opentext™ | Cybersecurity

atarlabs

パートナーハンドアウト

ATAR、ArcSight、Interset UEBA による統合防御

現代の SOC において運用効率とセキュリティ効率を高めるためには、SIEM、ユーザー / エンティティ振る舞い分析 (UEBA)、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

主なメリット

- ATAR の自動化機能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逃しや未解決のセキュリティギャップを解消。
- 各システムの知識を集結させて攻撃者に対応。

製品

- ATAR
- ArcSight
- 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。

ATAR に ArcSight と Interset のユーザー / エンティティ振る舞い分析 (UEBA) を統合することで、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るようになります。

ArcSight の強力な相関エンジンは、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の振る舞いと異常データを 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 のリアルタイムのイベント相関付けと Interset の機械学習を活用した異常検出により、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。

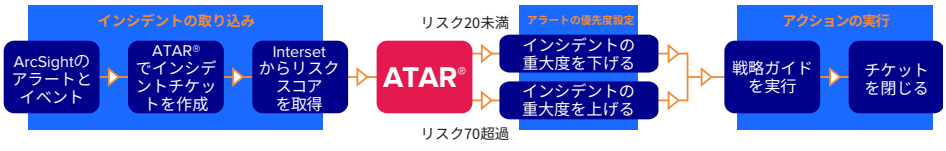
これらのソリューションは容易に統合できるため、追加投資を一切行うことなく、各ソリューションの利点を享受できます。

ユースケース 1：SIEM アラート数の削減

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：ATAR に ArcSight と Interset UEBA を統合することにより、インシデントの修正に加えて、アラートの優先度を設定して調査を行うことができるようになります。

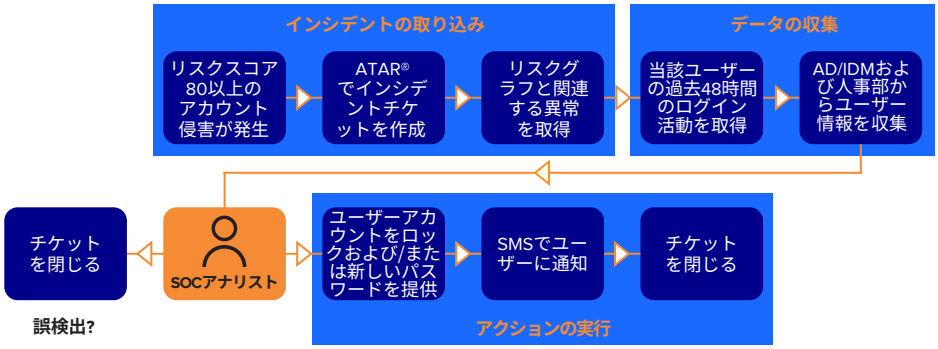
ArcSight によるアラートの優先度設定



ユースケース 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。

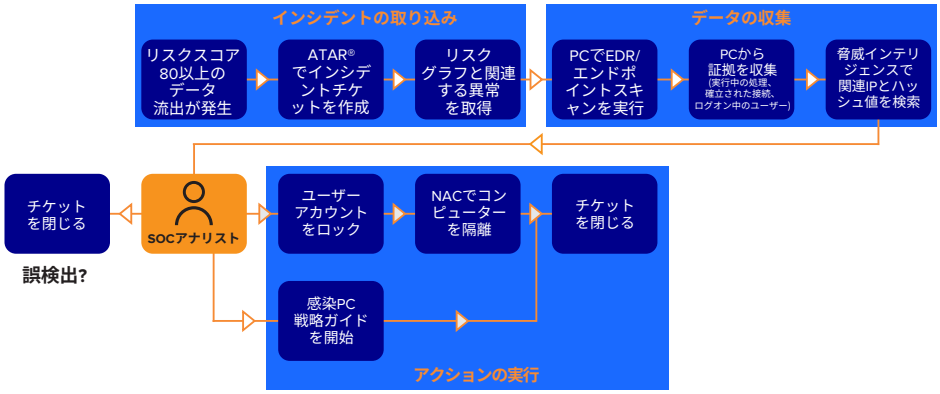
ソリューション：ATAR では、異常に関するデータを Interset から取り込み、インシデント管理サービスデスクでインシデントチケットを作成することができます。幅広い統合ポートフォリオ、オーケストレーション、自動化機能を通じて、インシデントを調査および確認し、必要なアクションを実行してアカウント侵害を防止できます。



ユースケース 3：データ流出

課題：ネットワーク境界を超える正常なトラフィックから異常なデータフローを検知して区別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知し、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 の防御ロボットが、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も頻繁に実行します。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通常の 15 ～ 20 倍のスピードでインシデントを分析して解決できるようになります。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

www.opentext.com

opentext™ | Cybersecurity | atarlabs

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。