VECTRA
SECURITY THAT THINKS®

ソリューション概要

CognitoによるMITREエンタープライズATT&CKフレームワークのサポート方法

MITRE ATT&CKフレームワークとは

MITRE Adversarial Tactics, Techniques and Common Knowledge（ATT&CK）フレームワークは、攻撃ライフサイクルの様々なフェーズにおけるサイバー攻撃者の振る舞いや、彼らが標的とするプラットフォームに関する情報を収集および整理したナレッジベース兼モデルです。

セキュリティ・プロフェッショナルは、明解かつ一貫した手法で攻撃を分類したATT&CKの振る舞いモデルによって、エンドポイントを悪用してネットワークに侵入した攻撃者を、容易に発見することが可能となります。

ATT&CKモデルは、レッドチームの訓練に使用できるだけでなく、敵対者をエミュレーションすることで、防御に関するテストや検証シナリオの作成にも活用することができます。また、自社のセキュリティ運用センター（SOC: Security Operation Center）の成熟度を評価するための優れた手段を企業に提供します。セキュリティチームは、このフレームワークを使って一般的な攻撃目標に対する防御力を検証して、そのギャップを明らかにしながら、戦略を継続的に向上させていくことができます。

ATT&CKはまた、侵入における一連のイベントについて言及する際の共通言語としても使用することができ、セキュリティコンサルタントやベンダーとの協業において、非常に有効なものとなります。

NDRがMITRE ATT&CK TTPの検知に最適となる3つの理由

泥棒を逮捕するためには、泥棒と同じ視点が不可欠。

1. ATT&CKは、攻撃者の視点を把握することで、防御側が攻撃者の各活動の動機を容易に追跡し、それらの活動や行動が防御の突破にどのように関与しているのかを理解できるようにします。

2. ネットワークは嘘をつきません。攻撃がいかに斬新なものであっても、攻撃が伝播する際には、常にその証跡がネットワークに残ります。攻撃が進行するにつれ、これが顕著になります。ログは消去することができます。エンドポイントのコントロールも回避することができます。しかし、ネットワークに残った証跡は消すことができません。

3. さらに、ネットワークの検知と対応（NDR）機能が、管理対象や管理対象外のデバイス、IoT、IIoT、サーバー、デスクトップなど、IPアドレスを持つ全てのデバイスをカバーします。これによって防御側は、全てのデバイスを個々に調査することなく、データセンターやクラウド、オフィスのネットワーク全体の完全なビューを取得することができます。

Vectra Cognito DetectのATT&CKモデルへの対応

Vectra® AI社が提供するCognito Detect™は、パブリッククラウドやプライベートのデータセンター、エンタープライズ環境におけるサイバー攻撃を検出して阻止する、最も迅速かつ効率的な手段となります。Cognito Detectは、AIを活用することで、外部からの攻撃をリアルタイムに可視化し、攻撃に関する詳細な情報を提供します。

Cognito Detectは、エンドポイントを侵害するために攻撃者が使用するテクニック、ATT&CKモデルの97%をカバーします。

以下の表は、MITRE ATT&CKマトリクスへのCognito Detectの対応を示したものです。

ATT&CKのテクニック：初期アクセス (Initial Access)	
テクニック	**Vectra製品の対応**
Web閲覧による感染 (Drive-by compromise)	直接検出。Vectra AI社の脅威インテリジェンス検知機能により、Web閲覧による感染箇所を検出します。
外部リモートサービス (External remote services)	直接検出。外部リモートアクセスの検知機能により、企業VPNを除くサービスを検出します。
フィッシング (Phishing)	直接検出。フィッシングリンクおよび内部スピアフィッシングを、Vectra AI社の脅威インテリジェンスとOffice 365内部スピアフィッシング検知機能で検出します。
正当なアカウント (Valid accounts)	直接検出。アカウントベースの検知機能によって、盗難された資格情報の使用を検出します。 検出対象として、不審な管理者、不審なリモートデスクトップ、不審なリモート実行、特権アクセス分析（Privileged Access Analytics）スイートおよび複数のVectra Office 365検知機能などがあります。
ハードウェアの追加 (Hardware additions)	テクニック実行前に間接的に検出。Cognito RecallのUSBドライブ挿入検知とデバイス監視機能によって検出します。
リムーバブルメディアを介した複製 (Replication through removable media)	振る舞いはローカルからホストに及びます。このためテクニック実行前に間接的に検出。Cognito RecallのUSBドライブ挿入検知機能によって検出します。

