大手医療関連企業

ArcSight Intelligence は内部脅威を無効化し、機密データの盗難を防止します。

仮説ベースの脅威ハンティングからアナリティクス主導の脅威ハンティングへ

この企業では 12,000 人を超える内部ユーザーが機密性の高い患者データにアクセスしており、内部脅威によってそれらのデータのセキュリティが危険にさらされる可能性があるという現実に目を向けることを余儀なくされていました。同社のセキュリティオペレーションセンター (SOC) は、実用的な仮説の作成、実行、テストまでを実施する仮説ベースの脅威ハンティングをすでに導入していました。この手法が目的としているのは、点と点を結び、何が正常であり何が正常でないのかを決定して、異常を特定することです。同社の最高情報セキュリティ責任者 (CISO) は、どのようなことを求めていたかについて、次のように説明しています。「仮説ベースの脅威ハンティングから生じる、大量の散漫な誤検知の管理に追われるのではなく、より正確な行動インテリジェンスに基づく仮説を作成することで、当社のハンティングの取り組みを増強して改善できないものかと考えていました」

CyberRes ArcSight Intelligence は、社内の最もリスクの高い振る舞いをコンテキストに基づいて表示し、SOC チームは脅威を視覚化して検証できる適切なツールとしてこれを利用できます。統計的確率と教師なし機械学習を用いて通常とは異なる振る舞いと本当の脅威とを結び付け、最も疑わしいエンティティを特定します。

「ArcSight Intelligence は、使用頻度の低いサーバーへの認証に成功し、その認証でグローバル全体にわたって複数サーバーへのアクセスを試みる振る舞いを検知しました。ある管理者 (結果的に解雇されました) に絞り込まれましたが、ArcSight Intelligence は、そのアカウントが停止された後にも再認証を試みていることを検知しました。すべての認証試行が特定され、無効化されました」

最高情報セキュリティ責任者
大手医療関連企業

内部脅威の無効化

ホスティングされたクラウド環境への導入後、ArcSight Intelligence は、EMC アプリケーションの機密データへのアクセスを試みる内部脅威を特定し無効化することができました。ある管理者がサーバーの脆弱性を悪用しており、もし成功していれば、データが盗まれるところでした。

同社は ArcSight Intelligence をデータソースにも拡張し、適用範囲を広げる計画を立てています。

概要

業界
医療

所在地
米国

課題
大規模な組織において、セキュリティ上の異常から、内部脅威を特定する、より効率的な方法を見つける

製品とサービス
CyberRes ArcSight Intelligence

成功ポイント

- 巧妙な内部脅威の特定および無効化
- アナリティクス主導の脅威ハンティングにより効率性と効果が向上
- 教師なし機械学習により脅威ハンティングの生産性が飛躍的に向上

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