opentext™ | Cybersecurity

ハンドアウト

ArcSight SODP と Splunk

適切な SecOps においては、ソリューション全体でデータを共有する統合セキュリティアーキテクチャを実装します。ArcSight SODP は、既存ツールの ROI を向上させることができる拡張性の高い相互運用可能なソリューションを提供します。

利点

ArcSight SODP によって Splunk を強化すると、次のことが可能になります。

- ライセンス使用コストを最大 90% 削減
- 20 以上ある独自スキーマではなく 1 つの共通標準スキーマにデータを解析
- イベントを正規化および分類することで、データソースに関わらずクエリーとレポーティングの処理を簡素化
- ハードウェアストレージコストを削減
- SODP への投資を即座に回収

ArcSight SODP により Splunk への投資を最適化

ArcSight Secure Open Data Platform (SODP) by OpenText がよいか、Splunk がよいかという議論は、セキュリティ業界でよく行われている議論と思われます。多くの場合、どちらの陣営の支持者も、自分の支持する製品が最高である理由に関して、強硬な姿勢を崩しません。それぞれのソリューションが採用しているアプローチは非常に異なりますが、どちらにも無視できない魅力的なメリットがあります。ArcSight SODP はオープンアーキテクチャアプローチを採用しており、そこでは複数のソースからリアルタイムで取得されたデータが容易に拡張、正規化、集約され、そうしてエンリッチ化されたデータが複数の宛先に配信されることで、分析が容易に行えるようになります。Splunk は、強力な検索機能と高度な組み込み分析機能が組み合わされることで、新しいデータソースを迅速に導入してオンボーディングできるようになります。単純に比較すれば両者とも類似の機能と利点を数多く含んでいますが、利用する人の立場によって、一方のソリューションが他方のソリューションよりも複数のカテゴリで必然的に優位に立つことになります。では、どのように選択すればよいのでしょうか。

それぞれのソリューションで利用できるにちがいない最高の機能からメリットを得るためには、選択の必要などないかもしれない、というのがベストアンサーです。ArcSight SODP と Splunk は、それぞれのソリューションの最も使用したい部分を組み合わせる形で適切に連携させることができます。またそれによって分析能力が強化され、全体的なライセンスコストが大幅に削減されます。

アプローチの違いを理解する

ArcSight SODP と Splunk がどのように連携するかを理解するには、まず、両者のアプローチの違いを理解する必要があります。1 つ目の違いは、データを取り込むときに何を行うかという点です。Splunk は、単にイベントデータを生データで収集してインデックスを作成します。検索を実行するときまで、またはデータをレンダリングするときまで、データの解析や正規化は行いません。これは「スキーマオンリード」と呼ばれています。このアプローチの利点は、新しいデータソースを追加して全種類のマシンデータの収集を開始することが極めて簡単にできることです。単に与えられるものを受け入れ、何も問われることはありません。欠点もあります。データを取り込むときに解析、集約、フィルタリングを行わないため、Splunk ライセンスの使用率が大幅に増し、ダウンストリームワークフローのデータ処理のオーバーヘッドが増大する可能性があります。

一方、ArcSight SODP は SmartConnector を使用して、データを取り込むときに正規化、分類、エンリッチ化、集約を実行します。この「スキーマオンライト」アプローチでは、すべてのデータソースにわたって一貫性のある構造化された形式でデータがエンリッチ化されるため、データを任意のビッグデータまたは分析ツールと容易に共有できます。さらに、イベントが適切に集約されるため、言い換えると共通のフィールドを最小限のデータ損失で維持しながら共通のイベントがグループ化されるため、データストアの大幅な削減につながる可能性があります。最終的に、ダウンストリームアプリケーションでデータを収集して解析する負担がなくなります。また、Splunk を含む分析ツールでは、迅速にデータを活用できるようになり、その一方で使用したりインデックスを作成したり処理を行ったりする必要があるデータの量が低減します。

さらに、ArcSight SODP は業界標準の Common Event Format (CEF) を使用して、すべてのマシンデータを共通のスキーマに正規化します。480 以上ある SmartConnector だけ

