ArcSight Intelligence for CrowdStrike による未知の脅威の検出

エンドポイントデータと UEBA により隠れた脅威を迅速に発見

CrowdStrike と ArcSight Intelligence の概要：

検出：

CrowdStrike の豊富なエンドポイントデータと高度な行動分析を組み合わせ、従来は検出が難しかった脅威を発見します。

検知：

すべてのエンティティに特有の普段の行動を学習し、普段と大きく違う行動や不審な行動を検出することで、内部ユーザーによる脅威や標的型攻撃を特定します。

対応：

数十億件のエンドポイントイベントから、優先度が付けられた脅威のリードの一覧が抽出されます。アラート対応の労力が軽減されるため、重要な脅威に集中できます。

はじめに

ArcSight Intelligence の User and Entity Behavior Analytics (UEBA) と CrowdStrike Falcon の豊富なセンサーデータを組み合わせることで、組織内部の隠れた脅威を可視化できます。さらに、とても簡単に始められます。CrowdStrike Store にログインして、ArcSight Intelligence アプリケーションをクリックします。[Try it free(無料トライアル)] をクリックすると、自動的に ArcSight Intelligence が Falcon センサーデータにアクセスできるようになります。ソフトウェアの導入やハードウェアの管理は必要ありません。すべてクラウドで行われます。30 日間分のデータを収集すると、ArcSight Intelligence の教師なし機械学習エンジンにより、CrowdStrike データ内の異常なアクティビティを検出するために必要なものがすべて揃います。これで、ArcSight Intelligence の最新のスレットハンティングユーザーインターフェイスにアクセスできるようになります。リスクの高い異常な行動と、組織内の特にリスクが高いエンティティを優先度付けしたリストが分かりやすく表示されます。

ArcSight Intelligence のインサイトをモニターする時間やスタッフが足りないかもしれない、というご心配はいりません。ArcSight Intelligence が追加オプションとして提供するスレットハンティングサービスでは、毎日、毎週もしくは隔週に一度の頻度でセキュリティの専門家チームがスレットハンティングを実施します。さらに、拡張が可能な ArcSight Intelligence の API により、既存の「メインコンソール」や、チケットシステム、SOAR プラットフォーム向けのイベント通知をオーケストレーションできます。

課題

内部ユーザーによる脅威や外部からの標的型攻撃などの脅威は、検知が困難なことでよく知られています。このような「未知」の脅威は複雑な方法で検出を回避し、発見の手掛かりとなる固定のシグネチャや既知の攻撃のパターンを持たないため、検出しにくいのです。さらに、特権アクセスを使用して、発見されないまま意図的にまたは偶然に詐欺行為、妨害行為、知的財産の窃取を行っているケースもよくあります。

ソリューション

Micro Focus ArcSight Intelligence UEBA の行動分析により、セキュリティチームは、CrowdStrike Falcon の詳細で正確なエンドポイントデータに基づいて企業内に潜伏している攻撃者または脅威を検出できます。ArcSight Intelligence は、ユーザーについての情報 (異常なログイン頻度、作業の日付や時刻、通常と異なる機器など) を利用して価値あるコンテキストを付加できるため、他の方法では発見が難しい脅威の検出に役立ちます。正しいユーザーのコンテキストがあるため、異常なログインパターン、通常と異なる、または突然のファイルやシステムのアクティビティ、ユーザーの偽装、内部スパイ、ローアンドスロー攻撃を検出することができます。特定された脅威のリードは、調査のために自社のセキュリティチームまたは CrowdStrike OverWatch サービスに渡すことができます。

お問い合わせ先：**CyberRes.com**
この記事はいかがでしたか？
シェアはこちら

ユースケース

- **内部ユーザーによる脅威の発見：**ArcSight Intelligence UEBA は、CrowdStrike の豊富なエンドポイントデータから、企業内のすべてのユーザーまたはエンティティの「ユニークノーマル」の行動を学習し、異常や不審な点がある新しい行動を特定することで、悪意のある内部ユーザーや過失行為をしたユーザーを発見できます。
- **標的型攻撃の発見：**外部からの攻撃が内部脅威の特徴を示すことがよくあります。たとえば、攻撃者が有効な資格情報を使ってシステムに侵入し、価値の高いデータを盗むなどです。ArcSight Intelligence は、CrowdStrike のエンドポイントデータの中から、ネットワークやシステムのアクセス権を取得した攻撃者の手掛かりを探すことができます。

主な機能

- **高度な分析による異常検出：**ArcSight Intelligence では、教師なし機械学習を活用して、ログファイルから利用可能なエンティティ (ユーザー、マシン、IP アドレス、サーバー、プリンターなど) を抽出し、関連するイベントを評価して、想定される動作を判断します。新しいイベントを、過去にみられた動作や、ユーザーまたはエンティティのピア (通常行動が似ている仲間) による動作と比較して評価することで、潜在的リスクを評価します。
- **優先度が設定されたリードに基づく集中的な調査：**ArcSight Intelligence UEBA は、教師なし機械学習と数学的確率に基づいて、特に疑いの大きいエンティティを示すリスクスコアを計算します。これにより、ArcSight Intelligence は数十億件のイベントから優先度が付けられた少数の脅威のリードを抽出します。アラート対応の労力が軽減されるため、重要な脅威の調査に集中できます。

お客様の声

ある接客業の大手企業では、ArcSight Intelligence により CrowdStrike の豊富なエンドポイントデータ (プロセス、ユーザー、マシンの行動) を活用して、国家レベルの高度な実力を持ったレッドチームによる攻撃を検知しました。このお客様は、行動分析の結果から攻撃のライフサイクル全体を発見し、攻撃に対処するための正しいコンテキストを企業のセキュリティチームに提供することに成功しました。次のような攻撃の特徴が特定されました。

- セキュリティ侵害を受けたアカウント
- リモートの攻撃
- OWA プロファイリング
- パスワードの推測
- ラテラルムーブメント（侵入後の攻撃）
- IP アドレスと攻撃ツール

Micro Focus ArcSight Intelligence について

Micro Focus ArcSight Intelligence UEBA は、検出が難しい内部ユーザーによる脅威や標的型攻撃を発見、対処するための新しい方法をセキュリティチームに提供します。ルールやしきい値は使用しません。ArcSight Intelligence は、教師なし機械学習によりシステムとユーザーに固有のデジタルフットプリントを分析します。ArcSight Intelligence は、数十億件のイベントから、優先度が付けられた高品質のセキュリティリードのリストを抽出します。これにより、セキュリティオペレーションセンター (SOC) は集中して迅速に業務を行えます。数ヶ月を要していたものがわずか数分で完了できます。詳しくはこちら：**www.microfocus.com/integrations-ArcSight Intelligence-crowdstrike**.

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

CyberRes
A Micro Focus Line of Business