MICRO FOCUS

データシート
セキュリティ

ArcSight Enterprise Security Manager

モジュール式のコンテンツ開発フレームワークとイベントトリアージに対応したリアルタイムの分散相関処理

数分の違いが成否を分ける状況で、Micro Focus® ArcSight Enterprise Security Managerを利用することで、大規模なサイバーセキュリティの脅威の検出、対処、およびトリアージに要する時間を大幅に短縮できます。先進的な分散相関処理エンジンを搭載したArcSight Enterprise Security Manager (ESM) を利用すると、セキュリティチームは社内および外部の脅威をすばやく検出して分析し、数時間または数日を要していた対応時間を数分まで短縮できます。また、シンプルなセキュリティオペレーションセンター (SOC) ワークフローとArcSight Marketplaceで提供される最新の脅威パッケージを利用することで、SOCは要員を増やすことなく、より多くの脅威に対処できるようになります。

製品概要

ArcSight ESMはスケーラブルで効率的なSIEMソリューション

ArcSight Enterprise Security Managerは、高度なデータエンリッチメント機能を備えた、リアルタイムの脅威検出、分析、ワークフロー、およびコンプライアンス管理を行う包括的なプラットフォームです。ArcSightはリアルタイムでサイバーセキュリティの脅威を検出し、アナリストに脅威の存在を示します。これにより、セキュリティ運用チームはセキュリティ侵害の兆候にすばやく対応することができます。脅威を自動的に識別して優先順位付けを行うことで、セキュリティ運用チームは通知される誤検出への対応に伴うコストと手間から解放されます。ESMを使用することで、SecOps組織は複数の環境をまとめて詳細に監視できるようになり、ワークフローを効率化してプロセスを合理化できます。優れた検出機能、リアルタイム相関、およびワークフローの自動化を通じて、SOCチームはインシデントを高い精度ですばやく解決できます。

Arcsightの強力なSmartConnectorとFlexConnectorテクノロジーを活用

ESMでは、Micro Focusの高度なイベント収集を利用して、500種類以上のデバイスからのデータのエンリッチ化と分析を行うことができます。ArcSightのADP SmartConnectorは、ネイティブWindowsイベント、API、ファイアウォールログ、Syslog、フラットファイル、Netflow、XML/JSON、および直接データベース接続の共通イベントフォーマット (CEF) をサポートしています。さらに、当社のFlexConnector開発フレームワークを使用すると、カスタムイベントパーサーを開発してESMに送付し、インデックス付けや、業界をリードする分散相関処理エンジンで使用できます。イベントソースを増やすことで、企業内の状況をさらに詳しく把握できるようになり、組織のセキュリティニーズに合わせてより複雑なユースケースを開発することも可能になります。

ArcSight Connectorは、カテゴライゼーションと正規化を行うことで、収集した元のログをSIEM製品内で使用するための汎用フォーマットに変換します。当社では共通イベントフォーマット (CEF) を使用しています。これは、セキュリティおよびネットワークテクノロジーの30種類のカテゴリを対象に、10年間に400以上のコネクターを作成してきたノウハウに基づいて、Micro Focusが開発した業界のデファクトスタンダードです。データのカテゴライゼーションと正規化を行うことで、調査や即座の対応が必要な状況をすばやく見つけ出し、緊急度の高いハイリスクな脅威に集中することができます。

リアルタイム、インテリジェント、強力、スケーラブル、カスタマイズ可能

- 最大100,000 EPSでの分散相関処理が可能な、業界で最もインテリジェントで強力な相関処理機能
- ArcSight Activate FrameworkおよびArcSight Marketplaceのコンテンツにアクセスして、最新のセキュリティ相関ルール、ダッシュボード、レポート、およびユースケースを利用可能
- モジュール式のパッケージにより、カスタムルール、ダッシュボード、その他のコンテンツをエクスポートし、システムまたはカスタマー間で共有
- 企業内のすべてのセキュリティイベントの管理、分析、およびレポート作成を集約することで、非効率なSOCの反復業務を解消
- MSP/MSSP対応により、分散セキュリティ環境に対応したマルチテナントの実装が可能
- サイバー脅威インテリジェンスのSTIXまたはCIF標準フィード経由での取り込みが可能

インテリジェントかつ動的なイベントリスクスコアリングと優先順位付け

ESM独自の優先順位計算式 (脅威レベル計算式ともいう) は、各イベントの重要度やネットワークに対する優先度を特定するための複数の評価基準で構成されています。この計算では、定義されたネットワーク/アセットモデル、オープンポート、および脆弱性データベース (X-Force、CVE、Bugtraqなど) と組み合わせたNessusやRetinaなどの製品からインポートした脆弱性スキャン結果など、数多くのデータポイントを利用します。たとえば、CVE-1999-0153を悪用することがわかっている攻撃があるとします。攻撃対象のシステムでその脆弱性が保護されておらず、攻撃対象ポートが開いている場合、システムはその攻撃が成功する可能性が大きいとみなして、高い優先度を付与します。

