ArcSight Data Platform

データカオスからセキュリティインサイトを導き出すオープンプラットフォーム

製品ハイライト

2016年[1]には、98%の企業がサイバー攻撃の被害を受けました。企業に対するサイバー攻撃の脅威は年々増加しており、推定コストは年間7,400万ドル[1]にも上っています。

セキュリティデータは、現代のセキュリティオペレーション環境を支えています。データソースやデータ形式は多種多様でさらに増加を続けており、すべてのニーズに対応できる単一のデータアーキテクチャーを構築することはほぼ不可能です。1年間に作成またはコピーされるデータ量は2年ごとに倍増してきており、2020年までに44ゼタバイトに達する見込みです[2]。IoT、物理環境、OT、およびITから生成されるデータの量と速度が急激に増加する中で、セキュリティオペレーションセンター (SOC) は脅威の検出に必要な膨大なデータを収集して処理しようと奮闘しています。データアクセスや重要なシステムとの接続性が限られていることが、大きな遅れやコストの原因になっています。こうした状況に加えて、2015年には米国だけで209,000を超えるサイバーセキュリティの求人が埋まっておらず、求人の数は2010年から2015年の間に74パーセント増加しています[3]。

データ量の増加、急速に変化する脅威環境、スキルのあるセキュリティ人材の不足に対応するには、SOCの根本的な再構築が必要です。

Micro Focus® ArcSight Data Platform (ADP) は、リアルタイムでデータをエンリッチ化し、オープンスタンダードをサポートすることでより効果的に脅威を検出できる将来に対応したデータソリューションです。ADPはセキュリティデータコネクターを使用して、データの収集とリア

1 Ponemon Institute—「2016 Cost of Cyber Crime Study & the Risk of Business Innovation」
2 IDC—「The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things」
3 米国労働省労働統計局レポート

主な機能

- Apache Kafkaをベースに構築されたEvent Brokerにより、あらゆるソースからデータを収集してあらゆる場所に送付
- リアルタイムでのデータのエンリッチ化により、Raw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がすぐに利用可能
- 400以上のデフォルトコネクターにより、あらゆるソースタイプからデータを収集
- Event Brokerメッセージバスにより、毎秒最大100万イベントの速度でデータを収集
- 一元化された管理コンソールにより、セキュリティ環境をエンドツーエンドで表示

主なメリット

- 可視化できるデータの範囲を広げることで、攻撃や企業イメージ低下のリスクを低減
- 脅威の検出と対応を迅速化することでリスクを軽減
- スキルのあるセキュリティ人材を効率的に活用
- データをHadoopや分析ツールで利用することで投資対効果を向上
- 複雑でコストのかかるデータの抽出と複数の通知先への分配を簡素化してコストを削減

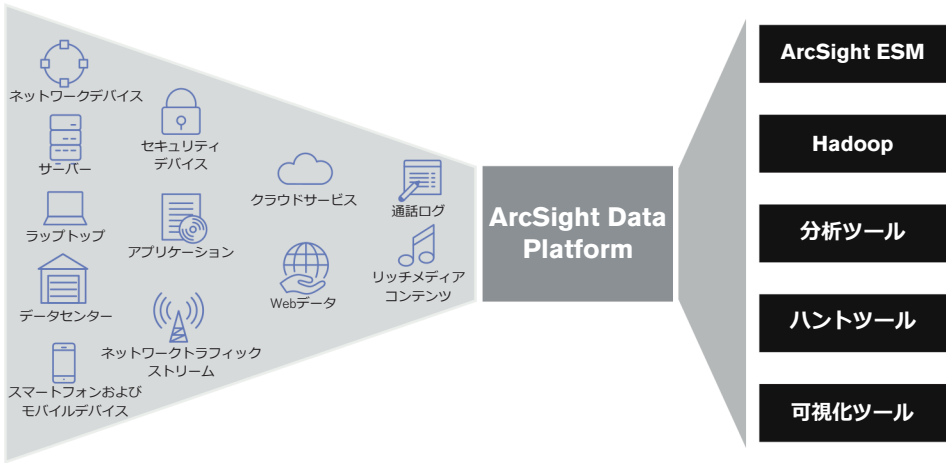

図1: あらゆるソースからのデータをどこにでも活用: オープンアーキテクチャー

ルタイムでのデータのエンリッチ化を行うことで、即座に対応可能な整理された情報をアナリストに提供します。ArcSight Data Platformに、Apache Kafkaをベースに構築されたインテリジェントなEvent Brokerを組み合わせて使用すると、あらゆる場所のあらゆるソースからシームレスにデータを取得して仲介することができます。

