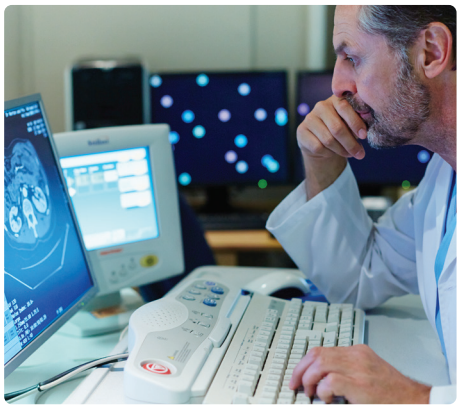
opentext™ | Cybersecurity

お客様事例

大手医療機関

ArcSight Intelligence が、患者の機密データに対するセキュリティ侵害を防止しています。



患者の機密データをサイバー攻撃から保護

医療機関であるこの組織は、非常に機密性の高い患者データを保有しているため、HIPAA などの厳格な規制コンプライアンスの対象となっています。同機関の最高情報セキュリティ責任者 (CISO) は、セキュリティの脅威を強く警戒しており、次のように発言しています。「企業ネットワークに対する高度な攻撃を検知して阻止する能力が私たちには必要です。また、内部脅威という現実的なリスクにも対処する必要があります。セキュリティオペレーションセンター (SOC) は素晴らしい仕事ぶりを見せていますが、当機関に最大のリスクをもたらす脅威の調査にアナリストを専念させることで、生産性を向上させたいと私たちは考えていました」

「ArcSight Intelligence によって、数百回の認証試行に失敗してもロックされていなかったアクティブな休眠ゲストアカウントが見つかりました。その作業はすべて就業時間外に行われました。機密サーバーへのアクセスの試みがありましたが、当機関のチームが、侵害の発生前にそのアクティビティを無効にすることができました」

最高情報セキュリティ責任者
大手医療機関

ArcSight Intelligence by OpenText™ は、セキュリティチームがそれまで知られていなかった脅威を発見して対応できるようにします。こうした状況でまさに必要とされていることです。その柔軟な導入オプションは、この組織のクラウドのビジョンに一致しており、またセキュリティチームは、特に ArcSight Intelligence の教師なし機械学習 (ML) 機能を高く評価しました。ML を活用することで、「固有の正常状態」のベースライン、言ってみれば各ユーザーやエンティティのデジタルの指紋が学習されます。このベースラインは、それ自体または同僚のものと継続的に比較することができます。この行動分析的なアプローチによって、セキュリティチームは従来見つけにくかった脅威を検出できるようになります。

ArcSight Intelligence による攻撃の防御の成功

ArcSight Intelligence の実装後は、外部の攻撃者を特定して無力化することができるようになり、組織にとって大きな成果となりました。

同機関は、ArcSight Intelligence を引き続き活用して、セキュリティチームの取り組みを強化および合理化する予定です。

概要

業種
医療

所在地
米国

課題
厳格なデータプライバシー規制を順守しながら、侵害が発生する前に高度なサイバー攻撃や内部脅威を検出して阻止

製品とサービス
ArcSight Intelligence

成功ポイント
- 攻撃を特定して無力化し、セキュリティ侵害を防止
- 機械学習機能による脅威ハンターの効率性の向上
- 企業の IT ポリシーに沿ったクラウドへの導入

768-JA0072-002 | O | 12/23 | © 2023 Open Text