VECTRA

How Cognito supports the Mitre ATT&CK framework

To catch a thief, you must think like a thief.

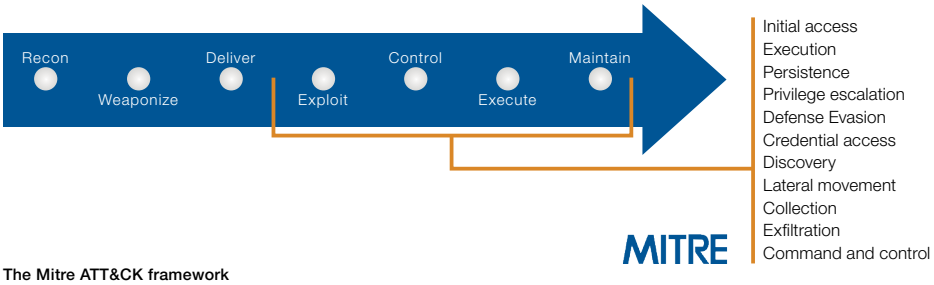
That's the idea behind Mitre Adversarial Tactics, Techniques and Common Knowledge (ATT&CK™) for Enterprise. ATT&CK for Enterprise is an adversary model and framework that describes the actions an adversary may take to compromise and operate within an enterprise network.

The ATT&CK framework provides a way to classify attacks in a clear, consistent manner, which makes it easier to find how the adversary exploited your endpoints and penetrated your network.

The framework details the tactics, techniques and procedures that attackers use to gain access and execute their objectives while operating inside a network. The ATT&CK framework focuses on critical phases of a cyberattack – exploit, control, maintain and execute.

Because ATT&CK takes the perspective of the adversary rather than the defender, it's easier for defenders to follow the adversary's motivation for individual actions and understand how those actions and dependences relate to specific classes of defenses.

The ATT&CK framework is used in intrusion detection, threat hunting, security engineering, threat intelligence, red teaming and risk management.



The Mitre ATT&CK framework

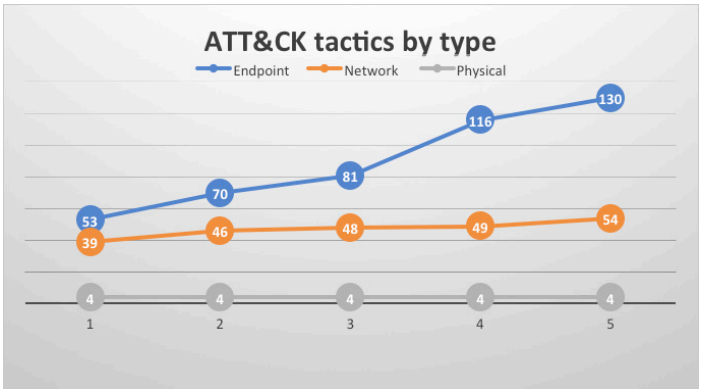
The framework provides a valuable way for organizations to compare their own overall security posture. Organizations can use the framework to validate their defenses against common attack vectors and identify gaps so they can continuously advance their defensive strategies.

Using the framework as a common language to describe the chain of events in an intrusion is also very useful when working with security consultants and vendors.

How Cognito aligns with the ATT&CK framework

Cognito® from Vectra® is the ultimate AI-powered cyberattack-detection and threat-hunting platform. The Cognito platform uses AI to automate cyberattacker detection in real time and enrich threat investigations with a conclusive chain of forensic evidence.

Vectra validated the Cognito platform against the ATT&CK framework in a live enterprise environment to determine overall alignment. Vectra covers 49 of 54 (91%) of the network tactics identified in the ATT&CK framework, which indirectly exposes tactics that attackers use to compromise endpoints.



New endpoint tactics are introduced at four-times the rate of network tactics. Vectra covers 49 of 54 (91%) network tactics.

New endpoint tactics are introduced at four-times the rate of network tactics. This makes the network an easier and more stable detection point because there are specific network behaviors that all cybercriminals must follow to successfully mount an attack.