ATT&CKのテクニック：実行 (Execution)	
テクニック	**Vectra製品の対応**
コマンドおよびスクリプトインタプリタ (Command and scripting interpreter)	直接検出。外部リモートアクセス、隠れたHTTPトンネル、隠れたHTTPSトンネル、隠れたDNSトンネル、不審な中継を、C&C検知機能で検出します。
クライアント実行のエクスプロイト (Exploitation for client execution)	直接検出。Office 365 マルウェアステージであるアップロードの検知によって、攻撃者の環境における既知の攻撃者のエクスプロイトを検出します。
スケジュール済みタスク/ジョブ (Scheduled task/job)	直接検出。不審なリモート実行による、リモートタスクのスケジュールを検出します。
ソフトウェア導入ツール (Software deployment tools)	直接検出。攻撃者が攻撃を継続するために使用する、侵入を受けたサードパーティーの脆弱性スキャナまたはソフトウェア配布システムを検出します。正常なスキャナや配布システムの振る舞いはトリアージされますが、ネットワークの新しい箇所でこれらのスキャナを使用した場合には、ポートスキャン、ポートスイープ、内部のダークネットスキャン、自動レプリケーションにより、それが検出されます。
システムサービス (System services)	直接検出。不審なリモート実行の検知機能により、リモートサービスの実行を検出します。
ユーザー実行 (User execution)	テクニック実行後に間接的に検出。C&Cチャネルが作成されたことを検出します。検出可能な対象としては、外部リモートアクセス、隠れたHTTPトンネル、隠れたHTTPSトンネル、隠れたDNSトンネル、不審な中継などがあります。
WMI (Windows Management Instrumentation)	直接検出。不審なリモート実行の検知機能により、WMIの起動を検出します。

ATT&CKのテクニック：永続化 (Persistence)	
テクニック	**Vectra製品の対応**
アカウント操作 (Account manipulation)	直接検出。Office 365アカウントの操作およびOffice 365の危険な運用に関する検知機能によって、不正な操作が行われているアカウントを検出します。
ブラウザ拡張 (Browser extensions)	直接検出。外部リモートアクセス、隠れたHTTPトンネル、隠れたHTTPSトンネル、隠れたDNSトンネル、不審な中継を、C&C検知機能で検出します。
外部リモートサービス (External remote services)	直接検出。外部リモートアクセスの検知機能によって、企業VPNを除くサービスを検出します。
Officeアプリケーションのスタートアップ (Office application startup)	直接検出。攻撃者がOffice365攻撃ツールである Ruler を使って、Office 365アプリケーションスタートアップのルーラー (ruler) を変更していることを検出します。
トラフィックシグナリング (Traffic signaling)	直接的な検出は、振る舞いに依存するため、正常なポート接続シーケンスについて学習する必要があります。 shell knockerクライアントとshell knockerサーバーから検出。
スケジュール済みタスク/ジョブ (Scheduled task/job)	直接検出。不審なリモート実行による、リモートタスクのスケジュールを検出します。
正当なアカウント (Valid accounts)	直接検出。アカウントベースの検知機能によって、盗難にあった認証情報が使用されたことを検出します。 検出対象としては、不審な管理者、不審なリモートデスクトップ、不審なリモート実行、特権アクセス分析 (Privileged Access Analytics) スイートおよび複数のVectra Office 365検知機能などがあります。
アカウントの作成 (Create account)	このテクニックが実行された後、アカウントが不審な方法で使用される場合が多くなっています。 このためアクション実施後に間接的に検出。特権アクセス分析 (Privileged Access Analytics) や、その他のアカウントセントリックの検知機能により検知します。

ATT&CKのテクニック：権限昇格 (Privilege escalation)

テクニック	Vectra製品の対応
グループポリシーの変更 (Group policy modification)	振る舞いはローカルからホストに及びます。このためテクニック実行後に間接的に検出。特権アクセス分析（Privileged Access Analytics）の検知など、アカウントベースの検知機能により、侵害認証情報の使用を検出します。
スケジュール済みタスク/ジョブ (Scheduled task/job)	直接検出。不審なリモート実行による、リモートタスクのスケジュールを検出します。
正当なアカウント (Valid accounts)	直接検出。アカウントベースの検知機能によって、盗難にあった認証情報が使用されたことを検出します。 検出対象としては、不審な管理者、不審なリモートデスクトップ、不審なリモート実行、特権アクセス分析（Privileged Access Analytics）スイートおよび複数のVectra Office 365検知機能などがあります。

