opentext™ | Cybersecurity

データシート

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 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ニーズ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。

製品の概要

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 by OpenText™ 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 製品ラインの目標の実現において重要な役割を果たします。

ArcSight Logger を使用すると、組織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。

ArcSight 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、レポートが組み込まれており、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。

主なメリット

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、

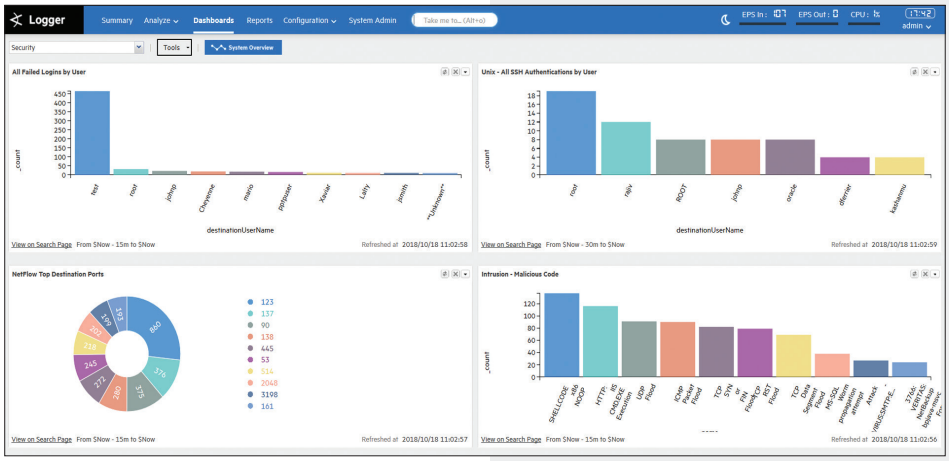

図 1. ArcSight Logger ダッシュボード

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ーに収集
- 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

データの検索、モニター、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。

柔軟な導入アーキテクチャ
ArcSight Logger をクラスターとして構成することで、データ収集の負荷を分散し、検索クエリをプラットフォーム全体に分散できます。Linux システム、VMware 仮想マシン (VM) (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、データが効率的に圧縮されるため、ストレージとメンテナンスのコストを削減できます。

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 by OpenText™、ArcSight Investigate by OpenText™、ArcSght Interest UEBA by OpenText™ 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) を利用でき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、変更、削除から (保存中および転送中の) データを保護します。ArcSight Logger では、Voltage SecureData Enterprise by OpenText™ により、次の機能がサポートされます。

- ArcSight 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 (保存中の) 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。
- Voltage Format Preserving Encryption (FPE) by OpenText™ 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。

ArcSight 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 スクリプトを使用して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 運用のモニター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。

導入と管理が容易
ArcSight Logger は、集中管理コンソールの ArcSight Management Center から構成、管理、モニターできるため、数回クリックするだけで簡単にデータに接続できます。大規模導入でも簡単に構成、管理、アップグレードできるため、ツール自体ではなく、ユースケースに集中できます。

主な特長

- 包括的なデータ収集
- 柔軟な導入アーキテクチャ
- 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
- 導入と管理が容易
- 機械学習のデータサイエンスコンテンツ

ArcSight 製品ラインを選ぶ理由
ArcSight SIEM by OpenText™ 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。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モニター / フォレンジックと高度なセキュリティ分析テクノロジー (検知、調査、ArcSight Interset UEBA の各ソリューション) 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出と対応、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。

「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モニターして、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
www.opentext.com

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 SIEM チームには他のベンダーの追随を許さない、セキュリティに関する専門知識と経験、そしてリーダーシップがあります。

OpenText™ 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/arcsightlogger

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。

760-JA0047-002 | O | 12/23 | © 2023 Open Text