VECTRA

お客様事例 | ホスピタリティ・専門サービス業

ファン・ゴッホ美術館、Vectra AIの活用で、Azure、アイデンティティ、データセンター全体で84%の真陽性率を達成

ファン・ゴッホ美術館は、フィンセント・ファン・ゴッホの世界最大のコレクションを所持しています。貴重な文化遺産の保存のほか、世界中から訪れる訪問者に作品を公開しています。美術館は、代替不可能な芸術作品の物理的なセキュリティ管理だけでなく、オンプレミスとクラウド環境の両方で、高解像度デジタル資産、顧客データ、財務情報などの重要な資産を保護する必要があります。

Van Gogh Museum Amsterdam

組織
ファン・ゴッホ美術館

業界
ホスピタリティ・専門サービス業

課題
ファン・ゴッホ美術館は、サイロ化されたツールと限られたコンテキストによって、ハイブリッド環境全体で脅威を検知し、攻撃者の活動を把握することが難しくなり、リスクが増大していました。

ソリューション
Vectra AIプラットフォームを導入することで、同館はネットワーク、クラウド、アイデンティティを一元的に可視化できるようになり、セキュリティチームは脅威を早期に検知して迅速に対応できるようになりました。

セキュリティの変革
プラットフォームの価値

Vectra AIのもたらすインパクト	成果
カバレッジ	• ネットワーク、アイデンティティ、クラウドを一元的に可視化し、脅威にさらされる機会を大幅に削減 • 毎月25件の脅威を検知
明瞭性	• 最小限のノイズで、84%の真陽性率を実現 • 理解しやすいアラートにより調査を効率化
コントロール	• 攻撃者の振る舞いを早期に検知し、迅速な対応を可能にする • 簡素化されたインシデント対応ワークフロー

Vectra AIと提携することで、ファン・ゴッホ美術館はセキュリティ運用を強化し、貴重な資産を保護するために必要な可視性、インテリジェンス、スピードを実現しました。84%の真陽性率と、主なアタックサーフェスににわたってカバレッジすることにより、チームはトラブルの最初の兆候で脅威を検知し、対応できるようになりました。

課題

かけがえのない文化資産とデジタル資産の保護

サイバー脅威がさらに標的型になる中、ファン・ゴッホ美術館はデジタルアーカイブや、来館者情報、財務データに対するリスクの高まりに直面していました。

「私たちのデジタルコレクションは、多くの人が認識している以上に大きな価値があります」とファン・ゴッホ美術館のCISOであるRob de Zwaan氏は語ります。

同博物館は大規模なクラウド移行を進めており、オンプレミスの資産をMicrosoft Azureに移行していました。このデジタルフットプリントの拡大により、新たなセキュリティの盲点が生じ、それに対処する必要がありました。

企業がハイブリッド環境に移行する中、現代のネットワークはオンプレミス、クラウド、アイデンティティを含むように進化しています。「オンプレミスとAzureの両方で、当館の環境を侵害しようとする、国家主導の攻撃者による侵入の試みが相次いでいました」とde Zwaan氏は指摘します。

既存のセキュリティツールは、アラートを生成するものの、サイロ化されたデータしか提供せず、セキュリティインシデントに関するコンテキストもほとんどないため、どの脅威に対処する必要があるのかを判断するのが困難でした。「Microsoftからは大量の情報が提供されましたが、構造化されておらず、“何かが起こった”がわかるだけで、具体的に何が問題なのかを自分で調べる必要がありました」と同氏は話します。

ソリューション

最新ネットワークの可視化

ファン・ゴッホ美術館は、ハイブリッド環境全体の包括的な可視性を得るためにVectra AIを導入しました。まずは、オンプレミスのインフラに対するネットワークの検知とレスポンスから始め、次に成長するAzureクラウド環境にも対応範囲を拡大。環境間を移動する攻撃者のリスクに対処しました。

この変革を支援するため、チームはVectra AIのクラウドセキュリティ機能も導入しました。「Vectra AIのプラットフォームは、ネットワーク、アイデンティティ、Azureにまたがる攻撃者の振る舞いをリアルタイムで可視化し、不審なアクティビティを相関させ、攻撃者が突く可能性のある隙を明らかにしてくれました」とde Zwaan氏は説明します。

導入直後に、その価値はすぐに明らかになりました。「Vectra AI導入後、ネットワーク内で予期しないトラフィックを即座に検知し、ブロックすることができました。全体的なセキュリティ体制の強化につながりました。」

調査を合理化する、理解できるセキュリティの洞察

セキュリティアラートの意味を理解することは、脅威を検知することと同じくらい重要ですが、従来のセキュリティツールでは、複数のポータルに散在する複雑な形式で情報を提示することが多く、チームは手作業でコンテキストをまとめることを余儀なくされていました。