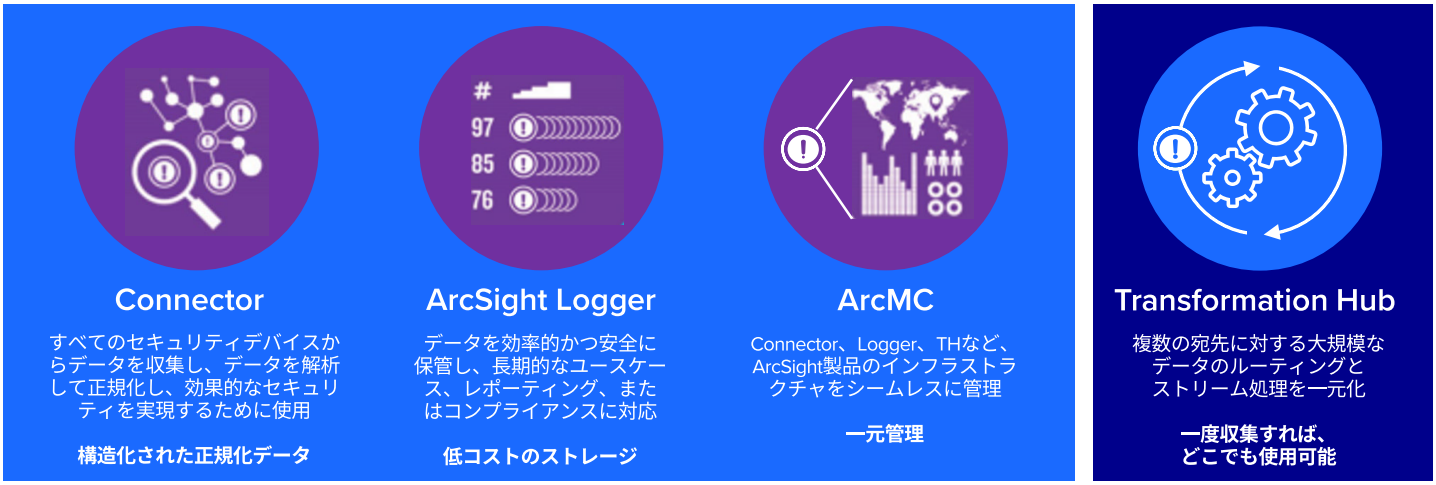

図 1. ArcSight Security Open Data Platform のポートフォリオ

でなく、カスタムデータフィード用の Flex Connector フレームワークも使用されるため、事実上あらゆる種類のデータを CEF 形式で収集して配信できます。共通のスキーマ内でデータが正規化されることで相関付けの処理が速くなり、対象の宛先がデータを利用することが容易になります。また、アナリストはイベントメッセージをベンダー依存にならないようにする共通の分類法を使用できるようになります。その結果、アナリストは 1 つのスキーマを学習するだけでさまざまなプラットフォームでほぼ同じ検索クエリーを使用できるようになるため、作業方法が大幅に簡素化され、強化されます。

Splunk では、共通情報モデル (CIM) と呼ばれる正規化手法が、検索時のスキーマまたはスキーマオンザフライとして使用されます。これは実際には 1 つのスキーマではないことに注意してください。Splunk では、23 種類のさまざまなスキーマが用意されており、データソースに応じて選択できます。この疑似的な正規化により、データの使用が複雑化し、データの効果的な相関付けが困難になります。また、お客様はデータの取得元のソースに固有のカスタムレポートやカスタムダッシュボードを作成しなければならなくなります。

ArcSight Security Open Data Platform (SODP) により Splunk を強化する方法

では、Splunk は、ArcSight SODP の CEF 形式のデータからどのようなメリットを得ることができるのでしょうか。ArcSight SODP に用意された SmartConnector では、複数の機能を利用できます。まず、任意のデータソースを一度オンボーディングしたら複数の宛先と同時に共有できるようになる機能があります。これらのコネクタはすべて、ArcMC 管理サーバーで単一のインターフェイスから容易にメンテナンスおよび導入できます。数回クリックするだけで新しい宛先にデータを送信することもできます。ArcSight SODP for Splunk アプリを追加で利用すると、Splunk がこれらの正規化されたイベントをすべて受け入れて把握できるようになります。

さらに、データソースと Splunk 環境の間でこのアプリと ArcSight SODP の SmartConnector を導入すると、非集約のデータではなく集約されたデータの受け取りを Splunk で開始できるようになります。場合によっては、この集約処理によって Splunk への情報の流れを 90%* までも減らしながら、分析に必要な重要な情報はすべて変わらずに提供されるようにすることができます。その仕組みがわかりやすくなる、基本的なシナリオの例を以下に示します。

- ユーザー Bob がログイン試行に 100 回失敗したことをシステムが報告するとします。その場合、Splunk への通常の非集約データストリームは、ユーザー Bob のログイン失敗イベントを生データで個別に 100 件受け取ります。
- ユーザー Bob がログイン試行に 100 回失敗したことをシステムが報告するとします。その場合、ArcSight SODP の SmartConnector は、ユーザー Bob がログイン試行に 100 回失敗したことを示す 1 つのイベントを生成し、この 1 つのイベントを Splunk に送信します。

