データシート

セキュリティ

ArcSight Logger

セキュリティインテリジェンスに関するマシンデータの収集、保存、分析機能を統合した Micro Focus ArcSight Logger は、企業の成長に合わせてサイバーセキュリティ、コンプライアンス、IT 運用部門のログ管理の要件に同時に対応できる、業界をリードするデータ収集ソリューションです。

製品概要

サイバーセキュリティの脅威の増加により、一元化されたマシンデータのログは急速に重要な情報源となりました。今日、セキュリティ分析による知見の獲得において、効率的なログ管理が重要な役割を果たしています。

ArcSight Logger は、組織全体のマシンデータのログを統合して保存し、それらのデータの迅速な検索とレポート処理を可能にすることで、規制準拠の負担を軽減し、セキュリティ担当者のフォレンジック調査をスピードアップできる包括的なログ管理ソリューションです。ArcSight Logger は、強力な階層アナリティクスによりセキュリティオペレーションの基盤となるという ArcSight の目標の実現において重要な役割を果たします。

Logger では、コスト効率の高い優れた圧縮比により、480 を超えるソースからデータログを収集し、それらのログを正規化されたクリーンなフォーマットで数年にわたって保存することができます。さらに、1 日に数百万 (数十億) 件のイベントを取り込んで保存できるだけでなく、セキュリティ担当者はそれらのデータを使用して効率的に異常を発見し、簡素化された検索とカスタマイズ可能なダッシュボードで迅速なフォレンジック調査を実行することができます。

Logger には、ノンストップのセキュリティコンプライアンスを可能にするコンテンツ、ダッシュボード、レポートが含まれており、PCI、SOX、HIPAA などの規制に対応できるコンテンツパッケージが用意されています。これにより、監査の負担が軽減するほか、関連する規制要件の遵守を証明するための時間も短縮されます。

要約すると、ArcSight Logger は、データの収集、保存、コンプライアンス、検索を簡素化するソリューションです。

主な利点

包括的なデータ収集

ArcSight Logger では、あらゆるソース (ログ、クリックストリーム、センサー、ストリーミングネットワークトラフィック、セキュリティデバイス、Web サーバー、カスタムアプリケーション、ソーシャルメディア、クラウドサービスなど) から毎日テラバイト単位のマシンデータを収集します。これにより、データの検索、監視、分析が可能になり、組織全体に関して重要なセキュリティインテリジェンスを得ることができます。

ArcSight Logger の概要：

- セキュリティ侵害を検出するために必要な大量の情報を幅広くスピーディに収集
- 数回クリックするだけで設定、アップグレード、メンテナンスが可能
- テラバイト規模のデータをコスト効率に優れた方法で保存および検索し、迅速な分散型ピア検索を実現

柔軟なデプロイメントアーキテクチャ

ArcSight Logger は、負荷分散されたコレクションを提供するクラスターとして構成できるため、プラットフォーム全体に対する検索クエリを使用することができます。Linux システム、VMware 仮想マシン (アプライアンスとして)、クラウド (AWS および Azure) にインストールできます。ArcSight Logger では、ローカルドライブまたは既存

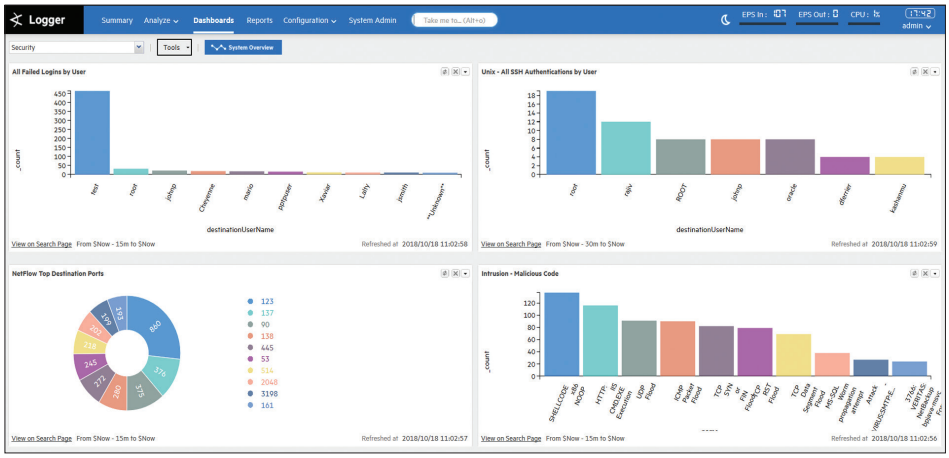

図 1. ArcSight Logger ダッシュボード

「ArcSight Logger のおかげで、PCI 要件の準拠に要する時間を短縮できました。ネットワークの異常を監視して、新たな脅威を完全に把握できるようになったのです。」

