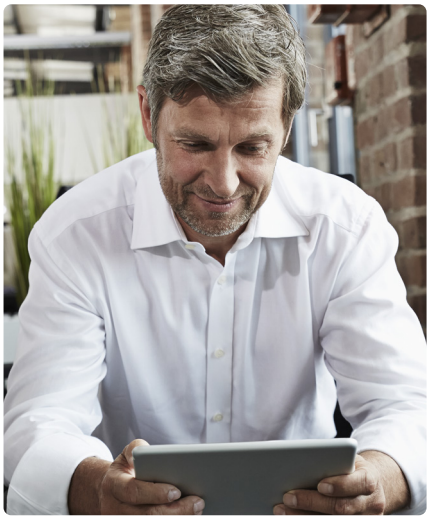
大手オンライン小売企業

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脅威の検知を確立して侵害を防止します。



セキュリティに「万能」は存在しない

この国際的に有名な企業は、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では月間数億人のアクティブユーザーがいます。このように大規模なユーザー数を抱えていると、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となります。同社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とって非常に重要であるため、大規模な AI チームを編成しています。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、当社にとってより理にかなっていたのです」

「ArcSight Intelligence が当社のデータやユーザーと連携しているため、Micro Focus は当社の企業計画および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信用はめったに実現しませんが、Micro Focus なら当然勝ち得るものです」

最高セキュリティ情報責任者
大手オンライン小売企業

クラウドの価値をすでに確信していたチームは、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な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、組織の主要プラットフォームを網羅できるようになりました。ほとんどのアラートは Secure-Works で管理されますが、要約された汎用的なアラートが例外的にチームに提供されます。組織はこれを補完するために、Crowd-Strike Falcon を導入しました。CrowdStrike Falcon は、攻撃の特定、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。「内部脅威や外部からの標的型攻撃は、検知が困難なことでよく知られて

概要

業界

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で、既存のセキュリティ対策を補完し、検知が難しいことで知られている内部脅威や標的型の外部攻撃に対抗

製品とサービス

Micro Focus 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
- レッドチーム攻撃をすべて検知
- 個人情報の流出を防止し、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
- ゼロトラスト戦略の確立

「ArcSight Intelligence は、レッドチーム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 接続を必須にするなど、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企業

お問い合わせ先：**CyberRes.com**
ソーシャルメディアはこちら

います。内部ユーザーは特権アクセスを利用して、不正行為、業務妨害、知的財産の窃取を行うことができます。Micro Focus ArcSight Intelligence を紹介されたときに、このツールは当社が目指す目標に最適だと気付きました」

レッドチーム攻撃を ArcSight Intelligence で検知

CrowdStrike と ArcSight Intelligence 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が通常状態の振る舞いを分析することで、内部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ような脅威も検知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のトリアージが可能になるため、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。

レッドチーム攻撃は、社内チームまたは外部のテストチームによって行われ、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、自組織に対して擬似的にサイバー攻撃をシミュレートするものです。CISO は、ArcSight Intelligence がレッドチーム攻撃を検知できたことに満足しています。「ArcSight Intelligence は、レッドチーム攻撃を安定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 接続を必須にするなど、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、同社は、臨時雇用者を増やすなど、従業員の構成を変更することを余儀なくされました。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した。なぜなら、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を回避することができました。

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、内部脅威に関連する最も一般的なユースケースの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 Micro Focus 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、およびそれら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の判断をしてもらっています。ArcSight Intelligence が当社のデータやユーザーと連携しているため、Micro Focus は当社の企業計画および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信用はめったに実現しませんが、Micro Focus なら当然勝ち得るものです」

CyberRes
A Micro Focus Line of Business