ATT&CKのテクニック：防御回避 (Defense evasion)

テクニック	Vectra製品の対応
防御の弱体化 (Impair defenses)	直接検出。Office 365のログやセキュリティツールの無効化によって、検知の回避を試みる攻撃者を検出します。
不正なドメインコントローラ (Rogue domain controller)	直接検出。Kerberosサーバーへのアクセス検知機能によって、不正なDCの作成を検出します。
トラフィックシグナリング (Traffic signaling)	直接的な検出は、振る舞いに依存するため、正常なポート接続シーケンスについて学習する必要があります。 shell knockerクライアントとshell knockerサーバーから検出。
正当なアカウント (Valid accounts)	直接検出。アカウントベースの検知機能によって、盗難にあった認証情報が使用されたことを検出します。 検出対象としては、不審な管理者、不審なリモートデスクトップ、不審なリモート実行、特権アクセス分析（Privileged Access Analytics）スイートおよび複数のVectra Office 365検知機能などがあります。
グループポリシーの変更 (Group policy modification)	GPOの変更は直接検出できません。このためアカウントベースの検出機能により、新しく作成された特権アカウントが使用されたことを、間接的に検出します。
認証プロセスの変更 (Modify authentication process)	実行後に間接的に検出。特権アクセス分析（Priviledged Access Analytics）スイートなど、アカウント中心の検知機能によって、侵害を受けたアカウントの使用があったことを検出します。
代替認証情報の利用 (Use alternate authentication material)	実行後に間接的に検出。特権アクセス分析（Priviledged Access Analytics）スイートなど、アカウント中心の検知機能によって、侵害を受けたアカウントの使用があったことを検出します。

ATT&CKのテクニック：認証情報アクセス (Credential access)

テクニック	Vectra製品の対応
総当たり攻撃 (Brute force)	直接検出。総当たり攻撃、SMB総当たり攻撃、Kerberos総当たりスイープ、Office365総当たり攻撃など、複数のプロトコルを検出します。
強制認証 (Forced authentication)	直接検出。CognitoのアウトバウンドSMBおよびWebDavトラフィックの向けのルールを使って検出します。
保存済みパスワードを使った認証情報 (Credentials from password stores)	実行後に間接的に検出。特権アクセス分析（Priviledged Access Analytics）スイートなど、アカウント中心の検知機能によって、侵害を受けたアカウントの使用があったことを検出します。
認証情報アクセスの不正使用 (Exploitation for credential access)	実行後に間接的に検出。特権アクセス分析（Priviledged Access Analytics）スイートなど、アカウント中心の検知機能によって、侵害を受けたアカウントの使用があったことを検出します。
入力のキャプチャ (Input capture)	間接的に検出。ホストのコントロールに使用されるC&Cや中継の検知機能によって検出します。対象は、外部リモートアクセス、隠れたHTTPトンネル、隠れたHTTPSトンネル、隠れたDNSトンネル、不審な中継となります。
中間者攻撃 (Man-in-the-middle)	テクニック実行前に間接的に検出。Cognito Recallの保存済み検索結果を使って、NetBIOSおよびLLMNRネットワークの使用を検出します。
認証プロセスの変更 (Modify authentication process)	実行後に間接的に検出。特権アクセス分析（Priviledged Access Analytics）スイートなど、アカウント中心の検知機能によって、侵害を受けたアカウントの使用があったことを検出します。

