VECTRA
SECURITY THAT THINKS.®

SOLUTION BRIEF

How Cognito supports the MITRE enterprise ATT&CK framework

What is the MITRE ATT&CK framework?

The MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) framework 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.

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.

Top 3 reasons why NDR Is well suited for detecting MITRE ATT&CK TTPs

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

1. 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.

2. The network never lies, and attacks, regardless of how novel, will always have a network footprint if they propagate. This is especially apparent as an attack progresses. Logs can be erased, endpoint controls can be evaded, but the network footprint cannot be erased.

3. Further, network detection and response (NDR) provides coverage for all devices that have an IP address – managed devices, unmanaged devices, IoT, IIoT, servers, and desktops. This allows defenders to get a complete view of their network across data center, cloud and office locations without having to instrument every individual device.

How Cognito Detect from Vectra aligns with the ATT&CK model

Cognito Detect™ from Vectra® is the fastest, most efficient way to find and stop cyberattacks 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.

Cognito Detect covers 97% of the network techniques identified by the ATT&CK model, which indirectly exposes techniques that attackers use to compromise endpoints.

Below is a table of Cognito Detect coverage of the MITRE ATT&CK matrix.

ATT&CK technique: Initial access	
Technique	**Vectra coverage**
Drive-by compromise	Direct coverage for drive-by compromise locations from the Vectra threat intel detection.
External remote services	Direct coverage for services other than corporate VPN via external remote access detection.
Phishing	Direct coverage for phishing links and internal spear-phishing from Vectra threat intel and Office 365 internal spear-phishing detections.
Valid accounts	Direct coverage for the use of stolen credentials via account-based detections. Applicable detections include suspicious admin, suspicious remote desktop, suspicious remote execution, the Privileged Access Analytics suite and multiple Vectra Office 365 detections.
Hardware additions	Indirect prior technique coverage from Cognito Recall by identification of USB drive insertion and device monitoring.
Replication through removable media	Behavior is local to host. Indirect coverage prior to technique from Cognito Recall by identification of USB drive insertion.

ATT&CK technique: Execution	
Technique	**Vectra coverage**
Command and scripting interpreter	Direct coverage from command-and-control detection portfolio via external remote access, hidden HTTP tunnel, hidden HTTPS tunnel, hidden DNS tunnel, suspicious relay.
Exploitation for client execution	Direct coverage for known attacker exploits in attacker environments via the Office 365 malware stage: Upload detection.
Scheduled task/job	Direct coverage for remote task scheduling via suspicious remote execution.
Software deployment tools	Direct coverage for compromised third party vulnerability scanners or software distribution systems can be used by attackers to continue their attacks. While the normal behavior of these scanners and distributors may be triaged the usage of these scanners on new parts of the network would be detected by port scan, port sweep, internal darknet scan and automated replication.
System services	Direct coverage for remote service execution via suspicious remote execution.
User execution	Indirect post technique coverage for command-and-control channels being created. Applicable detections include external remote access, hidden HTTP tunnel, hidden HTTPS tunnel, hidden DNS tunnel, suspicious relay.
Windows management instrumentation	Directed coverage for WMI invocation via the suspicious remote execution detection.

ATT&CK technique: Persistence	
Technique	**Vectra coverage**
Account manipulation	Direct coverage for accounts being manipulated via the Office 365 account manipulation and Office 365 risky exchange operation detections.
Browser extensions	Direct coverage from command-and-control detection portfolio via external remote access, hidden HTTP tunnel, hidden HTTPS tunnel, hidden DNS tunnel, suspicious relay.
External remote services	Direct coverage for services other than corporate VPN via external remote access detection.
Office application startup	Direct coverage for attacker's leveraging ruler to modify Office 365 application start-up provided by Office 365 attack tool: Ruler detection.
Traffic signaling	Direct coverage is behavioral and requires learning on the normal port connection sequences. Coverage via shell knocker client and shell knocker server.
Scheduled task/job	Direct coverage for remote task scheduling via suspicious remote execution.
Valid accounts	Direct coverage for use of the stolen credentials from account-based detections. Applicable detections include suspicious admin, suspicious remote desktop, suspicious remote execution, the Privileged Access Analytics suite and multiple Vectra Office 365 detections.
Create account	This technique is typically followed by the account being used in a suspicious manner. Indirect post action coverage from Privileged Access Analytics and other account-centric detections.

