

A Guide to MITRE ATT&CK for SOC Teams & Corresponding MITRE ATT&CK Cheat Sheet

🚀 As a Security Operations Team, your goal is to protect the system from incoming threats. Not only that, but you must be the first to know when a breach takes place. This means you are responsible for protection and detection, as well as incident response and recovery. You must also identify potential threats in your system to take pre-emptive measures by blocking as many attack pathways as possible while seamlessly integrating these measures in a way that does not disrupt organizational or business operations.

To do this, you must have a clear-cut understanding of adversaries' potential threats by analyzing their most commonly used tools and techniques. This is where MITRE ATT&CK comes into play...

What is MITRE ATT&CK?

🌟 MITRE ATT&CK can be viewed as a comprehensive, structured knowledge base of adversary tactics and techniques based on real-world observations. It aids SOC teams in understanding how adversaries operate, identifying gaps in security posture, and improving threat detection and response strategies within their domain.

MITRE | ATT&CK[®]

Matrices ▾Tactics ▾Techniques ▾Defenses ▾CTI ▾Resources ▾BenefactorsBlog 🌐Search 🔍

ATT&CK Matrix for Enterprise

layout: side ▾show sub-techniqueshide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	44 techniques	17 techniques	32 techniques	9 techniques	17 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)
Gather Victim Host Information (4)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (11)	BITS Jobs	Access Token Manipulation (3)	Access Token Manipulation (3)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture
Gather Victim Network Information (6)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (8)	Boot or Logon Autostart Execution (14)	Debugger Evasion	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process (3)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Domain or Tenant Policy Modification (2)	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery	Container and Resource Discovery	Data from Cloud Storage
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (3)	Domain or Tenant Policy Modification (2)	Execution Guardrails (2)	Modify Authentication Process (6)	Container and Resource Discovery	Debugger Evasion	Data from Configuration Repository (2)
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (17)	Escape to Host	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	Device Driver Discovery	Software Deployment Tools	Data from Information Repositories (3)
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote Services	Event Triggered Execution (17)	File and Directory Permissions Modification (2)	Multi-Factor Authentication Request Generation	Domain Trust Discovery	Taint Shared Content	Data from Local System
			Software Deployment Tools	Hijack Execution Flow (13)	Exploitation for Privilege Escalation	Hide Artifacts (12)	Multi-Factor Authentication Request Generation	File and Directory Discovery	Use Alternate Authentication Material (4)	Data from Network Shared Drive
			System Services (2)	Hijack Execution Flow (13)	Hijack Execution Flow (13)	Hijack Execution Flow (13)	Network Sniffing	Group Policy Discovery		Data from Removable Media
			User Execution (3)	Implant Internal		Impair Defenses (11)		Log Enumeration		
			Windows							

MITRE ATT&CK homepage

When SOC teams create security rules, such as firewall or SIEM rules, they must ensure that their rules cover all aspects of the attack vector space that an adversary could potentially exploit.

To understand more than 90% of possible attack tactics and techniques used by adversaries to disrupt an organization's security, SOC teams can use MITRE ATT&CK to ensure that all tactics and their corresponding techniques have associated cybersecurity in place.

Standards such as **NIST** provide a framework for cybersecurity by outlining five key aspects of cybersecurity operations: Identify, Protect, Detect, Respond, and Recover. When combined with MITRE ATT&CK, SOC teams can more effectively align their threat detection and response strategies with these principles. By mapping adversary tactics, techniques, and procedures (TTPs) to the NIST framework, SOC teams can enhance their ability to **identify threats, implement proactive defenses, detect malicious activity, respond to incidents in a structured manner, and recover from cyberattacks efficiently.**

Understanding the Framework

MITRE ATT&CK is structured into three key domains:

 **Enterprise** – Covers traditional IT environments, including small businesses, organizations, schools, and even governments. Tactics employed at the Enterprise level often include exploits targeting modern operating systems such as Windows, macOS, and Linux.

 **Mobile** – Focuses on threats targeting mobile devices and wireless networks. These attacks exploit mobile-specific vulnerabilities, such as those found in Android and iOS.

 **ICS (Industrial Control Systems)** – Addresses security risks in critical infrastructure (e.g., nuclear power plants). Since critical infrastructures often employ domain-specific protocols, additional precautions must be taken to protect against adversaries attempting to target these systems, such as attacks against **PLCs (Programmable Logic Controllers)** used to control things like water levels or heat.

Each domain is organized into a matrix consisting of three core components:

- **Tactics** – General methods employed by adversaries to achieve high-level goals (e.g., Initial Access, Reconnaissance, and Detection). These represent the "why" of an attack.
- **Techniques** – Alongside *Procedures*, they can be considered the "how" of an attack. They are the specific methods adversaries use to achieve their goals (e.g., Active Scanning for Reconnaissance or Phishing for Initial Access). Each technique may have multiple **sub-techniques** (e.g., Spearfishing Attachment and Spearfishing Link as sub-techniques of Phishing). Every technique is assigned a **unique ID** beginning with the letter T (e.g., Phishing has an ID of T1566). Each technique also includes **mitigation and detection strategies** for protection against the technique.