機能とメリット

卓越したスケーラビリティをもたらすデータの多様性と高速処理

ADPには、400を超えるデフォルトの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が用意されているため、あらゆるタイプのデータソースからデータを収集できます。また、新しいデータソースとバージョンアップデートがこれまでよりも短期間でサポートされるようになり、4週ごとに新しいパーサーがリリースされます。パーサーを作成するためのトークンベースのツールによって整合性が向上し、新しいコネクターの作成に要する時間が数日から数時間、数時間から数分へと短縮されています。インテリジェントなEvent Brokerでは、毎秒100万イベントという高速でデータを抽出し、複数の通知先にシームレスにデータを仲介することができます。

増加を続ける多種多様なデータソースの管理は非常に面倒です。ADPに付属しているArcSight Management Centreを利用すると、わかりやすい表示やメトリックが利用できます。すべてのデバイス、コネクター、および通知先をエンドツーエンドで表示することで、問題点をすばやく見つけ出し、修復に要する時間を短縮できます。管理コンソールでは、Instant Connector Deployment機能を導入し、一度に数百のノードでアクションを実行できるようにすることで、SOCリソースの管理がこれまでになく容易になり、時間も節約できます。

ArcSight Data Platform (ADP) は、セキュリティオペレーションを簡素化し、セキュリティオペレーションの対象範囲を広げることで攻撃のリスクを軽減します。また、大量のデータや多様なデータの高速での収集と管理を最適な形で実現します。

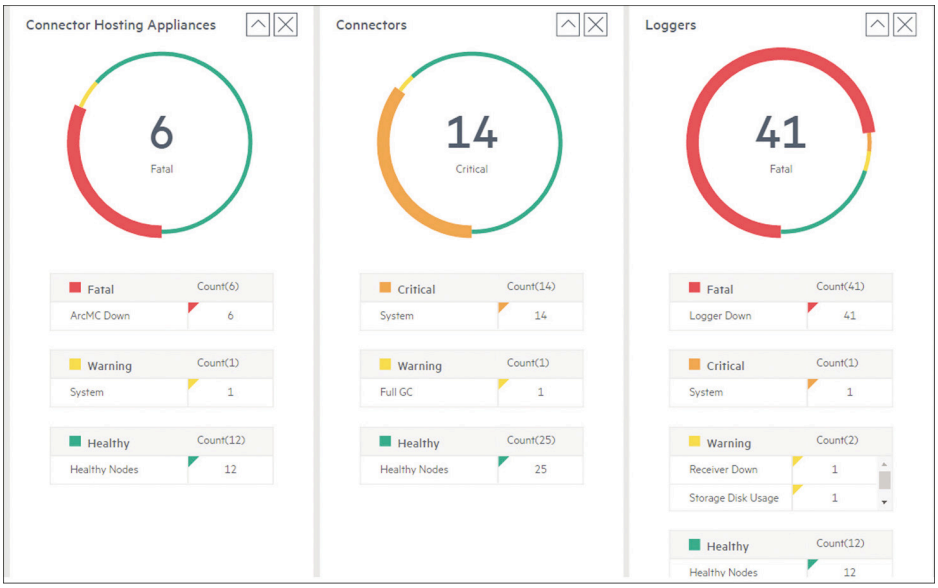

図2: ADPの一元化された管理コンソール—ダッシュボード

リアルタイムセキュリティコンテキストによるセキュリティインサイトの導出

ArcSight Data Platformは、Rawデータをリアルタイムでエンリッチ化することで、即座に対応可能な整理された情報をアナリストに提供します。ADPのSmartConnectorは、データ収集時にデータの正規化、カテゴリ分類、およびエンリッチ化を行います。これにより、長年培ってきた

