opentext™ | Cybersecurity

お客様事例

大手金融サービス企業

POC で得られた驚異的な結果により、ArcSight Intelligence for CrowdStrike を導入し、内部脅威に対抗することに成功しました。

誰がどのような目的でデータにアクセスするのか

これは、この企業の最高執行責任者がセキュリティチームに尋ねた重要な質問です。この企業では、外部脅威からデータを保護するために、大手 MSSP と CrowdStrike による高度なセキュリティ体制を備えていたものの、内部脅威から顧客の機密データを保護するために、さらなる可視化が必要であると認識していました。この課題について、同社は次のように説明しています。「1,000 人以上の従業員を擁する当社のシステムが記録するセキュリティイベントの件数は年間 66 億を超えるため、手作業による監視は難しいうえにコストも時間もかかります。当社では、1 名の専任スタッフが、内部脅威の可能性がある電子メールを手作業でチェックしています。これは明らかにプロセスとして不十分です。また、本質的にミスを犯しやすい人間に拠ってしまうという問題もあります。規制の厳しいこの業界では、会社の評判に傷がつく恐れが非常に高いため、既存のセキュリティインフラストラクチャを補完し、特に内部脅威対策に焦点を当てたソリューションを探しました」

「CrowdStrike と MSSP のインフラストラクチャに ArcSight Intelligence for CrowdStrike と脅威ハンティングサービスを追加することで、機密性の高い顧客データを保護し、風評被害のリスクを大幅に軽減することができました」

セキュリティマネージャー
大手金融サービス企業

ArcSight Intelligence の POC で得られた実用的なインサイト

幅広く市場を調べた結果、お客様は CyberRes が提供する ArcSight Intelligence for CrowdStrike にたどり着きました。これは、既存の CrowdStrike エンドポイントセキュリティへの投資を活かせるように設計されています。また、SaaS (Software-as-a-Service) ソリューションとして提供されるため、追加のエンドポイントエージェントは不要で、その役割は単純に、CrowdStrike のイベントデータを取り込み、高度な分析を実行することです。ArcSight Intelligence for CrowdStrike は SaaS ベースのアプローチであるため、所有コストを抑え、保守と管理の負担を軽減することができます。スタッフの増員は必要なく、サブスクリプションベースで運用されるため、設備投資 (CapEx) への影響もありません。この教師なし機械学習ソリューションは、すべての従業員、マシン、認証ソースにとって「通常」がどのようなものかを継続して学習するため、時間の経過とともに最適化されていきます。ArcSight Intelligence

概要

業界

金融

所在地

多国籍

課題

多忙を極めるセキュリティチームの負担を増やすことなく、内部脅威を検出し、すでに強固なセキュリティ体制をさらに強化

製品とサービス

ArcSight Intelligence for CrowdStrike

成功ポイント

- POC により明らかになった重大な内部脅威
- 3 か月で完全に達成できた ROI
- 高度な分析による効率性の向上
- 保守の必要がない SaaS 型のアプローチ
- 包括的な既存のセキュリティインフラストラクチャに統合された内部脅威検出

「当社のセキュリティ体制は改善され、利便性の高い ArcSight Intelligence for CrowdStrike の SaaS モデルのおかげで、セキュリティチームや管理スタッフに負担をかけることなく改善が実現したのです」

セキュリティマネージャー
大手金融サービス企業

お問い合わせ
www.CyberRes.com

for CrowdStrike にはオプションの脅威ハンティングサービスがありますが、このサービスには、ArcSight Intelligence for CrowdStrike を使用して組織内に潜む検知しにくい脅威を検知してきた実績があります。

同社は、ArcSight Intelligence for CrowdStrike が自社に適したソリューションであるかどうかを検証するために、概念実証 (POC) を実施することにしました。POC は、十分な知識を備えるスタッフチームの参加のもと、45 日間実施されました。この間、ArcSight Intelligence for CrowdStrike は 2,400 万件のイベントを処理し、9 万件以上の通常の振る舞いからの外れを特定しました。ArcSight Intelligence for CrowdStrike は、これらの外れから、脅威ハンターが悪意のある活動の対象にする可能性が高い脅威リードを数件特定しました。

「残念ながら、ユーザーが機密情報を USB デバイスにコピーしていることが判明しました」と、セキュリティマネージャーは言います。「私たちは、多数の疑わしいアプリケーションを確認しただけでなく、ログイン試行の失敗、大量のファイル作成、異常な件数のプロセスも確認しました。このことから、特定の財務アドバイザーアカウントが内部偵察活動を行っていた可能性があると考えました。これらの調査結果により、必要に応じて懲戒処分をより適切に管理できるよう人事プロセスをきめ細かく調整することができました」

この組織では「レッドチーム」(企業のセキュリティ体制をテストするために潜在的な攻撃を擬似的に仕掛けるチーム) を採用しており、Log4Shell 攻撃のシミュレーション、パスザハッシュ攻撃、DLL インジェクション攻撃などのアクティビティを ArcSight Intelligence for CrowdStrike で検出できることが証明されました。

3 か月で完全な ROI を達成し、風評被害のリスクを軽減

ArcSight Intelligence for CrowdStrike と CyberRes 脅威ハンティングサービスを組み合わせることで、組織のセキュリティ体制にもたらす価値を確信した COO は、経営幹部向けのビジネスケースの定義に着手しました。Micro Focus CyberRes のチームは、セキュリティ侵害が発生した場合の風評被害を見積もるのではなく、手作業を自動化された高度な分析ソリューションに置き換えることで、どのような運用効率を達成できるかを判断する計算ツールを作成しました。これは、内部脅威を検出するプロセスがより効果的になるという明らかな利点ではなく、財務にのみ焦点を当てたツールです。その結果、ArcSight Intelligence for CrowdStrike を導入してからわずか 3 か月で投資収益率 (ROI) を完全に達成できることが明確に示されました。

セキュリティマネージャーは次のように結論付けています。「CrowdStrike と MSSP のインフラストラクチャに ArcSight Intelligence for CrowdStrike と脅威ハンティングサービスを追加することで、機密性の高い顧客データを保護し、風評被害のリスクを大幅に軽減することができました。当社のセキュリティ体制は改善され、利便性の高い ArcSight Intelligence for CrowdStrike の SaaS モデルのおかげで、セキュリティチームや管理スタッフに負担をかけることなく改善が実現したのです」

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

opentext™ | Cybersecurity

OpenText Cybersecurity では、あらゆる規模の企業とパートナー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ます。予防から検知、復旧対応、調査、コンプライアンスまで、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介した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。