もう 1 つの利点として、SmartConnector は実際、Splunk に送信する前にイベントデータを複数の方法でエンリッチ化します。SmartConnector はこれが認証イベントであることを認識しているため、将来のレポーティングに備えてこのイベントをそのように分類します。また、送信元および送信先 IP の IP アドレスを検索し、それらのホスト名を解決します。最後に、Bob がアカウンティンググループの一員であることを認識したとすれば、Splunk に送信する前にその有用なコンテキストを同様に追加します。

ArcSight SODP で実行される集約は、Splunk ライセンスの不要なデータ使用量を大幅に削減するだけでなく、データストレージ要件も同様に引き下げる可能性があります。また、ArcSight SODP で実行されるデータ正規化によって、Splunk でのクエリーとレポーティングの処理が簡素化され、その一貫性が向上します。ArcSight SODP の SmartConnector は、23 の異なるスキーマではなく単一の CEF の

*社内ベンチマークテストで検証済み。ただし、削減される値は集約のしきい値によって変わります。

SOC は、脅威検知を行ううえで不可欠な「津波」規模のデータを取り込んで処理するため、自らを根本的に再構築する必要があります。

お問い合わせ
www.opentext.com

標準スキーマにデータを正規化するため、すべてのデータソースに対して機能する統一されたダッシュボードとレポートを構築できます。

以上のような Splunk の強化につながる利点はすべて、ArcSight SODP の Transformation Hub モジュールを使用しても同じように活用できます。Transformation Hub は、極めて拡張性の高いメッセージバスおよびストリーム処理クラスターであり、ネットワークの複雑さとコンピューティング要件を軽減する方法で複数のソースから複数の宛先へとデータをまとめて送信します。Transformation Hub で CEF フィールドのルーティングとフィルタリングを一元管理して、適切なデータを適切なアプリケーションに配信することができます。また、ストリーミングプロセッサとして SmartConnector の正規化や syslog データのエンリッチ化を実行できるため、お客様はデータストームや増大したデータフローを容易に処理できるようになります。Transformation Hub のクラスターは、数百のクライアントを毎秒数百メガバイトで処理できるように設計されており、複雑さの軽減と管理性の向上を実現しながら、最大規模の SOC のデータ取り込みと配信のニーズに対応できるように容易に拡張することが可能です。

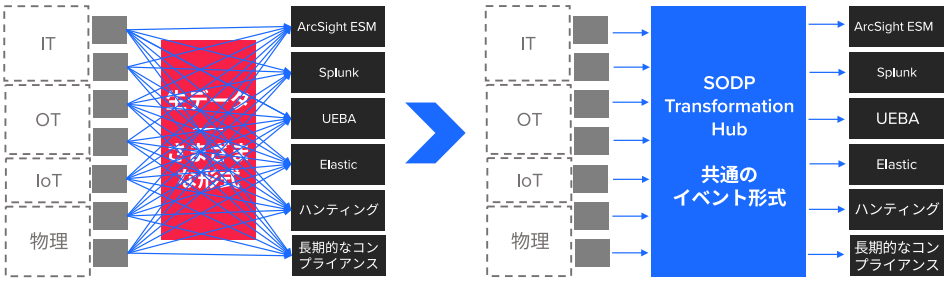

図 2. ArcSight SODP 採用前のアーキテクチャと採用後のアーキテクチャ

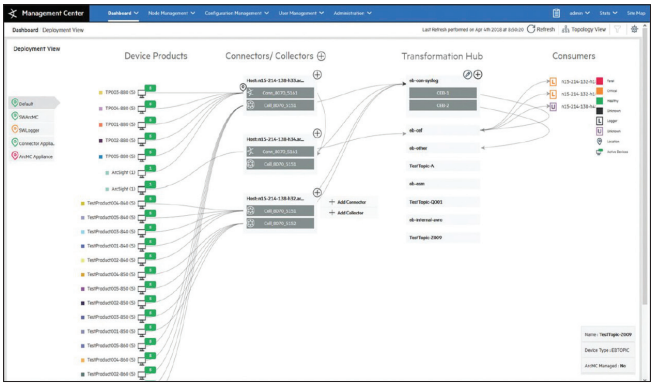

図 3. SODP の一元管理コンソール - エンドツーエンドでの監視が可能

ArcSight SODP と併用した Splunk をさらに活用

OpenText が ArcSight SODP で採用しているのがオープンアーキテクチャアプローチであり、このアプローチによって、コスト削減につながる集約とレポート機能を強化する正規化という利点が提供されます。ArcSight SODP は、ビッグデータセキュリティにしばしば伴う複雑さや混沌を解消し、SOC が Splunk 環境、データレイク、分析ツール、およびその他の最先端のセキュリティソリューションとエンリッチ化されたセキュリティデータを容易に共有して活用できるようにします。ArcSight SODP を利用して Splunk やその他のセキュリティソリューションへの投資をさらに有効活用する方法については、OpenText の担当者にお問い合わせください。

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。

761-JA0075-003 | O | 06/24 |