ハンドアウト

セキュリティ

ATAR、ArcSight、Interset UEBA による統合防御

SOC における運用と検知の生産性を上げるには、SIEM、ふるまい検知、SOAR の各機能を統合し、多層分析を活用する必要があります。

ATAR、ArcSight、Interset UEBA による統合防御の概要：

- **主な利点：**
  - ATAR による SOC の自動化とオーケストレーション機能を通じてセキュリティオペレーションを統合。
  - セキュリティ体制におけるインシデントの見落としや未解決のセキュリティギャップを解消。
  - 分断されたシステム上の情報を統合して攻撃者に対応。
- **製品：**
  - ATAR
  - Micro Focus ArcSight
  - Micro Focus Interset

エンドツーエンドのセキュリティオペレーションの実装 / 導入

企業は現在、攻撃者に後れを取ることなく先んじて対応しようと苦慮しています。問題は明確です。しかし、その解決策は、多くの企業にとっては手の届かないものとなっています。攻撃の複雑化とセキュリティオペレーションセンター (SOC) の人材不足により、既存の解決策はすぐに通用しなくなります。必要なテクノロジースタックを入手しても、それぞれのテクノロジーが連動していなければ、全体像を把握して行動を起こすことはできません。

Micro Focus ArcSight と Interset User and Entity Behavioral Analytics (UEBA) に ATAR を統合することにより、脅威に迅速に対応するための環境を構築し、卓越した機能を全社レベルで活用できます。

ArcSight の強力な相関分析エンジンは、ルールと脅威インテリジェンスを用いて企業全体の脅威をリアルタイムで特定し、アラートを送信します。ArcSight から受信したアラートに基づき、ATAR で脅威の評価、優先度設定、調査を行い、適切なアクションを実行して攻撃を除去できます。Interset UEBA で検出したユーザーふるまい／アノマリ検知データを ATAR に送信することにより、インシデントの検出と調査を強化できます。ATAR による ArcSight のリアルタイム相関分析と Interset の機械学習を活用したアノマリ検知により、人間の力だけでは不可能なスピードで攻撃に対応できます。

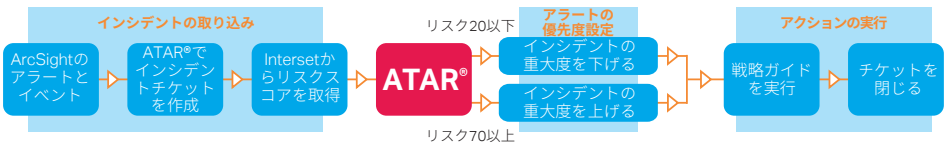
これらのソリューションは容易に統合できるため、追加投資を一切行うことなく、各ソリューションの利点を享受できます。

使用例 1：SIEM アラート数の減少

課題：毎日、数百件ものセキュリティアラートを受信するため、SOC チームは大量のアラートを評価して優先度を設定しなければならない。

ソリューション：Micro Focus ArcSight と Interset UEBA に ATAR を統合することにより、アラートの優先度を設定して、調査を行い、インシデントが修正されます。

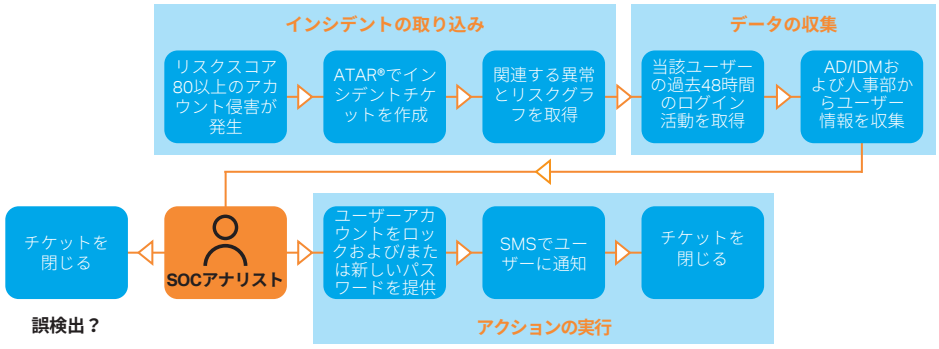
ArcSight によるアラートの優先度設定



使用例 2：アカウント侵害

課題：アカウント侵害の検出、調査、対応を迅速に行うことが極めて重要である。

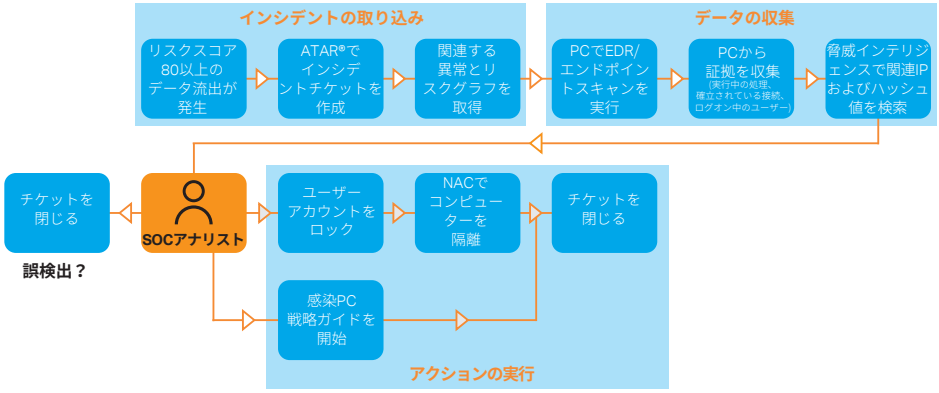
ソリューション：ATAR では、アノマリ検知の結果を Interset から取り込んで、インシデント管理サービスデスクでインシデントチケットを作成できます。幅広い統合ポートフォリオ、オーケストレーション、自動化機能を通じて、インシデントを調査および確認し、必要なアクションを実行してアカウント侵害を防止できます。



使用例 3：情報漏洩

課題：正常なトラフィックから異常なデータフローを区別して検知することが困難である。

ソリューション：Interset は、教師なし機械学習を用いて、データ流出に発展する可能性のある異常な振る舞いを検出して ATAR にアラートを送信します。アラートを受信した ATAR は、疑わしい PC に接続して証拠を収集し、ユーザーアカウントをロックして PC をネットワークから自動的に隔離します。



ATAR Labs について

ATAR Labs は、大量のサイバー攻撃に迅速に対応するための SOAR プラットフォーム ATAR を提供しています。人間の専門家がいなくても、ATAR の防御ロボットにより、あらかじめプログラムされた攻撃対応を自動で実行し、セキュリティオペレーションセンターにおける反復的なオペレーションを頻繁に実行できます。これにより、アラーム対応の 30 ～ 40% をプラットフォームに任せることができます。また、ATAR のインシデント調査機能と対応機能により、オペレーションセンターの専門家は 15 ～ 20 倍のスピードでインシデントを分析および解決できます。ATAR Labs の詳細については、**www.atarlabs.io** をご覧ください。

お問い合わせ先：
www.microfocus.com

Micro Focus について

Micro Focus は、組織の運営とビジネスの変革をサポートします。お客様中心のイノベーションを目標に掲げ、ソフトウェアにより、企業の構築、運用、セキュリティ対策、分析に欠かせないツールを提供します。これらのツールは、既存のテクノロジーと新しいテクノロジーのギャップを解消するように設計されており、デジタル変革を目指すお客様のイノベーションを、迅速かつ低リスクで実現します。Micro Focus の詳細については、**www.microfocus.com** をご覧ください。

詳細情報はこちら：
www.microfocus.com/secops

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