imperva

データシート

Impervaは、Splunkの最適化とコスト削減を実現する高性能のプリプロセッサを提供

Imperva は、Splunk のデータベースの監視コストを 95%削減し、生データへの透過的なアクセスを維持し、より豊富なセキュリティインサイトを提供します

多くの企業にとって、Splunk はネイティブログおよび DAM ツールで生成されたデータベースアクティビティログの主要なリポジトリの役割を果たしています。これらのログは Splunk にインデックス付けされたデータの 40%以上になる可能性があり、今後さらに拡大することを考えるとこのアプローチは非常に高価なものとなっています。

同時に、たいていの SOC チームは低レベルでの生データのやり取りを続けており、適切で迅速な実行をするのに必要な高品質なデータを受け入れません。 より高い価値のあるデータにするために、SOC チームが危険性のあるイベントをより有効に切り離すには、高品質な Splunk の開発努力と時間が必要です。

Imperva は Splunk の統合を強化し、両者の強みを活かします。Splunk のライセンスコストを削減すると同時に、セキュリティ対策を目的として構築された幅広い新機能を追加することで、データセキュリティプログラムを最適化します。Imperva のプリプロセッサは、生データから抽出されたインテリジェンスにのみわずかなコストで Splunk にプッシュし、Splunk がインシデント対応とエンタープライズレベルの相互関係にはるかなる効果を生みます。Splunk はデータセキュリティツールから危険性のあるイベントのみを受信するため、SOC チームが無関係な生データを苦労して調べるまでもなく容易に解明できます。 この前例のない可視化は、SOC チームが一連のイベントを容易に追跡し、単一ビューで的確にセキュリティインサイトを得られます。

Infosec のリーダー、Splunk データベースのインデックス機能コストを 95%削減

Imperva は、生データをキャプチャして保持し、分析して管理可能な情報にまで落とし込み、重要なイベントを直接 Splunk に転送するという作業をすべて行います。 Imperva はデータをエンリッチ化し、わかりやすいフォーマットで、重要なセキュリティイベントを明確に把握することで、アナリストをより効果的にサポートします。

SOC チームは、Imperva のマイニングで成功を得ます

高性能なプリプロセッサに加えて Imperva 独自の双方向統合をしたことで、Splunk のユーザーは大量のデータセットを Splunk にインデックス付けせずに、Splunk UI を使って Imperva に保存されるすべての生データにシームレスにアクセスできます。

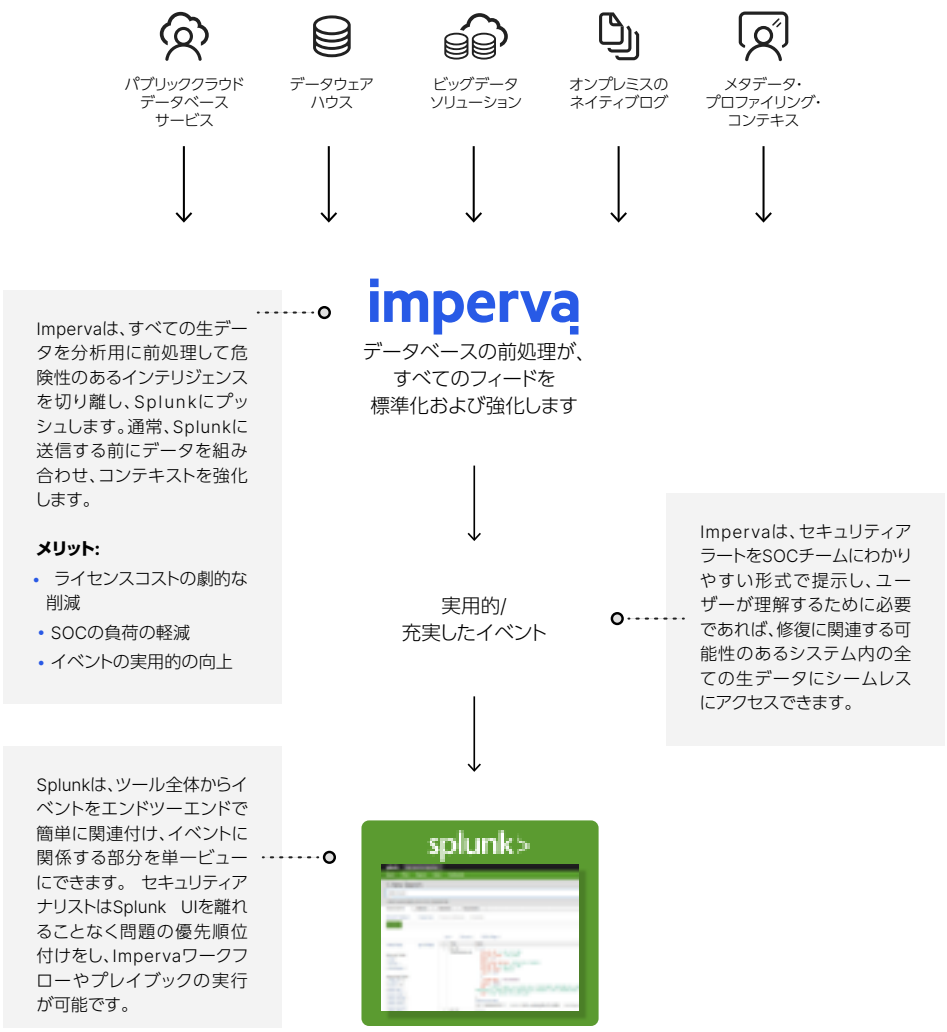
Imperva のプリプロセッサは、Splunk プラットフォームのもう 1 つの主なメリットである異種データのエンドツーエンドの相関を最適化します。

Splunk チームは、ツール全体からイベントをエンドツーエンドで容易に関連付け、イベントに関係する部分を単一ビューにします。 セキュリティアナリストは、Splunk UI を離れることなく問題の優先順位付けをし、Imperva ワークフローやプレイブックを実行できます。

Imperva はすべての生データを分析用に前処理し、危険性のあるインテリジェンスを切り離して Splunk にプッシュします。通常、Splunk に送信する前にデータを組み合わせてコンテキストを強化します。

これにより、Splunk のライセンスコストを大幅に削減し、データベースアクティビティの可視化と維持コスト効率化し、重要なイベントにコンテキストを付加して迅速な修復を実現します。

Impervaは、データやアプリケーションの安全性を追求する、アナリストに認められたサイバーセキュリティのリーダーです。



Copyright © 2020 Imperva. All rights reserved