opentext™ | Cybersecurity

お客様事例

大手オンライン小売業者

ArcSight Intelligence と CrowdStrike の連携により、隠れた脅威を明らかにし、手口が極めて巧妙な脅威と内部ユーザーによる脅威を検出できる方法を確立して侵害を防止できます。

セキュリティに「万能のソリューション」は存在しない

この国際的に有名な会社は、オンラインビジネスで急速な成長を遂げており、そのプラットフォームのアクティブユーザーは毎月数億人に上ります。このように大規模なユーザー層を抱えていると、多数の社内スタッフを必要とするため、偶発的または悪意のある内部ユーザーの脅威のリスクが高まります。また、サイバー犯罪者にとっても格好の標的になります。この組織の最高情報セキュリティ責任者 (CISO) は、人工知能 (AI) と機械学習 (ML) が会社とそのユーザーのデータを安全に保つための鍵になり得ると認識しており、次のように述べています。「データ分析は当社のビジネスにおいて非常に重要であるため、大規模な AI チームを組んでいます。しかし、このチームには、AI ベースのセキュリティモデルの構築、テスト、改良、導入ではなく、コアビジネスに専念してもらう必要があります。そのため、当社が活用できる専用のソリューションを保有しているパートナーを見つけることが、より理にかなっていたのです」

「ArcSight Intelligence は当社のデータやユーザーと連携しているため、Micro Focus (現在は OpenText の傘下) は当社の企業計画とそれに関連する戦略的なイニシアチブを知る唯一のサービスプロバイダーとして、振る舞いの監視およびその評価方法を調整できます。このレベルの信頼と自信は稀有なものですが、当然の結果でもあります」

最高セキュリティ情報責任者
大手オンライン小売業者

クラウドの価値をすでに確信していたこのチームは、セキュリティオペレーションセンター (SOC) をクラウドネイティブのマネージドセキュリティサービスプロバイダー (MSSP) にアウトソーシングすることにしました。これにより、エージェントのインフラストラクチャが軽量化され、Mac と Linux の両方をカバーできるようになったため、組織のすべての主要プラットフォームに対応できました。ほとんどのアラートは SecureWorks で管理されますが、要約された汎用的なアラートが例外としてチームに提供されます。組織はこれを補完するために、CrowdStrike Falcon を導入しました。CrowdStrike Falcon は、攻撃の識別、把握、対応に必要なイベントデータを収集し、エンドポイントのリアルタイムおよび過去のセキュリティイベントを可視化するように設計されています。「これにより、全体的なセキュリティは十分なレベルに達していますが、ユーザー側から見ると、まだ防御が甘いと感じていました」と CISO は述べ、次のように続けています。「内部ユーザーによる脅威や外部からの標的型攻撃は、検出が困難なことでよく知られています。ユーザーが特権アクセスを使用できるようにな

概要

業種

小売

所在地

グローバル

課題

ユーザーとワークステーションに焦点を当てた戦略により、既存のセキュリティ対策を補完し、検出するのが難しいことで知られている内部ユーザーによる脅威や標的型の外部攻撃に対抗

製品とサービス

ArcSight Intelligence

成功ポイント

- CrowdStrike と ArcSight Intelligence の組み合わせで非常に高い効果を発揮
- レッドチームによる攻撃をすべて検出
- PII の流出を防止し、GDPR の罰則適用を回避
- データ保護の強化による GDPR コンプライアンスの向上
- ゼロトラスト戦略を確立

「ArcSight Intelligence は、レッドチームによる攻撃を一貫して検知できる唯一のサービスです。たとえば、重要なアプリケーションすべてに VPN 接続が必要であることを確認するなど、ゼロトラスト戦略を確立する上で重要な役割を果たしました」

最高セキュリティ情報責任者
大手オンライン小売業者

お問い合わせ
www.opentext.com

れば、不正行為、業務妨害、知的財産の詐取を行うことが可能になります。ArcSight Intelligence を紹介されたときに、このツールがまさに当社が目指しているものだと気付きました」

レッドチームによる攻撃を ArcSight Intelligence で検出

CrowdStrike と ArcSight Intelligence by OpenText を組み合わせ、教師なし機械学習を活用して、すべてのユーザーやその他のエンティティの通常時の独自の振る舞いを測定することで、内部ユーザーによる脅威や標的型攻撃を特定します。これにより、独自のデジタルフットプリントが作成され、通常とは異なる振る舞いや不審な振る舞いを簡単に検出できるようになります。ArcSight Intelligence は、各ワークステーションで稼動している通常とは異なるプロセス、通常とは異なるログイン頻度、作業日時、通常とは異なるマシンからのアクセスなどのユーザー情報に新たに注目することで、脅威ハンターがいつもなら見逃してしまう脅威も検出することができます。振る舞いを分析することで、偶発的な問題と本物の脅威を振り分けられるようになるため、セキュリティチームは本当に重要な調査にのみリソースを集中させることができます。

レッドチームによる攻撃は、社内チームまたは外部のテストチームに委託して行われ、組織のセキュリティプログラムの有効性を評価するために、自社の組織に対して擬似的にサイバー攻撃を仕掛けました。CISO は、ArcSight Intelligence がレッドチームによる攻撃を検出できたことに満足しています。「ArcSight Intelligence は、レッドチームによる攻撃を安定して検出できる唯一のサービスです。たとえば、重要なアプリケーションすべてに VPN 接続が必要であることを確認するなど、ゼロトラスト戦略を確立する上で重要な役割を果たしました」

信頼できるパートナーシップによる GDPR コンプライアンスの向上

新型コロナウイルスの感染拡大時に、この組織は、臨時雇用者の使用を増やすなど、従業員の構成を変えざるを得ない状況に陥りました。このことは、セキュリティチームにとって特に慎重に対処する必要のある問題となります。セキュリティチームは生産性、柔軟性、セキュリティの間でバランスを取らなければならないからです。セキュリティチームは人事部門と連携し、ArcSight Intelligence を使用して、ユーザーアクティビティの監視を調整して、要注意の従業員に注意を向けるようにしました。その結果、大規模なデータ流出事故は発生しなくなりました。

データ流出には GDPR の高額の罰金が課される可能性があるため、データ流出の脅威は、内部ユーザーによる脅威に関連するユースケースの中でも最も一般的なものの 1 つです。ArcSight Intelligence は、重要なデータ移動の異常を特定し、侵害に至る前にこれらの脅威に焦点を当てます。ArcSight Intelligence の機能を強化するために、この CISO は OpenText™ の脅威ハンティングチームを活用しています。「ArcSight Intelligence の脅威ハンティングチームは、当社のデータ、ユーザーの振る舞い、それがセキュリティにどう関係しているのかを本当によく理解しています。このチームに特定の一連の振る舞いがシナリオに適しているかどうかを判断してもらっています。ArcSight Intelligence は当社のデータやユーザーと連携しているため、Micro Focus (現在は OpenText の傘下) は当社の企業計画とそれに関連する戦略的なイニシアチブを知る唯一のサービスプロバイダーとして、振る舞いの監視と評価の方法を調整できます。このレベルの信頼と自信は稀有なものですが、当然の結果でもあります」

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。

768-JA0034-003 | O | 12/23