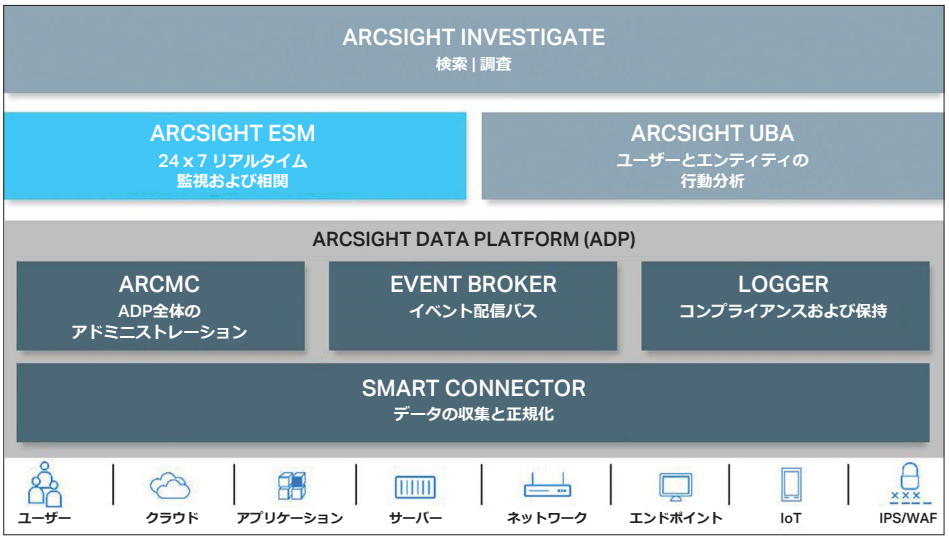

図1: ArcSightポートフォリオ

主なメリット

強力なリアルタイム相関処理

ArcSight ESMはイベントやアラートの相関処理を行い、環境内の優先度の高い脅威を見つけ出します。ESMの強力な相関処理エンジンでは、データを収集してイベントをリアルタイムで相関処理することで、プラットフォーム内のルールに違反する脅威を正確にエスカレーションできます。ESMでは、企業内の毎秒最大100,000件のイベントを相関処理できます。

カテゴライゼーションと正規化

カテゴライゼーションと正規化を行うことで、収集した元のログをSIEM製品内で使用するための汎用フォーマットに変換します。当社ではCEFを使用しています。これは、セキュリティおよびネットワークテクノロジーの30種類のカテゴリを対象に、10年間に300以上のコネクターを作成してきたノウハウに基づいて、Micro Focusが開発した業界のデファクトスタンダードです。データのカテゴライゼーションと正規化を行うことで、調査や即座の対応が必要な状況をすばやく見つけ出し、緊急度の高いハイリスクな脅威に集中することができます。

モジュール式の強力なコンテンツ開発セキュリティユースケースに対処するために作成されたカスタムコンテンツ (ルール、トレンド、ダッシュボード、レポート) は、簡単にパッケージ化して他のシステムに導入したり、他のビジネスユニットやArcSightコミュニティと共有したりできます。階層化されたESMアーキテクチャーでは、複数のESMで自動的にコンテンツシステムを同期するように設定できます。ArcSight Marketplaceおよ びActivate Frameworkのパッケージは、最新のセキュリティユースケース、ルール、およびサポート製品を反映して継続的に更新されます。このため、組織はアラートやトリアージに必要な脅威の情報を常に最新化し、SIEMソリューションをすばやく導入し、SIEMへの投資を短期間で回収できます。

ArcSight Data Platform (ADP) Event Brokerとの統合

スケーラビリティ、オープン性、高速処理といったビッグデータがもたらした課題に応えるため、ArcSight ESMはADP Event Brokerと完全に統合できます。

ADP Event Brokerは、最新のSOCに対応したオープンでスケーラブルなインテリジェントデータ取り込み/配信バスです。ESMは、ADPのEBオープンアーキテクチャーからイベント (パブリッシャーおよびコンシューマー) を送受信できます。これにより、Hadoop、データレイク、または社内の独自アプリケーションなどのサードパーティ製アプリケーションとのデータ共有が可能になります。このため、インテリジェントなSIEMであるArcSight ESMを企業内のすべてのセキュリティおよび分析ツールの中核機能として利用し、影響をすばやく修復し、セキュリティ上の脅威を前もって解消することができます。

ArcSight Investigateとの統合

ArcSight ESMはArcSight Investigateと 統 合することで、セキュリティ運用環境内で高速かつ使いやすい検索とデータ可視化を実現できます。ArcSight Investigateは、変化を続けるセキュリティチームのニーズに対応するため、最新の高度な分析プラットフォーム上に構築された次世代ハントおよび調査ソリューションです。ESMとArcSight Investigateを組み合わせて使用することで、SOCの担当者は組織内の未知のセキュリティ上の脅威をインテリジェントビューで検出して把握し、影響をすばやく修復し、セキュリティ上の脅威を前もって解消することができます。