- **Procedures:**

A unique aspect of MITRE ATT&CK is its **vast dataset of adversary procedures**. For every technique, it provides a detailed list of real-world attack steps and tools adversaries use, including specific malware, exploit kits, binaries, and hacking frameworks. For example, APT29 (a famous hacking group) has been observed using Mimikatz for Credential Dumping (T1003), and FIN7 (another famous hacking group) has leveraged PowerShell (T1059.001) for execution. This centralized dataset allows SOC teams and threat hunters to map observed activity to known adversary behaviors, making threat detection and attribution more precise.

MITRE ATT&CK also aligns itself with the **CIA Triad of Cybersecurity (Confidentiality, Integrity, Availability)**, prioritizing tactics and techniques that impact these core principles.

How SOC Teams Use MITRE ATT&CK

SOC teams worldwide use MITRE ATT&CK to correlate logs with attack techniques. Security Information and Event Management (SIEM) tools like Splunk and Elastic Security (ELK Stack) often leverage AI to classify attacks without relying on static manual rule configuration.

Red Team and Blue Team Exercises with MITRE ATT&CK

For **Red Teaming exercises**, MITRE ATT&CK is best utilized as a framework to decide which attacks performed by the red team align with specific categories within the MITRE framework (e.g., **Reconnaissance, Initial Access, Execution, Persistence, etc.**).

For **Blue Teaming exercises**, it allows teams to:

- Map adversary techniques to specific threats.
- Improve their detection and mitigation strategies.
- Analyze past incidents in the context of known adversary behaviors.

MITRE ATT&CK is often referenced in cybersecurity standards to ensure both red and blue teams have a structured approach to assessing and improving an organization's cybersecurity posture.

ATT&CK Navigator

MITRE offers the **ATT&CK Navigator**, a web-based tool for interacting with and customizing the ATT&CK matrices. As MITRE's official website states: *"It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more."*

The Navigator is great for teams looking to utilize MITRE's framework to improve defenses in an organized, well-structured manner, fill in gaps, and visualize the entire attack space with features such as highlighting and scoring certain techniques.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Exfiltration
Active Scanning (0/2)	Acquire Access (0/2)	Content Injection (0/2)	Cloud Administration Command (0/2)	Account Manipulation (0/2)	Abuse Elevation Control Mechanism (0/2)	Abuse Elevation Control Mechanism (0/2)	Adversary-in-the-Middle (4/4)	Account Discovery (4/4)	Exploitation of Remote Services (4/4)	Automated Exfiltration (0/1)
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/3)	Drive-by Compromise (0/3)	Command and Scripting Interpreter (1/1)	BITS Jobs (0/7)	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (4/4)	Application Window Discovery (4/4)	Internal Spearphishing (0/3)	Data Transfer Size Limits (0/1)
Gather Victim Identity Information (0/2)	Compromise Accounts (0/3)	Exploit Public-Facing Application (0/3)	Container Administration Command (0/1)	Boot or Logon Autostart Execution (0/14)	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (4/6)	Browser Information Discovery (4/4)	Automated Collection (0/2)	Exfiltration Over Alternative Protocol (0/3)
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/8)	External Remote Services (0/8)	Deploy Container (0/3)	Boot or Logon Initialization Scripts (0/5)	Account Manipulation (0/7)	Account Manipulation (0/7)	Exploitation for Credential Access (0/2)	Cloud Infrastructure Discovery (0/2)	Remote Service Session Hijacking (0/2)	Exfiltration Over C2 Channel (0/3)
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Hardware Additions (0/4)	Exploitation for Client Execution (0/4)	Browser Extensions (0/2)	Boot or Logon Autostart Execution (0/2)	Boot or Logon Autostart Execution (0/2)	Forced Authentication (0/2)	Cloud Service Discovery (0/2)	Remote Services (0/8)	Exfiltration Over Other Network Medium (0/1)
Phishing for Information (0/4)	Establish Accounts (0/3)	Phishing (0/4)	Inter-Process Communication (0/3)	Compromise Host Software Binary (0/2)	Domain or Tenant Policy Modification (0/2)	Domain or Tenant Policy Modification (0/2)	Forge Web Credentials (0/2)	Cloud Storage Object Discovery (0/2)	Replication Through Removable Media (0/2)	Exfiltration Over Web Service (0/4)
Search Closed Sources (0/2)	Obtain Capabilities (0/7)	Replication Through Removable Media (0/3)	Native API (0/5)	Create Account (0/3)	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Input Capture (0/4)	Container and Resource Discovery (0/2)	Data from Cloud Storage (0/2)	Scheduled Transfer (0/4)
Search Open Technical Databases (0/5)	Stage Capabilities (0/6)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/5)	Create or Modify System Process (0/5)	File and Directory Permissions Modification (0/2)	File and Directory Permissions Modification (0/2)	Modify Authentication Process (0/9)	Debugger Evasion (0/2)	Software Deployment Tools (0/2)	Transfer to Cloud Account (0/1)
Search Open Websites/Domains (0/3)	Trusted Relationship (0/4)	Valid Accounts (0/4)	Serverless Execution (0/1)	Event Triggered Execution (0/1)	Domain or Tenant Policy Modification (0/5)	Domain or Tenant Policy Modification (0/5)	Multi-Factor Authentication Interception (0/2)	Device Driver Discovery (0/2)	Taint Shared Content (0/2)	
Search Victim-Owned Websites (0/3)			Shared Modules (0/1)	Event Triggered Execution (0/1)	Hide Artifacts (0/2)	Hide Artifacts (0/2)	Multi-Factor Authentication Request Generation (0/2)	Domain Trust Discovery (0/2)	Use Alternate Authentication Material (0/4)	
			Software Deployment Tools (0/2)	External Remote Services (0/2)	Hijack Execution Flow (0/1)	Hijack Execution Flow (0/1)	Network Sniffing (0/2)	File and Directory Discovery (0/2)	Data from Information Repositories (0/5)	
			System Services (2/2)	Implant (0/3)	Indicator Removal (0/1)	Indicator Removal (0/1)	OS Credential Dumping (0/8)	Log Enumeration (0/2)	Data from Local System (0/2)	
			User Execution (0/3)					Network Service Discovery (0/2)	Data from Network Shared Drive (0/2)	
								Network Share (0/2)	Non-Standard Data (0/2)	

