フライヤー

Micro Focus ArcSight Data Platform (ADP)とSplunk

SecOpsの成功の鍵は、複数のソリューションでデータを共有できる統合されたセキュリティアーキテクチャーの実装です。Micro Focus ArcSight Data Platform (ADP) はスケーラブルで相互運用可能なソリューションであり、既存ツールのROI最大化を実現します。

メリット

SplunkをADPで強化することで、以下が実現します。

+ ライセンス利用コストを最大90%削減
+ 20以上の独自スキーマに代わって1つの共通の標準スキーマでデータを解析
+ イベントの正規化とカテゴリ分類によりデータソースと無関係にクエリとレポート作成を簡素化
+ ハードウェアストレージコストを削減
+ ADPの投資を短期間で回収

ArcSight Data Platform (ADP) によるSplunk投資の最適化

セキュリティ業界では、Micro Focus ArcSight (以下、ArcSight) とSplunkの優劣が議論の的になっています。両陣営ともに、自社製品がクラス最高であることを声高に主張して譲りません。これらのソリューションの手法はまったく異なりますが、それぞれに無視できない固有の長所があります。ArcSightは拡張が容易なオープンアーキテクチャー手法を採用しており、複数のソースからのデータをリアルタイムで正規化して集約し、処理したデータを複数の宛先に送って容易に分析することができます。Splunkでは、新しいデータソースを簡単に展開して導入でき、強力な検索機能と高度な組み込み分析を利用できます。この2つを並べてみると、多くの共通した機能や利点が見られますが、どちらかのソリューションが多くの面で他方よりも優れていると考えている人たちもいます。では、どうやって選べばいいのでしょうか。

正解は、選ばなくていいのです。両方の利点を手に入れる方法があるからです。ArcSightとSplunkを組み合わせることで、それぞれのソリューションの優れた点を活かし、解析機能を大幅に強化しながら、全体としてのライセンスコストを削減することができるのです。

手法の違いについて

ArcSightとSplunkを連携させる方法を理解するには、まずそれぞれの手法の違いについて知る必要があります。1つめの違いは、データ取り込みの際に何が起きるかです。Splunkは単にイベントデータを未処理のまま収集してインデックス化するだけで、データの解析や正規化は、検索あるいは表示の時点まで行われません。この方式は「スキーマオンリード」と呼ばれています。この手法の利点は、新しいデータソースを追加して、あらゆる種類のマシンデータの収集を開始するのが非常に簡単であることです。データはただ取り込まれるだけで、何の解釈もされません。一方で、欠点もあります。取り込み時にデータの解析、集約、フィルタリングが行われないため、Splunkライセンスの使用量が非常に多くなることがあります。また、データ処理のオーバーヘッドが下流のワークフローに持ち越されます。

これに対してArcSightは、SmartConnectorを使用することで、取り込み時にデータの正規化、カテゴリ分類、エンリッチメント、集約を行います。この「スキーマオンライト」手法では、すべてのデータソースに共通の構造化された形式にデータが加工されるため、あらゆるビッグデータツールや解析ツールとデータを容易に共有できます。さらに、イベントの適切な集約、すなわち共通のイベントをグループ化しながら、一般的なフィールドを最小限のデータロスで保存することにより、データストアを大幅に節約できます。その結果、下流のアプリケーションにデータの収集や解析の負荷を負わせる必要がなくなります。そして、解析ツール (Splunkを含む) からデータを簡単に利用でき、消費、インデックス化、処理が必要なデータ量を減らすことができます。

また、ArcSightでは、業界標準のCEF (Common Event Format) を使用して、すべてのマシンデータが共通のスキーマに正規化されます。400種類以上のSmartConnectorと、カスタムデータフィード用のFlexコネクターフレームワークにより、ほぼあらゆる種類のデータを収集してCEFで配布できます。共通のスキーマでデータを正規化することで、相関が高速化され、あらゆるターゲット宛先での利用が容易になる

