Security Open Data Platform

Micro Focus ArcSightソリューションの価値を引き出して維持します。

製品概要

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。

Micro Focus Security Open Data Platform (SODP)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に付加情報を追加することができる、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、リアルタイムに付加情報を追加して、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、どこにあるどのようなソースもシームレスにデータを取り込み、転送できます。

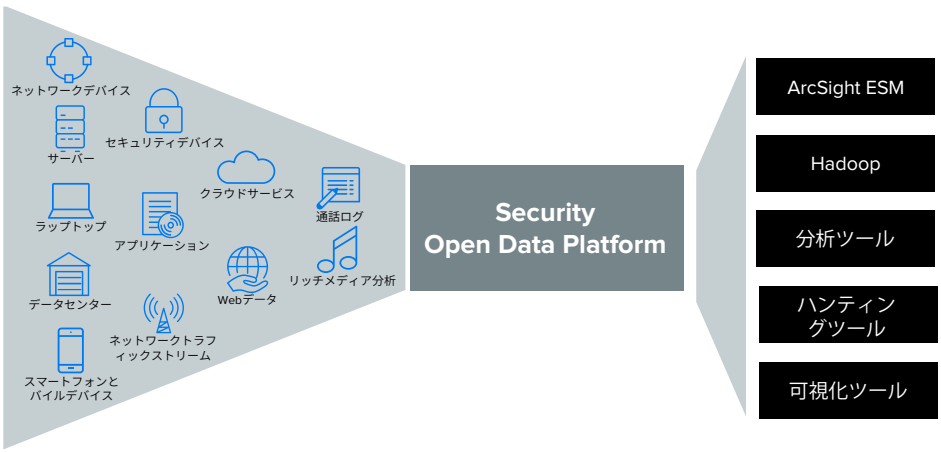

図 1. あらゆるデータをどこにでも送信できるオープンアーキテクチャ

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
- 収集した生データに対して、リアルタイムに情報を付加することで、セキュリティコンテキストを追加し、データをすぐに利用可能な状態にします
- 480超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
- 一元化された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、ArcSightファミリー以外のツールも、Transformation Hubのメッセージバスを利用することができます

主な利点

- データの可視性を向上して、攻撃と信用低下のリスクを低減
- 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

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480以上備えたSODPは、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転送できます。

多様化するデータソースの管理は、煩雑な仕事です。SODPのArcSight Management Center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。Instant Connector Deployment 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。

Security Open Data Platform (SODP)によってセキュリティ監視の対象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、大量で多様なデータの高速な収集と管理が最適化されます。

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

Security Open Data Platform は、リアルタイムでデータに付加情報を追加し、アナリストがすぐに対応できるように正規化された情報を提供します。SODPのスマートコネクターは、Micro Focus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、データ収集時にデータの正規化、分類し、付加情報を追加します。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。SODPが提供する暗号化された圧縮ログにより、傍受、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。

