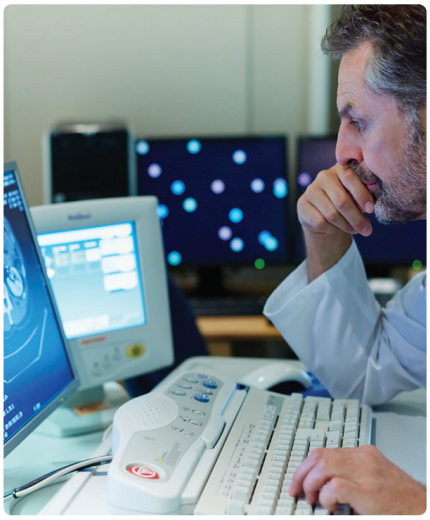
大手医療機関

ArcSight Intelligence は、機密性の高い患者データのセキュリティ侵害を未然に防ぎます。



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出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、私たちにとって最もリスクの高い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、チームは侵害が発生する前にその活動を停止させ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

CyberRes ArcSight Intelligence は、セキュリティチームが未知の脅威を発見して対応できるようにするもので、まさに、このような状況で必要とされているものです。その柔軟な導入オプションは、この組織のクラウドビジョンにマッチしており、またチームは、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、「ユニークノーマル」ベースライン、つまり、各ユーザーやエンティティのデジタルフィンガープリントが学習され、それ自体あるいは組織の他のユーザー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 による攻撃防御の成功

ArcSight Intelligence の導入後は、外部の攻撃者を特定して無力化できるようになり、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効率化する予定です。

概要

業界

医療

所在地

米国

課題

高度なサイバー攻撃や内部脅威を検知し、侵害が発生する前に阻止するとともに、厳しいデータプライバシー規制に準拠する

製品とサービス

CyberRes 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

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