ATT&CKのテクニック：認証情報アクセス (Credential access)	
テクニック	**Vectra製品の対応**
ネットワークスニッフィング (Network sniffing)	テクニック実行前および実行後に間接的に検出。LLMNRおよびNBT-NSといったスニッフィング可能なプロトコルの識別や、侵害した認証情報の使用を検出します。LLMNRおよびNBT-NSの使用に対する保存済み検索結果の呼び出しと、特権アクセス分析（Privileged Access Analytics）スイートのようなアカウントベースの検知機能によって検出します。
OS認証情報のダンプ (OS credential dumping)	このテクニックの実行後、アカウントが不審な方法で使用される場合が多くなっています。このためアクション実施後に間接的に検出。特権アクセス分析（Privileged Access Analytics）や、その他のアカウントセントリックな検知機能により検知します。
アプリケーションアクセストークンの盗み出し (Steal application access token)	間接的に検出。複数のOffice 365の検知機能によって、盗難トークンの使用を検出します。
Kerberosチケットの盗み出しまたは偽造 (Steal or forge Kerberos tickets)	実行後に間接的に検出。特権アクセス分析（Priviledged Access Analytics）スイートなど、アカウント中心の検知機能によって、侵害を受けたアカウントの使用があったことを検出します。
Webセッションcookieの盗み出し (Steal web session cookie)	認証情報を入手すると、攻撃者は通常とは異なる方法でそれを使用します。このためアカウントベースの検知機能と、複数のOffice 365検知モデルによって間接的に検知します。
2段階認証のインターセプト (Two-factor authentication interception)	C&Cのホストのコントロールを、テクニック実行前に間接的に検出し、また、侵害を受けた認証情報が使用されたことを、テクニック実行後に検出します。検出対象には、外部リモートアクセス、隠れたHTTPトンネル、隠れたHTTPSトンネル、隠れたDNSトンネル、不審な中継、不審な管理操作や特権アクセス分析（Privileged Access Analytics）の検知などがあります。
未使用認証情報 (Unused credentials)	実行後に間接的に検出。特権アクセス分析（Priviledged Access Analytics）スイートなど、アカウント中心の検知機能によって、侵害を受けたアカウントの使用があったことを検出します。

ATT&CKのテクニック：探索 (Discovery)	
テクニック	**Vectra製品の対応**
アカウントの探索 (Account discovery)	直接検知。RPCの偵察に着目したリモート探索によって検知します。
ドメイン信頼性の探索 (Domain trust discovery)	直接検知。LDAPリクエストに対するドメイン信頼性の探索は、Cognito Recallに定義したルールを使って検出することができます。
ファイルとディレクトリの探索 (File and directory discovery)	直接検出。Office 365の不審なeDiscovery検索の検知機能により、ファイルおよびEメールコンテンツの探索を検出します。
ネットワークサービススキャン (Network service scanning)	直接検出。ポートスキャン、ポートスイープ、内部ダークネットスキャンの検知機能によって検出します。
ネットワーク共有探索 (Network share discovery)	直接検出。RPCの偵察ベースの検知とSMB共有エミュレーションにより検出します。
パスワードポリシーの探索 (Password policy discovery)	直接検出。RPCの偵察ベースの検知機能により、RPCのパスワードポリシーの探索を検出します。
パーミッショングループの探索 (Permission groups discovery)	直接検出。RPC偵察ベースの検知機能により、リモートパーミッション探索を検出します。
リモートシステムの探索 (Remote system discovery)	直接検出。ポートスキャン、ポートスイープ、内部ダークネットスキャンの検知機能により、リモート探索を検出します。
システム情報の探索 (System information discovery)	直接検出。ポートスキャン、ポートスイープ、ダークネットおよびRPCベースの検知機能により、リモート探索を検出します。
システムネットワーク構成の探索 (System network configuration discovery)	直接検出。ポートスキャン、ポートスイープ、ダークネットおよびRPCベースの検知機能により、リモート探索を検出します。

