



# Mapping Cyberbit Range to MITRE ATT&CK for Enhanced Training

## **Introduction**

When an organization is breached, attackers will remain on networks for months before being detected. Once the attacker has been detected, there are a myriad of questions to answer:

- How did the attacker enter the network?
- How is the attacker moving around on the network?
- What action is the attacker taking while on the network?

For an experienced professional, many of the questions are second nature. However, mapping your training to the MITRE ATT&CK (Adversarial Tactics, Techniques, & Common Knowledge) Framework ensures that not only are these questions asked; they are answered as well.

## **About MITRE ATT&CK**

MITRE's ATT&CK Framework is defined as globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. The framework describes how attackers penetrate networks and then move laterally, escalate privileges, create a persistent state, or generally evade your defenses. ATT&CK looks at the "problem" from the perspective of the attacker, helping cybersecurity professionals determine what goals the attacker is aiming to achieve and what methods the attacker will use to achieve their goals. The Framework organizes attacker behaviors into a series of tactics, specific technical objectives that an attacker wants to achieve. For example, an attacker may perform lateral movement to move to a different part of the network where the specific data they are looking for is waiting to be exfiltrated.

Within each tactic category ATT&CK defines a series of techniques. Each technique describes one way an attacker may attempt to achieve their objective. Each tactic contains multiple techniques because different attackers may deploy different attack methodologies based on their own knowledge or circumstance (availability of tools, system configuration, etc.). Each technique defined in ATT&CK includes a description of the method deployed by the attacker, the systems or platforms the methodologies apply to, and, where known, which attackers or attack groups have been associated with the defined technique. Techniques also provide the process by which the SOC team can mitigate attacker behavior along with any published references to the technique being deployed.

Another important use of ATT&CK is to help you learn how to detect an attacker's actions on your network. The ATT&CK Framework includes resources that are purpose built to help you develop analytics that detect the techniques used by attackers as they attempt to breach, explore, and exfiltrate data from your databases. ATT&CK will also provide information on hacking collectives or groups and the campaigns they've conducted, allowing you to be as prepared as possible for a future attack.

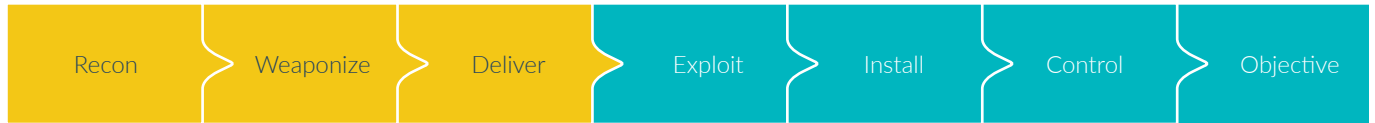
ATT&CK helps you understand how attackers might operate so that you can plan and build response playbooks to mitigate attacker incidents. Armed with this knowledge and "attack playbooks" you are now better prepared to understand how your adversaries prepare for, launches, and execute their attacks to achieve specific desired objectives.

# Enterprise Matrix in the ATT&CK Framework

ATT&CK Enterprise and PRE-ATT&CK combine to form the full list of tactics that align with the [Cyber Kill Chain](#). While PRE-ATT&CK mostly aligns with the first three phases the Cyber Kill Chain, ATT&CK Enterprise aligns with the final four phases.