ワークフローの自動化

ArcSight Enterprise Security Managerを利用すると、SOCチームはリアルタイムのトリアージチャネルと内蔵されたケース管理システムを通じて、検出されたアラートの効率的かつ効果的なトリアージを容易に実現できます。関心のあるイベント (EOI) をケースに添付して、下位レベルから上位レベルの応答者にエスカレーションできます。ケースを変更すると内部監査イベントが生成されるため、SLAやアナリスト応答時間のメトリックを詳細に追跡できます。これらの測定可能なメトリックを使用して、SOCチームは平均応答時間を短縮し、解決に適した人材にインシデントをエスカレーションできます。また、ArcSightは、サードパーティ製のチケット処理システムとも統合されます。

コンソール内またはルールアクションとしての自動応答

Action Connector (CounterAct) を使用すると、ArcSightとサードパーティ製デバイス間を統合できます。これにより、サードパーティ製デバイスをArcSightコンソールから制御できるようになります。ArcSight内からサードパーティ製デバイス上でコマンドを実行し、コマンドの出力をコンソールに返してアナリストが確認できます。リモートコマンドは、相関ルールエンジンでアクションとして実行したり、コネクターを右クリックして実行したりすることもできます。この機能を利用すると、モニター間のKVM接続や検出とアクションの切り替えが必要なくなり、コスト効率の高い運用を実現できます。ArcSightコンソールを離れずに変更やアクションを実行できることは、ユーザーにとって強力なソリューションになります。ESMがアクション、Logger検索、およびサードパーティアプリケーション/スクリプトの定義、管理、および起動を行うハブとして機能することで、ユーザーは各種アプリケーションのコマンドをコンソールでまとめて実行することができます。

マルチテナント

ArcSight ESMでは、複数の分散したビジネスユニットで1つのシンプルなSecOpsビューを利用できます。

イベントレベルで設定可能なマルチテナント機能とアクセス制御パーミッションを使用すると、企業はルールベースのしきい値と統一されたパーミッション役割、権限、および責任マトリックスを含む集中型の管理機能を使用できます。また、独自のルール、レポート、ダッシュボードをカスタマイズし、対象のシステム所有者とステークホルダーが利用できるようにすることができます。

主な特長

ESMのオプションパッケージ

高可用性 (HA)

複数のESMシステムによる最適化されたパフォーマンス環境を提供します。メインのシステムに通信や運用上の問題が発生した場合、自動的にフェイルオーバーできます。

レピュテーションセキュリティモニター (REPSM+) ― 脅威インテリジェンスフィード

クラウドベースの標準準拠の共有プラットフォームからの即時利用可能な脅威分析とレピュテーションインテリジェンスに基づいて、脅威に対応します。脅威データを自動的に取り込み、相関イベントで使用して、既知の不良イベントとの一致やセキュリティ侵害の兆候を探し出します。

コンプライアンスパッケージ―コンプライアンスの自動化とレポート作成

さまざまな規制準拠要件に容易に対応できます。また、クリティカルな問題を発見するコストと手間を軽減することで、リスクの回避、監査の準備、および生産性と運用効率の向上を行うことができます。

その他の機能

- **アクティブリスト** ― 数百万のエントリを保持できる動的なインメモリリストで、不審なトラフィックやエントリ動作を監視するウォッチリストとして使用できます。アクティブリストは、すべての相関ルールで使用できます。
- **レポートのスケジュール設定** ― レポートをスケジュール設定し、主要なステークホルダーに自動的に結果を提供します。
- **API** ― RESTベースのAPIを使用して、ESMからイベントまたはケースデータを取得します。
- **トレンド** ― 高速検索や長い期間またはイベント保持期間外でのレポート作成を行う際に、サイドテーブルで保存する関心のあるイベントを簡単に定義できます。
- **リモートコネクター設定** ― ArcSightコンソールで、リモートコネクターの設定を変更 (アグリゲーション、イベントフィルタリング、イベント時間調整など) できます。

「ArcSight ESMの高度な収集および相関処理機能により、日々生成される何千件ものイベントやログ記録を解明できます。このインテリジェントなシステムにより、重要なすべてのセキュリティインシデントをすばやく見つけて対処することができます。」

NetApp社、情報セキュリティマネージャー

お問い合わせ先
www.microfocus.com

- **カスタムイメージダッシュボード** — 地図や組織図などのカスタムグラフィック上にダッシュボードを重ねて表示します。
- **フォーマット保持暗号化 (FPE)** — Micro FocusのSecureDataテクノロジーを利用します。ArcSightはFPEを用いて、アナリストやArcSightユーザーに社会保障番号やクレジットカード番号などのセンシティブなデータを知られることがないような形で、相関処理機能を維持します。
- **データセキュリティ** — 否認防止およびデータの完全性を確保するため、不変のデータストレージによりデータ操作から保護します。

詳細情報
microfocus.com/arcsightesm

Micro Focus
英国本社
United Kingdom
+44 (0) 1635 565200

米国本社
Rockville, Maryland
+1 301 838 5000
+1 877 772 4450

www.microfocus.com

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