お客様事例 | 金融サービス

ブラックストーン社、Vectra AIの導入により、Microsoft 365における脅威のアラート数を90%削減

世界最大のオルタナティブ資産運用会社であるブラックストーンは、成功を収めつつ強靭なビジネスを構築することを目指しています。プライベート・エクイティ、不動産、テクノロジーなど幅広い資産に投資を行う同社は、組織が課題を解決し、価値を創出できるようにする革新的な戦略を打ち出してきた確かな実績を有しています。

組織

ブラックストーン

業界

金融サービス

課題

組織のセキュリティを維持するために、Microsoft 365データの可視性を確保する

選定基準

重大な脅威を迅速に特定するAIベースの検知・対応ソリューション、かつMicrosoft 365環境全体にわたるネットワーク可視性を提供するソリューション

成果

- Microsoft 365環境に対する新たな脅威検知を1日で50件以上追加
- アラート数を90%削減
- Vectra AIの予防層を突破する脅威を検知する能力により、セキュリティ体制の強化が必要な領域を特定できるようになった

ブラックストーンが成果を上げ続けている理由の一つは、自社の技術プラットフォームとビジネスミッションがどちらも卓越した性能を発揮するよう考えられている点にあります。同社はテクノロジーを活用してビジネスを推進しており、サイバーセキュリティはその方程式における重要な要素です。

グローバルに分散した環境を保護することは、特に潜在的なサイバー攻撃が渦巻く脅威環境において、決して容易なことではありません。

ブラックストーンのサイバーセキュリティ担当上級副社長であるKevin Kennedy氏をはじめとするセキュリティ運用チームは、同社をサイバー攻撃から守ることに注力しており、常に状況を注視することで、環境内で何か異常が見られた際に迅速に特定できることを理解しています。

365日24時間体制で全体像を把握

ブラックストーンが環境全体における潜在的な悪意のある活動を監視する一つの方法は、アラートの検知および対応機能を一元化することです。

Kennedy氏は、この取り組みについて「受信した情報や流入するあらゆる情報を確実に把握できるようになります。すべてを一箇所に集約できれば優先順位付けが可能になるため、これは非常に重要です」と述べています。

また、脅威の検知に関する具体的な詳細を把握することの重要性を強調しています。例えば、各検知が何を意味するのかを正確に把握すること、そしてイベントが検知を引き起こしてから、アナリストが対応し、調査を完了するまでにどれくらいの時間がかかるかを知ることは、すべて重要な指標であると同氏は語ります。

「これらの指標は、アナリストがどこに時間を費やしているかを的確に把握するために重要です。どの検知がノイズが多く、どの検知が精度が高いのかについて、非常に明確な把握ができるようになります。」

Vectra AIのDetect for Office 365によりアラート数を90%削減

脅威の検知と対応がブラックストーンの重点課題であることから、Vectra Detect for Azure AD and Microsoft 365の導入は、同社の戦略において重要な役割を果たしています。Kennedy氏は、Microsoft 365のデータに対する可視性を確保することが、組織のセキュリティを維持する上で不可欠であると指摘しています。同社は、Detect for Microsoft 365を活用して、受領する脅威検知の自動化と品質向上を図っており、これは以前使用していたネイティブの検知機能から一歩進んだ取り組みです。

Vectra AIと他のソリューションの大きな違いの一つは、人工知能 (AI) を活用してMicrosoft 365データ内の脅威の振る舞いを特定する能力にあります。これにより、ブラックストーンのサイバーセキュリティチームの脅威検知業務が円滑化されました。そして、検知結果はMITRE ATT&CKフレームワークにマッピングされます。それは、一般的な攻撃の振る舞いに対するカバー範囲を的確に把握することを可能にします。「低精度から高精度へのシグナル・ノイズ比の調整は、基本的にすべてVectra AIによって上流工程で行われます。Vectra AIのプラットフォームは、当社のサイバーセキュリティ防御能力の強化に寄与し、全社的なサイバーセキュリティプログラムの効率化を実現してくれました」とKennedy氏は述べています。

これは、時間の節約という点において、ブラックストーンのチームにとって大きな進歩となりました。Vectra AIを導入する前は、複雑な検知機能の開発に最大6か月を要していましたが、Detect for Microsoft 365では、「たった1日で完了するシンプルな統合を通じて、Office 365環境に対して50件以上の新たな脅威検知を追加することができました。Vectra AIの機械学習がモデル内でより多くの特徴やコンテキストを評価し、より正確な検知につながるため、アラートの量は90%削減されました」とKennedy氏は説明します。

「以前は、アラートがあまりにも多く、必要な情報を抽出するのが困難でした。Vectra AIプラットフォームのおかげで、調整を非常に迅速に行うことができ、現在では、Microsoft 365に関連するVectra AIから当社のケース管理ツールに送信される項目の精度が大幅に向上しています。」

「たった1日で完了したシンプルな統合により、MICROSOFT 365環境に対して50以上の新たな脅威検知を追加することができました。」

KEVIN KENNEDY 氏
シニア・バイス・プレジデント、
サイバーセキュリティ担当
ブラックストーン

今日のサイバー脅威に対する先制的なアプローチで道を切り拓く

ブラックストーンは、Vectra AIとの提携を通じて、今日の攻撃に対する防御策を講じています。Microsoft 365は重点領域の一つであり、アカウント乗っ取り攻撃がクラウドにおける最大の脅威の一つとなりつつある中、Vectra AIは攻撃者の振る舞いを分析し、特権アカウントが侵害されたタイミングを特定することで、このリスクを軽減します。

Kennedy氏によると、検知および対応能力の向上により、担当チームは、自社の予防システムにおいてどの部分に注力すべきかをより深く理解できるようになりました。

Vectra AIが持つ予防層を突破する脅威を検知する能力により、これまで把握できていなかった、より強固なセキュリティ体制が必要な領域を特定できるようになりました。

ブラックストーンはセキュリティ運用において、24時間365日の徹底した一元管理アプローチから、予防的な検知および対応の監視に至るまで、今日のサイバー脅威に対する防御において、あらゆる面で同社に最適な対策を実現しています。

Vectra AIについて

Vectra AIは、AIネイティブなセキュリティおよび可視化分野のリーダーです。高度なサイバー攻撃が既存の制御を回避し、検知を逃れて顧客のデータセンター、キャンパス、リモートワーク、アイデンティティ、クラウド、IoT/OT環境にアクセスした場合でも、Vectra AI プラットフォームは攻撃のあらゆる動きを監視し、リアルタイムで点と点を結び付けて、侵入を阻止します。また、AIセキュリティに関する39件の特許を取得し、MITRE DEFENDで最も多くのベンダーリファレンスを誇ります。他のツールでは検知できない攻撃を見つけ、阻止するために世界中の組織がVectra AIを活用しています。詳細については、https://ja.vectra.ai/ をご参照ください。

ja.vectra.ai/　　お問い合わせ:info-japan@vectra.ai