PRE-ATTACK

ENTERPRISE



The Enterprise Matrix included in the ATT&CK Framework consists of 12 tactics that attackers may use to breach and exfiltrate data from your network. The Matrix includes techniques spanning Windows, macOS, Linux, AWS, GCP, Azure, Azure AD, Office365 and SaaS tools. You can use the [MITRE ATT&CK Navigator](#) to filter through the different tactics and their assigned MITRE ATT&CK Techniques. This framework is on the MITRE Git and makes navigating attack techniques significantly easier.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-By Compromise	AppletCscript	Access_token_profile and Iaahtrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppletScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Batch History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	Account Manipulation	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted for Impact	
Hardware Additions	Compiled HTML File	AppCert DLLs	AppCert DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	File and Directory Discovery	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppCert DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Exploitation of Remote Services	Data from Local System	Custom Cryptographic Protocol	Disk Content Wipe	Disk Structure Wipe
Spearghishing Attachment	Control Panel Items	Application Shimming	Application Shimming	CMSTP	Credentials in Registry	Network Service Scanning	Internal Spearphishing	Data from Network Shared Drive	Data Encoding	EvilWinlogon Over Command and Control Channel	Endpoint Denial of Service
Spearghishing Link	Dynamic Data Exchange	Authentication Package	Bypass User Account Control	Code Signing	Credentials in Registry	Network Sniffing	Logon Scripts	Data from Removable Media	Data Obfuscation	Firmware Corruption	
Spearghishing via Service	Execution through API	BITS Jobs	DLL Search Order Hijacking	Compile After Delivery	Exploitation for Credential Access	Password Policy Discovery	Pass the Hash	Data Staged	Domain Fronting	EvilWinlogon Over Other Network Medium	Inhibit System Recovery
Supply Chain Compromise	Execution through Module Load	Bootkit	Dylib Hijacking	Compiled HTML File	Forced Authentication	Peripheral Device Discovery	Pass the Ticket	Email Collection	Domain Generation Algorithms	EvilWinlogon Over Physical Medium	Network Denial of Service
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Elevated Execution with Prompt	Component Firmware	Hooking	Permission Groups Discovery	Remote Desktop Protocol	Input Capture	Failback Channels	Resource Hijacking	
Valid Accounts	Graphical User Interface	Change Default File Hijacking	Component Object Model Hijacking	Component Object Model Hijacking	Input Prompt	Process Discovery	Remote File Copy	Man in the Browser	Query Registry	Runtime Data Manipulation	
	Install/Uninstall	Component Firmware	Exploitation for Privilege Escalation	Control Panel Items	Kernelboasting	Query Registry	Remote Services	Screen Capture	Multi-hop Proxy	Service Stop	
	Launchctl	Component Object Model Hijacking	Extra Window Memory Injection	DCShadow	Keychain	Remote System Discovery	Replication Through Removable Media	Video Capture	Multi-Stage Channels	Stored Data Manipulation	
	Local Job Scheduling	Create Account	File System Permissions Weakness	DaclFuzzable/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Software Discovery	Shared Webroot	SSH Hijacking	Port Knocking	System Shutdown/Reboot	
	LSASS Driver	DLL Search Order Hijacking	File System Permissions Weakness	Disabling Security Tools	Network Sniffing	System Information Discovery	Taint Shared Content	Third-party Software	Remote Access Tools	Transmitted Data Manipulation	
	Mhta	Dylib Hijacking	Hooking	DLL Search Order Hijacking	Password Filter DLL	System Network Configuration Discovery	Windows Admin Shares	Windows Remote Management	Remote File Copy		
	PowerShell	Image File Execution Options Injection	Launch Daemon	DLL Side-Loading	Private Keys	System Network Connections Discovery	Windows Remote Management	Standard Application Layer Protocol	Remote File Copy		
	Regsvcs/Regasm	External Remote Services	Launch Daemon	Execution Guardrails	Security Memory	System Owner/User Discovery	Windows Remote Management	Standard Cryptographic Protocol	Remote File Copy		
	Regsvr32	File System Permissions Weakness	New Service	Exploitation for Defense Evasion	Steel Web Session Cookie	System Service Discovery	Windows Remote Management	Standard Non-Application Layer Protocol	Remote File Copy		
	Rundll32	Hidden Files and Directories	Parent PID Spoofing	Extra Window Memory Injection	Two-factor Authentication Interception	System Time Discovery	Windows Remote Management	Uncommonly Used Port	Remote File Copy		
	Scheduled Task	Hooking	Path Interception	File and Directory Permissions Modification	Virtualization/Sandbox Evasion			Web Service			
	Scripting	Hypervisor	Port Monitors	File Deletion							
	Service Execution	Image File Execution Options Injection	Port Monitors	File System Logical Offsets							
	Signed Binary Proxy Execution	Kernel Modules and Extensions	PowerShell Profile	Outkeeper Bypass							
	Signed Script Proxy Execution	Kernel Modules and Extensions	Process Injection	Group Policy Modification							
	Source	Launch Agent	Scheduled Task	Hidden Files and Directories							
	Space after Filename	Launch Daemon	Service Registry Permissions Weakness	Hidden Users							
	Third-party Software	Launchctl	Setuid and Setgid	Hidden Window							
	Trap	LC_LOAD_DLLB Addition	Setuid and Setgid	Hidden Window							
	Trusted Developer Utilities	Local Job Scheduling	SID-History Injection	HISTCONTROL							
	User Execution	Startup Items	Sudo	Indicator Blocking							
	Windows Management Instrumentation	Login Items	Sudo Caching	Indicator Removal from Tools							
	Windows Remote Management	Logon Scripts	LSASS Driver	Indicator Removal from Host							
	XSL Script Processing	LSASS Driver	Valid Accounts	Indirect Command Execution							
		Modify Existing Service	Web Shell	Install Root Certificate							
		Netsh Helper DLL		Install/Uninstall							
		New Service		Launchctl							
		Office Application Startup		LC_MAIN Hijacking							
		Path Interception		Masquerading							
		Plist Modification		Modify Registry							
		Port Knocking		Mhta							
		Port Monitors		Network Share Connection Removal							
		PowerShell Profile		NTFS File Attributes							
		Rccommon		Obfuscated Files or Information							
		Re-opened Applications		Parent PID Spoofing							
		Redundant Access		Plist Modification							
		Registry Run Keys / Startup Folder		Port Knocking							
		Scheduled Task		Process Doppelganging							
		Screensaver		Process Hollowing							
		Security Support Provider		Process Injection							
		Server Software Component		Redundant Access							
		Service Registry Permissions Weakness		Regsvcs/Regasm							
		Setuid and Setgid		Regsvr32							
		Shortcut Modification		Rootkit							
		SID and Trust Provider Hijacking		Rundll32							
		Startup Items		Scripting							
		System Firmware		Signed Binary Proxy Execution							
		System Service		Signed Script Proxy Execution							
		Time Providers		SIR and Trust Provider Hijacking							
		Trap		Software Packing							
		Valid Accounts		Space after Filename							
		Web Shell		Template Injection							
		Windows Management Instrumentation Event Subscription		Timestamp							
		Windows Helper DLL		Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