The reason for such a high volume and growth in endpoint tactics across new versions of the framework is because the ATT&CK framework places a heavy weighting to persistence, privilege escalation, and defense evasion on the endpoint.

This fast introduction of new endpoint attacker techniques underlines the challenge of endpoint prevention and the need for network-based detection. Stopping endpoint compromise will continue to be an intractable problem.

When under attack, network traffic is the best source of truth to identify attacker behaviors across the attack lifecycle that are required for an attack to succeed. Attackers are increasingly using hidden tunnels, encryption and other clever methods to hide in legitimate traffic to spy, spread and steal.

Part of the Cognito platform, AI-driven Cognito Detect™ uses machine learning, data science and behavioral models to provide enterprise-wide visibility into hidden cyberattackers. It analyzes all network traffic from endpoints, servers, virtual workloads, and the cloud infrastructure, leaving attackers with nowhere to hide.

Thousands of events and historical context are consolidated by Cognito Detect to pinpoint compromised hosts that pose the biggest risk. Oceans of data are boiled down to show security analysts what matters most. Threat and certainty scores trigger notifications to the security operations team and through other enforcement points, SIEMs and forensic tools.

Cognito Detect continuously learns the local environment and detects fundamental attacker behaviors in network traffic, including lateral movement, execution, collection, exfiltration, and command-and-control phases identified in the ATT&CK framework.

In addition, Cognito Detect identifies attacker behaviors not explicitly described in the framework, such as port hijacking for backdoor activity, account scans and Active Directory reconnaissance.

Cognito Detect uses STIX threat intelligence to expose attacks based on known indicators of compromise. These are correlated with other attacker behaviors to ensure pinpoint accuracy of host threat and certainty scores as well as risk priority.

When it comes to fast-moving cyberattacks, the best defense is a good offense. The ATT&CK framework offers organizations a formalized process for red team and penetration testing so that they can strengthen their defenses.

Mapping Cognito platform capabilities to the ATT&CK matrix for enterprise

ATT&CK matrix	Validated Cognito support		
Persistence	• AppCert DLLs • Browser extensions	• Create account • External remote services	• Redundant access • Valid accounts
Privilege escalation	• AppCert DLLs	• Exploitation of vulnerability	• Valid accounts
Defense evasion	• Exploitation of vulnerability	• Redundant access	• Valid accounts
Credential access	• Account manipulation • Brute force • Credential dumping	• Credentials in files • Exploitation of vulnerability • Input capture	• Network sniffing • Private keys • Two-factor authentication interception
Discovery	• Account discovery • Application window discovery • File and directory discovery • Network service scanning • Network share discovery • Peripheral device discovery	• Permission groups discovery • Process discovery • Query registry • Remote system discovery • Security software discovery	• System information discovery • System network configuration discovery • System owner/user discovery • System service discovery • System time discovery
Lateral movement	• Remote desktop protocol • Remote file copy • Remote services	• Shared webroot • Taint shared content • Third-party software	• Windows admin shares • Windows remote management
Execution	• Command line interface • Graphical user interface • PowerShell	• Service execution • Third-party software	• Windows management instrumentation • Windows remote management
Collection	• Audio capture • Automated collection • Browser extensions • Clipboard data • Data staged	• Data from local system • Data from network shared drive • Data from removable media • Email collection • Input capture	• Man in the browser • Screen capture • Video capture
Exfiltration	• Automated exfiltration • Data compressed • Data encrypted	• Data transfer size limits • Exfiltration over alternate protocol	• Exfiltration over command and control channel • Scheduled transfer
Command and control	• Commonly used port • Connection proxy • Custom command and control protocol • Custom cryptographic protocol • Data encoding • Data obfuscation	• Domain fronting • Fallback channels • Multi-stage channels • Multi-hop proxy • Multi-band communication	• Multi-layer encryption • Remote file copy • Standard application • Uncommonly used port • Web service

VECTRA®
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai