VECTRA®

How Cognito supports the MITRE Enterprise ATT&CK model

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

That's the idea behind MITRE Enterprise Adversarial Tactics, Techniques and Common Knowledge (ATT&CK™). Enterprise ATT&CK is a curated knowledge base and model for cyber-adversary behavior that reflects the various phases of the attack lifecycle and the platforms attackers are known to target.

The ATT&CK behavior model provides a way to classify attacks in a clear, consistent manner, making it easier for security professionals to find how an adversary exploited their endpoints and penetrated their networks.

ATT&CK takes the perspective of the adversary, so defenders can more easily follow an adversary's motivation for individual actions and understand how those actions and dependences relate to specific classes of defenses.

The ATT&CK model describes tactics, which represent the "why" of the attack. Tactics are the short-term adversary goals during an attack. The model also defines the techniques, or how adversaries achieve their tactical goals. Enterprise ATT&CK includes techniques across Windows, Linux and Mac.

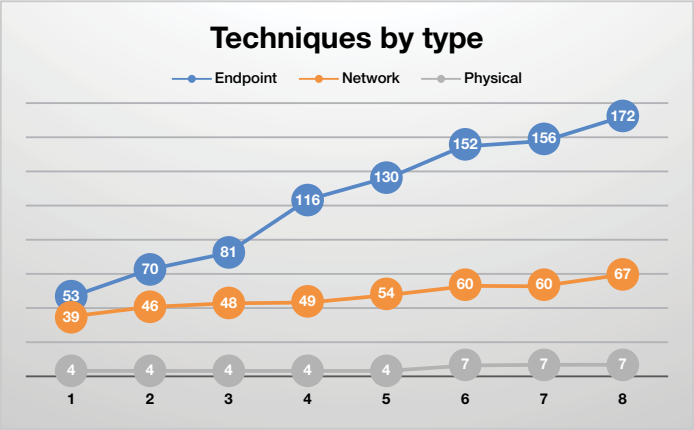
The ATT&CK model can be used for red team exercises as well as to create scenarios that emulate adversaries to test and verify defenses. It provides a valuable way for organizations to assess the maturity of their security operations center (SOC). Security teams can use the framework to validate their defenses against common attack vectors and identify defensive gaps so they can continuously advance their strategies.

ATT&CK also serves a common language to describe the chain of events in an intrusion, which is very useful when working with security consultants and vendors.

How Cognito Detect aligns with the ATT&CK model

Cognito Detect™ from Vectra® is the fastest, most efficient way to find and stop cyberattackers in public clouds, private data centers and enterprise environments. It uses artificial intelligence to deliver real-time attack visibility and put attack details at your fingertips.

Vectra validated Cognito Detect against the MITRE Enterprise ATT&CK model in a live enterprise environment to determine overall alignment. Cognito Detect covers 57 of 67 (85%) of the network techniques identified by the ATT&CK model, which indirectly exposes techniques that attackers use to compromise endpoints.



Vectra covers 57 out of 67 (85%) of the tactics identified in the ATT&CK model.

New endpoint techniques are introduced at four-times the rate of network techniques. The ATT&CK model heavily weights persistence, privilege escalation and defense evasion on the endpoint. The high volume and growth of endpoint techniques underscores the challenge of preventing endpoint compromise and the need for network-based detection.

Network traffic is the best source of truth to identify attacker techniques across the attack lifecycle. The network is a more stable detection point because criminals must use specific network behaviors to successfully mount an attack.

Cognito Detect provides real-time visibility into network traffic by extracting metadata from packets. Metadata analysis is applied to all internal (east-west) traffic, Internet-bound (north-south) traffic, virtual infrastructure and cloud computing environment.

Cognito Detect identifies, tracks and scores every IP-enabled device inside the network. This visibility extends to laptops, servers, printers, BYOD and IoT devices as well as all operating systems and applications, including traffic between virtual workloads in data centers and the cloud, even SaaS applications.

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

Customers can also import known indicators of compromise (IOCs) derived from threat intelligence as STIX files to have Cognito Detect hunt for matches. Cognito Detect then correlates these IoC matches with other attacker behaviors to ensure pinpoint accuracy of host threat and certainty scores to prioritize risk.

Vectra customers achieved a 34X workload reduction for Tier-1 analysts in detection, triage, correlation and prioritization of security incidents, enabling security operations teams to focus on the compromised devices that pose the highest risk.

Assess your defensive gaps

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

Vectra customers can get more detailed information about Cognito's support for the ATT&CK model at vectra.ai/support.

Mapping Cognito Detect capabilities to the ATT&CK Matrix for enterprise

ATT&CK tactic	ATT&CK technique: Validated Cognito support		
Persistence	• Account manipulations • Browser extensions • Logon scripts	• Create account • External remote services • Port knocking	• Redundant access • Valid accounts
Privilege escalation	• Valid accounts		
Defense evasion	• Valid accounts • Port knocking • Redundant access	• Web service • Valid accounts	• DCShadow • Group policy modification
Credential access	• Account manipulation • Brute force • Credential dumping • Input prompt • Credentials in files	• Credentials in registry • Input capture • Securityd memory • Network sniffing	• Private keys • Two-factor authentication interception • Bash history • Keychain
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 • Network sniffing	• System information discovery • System network configuration discovery • Systems network connection discovery • System service discovery • System time discovery • System owner/user discovery
Lateral movement	• Remote desktop protocol • Remote file copy • Remote services • AppleScript • Third-party software	• Shared webroot • Exploitation of remote software • Application deployment software • Logon scripts • Windows admin shares	• Windows remote management • Pass the ticket • Pass the hash • Distributed Component Object Model
Execution	• Command line interface • Graphical user interface • PowerShell • Service execution	• Third-party software • AppleScript • Windows management instrumentation	• Windows remote management • User execution • Source
Collection	• Audio capture • Automated collection • 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 • Data from information repositories
Exfiltration	• Automated exfiltration • Data compressed • Data encrypted	• Exfiltration over alternative protocol • Exfiltration over command and control channels	• Scheduled transfer • Data size transfer limits
Command and control	• Commonly used port • Connection proxy • Custom command and control protocol • Custom cryptographic protocol • Data encoding • Data obfuscation • Port knocking	• Domain fronting • Fallback channels • Multi-stage channels • Multi-hop proxy • Multi-band communication • Remote access tools • Multi-layer encryption	• Remote file copy • Standard application-layer protocol • Uncommonly used port • Web service • Standard cryptographic protocol • Domain generation algorithm
Initial access	• Valid accounts		
Impact	• Data encrypted for impact • Service stop	• Stored data manipulation	• Transmitted data manipulation

VECTRA®
Security that thinks®

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