Blue Team Level 1 Certification (Standard)
8 Topics | 1 Quiz
PA6) Taking Defensive Actions
12 Topics | 1 Quiz
PA7) Report Writing
7 Topics | 1 Quiz
PA8) Phishing Response Challenge
3 Topics | 1 Quiz
THREAT INTELLIGENCE DOMAIN
TI1) Introduction to Threat Intelligence
7 Topics
TI2) Threat Actors & APTs
6 Topics | 2 Quizzes
Section Introduction, Actors
Common Threat Agents
Motivations
Actor Naming Conventions
What are APTs?
Tools, Techniques, Procedures
Activity) Threat Actor Research
Activity) End of Section Review, Actors
TI3) Operational Threat Intelligence
7 Topics | 1 Quiz
TI4) Tactical Threat Intelligence
7 Topics | 1 Quiz
TI5) Strategic Threat Intelligence
5 Topics | 1 Quiz
TI6) Malware and Global Campaigns
6 Topics | 1 Quiz
DIGITAL FORENSICS DOMAIN
DF1) Introduction to Digital Forensics
5 Topics
DF2) Forensics Fundamentals
10 Topics | 5 Quizzes
DF3) Digital Evidence Collection
8 Topics | 1 Quiz
DF4) Windows Investigations
3 Topics | 3 Quizzes
DF5) Linux Investigations
4 Topics | 2 Quizzes
DF6) Volatility
3 Topics | 1 Quiz
DF7) Autopsy
4 Topics | 1 Quiz
SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN
SI1) Introduction to SIEM
7 Topics | 1 Quiz
SI2) Logging
6 Topics | 2 Quizzes
SI3) Aggregation
2 Topics | 1 Quiz

Tools, Techniques, Procedures

Known as "Tools, Techniques and Procedures", or "Tactics, Techniques and Procedures".

TTPs are the actions that threat actors take when conducting cyber attacks. They're used by defenders to track the tactics that different threat groups use, and lets us gather intelligence to aid security operations teams. By understanding how malicious actors perform attacks, we can implement defenses to stop or slow them down.

MITRE's ATT&CK Framework has over 260 different techniques mapped and split into 12 different categories:

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

EXAMPLE ONE

Let's go through an example. If security analysts at Organization A discover a script that is exfiltrating data, this will be mapped to a TTP. In this case, it is T1020. Now the security analysts and incident response team can use this to work backwards, identifying how the attackers gained initial access and conducted other activities such as privilege escalation and lateral movement. All of this information can be mapped as an attack path, and used to fully understand cyber attacks, how successful cyber attacks have occurred, and how to prevent a similar attack in the future.

Each TTP in the MITRE ATT&CK Framework also has mitigations and detection advice. If we look at this information for T1020, we're provided with the following:

Mitigations

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

Detection

Monitor process file access patterns and network behavior. Unrecognized processes or scripts that appear to be traversing file systems and sending network traffic may be suspicious.

Over time, defenders are able to build up attack paths for different incidents, and this process can potentially provide attribution for certain groups. If security analysts at Organization A observe a threat actor following a specific TTP path, they can see if any known APTs follow the same or a similar path, and then to a reasonable degree can attribute that group to the observed attack. The organization can then start implementing defenses against other tactics and malware this group uses as a proactive measure.

SI4) Correlation
6 Topics | 1 Quiz
SI5) Using Splunk
5 Topics | 2 Quizzes
INCIDENT RESPONSE DOMAIN
IR1) Introduction to Incident Response
8 Topics | 1 Quiz
IR2) Preparation Phase
10 Topics | 2 Quizzes
IR3) Detection and Analysis Phase
7 Topics | 4 Quizzes
IR4) Containment, Eradication, and Recovery Phase
5 Topics | 1 Quiz
IR5) Lessons Learned and Reporting
7 Topics
IR6) MITRE ATT&CK
13 Topics | 2 Quizzes

PROACTIVE DEFENSE

Instead of waiting for attacks to happen and recording the TTPs that were used, security teams could take a proactive approach and go through different TTPs looking to see if the organization has appropriate security controls and monitoring capabilities to detect and stop attackers using these known techniques. Penetration tests could be conducted with specific attack paths to see if they are effective, or if the company's defenses work to detect and defend against them. MITRE has a page dedicated to listing the TTPs used by certain threat groups (https://attack.mitre.org/groups/) so if an organization determined that APT30 is likely to get them, they could go through APT30's TTPs and ensure that defenses and monitoring capabilities are put in place.

Previous Topic
Mark Complete
Back to Lesson