opentext™ | Cybersecurity

お客様事例

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移行

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、自分が何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によってもたらされる、混乱のもとである膨大な誤検出の管理に追われるのではなく、より正確なインテリジェンスベースの振る舞い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」

「ArcSight Intelligence は、使用頻度の低い特定のサーバーへの認証が成功していることを検知しました。この認証によって、複数のサーバーへのアクセス試行がグローバルに行われました。ArcSight Intelligence はある管理者 (結果的に解雇されました) に的を絞り、それから、個々のユーザーの認証が終了した後で再認証を試みたアカウントを特定しました。すべての試行が特定され、無効化されました」

最高情報セキュリティ責任者
大手医療機関

ArcSight Intelligence by OpenText™ は、社内の最もリスクの高い振る舞いをコンテキストに合わせて表示し、SOC チームは脅威を視覚化して調査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、最も強い疑いのあるエンティティを特定します。

内部脅威の無効化

ホスト型クラウド環境に導入された 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。

同社はデータソースを ArcSight Intelligence に拡張してカバー範囲を広げる計画を立てています。

概要

業種
医療

所在地
米国

課題
大きな組織内でセキュリティの異常を通して内部脅威を特定するための、より効率的な方法を見つける

製品とサービス
ArcSight Intelligence

成功ポイント

- 高度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

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。