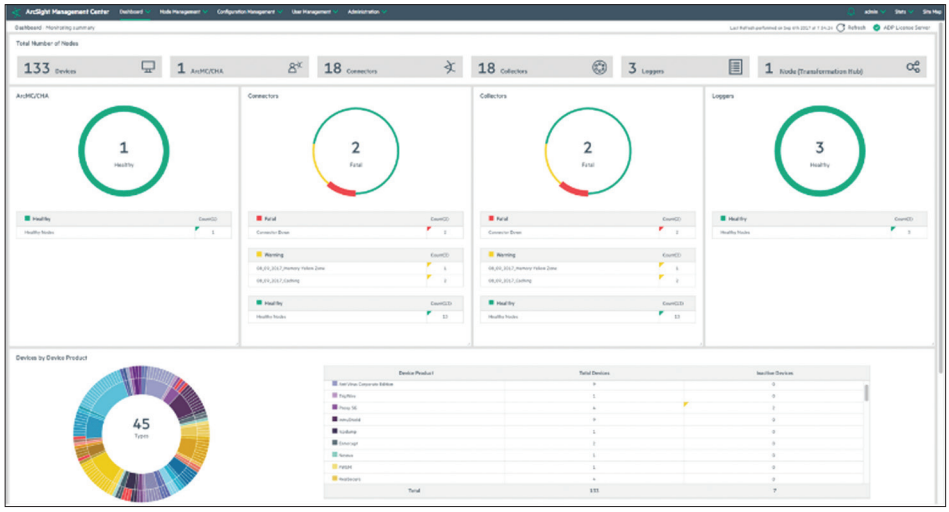

図 2.SODPの集中管理コンソール - ダッシュボード

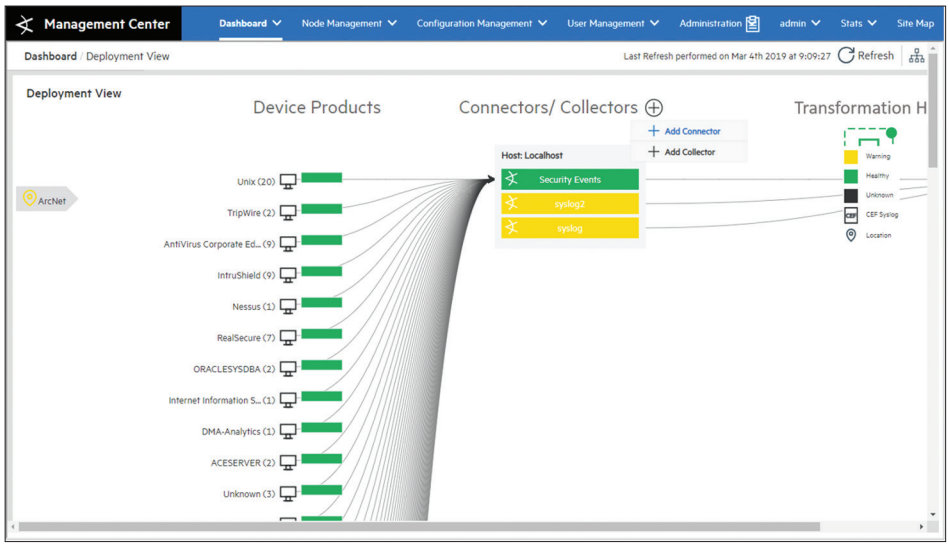

図 3. SODPの集中管理コンソール - エンドツーエンドのモニタリング

お問い合わせ先：CyberRes.com
この記事はいかがでしたか？
シェアはこちら

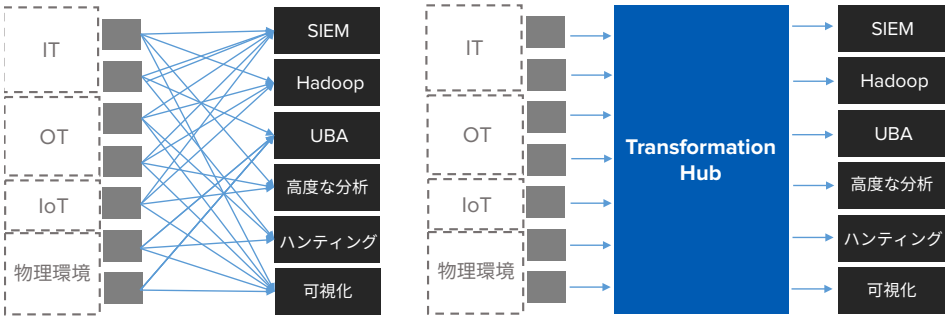

図 4. インテリジェントメッセージバスのアーキテクチャ

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。Security Open Data Platform (SODP)のトランスフォーメーションハブは、Apache Kafkaベースのメッセージバスであり、すべてのソースからデータを取り込んで複数の宛先に転送できるN:Mアーキテクチャを提供します。これによって、セキュリティ対象範囲を拡大し、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の組み合わせを採用することができます。

SODPのメッセージバスにより、ニーズに合わせて、データを広く活用することが可能になり、ROIを最大化できます。また、SODPは、トランスフォーメーションハブに内蔵されているKafkaのレプリケーション機能により高度なHA機能を提供します。

Micro Focus 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に付加価値を追加することができる、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転送できます。SODPは、エンタープライズ環境であっても十分にスケールし、アナリストが即座に対応できるよう、データに適切なコンテキストを追加します。

詳細情報はこちら：
www.microfocus.com/sodp

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

CyberRes
A Micro Focus Line of Business