グローバルメーカー

ArcSight Intelligence の概念実証 (POC) によって、進行中のブルートフォース攻撃 (総当たり攻撃) を検知し、対処しました。

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、脅威管理に関して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、CyberRes ArcSight Intelligence を使用して 30 日間の無料エンドポイント脅威検出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収集し、そのデータを CyberRes 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持ちました。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。サーバー上でブルートフォース攻撃が行われており、攻撃者は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。CyberRes チームは、アクションアイテムに優先順位付けしたレポートと、ArcSight Intelligence プラットフォームへのアクセス権を提供しました。

危険にさらされるリスクを最小限に抑え、差し迫る脅威を排除

ArcSight Intelligence を使用すると、検出された脅威には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、外部からの攻撃の可能性をなくすため、関連組織を含め、露出のリスクを最小化するために迅速な対策を講じました。

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、認識された脅威が次のレベルに移ったときに備えて、さらなる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

業界

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

製品とサービス

CyberRes ArcSight Intelligence

成功ポイント

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

マイクロフォーカスエンタープライズ株式会社
jp-info-enterprise@microfocus.com
www.microfocus-enterprise.co.jp