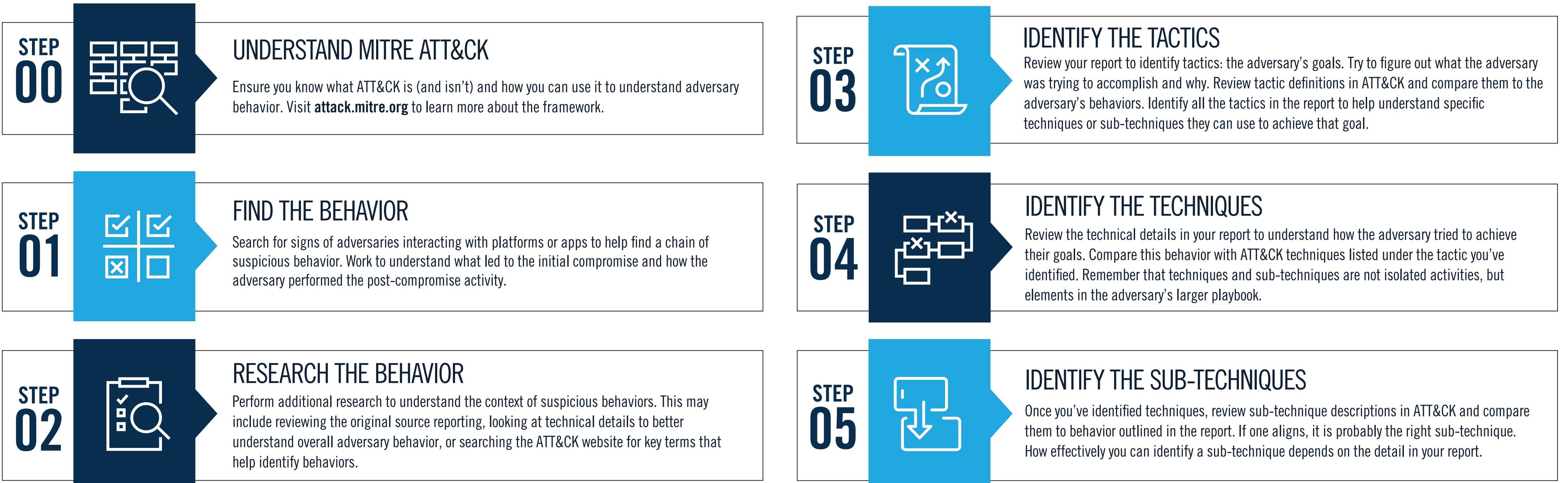




A BEST PRACTICE: MAPPING CYBER THREAT INTELLIGENCE TO ATT&CK

Cyber analysts use the MITRE ATT&CK framework to map real-world TTPs as part of their cyber threat intelligence strategies. The steps below are from CISA's "Best Practices for MITRE ATT&CK Mapping," which outlines key steps to successfully map CTI reports to ATT&CK. <https://www.cisa.gov/uscert/best-practices-mitre-attckr-mapping>



WORST PRACTICES: AVOID THESE ATT&CK PITFALLS

MITRE ATT&CK is one tool in a cyber analyst's toolbox, but it can take some care to use. All too often, defenders try to use ATT&CK in ways in ways that might even hurt their defenses. Here are three common mistakes ATT&CK users make, along with steps you can take to avoid these pitfalls.

TRYING TO ACHIEVE 100% COVERAGE Every organization faces its own unique cyber threats. Not every tactic or technique will apply to everyone. Instead of trying to defend against every tactic or technique in the matrix, prioritize the ones that are most relevant to you and ensure you are prepared for them.	LIMITING YOURSELF TO THE MATRIX Remember, the ATT&CK matrix only documents observed real-world, in-the-wild behaviors. But adversaries may (and probably do) have a series of other behaviors they use that have not yet been documented in ATT&CK. To get a full picture of the threats your organization faces:
SHOUTING “BINGO” WHEN YOU HAVE ONE TECHNIQUE Just because you've identified a single way an adversary has done technique doesn't mean it's time to declare success and color a box green. Adversaries have multiple ways they can perform most ATT&CK techniques. It's great that you've found one, but be sure you're looking for and understand other possible ways a technique might be accomplished.	 1. Leverage your own intelligence sources 2. Create and document your own observed techniques 3. Don't limit yourself to behaviors, a timely indicator can still catch an adversary

attack.mitre.org

- Access ATT&CK technical information
- Contribute to ATT&CK
- Follow our blog
- Watch ATT&CK presentations



@MITREattack

mitre-att&ck

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

To help cyber defenders gain a common understanding of the threats they face, MITRE developed the ATT&CK framework. It's a globally-accessible knowledge base of adversary tactics and techniques based on real world observations and open source research contributed by the cyber community.