ATT&CKのテクニック：探索 (Discovery)	
テクニック	**Vectra製品の対応**
システムオーナー/ユーザーの探索 (System owner/user discovery)	直接検出。複数のプロトコルを使用するアカウントを検出します。Kerberosアカウントエミュレーション、RDP偵察、自動レプリケーション、RPC偵察ベースの検知機能などによって、関連性を検出します。
システムサービスの探索 (System service discovery)	直接検出。RPC偵察ベースの検知機能により、リモートシステムサービスの探索を検出します。
システム時間の探索 (System time discovery)	直接検出。RPC偵察ベースの検知機能により、システムサービスの探索を検出します。
アプリケーションウィンドウの探索 (Application window discovery)	振る舞いはローカルからホストに及びます。テクニック実行前に間接的に検出。外部リモートアクセス、隠れたHTTPトンネル、隠れたHTTPSトンネル、隠れたDNSトンネル、不審な中継といったテクニックをサポートする、リモートコントロールツールを特定して検知します。
ネットワークスニッフィング (Network sniffing)	テクニック実行前、およびテクニック実行後に間接的に検出。LLMNRおよびNBT-NSといったスニッフィング可能なプロトコルの検知機能によって、侵害を受けた認証情報の使用を検出します。LLMNRおよびNBT-NSの使用に対する保存済み検索結果の呼び出しと、特権アクセス分析 (Privileged Access Analytics) スイートのようなアカウントベースを検出します。
ペリフェラルデバイスの探索 (Peripheral device discovery)	振る舞いはローカルからホストに及びます。このためテクニック実行前に間接的に検出。USBデバイス挿入の検知するCognito Recallのルールによって検知します。
プロセスの探索 (Process discovery)	振る舞いはローカルからホストに及びます。このためテクニック実行前に間接的に検出。リモートアクセスツールの使用やリモート偵察を、C&Cポートフォリオ やRPC偵察を検出します。
クエリ登録 (Query registry)	振る舞いはローカルからホストに及びます。このためテクニック実行前に間接的に検出。リモートアクセスツールの使用を、C&Cポートフォリオによって検知します。
ソフトウェアの探索 (Software discovery)	振る舞いはローカルからホストに及びます。このためテクニック実行前に間接的に検出。外部リモートアクセス、隠れたHTTPトンネル、隠れたHTTPSトンネル、隠れたDNSトンネル、不審な中継を検知し、このテクニックをサポートするリモートコントロールツールを検出します。
システムネットワーク接続の探索 (System network connections discovery)	テクニック実行前に間接的に検出。リモートコントロールチャネルおよびRPCのリモート探索の検知機能によって検知します。関連する検知として、C&Cスイートおよび RPC偵察ベースの検出があります。

ATT&CKのテクニック：ラテラルムーブメント (Lateral movement)	
テクニック	**Vectra製品の対応**
リモートサービスのエクスプロイト (Exploitation of remote services)	直接検出。自動レプリケーションおよび内部のステージローダーの検知機能によって検出します。
内部スピアフィシング (Internal spear phishing)	直接検出。Office 365内部スピアフィシングの検知機能によって、内部スピアフィシングEメールの送信を検出します。
ラテラルツールの転送 (Lateral tool transfer)	直接検出。Cognito Recallのルールと内部のステージローダーの検知機能によって、ラテラルツールの転送を検出します。
リモートサービス (Remote services)	直接検出。不審な管理操作と特権アクセス分析（Privileged Access Analytics）の検知機能によって検出します。
ソフトウェア導入ツール (Software deployment tools)	直接検出。攻撃者が攻撃を継続するために使用する、侵害済みのサードパーティーの脆弱性スキャナを検知します。このようなスキャナーの正常な動作は、トリアージされる可能性がありますが、これらのスキャナを、ネットワークの新しい部分に使用することで検出が行われます。 ポートスキャン、ポートスイープ、内部ダークネットスキャンおよび自動レプリケーション。
汚染共有コンテンツ (Taint shared content)	直接検出。WebDavおよびSMB共有に存在する、不審な .EXE、.DLL、.SCR、.BAT、またはVBSファイルを特定するCoginito Recallに定義したルールによって、リモートディレクトリの汚染を検出します。
リムーバブルメディアを介した複製 (Replication through removable media)	振る舞いはローカルからホストに及びます。このためテクニック実行前に間接的に検出。Cognito RecallのUSBドライブ挿入検知機能によって検出します。
代替認証情報の利用 (Use alternate authentication material)	実行後に間接的に検出。特権アクセス分析（Priviledged Access Analytics）スイートなど、アカウント中心の検知機能によって、侵害を受けたアカウントの使用があったことを検出します。

