opentext™ | Cybersecurity

お客様事例

グローバル展開するメーカー

ArcSight Intelligence の提案検証 (POC) によって、進行中の総当たり攻撃が検知され、修正されます。

ArcSight Intelligence で CrowdStrike を補完

グローバルなビジネスモデルを持つこのようなメーカーにとって、サイバーセキュリティは非常に重要です。すでに CrowdStrike の Endpoint Detection and Response (エンドポイントでの検出と対応、EDR) を導入していた同社ですが、脅威を管理するうえでさらにインテリジェンスが必要であると感じていました。同社のチームは CrowdStrike の機能を補完するため、ArcSight Intelligence by OpenText を使用して 30 日間の無料エンドポイント脅威検知プロジェクトを開始しました。世界中に分散する数千のエンドポイントの保護を必要とする同社は、ArcSight Intelligence が機械学習を活用してデータをコンパイルし、そのデータを Cybersecurity OpenText™ の脅威検出チームが綿密に分析するという手法に関心を引かれたのです。驚いたことに、複数のエンドポイントで異常が検出されました。サーバーが総当たり攻撃を受けており、攻撃者がネットワークをたどって組織内の他のマシンにアクセスしていることが明らかになりました。Cybersecurity のチームは、ArcSight Intelligence プラットフォームへのアクセス先とともに、実施項目に優先順位を付けたレポートを提出しました。

危険にさらされるリスクを最小限に抑え、当面の脅威を排除

ArcSight Intelligence を使用すると、検出された脅威に、優先順位付けの参考となる「脅威グレード」が付与されます。最初のデータレビューの後、同社のサイバーセキュリティチームは、社内のエンドポイントだけでなくその周辺の環境の外側 (関連組織を含む) に対する攻撃の可能性もなくすため、迅速に対策を講じました。

ArcSight の脅威ハンティングチームは、48 時間に及ぶ内部的な修正期間を経て、当面の脅威を排除するための実施可能な項目の処理を完了した後も、同社との連携を継続しました。またこの間に、認識された脅威が次のレベルに移ったときに備えて、追加の知見とガイダンスを提供しました。同社のサイバーセキュリティチームは現在、将来的に使用することを見込んで、ArcSight Intelligence の導入を進めているところです。

概要

業種

製造

所在地

米国

課題

世界中に分散する数千のエンドポイントを不正アクセスから保護する

製品とサービス

ArcSight Intelligence

成功ポイント

- 進行中のサーバー攻撃を特定して修正
- 機械学習機能を通じて提供される優先順位が付いた実用的なデータ
- 危険にさらされるリスクを最小限に抑制

opentext™ | Cybersecurity

OpenText Cybersecurity は、あらゆる規模の企業とパートナー様を対象に、包括的なセキュリティソリューションを提供しています。予防から検出、復旧対応、調査、コンプライアンスに至るエンドツーエンドの統合プラットフォームにより、包括的なセキュリティポートフォリオを通じてサイバーレジリエンスの構築をサポートします。コンテキストに基づくリアルタイムの脅威インテリジェンスから得られた実用的なインサイトを活用できるため、OpenText Cybersecurity のお客様は、優れた製品、コンプライアンスが確保されたエクスペリエンス、簡素化されたセキュリティというメリットによって、ビジネスリスクを管理できます。

768-JA0067-002 | O | 12/23 |