Used by organizations around the world, ATT&CK provides a shared understanding of adversary tactics, techniques and procedures and how to detect, prevent, and/or mitigate them.

ATT&CK is open and available to any person or organization for use at no charge.

For more than 60 years, MITRE has worked in the public interest. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | ATT&CK®
Enterprise Framework v15



MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

MITRE ATT&CK® ENTERPRISE FRAMEWORK

RECONNAISSANCE 10 techniques	RESOURCE DEVELOPMENT 8 techniques	INITIAL ACCESS 10 techniques	EXECUTION 14 techniques	PERSISTENCE 20 techniques	PRIVILEGE ESCALATION 14 techniques	DEFENSE EVASION 43 techniques	CREDENTIAL ACCESS 17 techniques	DISCOVERY 32 techniques	LATERAL MOVEMENT 9 techniques	COLLECTION 17 techniques	COMMAND AND CONTROL 18 techniques	EXFILTRATION 9 techniques	IMPACT 14 techniques
Active Scanning	Acquire Infrastructure	Valid Accounts	Scheduled Task/Job		Modify Authentication Process	System Service Discovery	Remote Services	Data from Local System	Data Obfuscation	Exfiltration Over Other Network Medium		Data Destruction	
Gather Victim Host Information	Compromise Accounts	Replication Through Removable Media	Windows Management Instrumentation		Valid Accounts	Network Sniffing	Software Deployment Tools	Data from Removable Media	Fallback Channels	Application Layer Protocol	Scheduled Transfer	Data Encrypted for Impact	
Gather Victim Identity Information	Compromise Infrastructure	Develop Capabilities	Trusted Relationship	Software Deployment Tools	Hijack Execution Flow	OS Credential Dumping	Application Window Discovery	Replication Through Removable Media	Input Capture	Proxy	Data Transfer Size Limits	Inhibit System Recovery	
Gather Victim Network Information	Establish Accounts	Supply Chain Compromise	Create or Modify System Process	Hardware Additions	Boot or Logon Initialization Scripts	Direct Volume Access	Brute Force	System Network Configuration Discovery	Data Staged	Communication Through Removable Media	Defacement	Firmware Corruption	
Obtain Capabilities	Hardware Additions	Shared Modules	Event Triggered Execution	User Execution	Rootkit	Two-Factor Authentication Interception	Internal Spearphishing	Screen Capture	Use Alternate Authentication Material	Email Collection	Web Service	Exfiltration Over C2 Channel	
Stage Capabilities	Exploit Public-Facing Application	Boot or Logon Autostart Execution	Obfuscated Files or Information	Exploitation for Client Execution	Indicator Removal	Exploitation for Credential Access	System Owner/User Discovery	Clipboard Data	Multi-Stage Channels	Use Alternate Authentication Material	Web Service	Resource Hijacking	
Gather Victim Org Information	Acquire Access	Account Manipulation	External Remote Services	Phishing	Process Injection	Exploitation for Credential Access	System Network Connections Discovery	Lateral Tool Transfer	Automated Collection	Clipboard Data	Multi-Stage Channels	Network Denial of Service	
Phishing for Information	External Remote Services	Office Application Startup	System Services	External Remote Services	Access Token Manipulation	Steal Web Session Cookie	Taint Shared Content	Audio Capture	Ingress Tool Transfer	System Network Connections Discovery	Endpoint Denial of Service	System Shutdown/Reboot	
Search Closed Sources	Drive-by Compromise	Command and Scripting Interpreter	Create Account	Abuse Elevation Control Mechanism	Unsecured Credentials	Permission Groups Discovery	Exploitation of Remote Services	Video Capture	Automated Collection	Steal Web Session Cookie	Audio Capture	Exfiltration Over Web Service	
Search Open Technical Databases	Content Injection	Browser Extensions	Domain or Tenant Policy Modification	Native API	Credentials from Password Stores	File and Directory Discovery	Browser Session Hijacking	Traffic Signaling	Automated Collection	Exploit Remote Services	Video Capture	System Shutdown/Reboot	
Search Open Websites/Domains		Traffic Signaling	Escape to Host	Inter-Process Communication	Trusted Developer Utilities	Remote Service Session Hijacking	Remote Access Software	Automated Exfiltration	Exploit Remote Services	Exploit Remote Services	Exploit Remote Services	Account Access Removal	