## **How does the ATT&CK Framework help advance SOC Team Operations?**

MITRE ATT&CK helps companies who are interested in in threat-informed defense. The frameworks help you to identify attacks and likely threat actors by helping you map the way malicious actors behave on your network. By breaking down the different techniques and mapping them together, Blue Teams can use ATT&CK to anticipate an attackers next move or a Red Team can mimic an incident using known attack methodologies from specific hacking collectives. To learn more about getting started with MITRE ATT&CK you can check out their whitepaper: [Getting Started with ATT&CK](#).

## **Mapping Training and Education Programs to MITRE ATT&CK**

### **For Educators**

Ensuring your students are armed with the “attacker playbook” will ensure their success while working in a SOC. MITRE ATT&CK is a valuable reference tool to develop curriculums, coursework, seminars, and research of different combinations of attack techniques. Knowledge of attacker behavior is vital to the success of students who plan to have a bright future in cybersecurity. For example: if a student is knowledgeable enough to understand that attackers who use certain entry techniques will usually also perform lateral movement as their next step and be familiar with the different techniques that can be used by attackers to achieve this goal, they can mitigate the lateral movement, and thus the attack itself. Taking the next step and allowing your students to experience the technique on a cyber range will give them the experience to identify the technique in the real-world, giving your students a leg up on the malicious actor.

