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インサイトに基づき、ArcSight Intelligence for CrowdStrike を導入し、内部ユーザーによる脅威に対抗。

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、この組織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。この組織は、外部からの脅威を防止するために、大手 MSSP と CrowdStrike を採用した高度なセキュリティ体制を備えていたものの、内部ユーザーによる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だと認識していました。この課題について、お客様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、手作業で検査しようとしたのでは、難しいうえにコストも時間もかかります。当社では、内部ユーザーによる脅威の可能性がないかを確認するため、フルタイムのスタッフに手作業で電子メールをチェックしてもらっています。これは明らかに、拡張性のあるプロセスとは言えません。また、人の手に頼っているという問題もあり、人というのはミスを犯しやすいものです。規制の厳しい業界では、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、特に内部ユーザーによる脅威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、評判に傷がつく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、このお客様は Cybersecurity が提供する ArcSight Intelligence by OpenText™ for CrowdStrike にたどり着きました。この製品は、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。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。また、SaaS ベースのアプローチを採用しているため、所有コストを削減し、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。このソリューションは教師なし機械学習の機能を備えており、それぞれの従業員、マシン、認証ソースにとって「通常」とはどのようなものかを常に学習するため、時間の経過とともに最適化されます。ArcSight Intelligence for CrowdStrike にはオプションの脅威ハンティングサービス

概要

業種

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、内部ユーザーによる脅威を検知して、すでに強固なセキュリティ体制をさらに強化する

製品とサービス

ArcSight Intelligence for CrowdStrike

成功ポイント

- 重大な内部ユーザーによる脅威が POC で明確化
- 3 か月で ROI を完全に達成
- 高度な分析による効率の向上
- 保守の必要のない SaaS 型のデリバリー
- 内部ユーザーによる脅威を検知する機能を既存の包括的なセキュリティインフラストラクチャに統合

「当社のセキュリティ体制を改善することができました。この改善は、利便性の高い ArcSight Intelligence for CrowdStrike の SaaS モデルのおかげで、しかも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実現できました」

セキュリティマネージャー
大手金融サービス企業

お問い合わせ
www.opentext.com

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。

この組織は、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テストするため、提案検証 (POC) を実施することにしました。POC は、十分な知識を備えた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、通常の振る舞いからの逸脱を 9 万件以上識別しました。ArcSight Intelligence for CrowdStrike は、これらの逸脱を手掛かりに、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、何人かの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述べています。「私たちは、多数の疑わしいアプリケーションだけでなく、ログイン試行の失敗、大量のファイル作成、膨大な数のプロセスも特定しました。このことから、特定の財務アドバイザーアカウントで内部偵察活動が行われ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) を用いる手法を採用し、シミュレーションによる Log4Shell 攻撃、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も ArcSight Intelligence for CrowdStrike が検出できることをセキュリティチームが明らかにしました。

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 Cybersecurity 脅威ハンティングサービスの組み合わせが組織のセキュリティ体制に価値をもたらすことを確信した 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。OpenText Cybersecurity のチームは、セキュリティ侵害が発生した場合の評判への悪影響に伴うコスト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、どれほどの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、内部ユーザーによる脅威を検出するプロセスの効果を大幅に向上させるという明確なメリットは脇に置いておき、財務的な要素にのみ焦点を当てたツールです。このツールにより、ArcSight Intelligence for CrowdStrike の購入後わずか 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、評判に傷がつく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を改善することができました。この改善は、利便性の高い ArcSight Intelligence for CrowdStrike の SaaS モデルのおかげで、しかも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実現できました」

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。