opentext™ | Cybersecurity

データシート

ArcSight Security Open Data Platform

ArcSight ソリューションの価値を引き出して維持

製品の概要

今後 2 年以内にデータ侵害を受ける可能性がある企業の割合は 29.6% とされています[1]。組織に対するサイバー攻撃の脅威は年々増加しており、2021 年までに損害額は年間 6 兆ドルを超えると見込まれています[2]。

最新のセキュリティオペレーション環境を支えるのは、セキュリティデータです。データとデータ形式の異なるソースの数が増えると、すべての要件を満たす単一のデータアーキテクチャを構築することは不可能に近くなります。1 年間に作成およびコピーされるデータの量は 2 年ごとに倍増しており、2020 年までには 44 ゼタバイトに達する見込みです[3]。IoT、物理環境、OT、IT のデータの量とスピードが急速に増加しているため、セキュリティオペレーションセンター (SOC) は、脅威検出に必要な大量のデータの取り込みと処理に苦慮しています。データアクセスと重要なシステムの接続が制限されると、大幅な遅延とコストが発生します。

データ量の増加、急速に変化する脅威の状況、優秀なセキュリティスタッフの不足に適応するには、SOC の根本的な再構築が必要です。

ArcSight Security Open Data Platform (SODP) by OpenText は、オープンスタンダードのサポートによって脅威検出を改善し、データをリアルタイムでエンリッチメントできる、将来を見据えたデータソリューションを提供します。SODP は、セキュリティデータコネクターによりデータを収集し、リアルタイムでエンリッチメントして、アナリストがすぐに対応できるように整理された情報を提供します。また、Apache Kafka を基盤としたインテリジェントなトランスフォーメーションハブにより、ソースの種類や場所を問わず、シームレスにデータを取り込み、仲介できます。

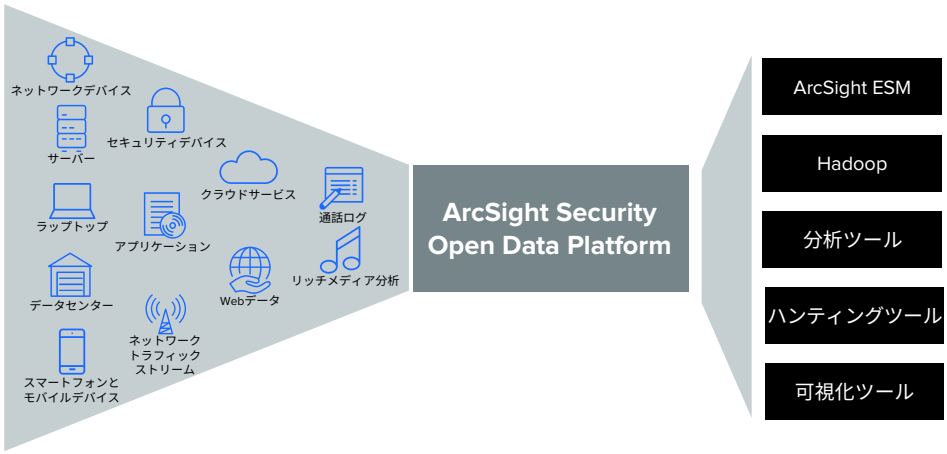

図 1. あらゆるデータをどこにでも送信できるオープンアーキテクチャ

主な機能

- Apache Kafka により構築されたトランスフォーメーションハブにより、あらゆるソースからデータを取り込んであらゆる場所に転送
- リアルタイムのデータのエンリッチメントにより、未加工のデータにセキュリティコンテキストを追加することでデータをすぐに使用可能
- 480 以上のすぐに使用できるコネクターによりあらゆる種類のソースからデータを収集
- 集中管理コンソールにより、セキュリティ環境のエンドツーエンドのビューを提供
- 「ゲストデータ」機能により、すべての IT 要件を満たすトランスフォーメーションハブのメッセージバスを使用可能

主なメリット

- データの可視性を向上して、攻撃と信用低下のリスクを削減
- 迅速な脅威検出と対応によりリスクを低減
- 優秀なセキュリティスタッフを効率的に活用
- Hadoop と分析ツールのデータを使用することで既存の投資を活用
- データを抽出し複数の宛先に送信するコストと複雑さを低減

1. Ponemon Institute—Cost of a Data Breach Report 2019
2. CSO online: Top 5 cybersecurity facts, figures and statistics for 2018
3. IDC—The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things

