VECTRA
SECURITY THAT THINKS.®

ケーススタディ

投資銀行Greenhill、Office 365 SaaSへのサイバー攻撃を阻止

Greenhill and Co.の事業の中核は、顧客のリスク管理を支援することです。

ニューヨークに本社を置くこの大手投資銀行は、世界中の機関や政府に対し、大型の合併、買収、再編に関する財務的なアドバイスを提供しています。

Greenhillの顧客には、Alcoa、Experian、Gannett、GlaxoSmithKline、および米国、カナダ、英国、オーストラリア政府が含まれます。

サイバーリスクを減らす

Greenhillでは、ビジネスリスクとサイバーリスクの両方を軽減する取り組みを定期的に行っています。「サイバー攻撃に関する振る舞いを特定するために、ネットワークの可視性を高める必要がありました」とGreenhillのCIOであるJohn Shaffer氏は述べています。

「近年の攻撃は、ファイアウォールやIDS、その他のレガシーセキュリティシステムを回避してネットワーク内に広がり、盗むべき資産を探しています」

John Shaffer氏
CIO、Greenhill

GreenhillではSIEMツールを使用していましたが「大量にあるファイアウォールのログのうち、脅威の深刻度を見極めるのに苦労していました」と同氏は言います。

また、Microsoft Office 365などのSaaSプラットフォームにおいて、毎月30%以上の事業部が被害に遭っており、認証情報の不正利用やアカウントの乗っ取りが増加していることにも懸念を抱いていました。攻撃者は、ソーシャルエンジニアリングの手法で人間の振る舞いを悪用し、アカウントの権限を変更して重要なビジネスデータを盗むのです。

Greenhill

組織
Greenhill

業種
金融サービス

課題
ネットワークの可視性を高め、脅威の深刻度を簡単に識別する必要があった

選定基準
調査すべき重要な脅威を迅速に特定し、ネットワークの可視化を実現するAIベースのネットワーク検知および対応（NDR）ソリューションであること

結果
- ログを追いかけるのではなく、調査や積極的な脅威ハンティングに集中できるようになった
- 自信を持ってOffice 365 における不正な権限の変更やアカウント乗っ取りを特定できると言えるようになった
- AIベースのアルゴリズムにより、セキュリティ担当の時間と労力を節約できるようになった
- ネットワーク上での攻撃者の振る舞いを特定し、エンドポイントで即座に攻撃を停止できるようになった

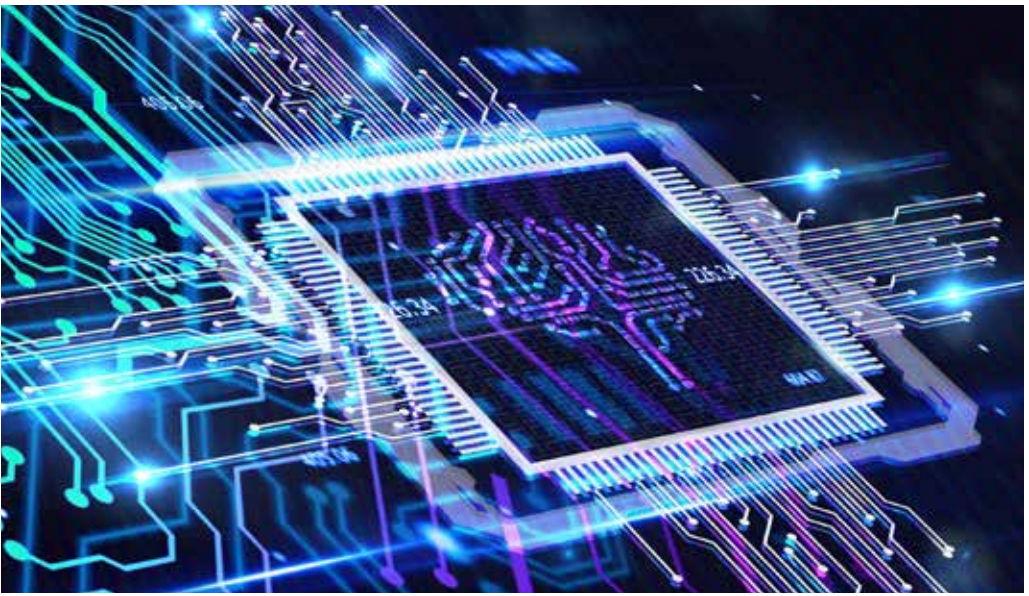
ソリューション：Cognito NDRプラットフォーム

Greenhillは、Vectra® AIのCognito® ネットワーク検知および対応 (NDR)プラットフォーム上で動作する、Cognito Detect™ AIソフトウェアを早期に採用しました。

Cognito Detectは、AIを活用して、クラウドやデータセンターのワークロード、Microsoft Office 365などのSaaSサービス、ユーザーやIoTデバイスにおけるサイバー攻撃者を瞬時に特定し、阻止します。