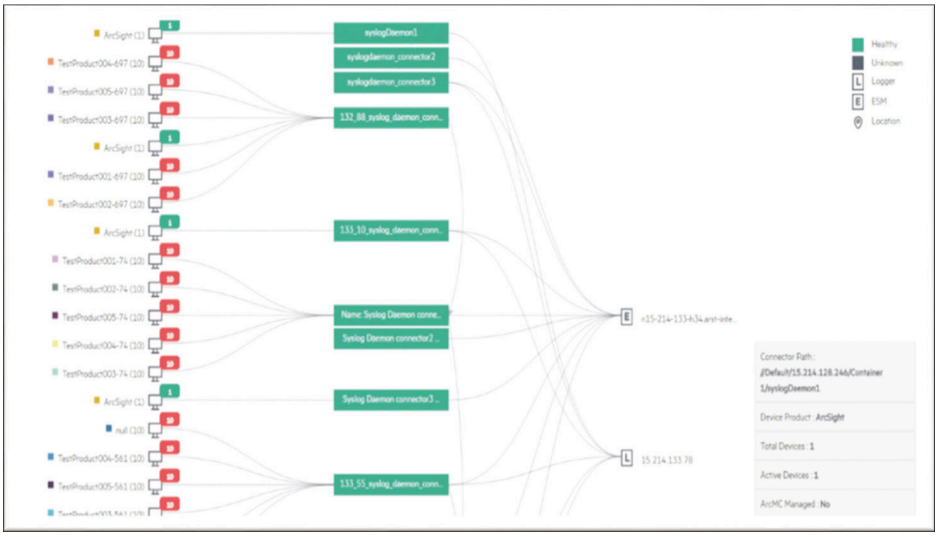

図3: ADPの一元化された管理コンソール—エンドツーエンドの監視

ArcSightのセキュリティ技術やノウハウが付加されます。データはすでに構造化されて整理された状態になっているため、調査やイベント相関処理をすばやく正確に行い、脅威の検出に役立てることができます。

コンプライアンス要件に対応し、サイバー攻撃によるデータ改ざんを防ぐには、データの信頼性と完全性を確保することが重要です。ADPでは暗号化および圧縮されたログを提供することで、盗難、改ざん、および削除からデータを保護します。伝送中のデータはすべて、TLS (Transport Layer Security) で保護されます。

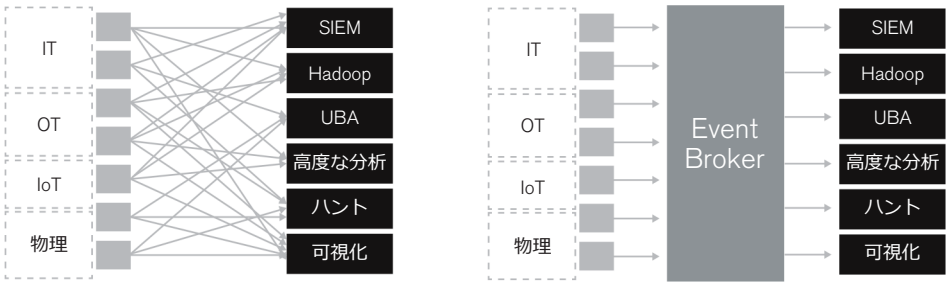

図4: インテリジェントメッセージバス アーキテクチャー

オープンアーキテクチャーの活用

ソースの数が増加し、リアルタイム分析やアーカイブを行うために複数の通知先へ伝送されるデータ量が大幅に増えていくと、N:1のアーキテクチャーがセキュリティオペレーションの成長およびニーズの妨げになります。ArcSight Data Platformには、Apache Kafkaベースのメッセージバスであるevent Brokerが付属しています。このEvent Brokerでは、N:Mのアーキテクチャーを利用して、すべてのソースからデータを収集し、そのデータを複数の通知先に仲介できます。これにより、セキュリティ環境をさらに広げ、既存のデータレイク、分析ツール、およびその他のテクノロジーで収集されたデータを利用できるようになります。このように、さまざまなユースケースで取得したデータを利用することで投資を有効活用し、将来にわたって機能するセキュリティオペレーションを実現できます。

オープンアーキテクチャーを利用することで、データの保管、検索、および分析方法を柔軟に選択し、ビジネスのニーズに合わせた最適なテクノロジーを使用することができます。

まとめとなりますが、ArcSight Data Platform (ADP) は、リアルタイムでデータをエンリッチ化し、オープンスタンダードをサポートすることで、より効果的に脅威を検出できる将来に対応したデータソリューションです。オープンアーキテクチャーのメッセージバスにより、すでに存在するN:Mのアーキテクチャーを結び付けて、すべてのソースからデータを収集し、そのデータを複数の通知先に仲介することができます。これにより、セキュリティ環境をさらに広げ、既存のデータレイク、分析ツール、およびその他のテクノロジーで収集されたデータを利用できるようになります。このようにして、さまざまなユースケースで取得したデータを利用することで投資を有効活用し、将来にわたって機能するセキュリティオペレーション、データレイク、分析ツール、およびその他のセキュリティテクノロジーをSOCに展開することで、任意の場所から任意の場所へのデータ送信が可能になります。ADPは企業の規模に合わせて導入でき、データに意味を付加することで即座に対応可能な整理された情報をアナリストに提供できます。

詳細情報

www.microfocus.com/adp

www.microfocus.com

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
0120 923 333

www.microfocus-enterprise.co.jp