MITRE ATT&CK Navigator example

Cheat Sheet

As there is still a need for SOC teams to understand what each tactic actually means, and it can take some time before the terminology and the definition of each tactic settles along with its context to an attack sequence, we have thus created a cheat sheet to assist SOC teams who are new to the MITRE ATT&CK framework or need a quick refresher.

The cheat sheet provides a concise **summary of each tactic in MITRE's Enterprise ATT&CK matrix**, with practical examples to illustrate their use. This ensures that SOC teams have an easy-access reference for identifying, protecting, detecting, responding, and recovering from cyber threats.

Tactic	Overview	Examples
Reconnaissance	Techniques used to gather information about the target system before launching an attack.	Active Scanning, Phishing for Information, Search Open Websites/Domains
Resource Development	Acquiring resources like credentials, infrastructure, or malware to support an attack.	Acquire Infrastructure, Establish Accounts, Develop Capabilities

Initial Access	Techniques used to gain a foothold within a target network.	Phishing, Exploit Public-Facing Application, Drive-by Compromise
Execution	Executing malicious code to achieve attacker objectives.	Command and Scripting Interpreter, Exploitation for Client Execution, Scheduled Task/Job
Persistence	Maintaining access to the target system after gaining initial access.	Boot or Logon Autostart Execution, Hijack Execution Flow, Account Manipulation
Privilege Escalation	Gaining higher-level permissions to further compromise the system.	Abuse Elevation Control Mechanism, Exploitation for Privilege Escalation, Access Token Manipulation
Defense Evasion	Avoiding detection by security tools and analysts.	Obfuscation/Deobfuscation, Disable Security Tools, Indicator Removal
Credential Access	Stealing or brute-forcing credentials to expand access.	Brute Force, Credential Dumping, Input Capture
Discovery	Identifying system information, security tools, and account privileges.	Network Service Scanning, File and Directory Discovery, Software Discovery
Lateral Movement	Moving within the network to reach valuable assets.	Remote Services, Internal Spearphishing, Lateral Tool Transfer
Collection	Gathering data of interest before exfiltration.	Screen Capture, Keylogging, Audio Capture
Command and Control	Establishing communication between the attacker and compromised systems.	C2 over Web Protocols, Encrypted Channel, Remote Access Software
Exfiltration	Removing sensitive data from the compromised system.	Automated Exfiltration, Exfiltration Over Web, Scheduled Transfer
Impact	Manipulating, disrupting, or destroying systems, data, or services.	Data Encryption for Impact, Disk Wipe, Defacement

MITRE ATT&CK Cheat Sheet for Enterprise Tactics

Conclusion: Message to SOC Teams

Use MITRE ATT&CK. The tools are available to help you enhance your security posture. This framework is continually updated by MITRE to provide the latest intelligence on adversary tactics, techniques, and real-world attack procedures. Leverage this knowledge base to proactively defend against evolving cyber threats.