ATT&CK technique: Privilege escalation	
Technique	**Vectra coverage**
Group policy modification	Behavior is local to host. Indirect post technique coverage from use of compromised credentials via account-based detections including Privileged Access Analytics detections.
Scheduled task/job	Direct coverage for remote task scheduling via suspicious remote execution.
Valid accounts	Direct coverage for use of the stolen credentials from account-based detections. Applicable detections include suspicious admin, suspicious remote desktop, suspicious remote execution, the Privileged Access Analytics suite and multiple Vectra Office 365 detections.

ATT&CK technique: Defense evasion	
Technique	**Vectra coverage**
Impair defenses	Direct coverage for attackers attempting to evade detections via the Office 365 log disabling attempt and Office 365 disabling of security tools detections.
Rogue domain controller	Direct coverage for the creation of rogue DCs via the Kerberos server access detection.
Traffic signaling	Direct coverage is behavioral and requires learning on the normal port connection sequences. Coverage via shell knocker client and shell knocker server.
Valid accounts	Direct coverage for use of the stolen credentials from account-based detections. Applicable detections include suspicious admin, suspicious remote desktop, suspicious remote execution, the Privileged Access Analytics suite and multiple Vectra Office 365 detections.
Group policy modification	GPO modification is not directly detected. Indirect coverage post technique from the usage of newly created privileged accounts via account-based detections.
Modify authentication process	Indirect coverage post exploitation for the usage of a compromised account via account centric detections like the Privileged Access Analytics suite.
Use alternate authentication material	Indirect coverage post exploitation for the usage of a compromised account via account centric detections like the Privileged Access Analytics suite.

ATT&CK technique: Credential access	
Technique	**Vectra coverage**
Brute force	Direct coverage for multiple protocols via brute force, SMB brute force, Kerberos brute sweep and Office 365 brute force.
Forced authentication	Direct coverage via rules in Cognito Recall custom for outbound SMB and WebDav traffic.
Credentials from password stores	Indirect coverage post exploitation for the usage of a compromised account via account centric detections like the Privileged Access Analytics suite.
Exploitation for credential access	Indirect coverage post exploitation for the usage of a compromised account via account centric detections like the Privileged Access Analytics suite.
Input capture	Indirect coverage via detection of command-and-control and relays used to control the host. External remote access, hidden HTTP tunnel, hidden HTTPS tunnel, hidden DNS tunnel, and suspicious relay.
Man-in-the-middle	Indirect coverage prior to technique via the identification of NetBIOS and LLMNR network usage with Cognito Recall saved searches.
Modify authentication process	Indirect coverage post exploitation for the usage of a compromised account via account centric detections like the Privileged Access Analytics suite.

ATT&CK technique: Credential access (con't)	
Technique	**Vectra coverage**
Network sniffing	Indirect coverage prior and post technique from the identification of sniffable protocols like LLMNR and NBT-NS and the usage of compromised credentials. Coverage provided by recall save searches for LLMNR and NBT-NS usage and account-based detections like the Privileged Access Analytics suite
OS credential dumping	This technique is typically followed by an account being used in a suspicious manner. Indirect post action coverage from Privileged Access Analytics and other account-centric detections.
Steal application access token	Indirect coverage for usage of stolen tokens provided by multiple Office 365 detections.
Steal or forge Kerberos tickets	Indirect coverage post exploitation for the usage of a compromised account via account centric detections like the Privileged Access Analytics suite
Steal web session cookie	Once credentials are obtained attackers will use them in unusual ways.\n\n Indirect coverage post technique from account-based detection portfolio and multiple Office 365 detection models.
Two-factor authentication interception	Indirect prior technique coverage from detection of command-and-control control the host and post technique coverage from usage of compromised credentials. Applicable detections include external remote access, hidden HTTP tunnel, hidden HTTPS tunnel, hidden DNS tunnel, suspicious relay and suspicious admin and Privileged Access Analytics detections.
Unused credentials	Indirect coverage post exploitation for the usage of a compromised account via account centric detections like the Privileged Access Analytics suite.