Shaffer氏は「我々が対処するほとんどの脅威は、ウイルス対策ソフトウェアやシグネチャベースなど、従来のツールでは解決できません。本当の攻撃者は、回避する方法を知っているからです。巧妙な手法を使う攻撃者が何をしているのか把握するためには、Vectra AIのAIと機械学習が活躍します」と言います。

Cognito Detectは、AIベースの機械学習アルゴリズムを使用して、クラウド、データセンター、IoT、エンタープライズネットワーク全体で、最もビジネスリスクが高い進行中の攻撃に関する振る舞いを自動的に検知し、優先して対応します。



「Cognito Detect for Office 365 によって、攻撃者がどのように侵害しアカウントを乗っ取っているかを理解できます。長年Vectra AIのソリューションを使っていますが、自信を持ってOffice 365における不正な権限の変更やアカウント乗っ取りを特定し、阻止することができると言えるようになりました」

Cognito Detectを使うことで、攻撃者の検知やトリアージのような、手動で行うTier 1 および Tier 2 セキュリティタスクを自動化し、Greenhillのセキュリティオペレーションのワークロードは大幅に削減されました。

「Cognitoによる自動化は大きな変化をもたらしました。今までは大量のセキュリティログに目を通した後、膨大な量のアラート対応するため疲弊していました。今では、ログを追いかけるのではなく、調査と積極的な脅威探索に集中できます」とShaffer氏は述べています。

より決定的なインシデント調査とAIによる脅威ハンティングのために、Cognito Detectはすべてのネットワークトラフィックからメタデータを抽出し、侵害されたすべてのユーザー、アカウント、デバイス、その攻撃が大規模なキャンペーンの一部であるかどうかなど、各攻撃に関する詳細なセキュリティコンテキストでエンリッチ化します。

Shaffer氏が初めてCognito Detectを導入したとき、銀行のネットワーク上に奇妙なトラフィックパターンがあるとのアラートを受けました。確認すると、それは会社独自の脆弱検出スキャナーであることが判明しました。

「他の多くのセキュリティシステムでは、これも攻撃者が社内ネットワークをスキャンしているように見えたでしょう。このことからも分かるように、ネットワークで何が起こっているかを知ることは重要です」とShaffer氏は指摘します。

「VectraのAIベースのアルゴリズムは、正常な振る舞いと悪意のある振る舞いの違いを学習し、セキュリティ担当者の作業時間と労力を削減します」

Office 365におけるデータ漏洩を阻止

Cognito Detect for Office 365は、Cognito NDRプラットフォーム上で動作するAzure Active Directory、SharePoint、OneDrive、Exchange、Teamsなど複数のOffice 365 SaaSサービスからアクティビティログを取り込みます。

Office 365アプリケーションの動作を深く理解しているので、AIベースの機械学習アルゴリズムを適用し、隠れたサイバー攻撃者を積極的に検知、対応し、データ漏洩を阻止します。

Cognito Detect for Office 365は、認証情報の不正使用やアカウントの乗っ取りを特定するために、ログイン、ファイルの作成と操作、データ損失保護の設定、メールボックスの転送設定、自動化の変更における悪意のある振る舞いパターンを分析します。

検知された情報は、ユーザーアカウントの権限に関連付けられ、リスクに基づいて優先順位が付けられます。これにより、Greenhillは攻撃のシナリオを完全に把握し、攻撃にすばやく対応して軽減し、データ漏洩を阻止することができます。

投資の保護と作業負荷の軽減

Cognito NDRプラットフォームは、対応時間を短縮するために、EDR、SIEM、SOARツール、ファイアウォール、NACなどのサードパーティのセキュリティソリューションと、脅威に関する洞察やコンテキストを統合して共有し、エンドツーエンドの脅威管理と可視化を実現します。

Greenhillが最も信頼しているのは、Vectra AIのNDRとCrowdStrike社のEDRの2つのソリューションです。

「毎日が攻撃者の一歩先を行くための競争のようなものです。ネットワーク上の攻撃者の振る舞いをピンポイントで特定し、エンドポイントでの攻撃を即座にシャットダウンする最速の方法を必要としています。Vectra AIのソリューションはネットワーク上で先手を打ち、CrowdStrike社のソリューションはエンドポイントでのセキュリティを支えます」とShaffer氏は述べています。

同氏によると、攻撃の全容を把握し、被害の拡大を阻止し、データ漏洩を回避するためには、Vectra AIとCrowdStrike社からのセキュリティ情報を相関させ、分析することが必要だと言います。

「Vectra AIは、多くのセキュリティシステムのように、膨大な量のアラートを通知することはありません。データはダイレクトで、ルールを書く必要もありません。時間の経過とともに、AIベースのアルゴリズムは、正常な振る舞いと悪意のある振る舞いの違いを学習し、セキュリティ担当の作業時間と労力を削減します」

「Vectra AIのソリューションはネットワーク上で先手を打ち、CrowdStrike社のソリューションはエンドポイントでのセキュリティを支えます」

詳細については、info-japan@vectra.aiまでお問い合わせください。