Micro Focus 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 Micro Focus ArcSight を選ぶ 5 つの理由について解説します。ArcSight は、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分析エンジン。**ArcSight Enterprise Security Manager (ESM) 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、大規模な組織で発生するデータを処理するように構築されているため、受信した膨大な量のイベントログにほぼ瞬時に対応できます。ArcSight ESM は、あらゆるデータソースからもたらされる情報を解析し、お客様の組織に非常に高いレベルのエンタープライズセキュリティを提供します。カスタマイズ性に非常に優れており、アラートをトリガーする会社独自のルールセットを作成することができます。シンプルな自動応答と複雑な自動応答の両方に対応しており、オンデマンドまたは特定のアラートで応答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。**Micro Focus ArcSight 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ています。また、Anomali、Ixia、LookingGlass などの企業とパートナーとして提携することにより、最新のデータ保護機能をお客様の組織に提供します。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 Micro Focus ArcSight と Interset がどのように連携するかについて、**mitre.microfocus.com** でご紹介しています。

3. **UEBA の統合。**Interset for User Behavioural and Entity Analytics (UEBA) を組み込むことは、ArcSight のセキュリティ機能を大幅に向上す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重要で実用的な情報を、導入後の 30 日で得ることができます。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理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観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、対応できます。会社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、異常があれば迅速に特定してアラートを発行します。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を調べ、優先度を設定して、対応が必要なアラートを直ちに特定することができます。

最新バージョンの ArcSight 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使用できます。

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 参照**

SODP
- **新しい SmartConnector**
- **コンテナベースのデプロイ**
- **高度なクラウドコネクターのサポート**

「ArcSight MarketplaceとActivateフレームワークで、Micro Focus 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改善することができました。」

MAJEED BEHZADI氏
Executive Manager、Group Information Security Management、IT Infrastructure Design
Kuwait Finance House

お問い合わせ先：
www.microfocus.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。**Micro Focus ArcSight が提供する Security Open Data Platform (SODP) は、セキュリティデータを収集、整理、エンリッチ、送信します。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 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 のインフラストラクチャはオープンなため、現在お使いの機能を活用しながら、データを整理して一元化することのメリットが得られます。

5. **コミュニティによる充実したサポート。**Micro Focus 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、充実したサポートを受けることができます。分からないことがあったときは、すでにだれ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、Micro Focus のサポートチームが早期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。独自の ArcSight パッケージを作成して ArcSight Marketplace で販売することもできます。

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

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