ATT&CKのテクニック：収集 (Collection)	
テクニック	**Vectra製品の対応**
共有ドライブからのデータ (Data from network shared drive)	直接検出。SMB共有エミュレーションの検知機能によって、データ収集のための共有マウントを検知します。
ステージ済みデータ (Data staged)	直接検出。Data Smugglerによるデータの収集と送信を検出します。
Eメールの収集 (Email collection)	直接検出。Office 365の不審なEメールの転送や、Office 365攻撃者ツールであるRulerの検知機能によって、複数の手段を使ってEメールを取集する攻撃者を検出します。
マン・イン・ザ・ブラウザ (Man in the browser)	直接検出。HTTP/Sの隠れたトンネルから検出します。
アーカイブデータの収集 (Archive data collection)	テクニック実行後に間接的に検出。Smash and Grab、Smuggler、隠れたHTTPやHTTPSトンネル流出などによって、アーカイブ済みメディアのデータの持ち出しが発生したことを検出します。
オーディオキャプチャ (Audio capture)	リモートアクセスツールの中には、オーディオを取得できる機能を備えているものがあります。このためテクニック実行前に間接的に検出。外部リモートアクセス、隠れたHTTPトンネル、隠れたHTTPSトンネル、隠れたDNSトンネル、不審な中継を検知し、C&Cチャネルから検出します。
自動収集 (Automated Collection)	テクニック実行前に、共有ディスカバリからテクニック実行後に、またデータの持ち出しから検出を行います。関連する検出：SMB共有列挙とSmash and Grabを検出します。
クリップボードデータ (Clipboard data)	振る舞いはローカルからホストに及びます。このため間接的に検出。外部リモートアクセス、隠れたHTTPトンネル、隠れたHTTPSトンネル、隠れたDNSトンネルおよび不審な中継を、C&C検知機能で検出します。
情報リポジトリからのデータ (Data from information repositories)	テクニック実行後に間接的に検出。Smash and Grab、Data Smuggler、HTTPトンネル流出、HTTPS流出の発生を検出します。

ATT&CKのテクニック：収集 (Collection)	
テクニック	**Vectra製品の対応**
ローカルシステムからのデータ (Data from local system)	テクニック実行前に間接的に検出。外部リモートアクセス、隠れたHTTPトンネル、隠れたHTTPSトンネル、隠れたDNSトンネル、不審な中継を、このテクニックをサポートするリモートコントロールツールを特定することで検出します。
リムーバブルメディアからのデータ (Data from removable media)	振る舞いはローカルからホストに及びます。このためテクニック実行前に間接的に検出。Cognito RecallのUSBドライブ挿入検知機能によって検出します。
入力のキャプチャ (Input capture)	間接的に検出。ホストのコントロールに使用されるC&Cや中継の検知機能によって検出します。対象は、外部リモートアクセス、隠れたHTTPトンネル、隠れたHTTPSトンネル、隠れたDNSトンネル、不審な中継となります。
中間者攻撃 (Man-in-the-middle)	テクニック実行前および実行後に間接的に検出。LLMNRおよびNBT-NSといったスニッフィング可能なプロトコルの検知や、侵害した認証情報の使用を、Cognito Recallルールを使って検出します。
スクリーンキャプチャ (Screen capture)	テクニック実行前に間接的に検出。外部リモートアクセス、隠れたHTTPトンネル、隠れたHTTPSトンネル、隠れたDNSトンネル、不審な中継を、このテクニックをサポートするリモートコントロールツールを特定することで検出します。
ビデオキャプチャ (Video capture)	テクニック実行前に間接的に検出。外部リモートアクセス、隠れたHTTPトンネル、隠れたHTTPSトンネル、隠れたDNSトンネル、不審な中継を、このテクニックをサポートするリモートコントロールツールを特定することで検出します。

ATT&CKのテクニック：C&C (Command and control)

テクニック	Vectra製品の対応
アプリケーション層プロトコル (Application layer protocol)	直接検出。外部リモートアクセス、隠れたHTTPトンネル、隠れたHTTPSトンネル、隠れたDNSトンネル、不審な中継、不審な管理操作を、C&C検知機能および管理者プロトコルの使用から検出します。
データエンコーディング (Data encoding)	直接検出。外部リモートアクセス、隠れたHTTPトンネル、隠れたHTTPSトンネル、隠れたDNSトンネル、不審な中継を、C&C検知機能で検出します。
データの難読化 (Data obfuscation)	難読化コントロールチャネルを直接検知します。 外部リモートアクセス、隠れたHTTP/Sトンネル、隠れたDNSトンネル、マルチホーム接続トンネル、不審な中継から、検出を行います。
動的レゾリューション (Dynamic resolution)	不審なドメインの検知によって、直接検出します。このアルゴリズムは、ランダムな文字ケースに対応していますが、現状ではランダムなワードケースに対応していません。注意：攻撃者がC&CにDGAを使用するケースは、減少傾向にあります。
暗号化チャネル (Encrypted channel)	直接検出。外部リモートアクセス、隠れたHTTPトンネル、隠れたHTTPSトンネル、隠れたDNSトンネル、不審な中継を、C&C検知機能で検出します。
フォールバックチャネル (Fallback channels)	直接検出。攻撃者が、プライマリの通信が阻止された場合に追加で使用するC&Cチャネルを検出します。隠れたHTTP/Sトンネル、外部リモートアクセス、隠れたDNSトンネル、不審な中継、マルチホーム接続トンネル、Office 365 Power Automateベースの検知によって、検出します。
Ingress転送ツール (Ingress transfer tools)	トンネル経由のコピーを直接検出します。外部リモートアクセス、隠れたHTTP/Sトンネル、隠れたDNSトンネル、マルチホーム接続トンネル、不審な中継から、検出を行います。
マルチステージチャネル (Multistage channels)	C&C検知スイートを使って、直接検出します。