### **For SOC Managers and CISOs**

Preventing a critical attack is one of the primary responsibilities of any SOC. Critical to achieving this goal is advance knowledge of how your attacker will behave when attempting or after they successfully breach a network. Since a lack of skilled staff is the top issue facing a SOC for the past two years (SANS SOC Survey 2019), arming your team with the knowledge of attacker behavior and allowing them to train against these known behaviors gives your SOC team an advantage when attempting to expel and lock out an attacker from your network. Building your training plan with MITRE ATT&CK at the forefront ensures that you can expose your team to many of the techniques outlined in ATT&CK, ensuring true preparation in the face of any attack. Training your team on a cyber range allows them to mitigate the techniques being used, ensuring that your team will be able to perform when they see a malicious attacker on the network they've been tasked with protecting.

### **For Recruiters and HR Managers**

It is becoming increasingly difficult and competitive for you to hire candidates who are truly qualified to be a member of the SOC team in your organization. Mapping recruiting guidelines to MITRE ATT&CK will allow you to accurately test if incoming Pen Testers can execute the techniques they should be able to given the skills they may claim to have. Additionally, Blue Team members should also have intimate knowledge of MITRE ATT&CK to ensure they know how attacker behave. Possessing this knowledge will allow potential job candidates to perform more effectively and efficiently in their role. Testing incoming Blue and Red Team members on a cyber range against live attacks can provide evidence to their knowledge of MITRE ATT&CK and prove their strategic ability to mitigate incidents while they are occurring on a network.

## Mapping Cyberbit Range to MITRE ATT&CK

Cyberbit Range and all scenarios included within Cyberbit Range are mapped to the techniques and methodologies used by attackers as set out by MITRE ATT&CK. This will allow you to break down your training so that your team is exposed, in real time, to the different techniques and methodologies outlined by ATT&CK, ensuring that your team will be prepared for the inevitable attack when it comes.

In order to fully grasp the number of techniques students or trainees will be exposed to in a single scenario on Cyberbit Range, we have broken down a few of our scenarios:

### Dragonfly

Today more than ever, the human factor is the focus of attacks over the internet - targeting users as the weakest link in the security chain. In this attack scenario, a seemingly innocent email can be the source of a sophisticated cyber attack. While closely monitoring the attacker's steps, trainees will get a close look at different attack techniques for lateral movement, privilege escalation and data exfiltration using web vulnerability.



MITRE Techniques in Scenario:

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Lateral Movement	Collection	Command and Control
Spearphishing Link (T1192)	Command-Line Interface (T1059)	Hidden Files and Directories (T1158)	Web Shell (T1100)	Hidden Files and Directories (T1158)	Exploitation of Remote Services (T1210)	Data from Local System (T1005)	Fallback Channels (T1008)
	Exploitation for Client Execution (T1203)	Redundant Access (T1108)		Redundant Access (T1108)		Data Staged (T1074)	Web Service (T1102)
	PowerShell (T1086)	Web Shell (T1100)		Scripting (T1064)		Screen Capture (T1113)	
	Scripting (T1064)			Template Injection (T1221)			
	User Execution (T1204)			Web Service (T1102)			

## Apache Shutdown

This attack scenario emulates an attack on an organization's publicly accessible services. The attack disrupts the operation of the service and utilizes basic methods to strengthen the attacker's foothold in the system. In this scenario, the trainees will be confronted with a disruption to business-critical components and will be required to act swiftly in order to maintain as much up-time as possible and mitigate the attack. The trainees will also witness different techniques for housekeeping and persistence.



