT&... IN PROGRESS

The MITRE ATT&CK™ framework is a comprehensive collection of tactics and techniques used by adversaries, which can be utilized by both blue and red team members to improve the security posture of an organization. Below we will cover some applications for defensive and offensive purposes.

FOR DEFENSIVE ROLES

- By looking at each tactic and technique within the framework, defenders can work out which areas they have good visibility over, and areas that they don't. They can then work to improve visibility and detection capabilities by writing rules or alerts that will trigger on suspicious or malicious activity (a good tool for this is ATT&CK Navigator, which you'll be using later!).
- Threat hunters can also use this tactics and techniques to proactively hunt for malicious activity inside the network, working to discover and stop covert or unknown threats.

FOR OFFENSIVE ROLES

- Adversary emulation is the process of performing a penetration test or red team exercise while copying the tactics and techniques of a threat actor that is likely to target the organization. For example, if we work for a telecommunications company, then APT 19 may want to target us, as they have attacked organisations in the same industry before. We could task our offensive security team with attacking the organisation, but copying the techniques used by APT 19. This will allow the blue team to test their detection capability, and if there are any blind spots the red team will report on this so they can be addressed.

The following lessons will introduce you to the 12 stages in the ATT&CK framework, so that you can feel more confident mapping cyberattacks to these steps, and improve your understanding of tactics and techniques used by adversaries during cyber operations. We will also provide further reading material if you wish to learn more about this framework, and we'll also include links to MITRE's own training courses.

Previous Lesson
Mark Complete ✓
Back to Lesson
Next Topic