図1: ArcSight Data Platform (ADP) のポートフォリオ

とともに、アナリストが共通の分類を使用できるので、イベントメッセージがベンダーに依存しなくなります。これにより、アナリストの作業が大幅に簡素化され、強化されます。1つのスキーマだけを知っていればよく、さまざまなプラットフォームに対してほぼ同一の検索クエリを使用できるからです。

Splunkでは、検索時のスキーマやスキーマオンザフライとして、Common Information Model (CIM) という独自の正規化方法が用いられます。これは実際には、1つのスキーマでないことに注意が必要です。Splunkでは23種類の異なるスキーマが採用されており、データソースに応じて選択することになります。このような擬似的な正規化のために、データの使用が複雑になり、データの効果的な相関が困難になるとともに、それぞれのデータソースに固有のカスタムレポートやダッシュボードを作成する必要が生じます。

ArcSight Data Platform (ADP) によるSplunkの機能強化

では、SplunkからArcSightのCEF形式のデータを利用するにはどうすればいいでしょうか。ArcSight Data Platform (以下、ADP) で提供されているSmartConnectorは、さまざまな機能を果たします。

まず、どんなデータソースであっても、オンボーディングを1回行うだけで、さまざまな宛先と同時に共有できます。ArcMC管理サーバーを使用することで、これらすべてのコネクターの管理と展開を、1つのインターフェイスから容易に行うことができます。数回クリックするだけで、新しい宛先にデータを送信できます。ArcSight for Splunkアプリケーションを利用することで、これらすべての正規化されたイベントをSplunkで受け取って解釈できます。

さらに、このアプリケーションとADPのSmartConnectorをデータソースとSplunk環境の間に展開することで、非集約データでなく集約されたデータをSplunkで受け取ることができます。場合によっては、この集約により、Splunkへの情報の流れを最大90%削減できます。* その場合でも、分析に必要な重要な情報はいっさい失われません。基本的なシナリオを例として、その仕組みを説明します。

- たとえば、Bobというユーザーによるログイン試行の100回の失敗がシステムから報告された場合、Splunkへの通常の非集約データストリームでは、ユーザー Bobの失敗したログインイベントがそのまま100個別々に届きます。
- Bobというユーザーによるログイン試行の100回の失敗がシステムから報告された場合、ADPのSmartConnectorは、ユーザー Bobのログイン試行が100回失敗したことを示す1個のイベントを作成して、それをSplunkに送信します。

もう1つの利点として、SmartConnectorはSplunkに送信する前にイベントデータに対してさまざまなエンリッチメントを行います。SmartConnectorはこれが認証イベントであることを知っているので、将来のレポート作成のためにそれに応じたカテゴリ分類を行います。また、ソースと宛先のIPアドレスをそれぞれのホスト名に解決します。さらに、Bobがアカウンティンググループの一員であることがわかったとしたら、その情報を参考コンテキストとして付加してから、Splunkに送信します。

* 社内ベンチマークテストにより検証。ただし、削減率は集約しきい値によって異なります。

脅威検出に必要な膨大なデータの流れを取り込んで処理するためには、SOCの根本的な再構築が必要です。

お問い合わせ先:
www.microfocus.com

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

ADPによる集約は、Splunkライセンスによる不要なデータ使用を大幅に減らすことだけでなく、データストレージ要件の低減にも役立ちます。また、ADPのデータ正規化を利用することで、Splunkでのクエリやレポート作成がシンプルになり、一貫性が高まります。ADPのSmartConnectorによってデータが1つのCEF標準スキーマに正規化され、23種類の異なるスキーマを扱う必要がなくなるので、すべてのデータソースに対して使用できる統一されたダッシュボードとレポートのセットを作成できます。