Search Victim-Owned Websites		BITS Jobs	BITS Jobs	BITS Jobs	Proxy Execution	Forced Authentication	Dynamic Resolution	Protocol Tunneling	Exploit Remote Services	Exploit Remote Services	Exploit Remote Services	Disk Wipe	
		Server Software Escalation	Container Administration Component	Container Administration Command	Steal or Forge Kerberos Tickets	Peripheral Device Discovery	Non-Standard Port	Transfer Data to Cloud Account	Exploit Remote Services	Exploit Remote Services	Exploit Remote Services	Data Manipulation	
			Pre-OS Boot	Pre-OS Boot	Traffic Signaling	Network Share Discovery	Adversary-in-the-Middle	Protocol Tunneling	Exploit Remote Services	Exploit Remote Services	Exploit Remote Services	Financial Theft	
			Deploy Container	Deploy Container	Signed Script Proxy Execution	Password Policy Discovery	Browser Information Discovery	Archive Collected Data	Exploit Remote Services	Exploit Remote Services	Exploit Remote Services		
			Serverless Execution	Serverless Execution	Rogue Domain Controller	Indirect Command Execution	Forge Web Credentials	Encrypted Channel	Data from Information Repositories	Exploit Remote Services	Exploit Remote Services		
			Cloud Administration Command	Cloud Administration Command	BITS Jobs	Multi-Factor Authentication Request Generation	Virtualization/Sandbox Evasion	Non-Standard Port	Non-Standard Port	Exploit Remote Services	Exploit Remote Services		
				Implant Internal Image	XSL Script Processing	Template Injection	Cloud Service Dashboard	Protocol Tunneling	Protocol Tunneling	Exploit Remote Services	Exploit Remote Services		
				Modify Authentication Process	File and Directory Permissions Modification		Software Discovery	Transfer Data to Cloud Account	Transfer Data to Cloud Account	Exploit Remote Services	Exploit Remote Services		
				Power Settings	Virtualization/Sandbox Evasion		Query Registry	Content Injection	Content Injection	Exploit Remote Services	Exploit Remote Services		
					Unused/Unsupported Cloud Regions		Remote System Discovery	Content Injection	Content Injection	Exploit Remote Services	Exploit Remote Services		
					Use Alternate Authentication Material		Network Service Scanning	Content Injection	Content Injection	Exploit Remote Services	Exploit Remote Services		
					Impair Defenses		Process Discovery	Content Injection	Content Injection	Exploit Remote Services	Exploit Remote Services		
					Hide Artifacts		System Information Discovery	Content Injection	Content Injection	Exploit Remote Services	Exploit Remote Services		
					Masquerading		Account Discovery	Content Injection	Content Injection	Exploit Remote Services	Exploit Remote Services		
					Deobfuscate/Decode Files or Information		System Time Discovery	Content Injection	Content Injection	Exploit Remote Services	Exploit Remote Services		
					Signed Binary Proxy Execution		Domain Trust Discovery	Content Injection	Content Injection	Exploit Remote Services	Exploit Remote Services		
					Exploitation for Defense Evasion		Cloud Service Discovery	Content Injection	Content Injection	Exploit Remote Services	Exploit Remote Services		
					Execution Guardrails		Container and Resource Discovery	Content Injection	Content Injection	Exploit Remote Services	Exploit Remote Services		
					Modify Cloud Compute Infrastructure		Cloud Infrastructure Discovery	Content Injection	Content Injection	Exploit Remote Services	Exploit Remote Services		
					Pre-OS Boot		System Location Discovery	Content Injection	Content Injection	Exploit Remote Services	Exploit Remote Services		
					Subvert Trust Controls		Cloud Storage Object Discovery	Content Injection	Content Injection	Exploit Remote Services	Exploit Remote Services		
					Build Image on Host		Group Policy Discovery	Content Injection	Content Injection	Exploit Remote Services	Exploit Remote Services		
					Deploy Container		Debugger Evasion	Content Injection	Content Injection	Exploit Remote Services	Exploit Remote Services		
					Modify System Image		Device Driver Discovery	Content Injection	Content Injection	Exploit Remote Services	Exploit Remote Services		
					Network Boundary Bridging		Log Enumeration	Content Injection	Content Injection	Exploit Remote Services	Exploit Remote Services		
					Weaken Encryption								
					Reflective Code Loading								
					Debugger Evasion								
					Plist File Modification								
					Impersonation								

MITRE | ATT&CK®
Enterprise Framework
attack.mitre.org