ATT&CKのテクニック：C&C (Command and control)	
テクニック	**Vectra製品の対応**
非アプリケーション層プロトコル (Non-application layer protocol)	外部リモートアクセス、不審な中継の検知によって、直接検出します。
非標準ポート (Non-standard port)	直接検出。外部リモートアクセス、隠れたHTTPトンネル、隠れたHTTPSトンネル、隠れたDNSトンネル、不審な中継を、C&C検知機能で検出します。
プロトコルトンネリング (Protocol tunneling)	直接検出。外部リモートアクセス、隠れたHTTPトンネル、隠れたHTTPSトンネル、隠れたDNSトンネル、不審な中継を、C&C検知機能で検出します。
プロキシ (Proxy)	不審な中継、外部リモートアクセスによって、直接検出します。
リモートアクセスソフトウェア (Remote access software)	外部リモートアクセスにより、リモートコントロールツールを、直接検出します。
トラフィックシグナリング (Traffic signaling)	直接的な検出は、振る舞いに依存するため、正常なポート接続シーケンスについて学習する必要があります。shell knockerクライアントとshell knockerサーバーから検出。
Webサービス (Web service)	直接検出。無許可のWebサービスをCognito Recallのルールから検知し、C&Cの使用を検出します。
リムーバブルメディア経由の通信 (Communication through removable media)	振る舞いはローカルからホストに及びます。このためテクニック実行前に間接的に検出。Cognito RecallのUSBドライブ挿入検知機能によって検出します。

ATT&CKのテクニック：持ち出し (Exfiltration)	
テクニック	**Vectra製品の対応**
自動流出 (Automated exfiltration)	直接検出。Smash and Grab、Data Smuggler、隠れたHTTP/Sトンネル流出を検知し、自動流出を検出します。
データ転送サイズ制限 (Data transfer size limits)	直接検出。Smash and Grab、Data Smuggler、HTTPトンネル流出、HTTPSトンネル流出により、複数に分解したデータの持ち出しを検出します。
代替プロトコルを使った流出 (Exfiltration over alternative protocol)	直接検出。外部リモートアクセス、Smash and Grab、Data Smugglerにより検出します。
C&Cチャネル経由の流出 (Exfiltration over command-and-control channel)	直接検出。Smash and Grab、Data Smuggler、HTTPトンネル流出、HTTPSトンネル流出の検知によって検出します。
Webサービス経由の流出 (Exfiltration over web service)	直接検出。Smash and Grab、Data Smuggler、HTTPトンネル流出、HTTPSトンネル流出の検知によって検出します。
スケジュール転送 (Scheduled transfer)	直接検出。Smash and Grabによって、1時間を超える流出を検出します。
物理メディア経由の流出 (Exfiltration over physical medium)	振る舞いはローカルからホストに及びます。このためテクニック実行前に間接的に検出。Cognito RecallのUSBドライブ挿入検知機能によって検出します。

ATT&CKのテクニック：影響 (Impact)	
テクニック	**Vectra製品の対応**
データ暗号化による影響 (Data encrypted for impact)	直接検出。ランサムウェアファイルのアクティビティを検出し、ファイル共有（ランサムウェア）のデータの、リモート暗号化を検出します。
リソースハイジャック (Resource hijacking)	直接検出。ビットコインの検知により、暗号化通貨発掘のためのリソースハイジャックを検出します。

お問合せ：

CoginitoのMITRE ATT&CKフレームワークのサポート詳細については、弊社サービス担当、info-japan@vectra.ai **までお願いします。**

Version:**071920**