「Microsoftでは、相関ID、ユーザーID、無限の文字列など、すべてがIDです。25分かけてポータル間を飛び回り、その意味を理解しようとしたものの、結局は無関係なものだったということが多くありました。私は人間です。そして、Vectra AIは人間の言語で話してくれます。機密ファイルにアクセスしようとするユーザーであれ、挙動不審なサーバーであれ、何が起きているのかを正確に教えてくれます。一分一秒を争うような状況では、このような明確な情報は、大変貴重です」とde Zwaan氏は述べます。

この明瞭性はクラウド環境にも及んでいます。セキュリティデータを手作業でつなぎ合わせる必要がなくなり、重大な変更が発生したときには、明確で実用的なアラートを受け取ることができるようになりました。

「Vectra AI for Azureは、ストレージの認証情報やアクセス設定に変更があった場合にアラートを発し、貴重なデータがインターネット上に流出しないようサポートしてくれます」と同氏は語ります。

「Vectra AIのプラットフォームは、ネットワーク、ID、Azure環境にわたる攻撃者の振る舞いをリアルタイムで可視化し、不審な振る舞いを相関させ、攻撃者が悪用する可能性のあるギャップを浮き彫りにしました。」

ファン・ゴッホ美術館
CISO
Rob de Zwaan 氏

「当館のセキュリティポスチャは劇的に改善されました。ネットワーク、Entra ID、M365、Azure環境全体にVectra AIを導入して以来、防御能力は倍増しました。」

ファン・ゴッホ美術館
CISO
Rob de Zwaan 氏

脅威の早期検知で優位性を確立する

ファン・ゴッホ美術館は、セキュリティが進化する脅威との継続的な競争であることを理解しています。

「ハッカーと争っていると、常に数歩遅れてしまいます。彼らは驚くほど悪才に長け、私たちが守ろうとしている間に瞬時に戦術を変えることができます」とde Zwaan氏は述べます。

しかし、Vectra AIはこの力関係を根本的に変えました。「Vectra AIによって、不審な振る舞いをより早い段階で発見することができます。被害が発生してから侵害を発見するのではなく、最も重要なときに対策を講じることができるのです。この早期アラートによって、必要となるアドバンテージを得ることができるのです」と同氏は語ります。

可視性が高まったことで、チームにとってより実用的なアラートが出るようになりました。「より多くのアラートを目にするようになりましたが、それは実際に可視化されたからです。毎月約25件の真正インシデントを処理しており、真正率は84%です。」

美術館の全体的なセキュリティーへの影響は相当なものです。「当館のセキュリティポスチャは劇的に改善されました。ネットワーク、Entra ID、M365、Azure環境全体にVectra を導入して以来、防御能力は倍増しました。」

統一されたセキュリティ管理

セキュリティインシデントの管理には迅速な対応が求められるため、チームは統合ソリューションであることを重視しています。「Vectra AIは、これまで使用してきた他のソリューションよりも直感的です。ネットワーク、アイデンティティ、クラウドのすべてのコンポーネントが同じように見え、同じように機能し、一貫した結果をもたらします。」

環境間でシームレスなインターフェイスを持つ単一のプラットフォームを持つことで、チームはより迅速に対応できるようになりました。「他の製品では、インシデント発生時に複数のポータルを開く必要があり、貴重な時間を浪費していました。緊急事態が発生した場合、対応できる時間は数分しかなく、一分一秒を争います。」

「他の製品を探すために時間を無駄にしないでください。Vectra AIがあれば良いのです。」

ファン・ゴッホ美術館
CISO
Rob de Zwaan 氏

結果

何が危険に晒されているのかを理解する

Vectra AIを導入して以来、ファン・ゴッホ美術館は防御を大幅に強化し、脅威の早期発見を実現し、インシデント対応プロセスを合理化しました。

成功において最も重要だったのは、同館が独自の課題を理解してくれるセキュリティパートナーを見つけたことにもあります。de Zwaan氏は次のように説明します。「Vectra AIは、守ろうとしていることを理解するために時間を割いてくれます。特定の問題やその問題から生まれる疑問を理解し、的を絞ったソリューションを提供してくれます。」

同じような課題に直面している組織に対して、「他の製品を探すために時間を無駄にしないでください。Vectra AIがあれば良いのです」と同氏はコメントしています。

「お客様事例」をもっと読む

Vectra AIとは

Vectra AIは、現代のネットワークを最新の攻撃から保護するAI主導のサイバーセキュリティを提供しています。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、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、当社はAIセキュリティに関する35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**