ATT&CK technique: Discovery	
Technique	**Vectra coverage**
Account discovery	Direct coverage via remote discovery via RPC recon focused detections.
Domain trust discovery	Direct coverage for domain trust coverage over LDAP request may be covered with a rules defined in Cognito Recall.
File and directory discovery	Direct coverage for discovery of files and email contents via Office 365 suspicious eDiscovery search detection.
Network service scanning	Direct coverage via port scan, port sweep, and internal darknet scan detections.
Network share discovery	Direct coverage via RPC recon based detections and SMB share enumeration.
Password policy discovery	Direct coverage for RPC discovery of password policies via RPC recon-based detections.
Permission groups discovery	Direct coverage for remote permission discovery provided by RPC recon-based detections.
Remote system discovery	Direct coverage for remote discovery via port scan, port sweep and internal darknet scan detections.
System information discovery	Direct coverage for remote discovery via port scan, port sweep, darknet and RPC-based detections.
System network configuration discovery	Direct coverage for remote discovery via port scan, port sweep, darknet and RPC-based detections.

ATT&CK technique: Discovery (con't)	
Technique	**Vectra coverage**
System owner/user discovery	Direct coverage for account discovery over multiple protocols. Relevant detections include Kerberos account enumeration, RDP recon, automated replication and RPC recon-based detections.
System service discovery	Direct coverage for remote system service discovery via RPC recon-based detections.
System time discovery	Direct coverage for system service discovery via RPC recon-based detections.
Application window discovery	Behavior is local to host. Indirect coverage prior to technique from the identification of remote-control tools that support this technique via external remote access, hidden HTTP tunnel, hidden HTTPS tunnel, hidden DNS tunnel, suspicious relay detections.
Network sniffing	Indirect coverage prior and post technique from the identification of protocols that can be sniffed such as LLMNR and NBT-NS and the usage of compromised credentials. Coverage provided by recall save searches for LLMNR and NBT-NS usage and account-based detections like the Privileged Access Analytics suite.
Peripheral device discovery	Behavior is local to host. Indirect coverage prior to technique from Cognito Recall rules for the identification of USB device insertion.
Process discovery	Behavior is local to host. Indirect coverage prior to technique from remote access tooling and remote reconnaissance via the command-and-control portfolio and RPC recon related detections.
Query registry	Behavior is local to host. Indirect coverage prior to technique from remote access tooling via the command-and-control portfolio.
Software discovery	Behavior is local to host. Indirect coverage prior to technique from the identification of remote-control tools that support this technique via external remote access, hidden HTTP tunnel, hidden HTTPS tunnel, hidden DNS tunnel, suspicious Relay detections.
System network connections discovery	Indirect coverage prior to technique by detection of remote-control channel and remote discovery over RPC. Relevant detections include command-and-control suite and RPC recon-based detections.