MITRE Techniques in Scenario:

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Command and Control	Impact
External Remote Services (T1133)	Local Job Scheduling (T1168)	External Remote Services (T1133)	Scheduled Task (T1053)	Redundant Access (T1108)	Brute Force (T1110)	Network Service Scanning (T1046)	Remote Services (T1021)	Fallback Channels (T1008)	Service Stop (T1489)
Valid Accounts (T1078)	Scheduled Task (T1053)	Local Job Scheduling (T1168)	Valid Accounts (T1078)	Valid Accounts (T1078)				Web Service (T1102)	
		Redundant Access (T1108)		Web Service (T1102)					
		Scheduled Task (T1053)							
		Valid Accounts (T1078)							

## CI Flaw

Domain Admins members have FULL administrative rights to all workstations, servers, Domain Controllers, Active Directory, Group Policy and more. This excessive power makes the domain admin credentials a gold mine for attackers. From slowly collecting pieces of information on the target network using different techniques such as sniffing and brute-forcing, to generating payloads using Metasploit, the trainees will need to find their way to achieve the goal of retrieving the domain admin credentials.



MITRE Techniques in Scenario:

Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Credential Access	Discovery
Graphical User Interface (T1061)	File System Permissions Weakness (T1044)	Hooking (T1179)	Masquerading (T1036)	Brute Force (T110)	Network Sniffing (T1040)	Exploitation of Remote Services (T1210)
PowerShell (T1086)	Hooking (T1179)		Redundant Access (T1108)	Credential Dumping (T1003)	Software Discovery (T1518)	Remote Desktop Protocol (T1076)
Scripting (T1064)	Redundant Access (T1108)		Scripting (T1064)	Forced Authentication (T1187)	System Network Configuration Discovery (T1016)	
Service Execution (T1035)	Shortcut modification (T1023)			Hooking (T1179)	System Owner/User Discovery (T1033)	
				Network Sniffing (T1040)		

## About Cyberbit Range

Cyberbit Range is a cybersecurity training platform providing SOC teams with the closest possible experience of a real-world cybersecurity incident. The platform simulates real-world cyberattacks which are injected into a virtual network. Trainees are immersed in a virtual SOC, where they practice responding to the attacks using commercially licensed security tools like the ones they would use in their day-to-day work. Cyberbit Range provides scenarios ranging from entry-level network security to extensive multi-stage attacks, ransomware, DDoS and Trojans. The combination of real-world attacks, networks and security tools, results in a hyper-realistic experience that dramatically improves trainees' skill levels, reduces time-to-respond, and improves soft skills like teamwork and communications.

### Key Capabilities of Cyberbit Range



**Automated Cyberattack Simulation** accurately simulates attack scenarios ranging from basic threats to complex multi-stage attacks



**Individual and Team Training** to work on both individual skills as well as teamwork and communication skills



**Comprehensive Virtual Networks** are included within Cyberbit Range, resembling a typical corporate network infrastructure



**Automated Trainee Assessment** tracks and grades users automatically based on their performance



**Real-World Security Tools** including commercial SIEMs, firewalls, and endpoint security tools



**OT Training Options** enabling critical infrastructure security and network staff to train in responding to OT specific and IT/OT attacks

## ABOUT CYBERBIT™

Cyberbit provides hands-on cybersecurity education and training and addresses the global cybersecurity skill gap through its world-leading cyber range platform. Colleges and universities use Cyberbit Range to increase student enrollment and retention, train industry organizations, and position their institution as regional cybersecurity hubs by providing simulation-based learning and training. The Cyberbit Range platform delivers a hyper-realistic experience that immerses learners in a virtual security operations center (SOC),

where they use real-world security tools to respond to real-world, simulated cyberattacks. As a result, it prepares students for their careers in cybersecurity from day-one after their graduation and reduces the need to learn on the job. Cyberbit delivers over 100,000 training sessions annually across 5 continents. Customers include Fortune 500 companies, MSSPs, system integrators, higher education institutions and governments. Cyberbit is headquartered in Israel with offices in the US, Europe, and Asia.