特長および利点

幅広いデータ対応とスピードにより拡張性を実現

ArcSight SODP は、480 以上のすぐに使用できるセキュリティデータコネクターとカスタムコネクター作成ツールを備えており、あらゆる種類のデータソースからデータを収集できます。4 週間ごとにリリースされる新たなパーサーにより、新たなデータソースとバージョンアップデートをスピーディーにサポートします。トランスフォーメーションハブの Syslog コネクターにより、ネットワークトラフィックを低減しながらエンタープライズ環境を簡単に拡張できます。トークンベースのツールでパーサーを構築できるため、新たなコネクターを構築する際の一貫性が向上し、数日から数時間、あるいは数時間から数分に時間を短縮できます。インテリジェントなトランスフォーメーションハブは、数十万 EPS (1 秒間に処理可能なイベント数) でデータを抽出し、複数の宛先にシームレスにデータを仲介できます。

多様化するデータソースの管理は、煩雑な仕事です。ArcSight SODP に付属する ArcSight Management Center by OpenText は、直感的なビジュアルと指標を提供します。すべてのデバイス、コネクター、宛先についてエンドツーエンドのビューを提供するため、即座に問題を特定して、短時間で解決できます。また、管理コンソールにより、これまでになく簡単に SOC のリソースを管理できます。即時コネクター導入機能に加えて、数百ノードへのアクションを一度で簡単に実行することも可能なため、時間を節約できます。

ArcSight Security Open Data Platform (SODP) によってセキュリティの適用範囲を拡張できるため、セキュリティオペレーションが簡素化し、攻撃のリスクが低減します。また、最適化により、大量で多様なデータを高速に収集して管理できます。

リアルタイムのセキュリティコンテキストによるインサイトの提供

ArcSight Security Open Data Platform は、リアルタイムでデータをエンリッチメントして、アナリストがすぐに対応できるように整理された情報を提供します。ArcSight SODP のスマートコネクターは、OpenText が長年に渡って培ったセキュリティの専門知識を活用して、取り込み時にデータの正規化、分類、エンリッチメントを実行します。データはすでに構造化および体系化されているため、脅威の検出を支援するイベントの相関と調査を素早く正確に行うことができます。

コンプライアンス要件を満たすとともに、サイバー攻撃によるデータの不正操作を防止するには、データの信頼性と整合性を確立することが重要です。ArcSight SODP が提供する暗号化された圧縮ログにより、傍受、

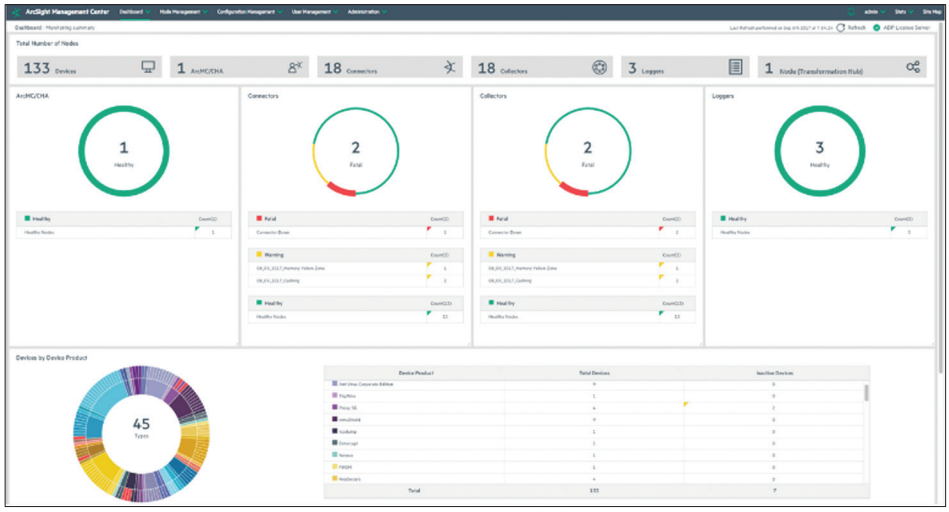

図 2. SODP の集中管理コンソール - ダッシュボード

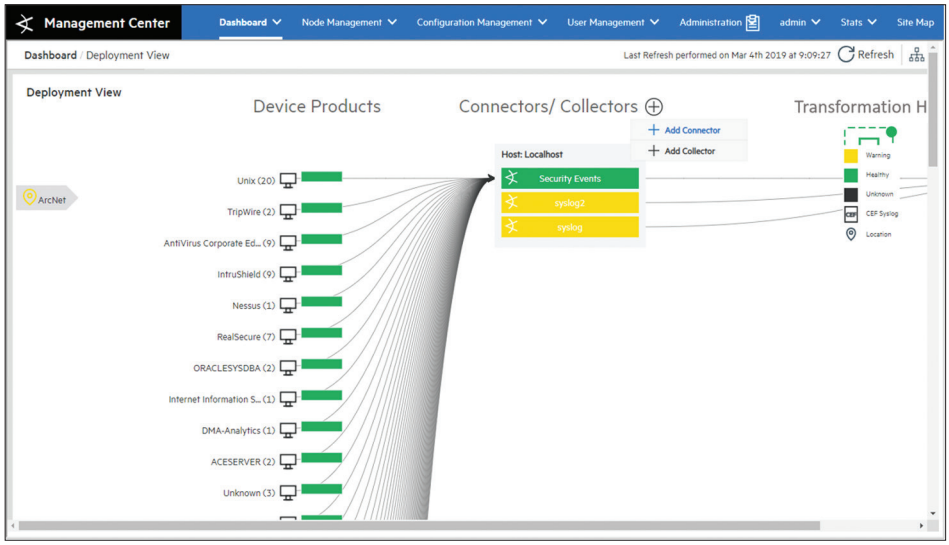

図 3. ArcSight SODP の集中管理コンソール - エンドツーエンドのモニタリング

お問い合わせ
www.opentext.com

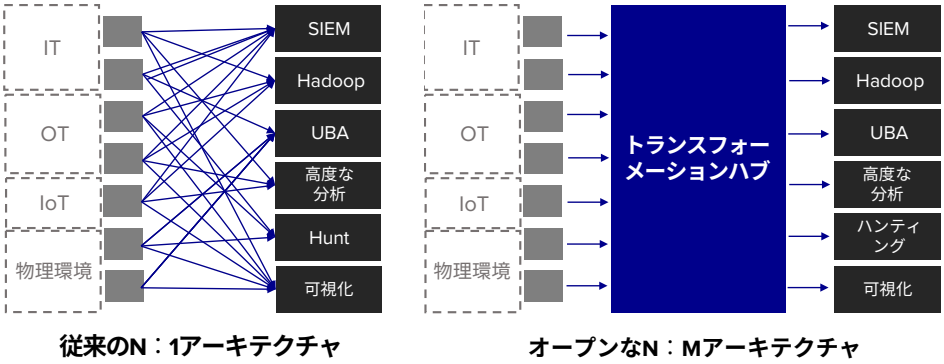

図 4. インテリジェントメッセージバスのアーキテクチャ

改ざん、削除からデータを保護できます。転送中のすべてのデータは、Transport Layer Security (TLS) によって保護されます。

オープンアーキテクチャの活用

リアルタイムの分析とアーカイブのために複数の宛先に送信するデータのソースと量が増えるなか、N：1 アーキテクチャは、セキュリティオペレーションのニーズと拡大の足かせになっています。ArcSight Security Open Data Platform (SODP) のトランスフォーメーションハブ (Apache Kafka ベースのメッセージバス) は、すべてのソースからデータを取り込んで複数の宛先に仲介できる N：M アーキテクチャを採用しています。これによって、セキュリティ環境を拡大し、収集されたデータを既存のデータレイクや分析ツールなどのテクノロジーで活用できます。取得したデータを複数のユースケースに使用し、将来を見据えたセキュリティオペレーションを確立することにより、ROI が改善します。

オープンアーキテクチャのため、データの保存、検索、分析方法を柔軟に選択できるほか、ビジネス要件に最適なテクノロジーを組み合わせて使用できます。

IT データニーズに合わせて ArcSight SODP の Kafka ベースのメッセージバスを使用することで、ROI を最大化できます。また、ArcSight SODP は、トランスフォーメーションハブの Kafka レプリケーションによって高度な HA 機能を提供します。

ArcSight Security Open Data Platform は、オープンスタンダードのサポートによって脅威検出を改善し、データをリアルタイムでエンリッチメントできる、将来を見据えたデータソリューションを提供します。オープンアーキテクチャのメッセージバスにより、既存の N：M アーキテクチャに接続して、すべてのソースからデータを取り込んで複数の宛先に仲介できます。ArcSight SODP がエンタープライズ環境を拡張し、データにコンテキストを追加することで、アナリストは整理された情報に基づいて即座に対応できます。

詳細はこちら：
www.microfocus.com/sodp

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-JA0035-003 | O | 12/23