ArcSight を選ぶ 5 つの理由

このドキュメントでは、セキュリティ運用ソリューションとして ArcSight 製品ラインを選ぶ 5 つの理由について説明します。ArcSight プラットフォームは、リアルタイムの相関付けや活発なコミュニティへの参加など、リアルタイムのセキュリティ情報の監視、潜在的な脅威の特定、被害の最少化に必要な機能を備えています。

1. **業界トップクラスの相関エンジン。**ArcSight Enterprise Security Manager (ESM) by OpenText™ の脅威をリアルタイムに検出して対応する機能により、脅威の発生を確認してすぐに阻止することができます。他の SIEM ソリューションとは異なり、ArcSight ESM は大規模な組織で発生するデータを処理できるように構築されているため、膨大な量の受信イベントログにほぼ即座に対応できます。ArcSight ESM は、あらゆるデータソースからの情報を解析し、お客様の組織において非常に高いレベルのエンタープライズセキュリティを実現します。カスタマイズ性が非常に高く、インスタントアラートをトリガーする企業独自のルールセットを作成することができます。シンプルな自動対応と複雑な自動対応の両方が可能で、オンデマンドまたは特定のアラートで対応をトリガーできます。また、主要な SOAR ソリューションやデジタルワークフローソリューション (ServiceNow や ATAR Labs など) と統合できます。

2. **脅威インテリジェンス。**ArcSight Interset by OpenText™ は、最新の脅威インテリジェンスを使用してお客様の組織の安全を守ります。ArcSight ESM は、MITRE ATT&CK および MISP CIRCL と自動的に統合されます。また、Anomali、Ixia、LookingGlass などのパートナー企業のソリューションと統合されるため、お客様の組織で最新のデータ保護機能を利用することができます。Micro Focus は、MITRE ATT&CK Framework を ArcSight ESM および Logger の各レポートとダッシュボードに組み込むことにより、セキュリティ対策全体を簡単に評価できるようにしました。お客様の組織を守るために ArcSight Interset がどのような連携を行っているかをご確認ください。

3. **UEBA の統合。**Interset for User Behavioural and Entity Analytics (UEBA) を組み込むことは、ArcSight Interset のセキュリティ機能を大幅に向上させるうえで非常に重要です。UEBA により、ユーザーのアクティビティに関する有用で実用的な情報を、導入後の 30 日間で入手できます。現在販売されているその他の UEBA 製品とは異なり、Interset の解析機能には教師なし機械学習と高度な数学モデルが採用されているため、損害が発生する前に、よりインテリジェントな情報を提供します。この広範なアプローチと直感的に使用できるインターフェイスにより、お客様の組織に大きな被害をもたらす脅威をより正確かつ効率的に検出、調査し、対応することができます。企業のユーザーが通常どのような行動をするかの情報を把握し、異常があれば即座に特定してアラートを発します。Interset がルールセットを作成するため、この処理にお客様が時間を使う必要はありません。UEBA により、日々発生する膨大な量のアラートから取捨選択して、今すぐ対応が必要な少数のアラートを優先することができます。

最新バージョンの ArcSight 製品ラインをお使いでしょうか？最新リリースにアップグレードすると以下の機能をご利用いただけます。

ArcSight ESM
- グローバル ID
- すぐに使えるコンテンツ
- ServiceNow との強力な統合
- MISP CIRCL 統合
- MITRE ATT&CK ダッシュボード

ArcSight Logger
- 機械学習パッケージ
- MITRE ATT&CK レポート
- デモビデオ
- GIS 検索

ArcSight Security Open Data Platform
- 新しい SmartConnector
- コンテナベースの導入
- 高度なクラウドコネクターのサポート

「私たちは、ArcSight Marketplace と Activate フレームワークにより、Micro Focus (現在は OpenText の傘下) SOC の技術者と ArcSight コミュニティが開発したセキュリティルールセット、ダッシュボード、レポートを活用しています。これにより、セキュリティ対策と応答時間を大幅に向上させることができました。」

Majeed Behzadi 氏
グループ情報セキュリティ管理および IT インフラストラクチャ設計部門責任者
Kuwait Finance House

お問い合わせ
www.CyberRes.com

4. **オープンで効率的な拡張性に優れたデータプラットフォーム。**ArcSight が提供する Security Open Data Platform (SODP) by OpenText™ は、セキュリティデータを収集、整理、拡充、配信します。すべてのデータソースからデータが収集されて Common Event Format (CEF) に集められるため、データを効率的に分析できます。ArcSight の SODP はパートナー企業のソリューションと統合できるため、お使いのセキュリティソリューションを活用して投資資本利益率 (ROI) を改善できるほか、セキュリティ対策の範囲を自由に拡大できます。ArcSight の SODP インフラストラクチャはオープンであり、現在お使いの機能を活用しながら、整理され一元化されたデータのメリットを得ることができます。

5. **コミュニティによる充実したサポート。**ArcSight には、数千人のユーザーが参加している ArcSight コミュニティがあり、非常に充実したサポートを受けることができます。疑問があれば、すでに誰かが回答した内容がコミュニティ内で見つかる可能性が十分にあります。もし見つからなかった場合でも、当社のサポートチームが早急に必要なサポートを行います。ArcSight Marketplace には、ArcSight で確認済みの多数のアプリや、コミュニティが作成したコンテンツパッケージが登録されています。意欲があれば、独自の ArcSight パッケージを作成して ArcSight Marketplace で販売することができます。

詳細情報はこちら：
www.microfocus.com/ja-jp/products/security-operations/overview

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。