セキュリティ責任者
Fortune 500のファイナンシャルサービス企業

お問い合わせ先:
www.microfocus.com

の SAN 資産をメインのデータストアとして活用できます。ストレージがオンボードかオフボードかに関係なく、データを効率的に圧縮するため、ストレージとメンテナンスのコストが削減できます。

拡張可能なテキストベースのハイパフォーマンスフォーマットである Common Event Format (CEF) によりデータを容易に収集して集約できるため、ArcSight ESM、ArcSight Investigate、Interset UEBA などのエンタープライズ管理システムや、イベントのオーケストレーション、自動化、相関、優先度設定、セキュリティイベントの分析 (またはこれらすべて) を提供するサードパーティ製アプリケーションで分析できます。

安全性と信頼性の高いデータ収集

ArcSight Logger ソフトウェアは、暗号化された圧縮ログを提供することにより、傍受、改ざん、削除から (保存中および転送中の) データを保護します。Logger では、付属の SecureData アドオン (Voltage) により、次の機能をサポートします。

- Logger アプライアンスのセキュアな暗号化により、使用されていない (保管中の) 機密データを暗号化します。TLS および SSL 暗号化プロトコルのサポートにより、転送中のデータも保護します。
- セキュリティ管理とユーザーおよびグループの役割の定義が可能です。管理者は、ユーザーの役割とグループの権限に基づいて、レポートとレポートカテゴリにアクセス権を設定できます。また、特定のデータ列を暗号化して、復号化の権限を選択的に付与することもできます。
- フォーマット保持暗号化 (FPE) により、許可なくデータが公開されるのを防止し、保存中、転送中、使用中のデータを保護します。
- 連邦情報処理標準 140-2 (FIPS 140-2)。

超高速調査とフォレンジック

数秒の差で攻撃の成功と阻止が分かれる状況では、適切な情報を適切なタイミングで取得することが重要です。ArcSight Logger では、シンプルな検索インターフェイスにより、インデックス化されたデータを超高速で調査し、注意が必要な検索パターンをリアルタイムのアラートに容易に変換できます。

Logger の機械学習のデータサイエンスコンテンツは、調査のスピードアップに役立ちます。あらかじめ含まれているコンテンツを利用できるほか、Python スクリプトを使用する独自のデータサイエンスアルゴリズムを開発することも可能です。

ArcSight Logger は、数年にわたる数十億件のイベントのアドホック検索を 10 秒未満で実行できるため、侵害を特定して詳細に分析することができます。

ノンストップのコンプライアンス

ArcSight Logger には、サイバーセキュリティ、コンプライアンス、アプリケーションセキュリティ、IT 運用の監視に役立つコンテンツが含まれます。PCI、ITGOV、HIPAA、NERC、Sarbanes-Oxley (SOX) 向けの追加のコンプライアンスコンテンツパッケージがアドオンオプションとして用意されています。アメリカ国立標準技術研究所 (NIST)800–53、ISO-17799、SANS などの標準的な規格にも対応可能です。

デプロイと管理が容易

ArcSight Logger は、集中管理コンソールの ArcSight Management Center から構成、管理、監視できるため、数回クリックするだけで簡単にデータに接続できます。大規模なデプロイメントでも簡単に構成、管理、アップグレードできるため、ツール自体ではなく、目的に集中できます。

主な特長

- 包括的なデータ収集
- 柔軟なデプロイメントアーキテクチャ
- 高い安全性と信頼性
- 超高速検索と調査
- ノンストップのコンプライアンス
- デプロイと管理が容易
- 機械学習のデータサイエンスコンテンツ

ArcSight を選ぶ理由

ArcSight の次世代 SIEM は、拡張性に優れた強力なプラットフォームです。セキュリティの専門家がセキュリティのプロフェッショナル向けに開発した統合ソリューションです。セキュリティ情報、ビッグデータの収集、ネットワーク、ユーザーおよびエンドポイントの監視、高度なセキュリティ分析テクノロジー (検知、調査、UEBA のソリューション) を独自に統合した包括的なアプローチにより、セキュリティインテリジェンスを提供します。リアルタイムでの脅威の検知と対応、コンプライアンスの自動化と保証、IT 運用に関するインテリジェンスを提供することにより、階層化された強力な分析アプローチによる企業の自己防衛を実現します。

自社の SIEM ソリューションの強固さを主張するベンダーは数多くありますが、ArcSight のチームには、セキュリティに関する専門知識と経験があり、他のベンダーには真似できないリーダーシップがあります。

Micro Focus は、次世代ソリューション、実証済みの手法、世界最大クラスの複雑な SOC を扱ってきた 18 年以上の経験という他社にはない能力により、優れたセキュリティ対策と運用を支援します。

ログ管理の詳細
www.microfocus.com/ja-jp/arcsightlogger

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

160-JA0272-002 | M | 09/20 | © 2020 Micro Focus or one of its affiliates. Micro Focus および Micro Focus ロゴは、英国、米国、およびその他の国における Micro Focus、その子会社、関連会社の商標または登録商標です。その他すべての商標は、該当する所有者に帰属します。