ATT&CK technique: Lateral movement	
Technique	**Vectra coverage**
Exploitation of remote services	Direct coverage via automated replication and internal stage loader detections.
Internal spear phishing	Direct coverage for sending internal spear-phishing emails provided by Office 365 internal spear-phishing detection.
Lateral tool transfer	Direct coverage for lateral tool transfer from Cognito Recall rules and internal stage loader detection
Remote services	Direct coverage via suspicious admin and Privileged Access Analytics detections.
Software deployment tools	Direct coverage for compromised third-party vulnerability scanners being used to by attackers to continue their attacks. While the normal behavior of these scanners may be triaged the usage of these scanners on new parts of the network would be detected. Port scan, port sweep, internal darknet scan, and automated replication.
Taint shared content	Direct coverage for remote directory tainting via rules defined in Cognito Recall for finding suspect .EXE, .DLL, .SCR, .BAT, and/or .VBS files in WebDav and SMB shares.
Replication through removable media	Behavior is local to host. Indirect coverage prior to technique from Cognito Recall by identification of USB drive insertion.
Use alternate authentication material	Indirect coverage post exploitation for the usage of a compromised account via account centric detections like the Privileged Access Analytics suite.

ATT&CK technique: Collection	
Technique	**Vectra coverage**
Data from network shared drive	Direct coverage for share mounting for collection via SMB share enumeration detection.
Data staged	Direct coverage for data collection and push via data smuggler.
Email collection	Direct coverage for attacker collection of emails through multiple methods via the Office 365 suspicious mail forwarding and Office 365 attacker tool: Ruler detections.
Man in the browser	Direct coverage via HTTP/S hidden tunnel.
Archive data collection	Indirect coverage post technique for the follow on data exfiltration of archived media via smash and grab, smuggler, hidden HTTP tunnel exfiltration and hidden HTTPS tunnel exfiltration.
Audio capture	Remote access tools can have functionality that allows them to obtain audio. Indirect coverage prior to technique coverage via command-and-control channel from external remote access, hidden HTTP tunnel, hidden HTTPS tunnel, hidden DNS tunnel, suspicious relay.
Automated Collection	Indirect coverage prior to technique prior to technique from share discoverer and post technique from exfiltration. Relevant detections: SMB share enumeration and smash-and-grab detections.
Clipboard data	Behavior is local to host. Indirect coverage from command-and-control detection portfolio via external remote access, hidden HTTP tunnel, hidden HTTPS tunnel, hidden DNS tunnel, and suspicious relay.
Data from information repositories	Indirect coverage post technique via smash and grab, data smuggler HTTP tunnel exfiltration and HTTPS tunnel exfiltration.

ATT&CK technique: Collection (con't)	
Technique	**Vectra coverage**
Data from local system	Indirect coverage prior to technique from the identification of remote-control tools that support this technique via external remote access, hidden HTTP tunnel, hidden HTTPS tunnel, hidden DNS tunnel, and suspicious relay detections.
Data from removable media	Behavior is local to host. Indirect coverage prior to technique from Cognito Recall by identification of USB drive insertion.
Input capture	Indirect coverage via detection of command-and-control and relays used to control the host. External remote access, hidden HTTP tunnel, hidden HTTPS tunnel, hidden DNS tunnel, and suspicious relay.
Man-in-the-middle	Indirect coverage prior and post technique from the identification of sniffable protocols like LLMNR and NBT-NS and the usage of compromised credentials via Cognito Recall rules
Screen capture	Indirect coverage prior to technique from the identification of remote-control tools that support this technique via external remote access, hidden HTTP tunnel, hidden HTTPS tunnel, hidden DNS tunnel, and suspicious relay detections.
Video capture	Indirect coverage prior to technique from the identification of remote-control tools that support this technique via external remote access, hidden HTTP tunnel, hidden HTTPS tunnel, hidden DNS tunnel, and suspicious relay detections.

