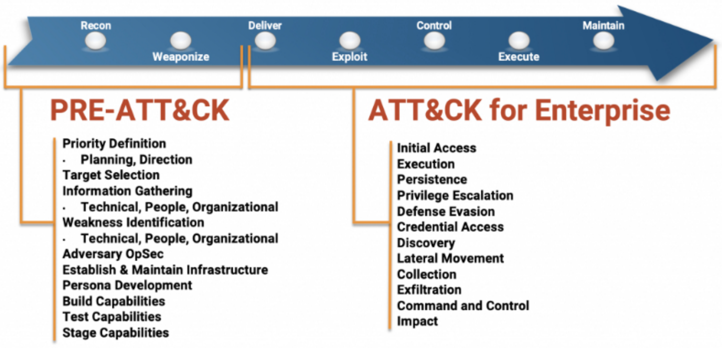
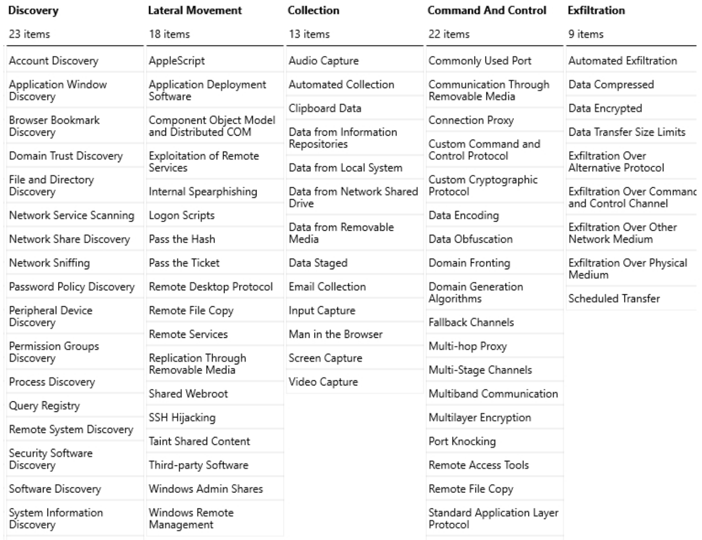
# MITRE ATT&CK Framework

Blue Team Level 1 Certification (Standard) > TI3) Operational Threat Intelligence > MITRE ATT&... **IN PROGRESS**

MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) is a knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target. Since it was introduced in 2013, it has become one of the most respected and referenced resources for cyber security professionals. This model consists of tactics, techniques and procedures and contains exhaustive information about types of attacks and their corresponding behavior. The primary use case of ATT&CK is for identifying the behavior of APTs and it explores the various ways that these APTs can compromise a computer and/or network.



As of writing, there are over 250 techniques that correspond with the tactics and would be too exhaustive to include here. Below is a screenshot of a small section of the Attack Navigator platform on Github.io. Take a look for yourself!



| Discovery | Lateral Movement | Collection | Command And Control | Exfiltration |
|---|---|---|---|---|
| 23 items | 18 items | 13 items | 22 items | 9 items |
| Account Discovery | AppleScript | Audio Capture | Commonly Used Port | Automated Exfiltration |
| Application Window Discovery | Application Deployment Software | Automated Collection | Communication Through Removable Media | Data Compressed |
| Browser Bookmark Discovery | Component Object Model and Distributed COM | Clipboard Data | Connection Proxy | Data Encrypted |
| Domain Trust Discovery | Exploitation of Remote Services | Data from Information Repositories | Custom Command and Control Protocol | Data Transfer Size Limits |
| File and Directory Discovery | Internal Spearphishing | Data from Local System | Custom Cryptographic Protocol | Exfiltration Over Alternative Protocol |
| Network Service Scanning | Logon Scripts | Data from Network Shared Drive | Data Encoding | Exfiltration Over Commanc and Control Channel |
| Network Share Discovery | Pass the Hash | Data from Removable Media | Data Obfuscation | Exfiltration Over Other Network Medium |
| Network Sniffing | Pass the Ticket | Data Staged | Domain Fronting | Exfiltration Over Physical Medium |
| Password Policy Discovery | Remote Desktop Protocol | Email Collection | Domain Generation Algorithms | Scheduled Transfer |
| Peripheral Device Discovery | Remote File Copy | Input Capture | Fallback Channels | |
| Permission Groups Discovery | Remote Services | Man in the Browser | Multi-hop Proxy | |
| Process Discovery | Replication Through Removable Media | Screen Capture | Multi-Stage Channels | |
| Query Registry | Shared Webroot | Video Capture | Multiband Communication | |
| Remote System Discovery | SSH Hijacking | | Multilayer Encryption | |
| Security Software Discovery | Taint Shared Content | | Port Knocking | |
| Software Discovery | Third-party Software | | Remote Access Tools | |
| System Information Discovery | Windows Admin Shares | | Remote File Copy | |
| | Windows Remote Management | | Standard Application Layer Protocol | |

## ATT&CK FOR THREAT INTEL

● 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

○ 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

**BTL1 EXAM**

○ Exam Preparation

○ Using RDP and SSH

○ How to Start Your Exam

ATT&CK gives analysts a common language to structure, compare, and analyze threat intelligence.

- Getting Started with ATT&CK: Threat Intelligence Blog Post: This blog post describes how you can get started using ATT&CK for threat intelligence at three different levels of sophistication
- ATT&CKing Your Adversaries Presentation: This presentation covers how to use ATT&CK to take cyber threat intelligence and operationalize it into behaviors that can drive relevant detections.
- Blog posts on threat intelligence: These blog posts explain the fundamentals of how to use ATT&CK for threat intelligence.
- ATT&CKing the Status Quo Presentation: This middle part of this presentation provides an introduction to using ATT&CK for threat intelligence. Slides are also available.
- ATT&CKing with Threat Intelligence Presentation: This presentation provides perspective on how to use threat intelligence for ATT&CK-based adversary emulation. Slides are also available.
- ATT&CK Navigator Use Case for Threat Intelligence: This demo provides an overview of the ATT&CK Navigator as well as a threat intelligence use case for how to compare group behaviors. A corresponding written tutorial on comparing Navigator layers is available here.

## ATT&CK vs. KILL CHAIN

Similar to the Cyber Kill Chain by Lockheed Martin, ATT&CK is used to describe the phases of a cyber-attack. However, the primary difference between the two, is that the Cyber Kill Chain proposes a well-defined sequence of events, while an ATT&CK scenario defines the techniques used on a case to case basis. Using the ATT&CK framework helps identify specifically how an attack was performed and using their website, lets any security researcher explore both methods of attacks and APT groups that use them. The Cyber Kill Chain is an overall more generic method of identifying an attack and that is why many security professionals prefer the ATT&CK framework or a hybrid solution of both.

‹ Previous Topic

Mark Complete ✓

Next Topic ›

Back to Lesson