SPLUNK® USER BEHAVIOR ANALYTICS

サイバー攻撃と内部脅威を検出

- 既知、未知、および隠れたサイバー攻撃と内部脅威の**検出を強化**
- 脅威に優先順位を付け、誤検知を回避して、**セキュリティアナリストの有効性を高める**
- SOC アナリスト、インシデント対応担当者、SIEM 管理者向けの**使いやすさ**

高度なセキュリティ分析

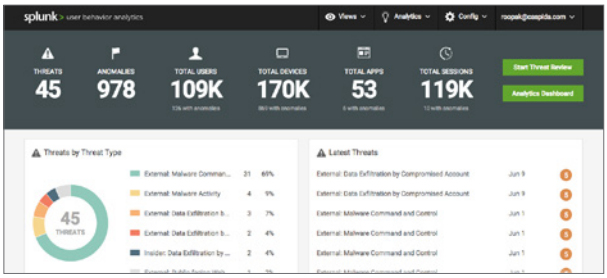
巧妙化したサイバー攻撃は隠れていて検出が難しいものですが、機密データを保護するにはこのような脅威への対応が不可欠です。つまり、今のセキュリティチームには、組織の規模やスキルセットにかかわらず、自社の環境に隠れている脅威を検出して対応するという責務が課せられています。

Splunk User Behavior Analytics (Splunk UBA) は、既知、未知、および隠れた脅威を検出できるようにサポート。多次元の行動ベースライン、動的なピアグループ分析、教師なし機械学習を使用して、データ流出や IP（知的財産）窃取につながる、侵害または不正使用されたアカウントやデバイスを検出します。Splunk UBA は、セキュリティアナリストやセキュリティハンターのワークフローに対応。必要な管理は最小限で済み、既存のインフラストラクチャと連携して隠れた脅威を検出します。

行動ベースの脅威検出とは：行動ベースの脅威検出は、シグネチャや人手による分析を必要としない機械学習方法論に基づいています。ユーザー、デバイス、サービスアカウント、アプリケーションのマルチエンティティの行動プロファイリングとピアグループ分析が可能です。その結果、脅威と異常の高精度な検出が自動化されます。

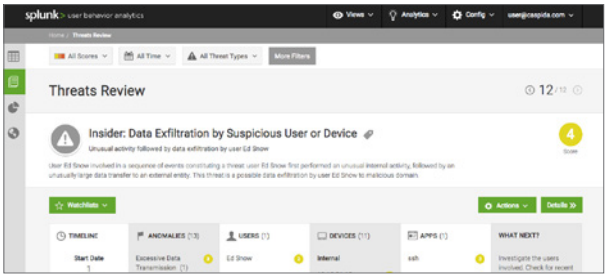
コンテキスト対応のインテリジェンスを提供するには、継続的な監視と高度な分析によって、セキュリティ運用のライフサイクル全体 (防止、検出、対応、緩和から継続的なフィードバックループまで) を統合することが必要です。Splunk Enterprise、Splunk Enterprise Security (Splunk ES)、Splunk UBA が連携して、次のことを実現します。

- 脅威検出技術によって Splunk Enterprise と Splunk ES のサーチ/パターン/式 (ルール) ベースのアプローチを拡張し、巧妙化したキルチェーンを可視化して脅威を検出
- Splunk Enterprise ですぐに利用可能な大規模なデータを活用する、機械学習、統計プロファイリング、その他の異常検出技術をセキュリティチームに提供
- 機械学習手法と高度な分析機能の組み合わせにより、組織の規模やスキルセットにかかわらず、既知および未知の脅威を監視、アラート、分析、調査、対応、共有、検出可能



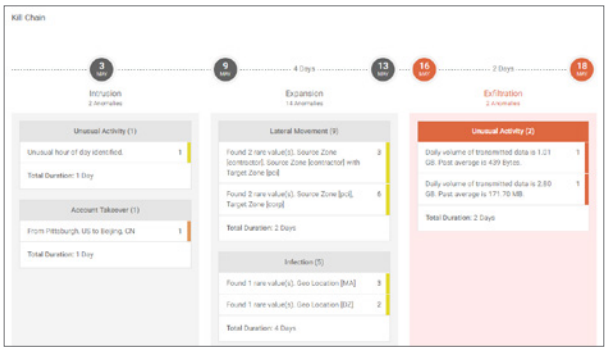
効率化された脅威ワークフロー

数十億件の Raw イベントを、数千件の異常、さらには数十件の脅威へと絞り込み、迅速なレビューと解決を実現。セキュリティの意味に対応した機械学習アルゴリズム、統計、カスタムの ML 主導の異常相関を活用して、人手による分析を行うことなく、隠れた脅威を特定します。



脅威のレビューと調査

キルチェーン内で脅威を可視化して、コンテキストを獲得。これらの脅威は、機械学習の能力によって生成され、ユーザー、アカウント、機器、アプリケーションなど複数のエンティティで確認された異常を、人手による分析を行うことなく、さまざまな攻撃パターンへと組み合わせます。



キルチェーンと攻撃ベクトルの検出

マルウェアまたは悪質な内部脅威者の横展開移動による拡散を検出したり、リアルタイムで検出される異常なアクティビティ (動的に生成されたドメイン名、異常な AD アクティビティなど) に対応したりします。行動ベースの異常 (異常なマシンアクセス、異常なネットワークアクティビティなど) の検出、ボットネットまたは CnC アクティビティ (マルウェアビーコンなど) の特定などを行います。

プラットフォームアーキテクチャとデプロイオプション

Splunk UBA には、拡張性、コスト効率、オープンデータの持続性を実現するために Hadoop エコシステムが含まれています。リアルタイムの大規模イベント分析を目的として設計されており、処理と分析のための時系列とグラフデータベースが含まれています。RESTful API は、データの取り込みから分析までのタスクを自動化。Splunk UBA の拡張性は、数百テラバイト以上のデータと数十億件のイベントに対応できることが実証されています。オンプレミスでソフトウェアとして、仮想マシン上に、またはお客様が管理するパブリッククラウドのインスタンス (AWS) としてデプロイ可能です。

Splunk をダウンロードするか、オンラインサンドボックスをお試しください。Splunk なら、クラウドかオンプレミスか、また組織の規模の大小などにかかわりなく、お客様のニーズに最適なデプロイモデルが見つかります。Splunk User Behavioral Analytics の詳細については、こちらをご覧になるか、ubainfo@splunk.com までお問い合せください。

詳細はこちら：www.splunk.com/ja_jp/talk-to-sales.html
〒100-0004 千代田区大手町1-1-1 大手町パークビルディング 8階

www.splunk.com/ja_jp
splunkjp@splunk.com

PB-Splunk-UBA-A4-107x_JA-201805