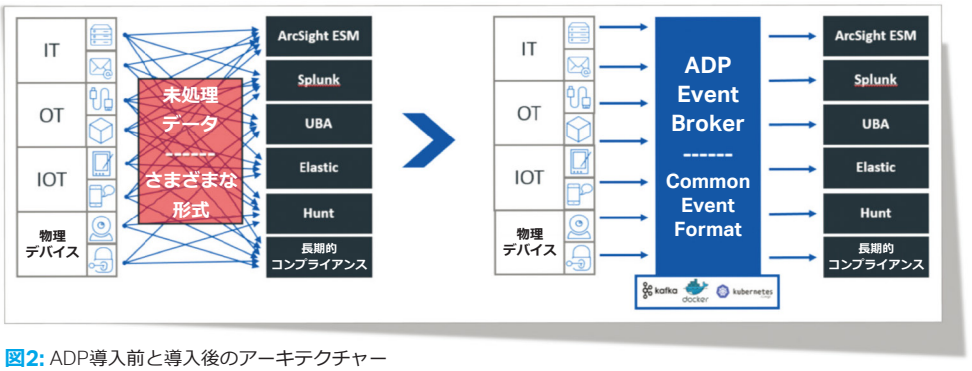

図2: ADP導入前と導入後のアーキテクチャー

このSplunkの機能強化のメリットは、ADPのEvent Brokerモジュールを通じても実現できます。Event Brokerは大規模な展開が可能な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、複数のソースから複数の宛先へのデータを統合することで、ネットワークの複雑性とコンピューティング要件を低減する効果があります。Event Brokerは、CEFフィールドに対するルーティングとフィルタリングを一元管理し、適切なデータを適切なアプリケーションに届けることを可能にします。また、syslogログデータに対するSmartConnector正規化とエンリッチメントをストリーミングプロセッサーとして実行することで、データストームや増加したデータフローの処理を容易にします。Event Brokerのクラスターは、数百のクライアントで毎秒数百メガバイトの処理を実行できるように設計されており、大規模なSOCのデータ取り込みと配信のニーズを満たしながら、複雑さを減らし、管理を容易にすることができます。

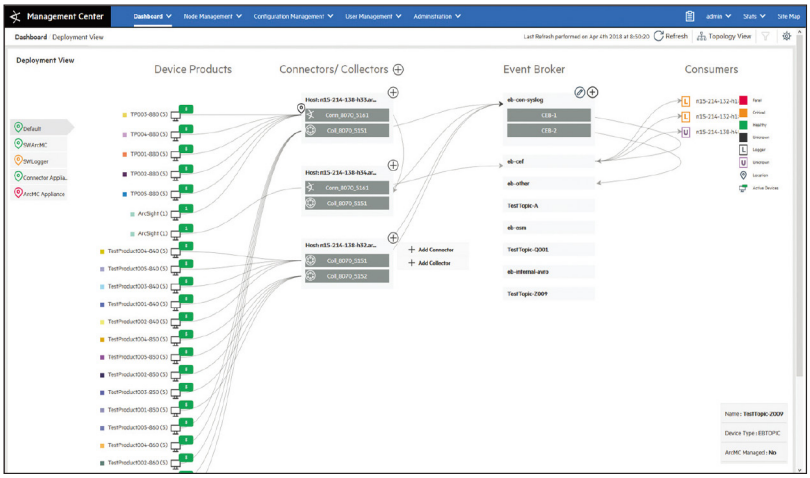

図3: ADPの一元化された管理コンソール - エンドツーエンドの監視

ADPでSplunkをさらに活用

ADPで集約によるコスト削減や正規化によるレポート作成機能の強化が可能になるのは、Micro FocusがADPで採用したオープンアーキテクチャーのおかげです。ADPを使うことで、SOCは、ビッグデータのセキュリティにつきものの複雑さや混乱を回避して、エンリッチ化したセキュリティデータを、Splunk環境、データレイク、解析ツール、およびその他の最高のセキュリティソリューションと共有して活用できます。ADP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からさらに多くの価値を引き出す方法の詳細については、Micro Focus®セールス担当者までお問い合わせください。

詳細情報
www.microfocus.com/adp