ATT&CK technique: Command and control	
Technique	**Vectra coverage**
Application layer protocol	Direct coverage from command-and-control detection portfolio and admin protocol exploitation via external remote access, hidden HTTP tunnel, hidden HTTPS tunnel, hidden DNS tunnel, suspicious relay, and suspicious admin.
Data encoding	Direct coverage from command-and-control detection portfolio via external remote access, hidden HTTP tunnel, hidden HTTPS tunnel, hidden DNS tunnel, and suspicious relay.
Data obfuscation	Direct coverage for obfuscated control channels. Coverage provided via external remote access, hidden HTTP/S tunnel, hidden DNS tunnel, multihome fronted tunnel, and suspicious relay.
Dynamic resolution	Direct coverage provided by the suspect domain detection. This algorithm covers the random letter case but does not currently provide coverage for the random word case. Note: DGA use by attackers for command-and-control is on the decline.
Encrypted channel	Direct coverage from command-and-control detection portfolio via external remote access, hidden HTTP tunnel, hidden HTTPS tunnel, hidden DNS tunnel, and suspicious relay.
Fallback channels	Direct coverage for attackers using an additional command-and-control channels in case their primary communications are thwarted. Coverage via HTTP/S hidden tunnel, external remote access, hidden DNS tunnel, suspicious relay, multihome fronted tunnel, and Office 365 power automate-based detections.
Ingress transfer tools	Direct coverage for copy over tunnels. Coverage provided via external remote access, hidden HTTP/S tunnel, hidden DNS tunnel, multihome fronted tunnel, and suspicious relay.
Multistage channels	Direct coverage via command-and-control detection suite.
Non-application layer protocol	Direct coverage via the external remote access and suspicious relay detections.

ATT&CK technique: Command and control (con't)	
Technique	**Vectra coverage**
Non-standard port	Direct coverage from command-and-control detection portfolio via external remote access, hidden HTTP tunnel, hidden HTTPS tunnel, hidden DNS tunnel, and suspicious relay.
Protocol tunneling	Direct coverage from command-and-control detection portfolio via external remote access, hidden HTTP tunnel, hidden HTTPS tunnel, hidden DNS tunnel, and suspicious relay.
Proxy	Direct coverage via suspicious relay and external remote access.
Remote access software	Direct coverage for remote control tools via external remote access.
Traffic signaling	Direct coverage is behavioral and requires learning on the normal port connection sequences. Coverage via shell knocker client and shell knocker server.
Web service	Direct coverage for command-and-control usage from the identification of unsanctioned web service via rules in Cognito Recall.
Communication through removable media	Behavior is local to host. Indirect coverage prior to technique from Cognito Recall by identification of USB drive insertion.

ATT&CK technique: Exfiltration	
Technique	**Vectra coverage**
Automated exfiltration	Direct coverage for automated exfiltration via smash and grab, data smuggler, hidden HTTP/S tunnel exfiltration detections.
Data transfer size limits	Direct coverage for exfiltration in multiple chunks via smash and grab, data smuggler, HTTP tunnel exfiltration and HTTPS tunnel exfiltration.
Exfiltration over alternative protocol	Direct coverage via external remote access, smash and grab, and data smuggler.
Exfiltration over command-and-control channel	Direct coverage for exfiltration via smash and grab, data smuggler, HTTP tunnel exfiltration and HTTPS tunnel exfiltration detections.
Exfiltration over web service	Direct coverage for exfiltration via smash-and-grab, data smuggler HTTP tunnel exfiltration and HTTPS tunnel exfiltration detections
Scheduled transfer	Direct coverage for exfil over hour long time ranges via smash and grab.
Exfiltration over physical medium	Behavior is local to host. Indirect coverage prior to technique from Cognito Recall by identification of USB drive insertion.

ATT&CK technique: Impact	
Technique	**Vectra coverage**
Data encrypted for impact	Direct coverage for remote encryption of data in file shares (ransomware) via the ransomware file activity detection.
Resource hijacking	Direct coverage for resource hijacking to mine crypto currency via bitcoin detection.

For more information about how Cognito supports the MITRE enterprise ATT&CK framework, please contact a service representative by email at sales-inquiries@vectra.ai.

Email info@vectra.ai vectra.ai