Splunk UBAを使用した内部脅威の検出

ハイライト

- **行動モデリングとピアグループ分析によって内部脅威を特定**
- **内部脅威の検出に特化した豊富な異常および脅威モデル**
- **ルール、シグネチャ、人による分析を必要としない、完全自動の継続的な脅威監視**

よく知られているとおり、攻撃やデータ損失の3分の2以上は内部から仕掛けられています。操作ミスやアカウントの乗っ取りによるものもあれば、悪意によるものもあります。そのため企業は常に、従業員、請負業者、パートナーによる疑わしい行動がないか、環境を監視しておく必要があります。その疑わしい行動をつなぎ合わせてパターンを見いだし、すぐに使用できる方法で内部脅威を迅速に示さなければ、データ損失や経済的損失を防止することはできません。

課題

内部者の強み、それは組織内にいること、そして環境にアクセスできることです。境界の防御やルールベースのシステムでは内部者の悪意ある行動を効果的に検出できず、もちろん防ぐことも困難です。そのため、内部脅威は最も捕捉が難しく、重要な企業データや顧客データの流出を成功させる確率が最も高くなります。

内部者はすでに必要な権限を持っているため、ルールベースのシステムやチェックでは、悪意ある行動や疑わしい行動を検出できません。悪意をもって権限を使用したとしても、すべて無害で正当なアクションに見えるため、最新の高度なセキュリティツールさえ突破してしまいます。知的財産の窃盗や金銭目的の不正行為をはじめとする企業犯罪が検出されるころには、すでに手遅れです。

解決策

内部脅威にはさまざまな形態がありますが、ユーザーの行動や資産の動きが過去の履歴や同種のグループの行動から逸脱する、という点は共通です。この逸脱は、不正行為や悪意ある活動のサインである可能性があり、これらの攻撃者を検出するための鍵となります。

エンティティ(特にユーザー、デバイス、システムアカウント、特権アカウント)の行動をマイニングすることで、たとえ発生の間隔が長く頻度が少ない異常でも検出できます。

Splunk User Behavior Analytics (Splunk UBA)はこうした攻撃者が社内、クラウド、モバイルの環境を動き回った痕跡を捕捉するだけでなく、高度な機械学習アルゴリズムでこれらの環境を走査することで、ベースラインの設定、逸脱の検出、異常の発見を継続的に行います。パターン検出と高度な相関付けを駆使してこのような異変をつなぎ合わせれば、やがて意味のあるシーケンスとなり、実際のキルチェーンを明らかにすることができます。このキルチェーンはわかりやすいだけでなく、迅速な対応に活かすことができます。

「私たちの最大の課題は、膨大な資産を抱える銀行ならではといえます。この問題を解決できるのは、行動ベースのアプローチによる従業員監視だけでした」

—米国大手銀行 最高情報セキュリティ責任者

ユーザーとエンティティの行動

内部脅威を特定する際に重要なのは、ユーザーとエンティティの行動とそのコンテキストを理解することです。Splunk User Behavior Analyticsは、疑わしい行動を検出するために、継続的な自己学習によってユーザー、デバイス、アプリケーション、特権アカウント、共有サービスアカウントごとのベースラインを生成します。このベースラインによって、通常からの逸脱を知ることができます。

また、Splunk User Behavior Analyticsではユーザーやアカウントごとに脅威の度合いを示すスコアが付けられます。そのため、内部脅威を日常的に確認できるだけでなく、特に悪質なユーザーを監視して予防策をとることもできます。

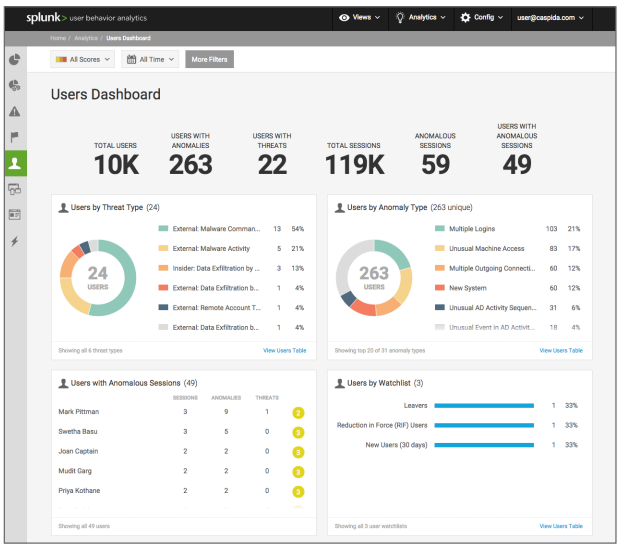
脅威検出の例

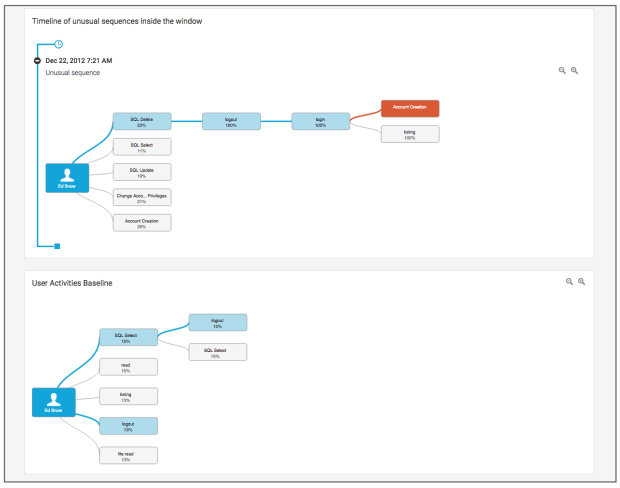
- **特権アカウントの悪用** – アクセス権の不適切な使用
- **権限のエスカレーション** – IDやアクセスの資格情報の変更
- **データ流出** – マルウェアや攻撃者による、組織内の個人データ、内部データ、機密データを盗む行為
- **通常と異なる行動** – 外部ドメインへのアクセスや、権限の高いアセットへのリモートアクセス、および通常とは異なるログイン時間やログイン場所
- **資格情報の侵害**– 悪意のある目的でのアカウントへの不正アクセス

行動分析にSplunkが役立つ理由

機械学習や統計的プロファイリングをはじめとする異常検出技術には、そのための基盤が必要です。高度な分析を支えるために、優れた拡張性を備えた、すぐに使用できるデータプラットフォームが求められます。ユーザーには使いやすさと優れた品質を提供し、広範なセキュリティシステムおよびエンタープライズシステムのデータを網羅するプラットフォームが必要です。コンテキストに適した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)を統合する必要があります。この行動分析の脅威検出機能は、SplunkおよびSplunk ESが脅威検出に使用しているサーチ、パターン、式(ルール)に基づくアプローチを拡張します。

Splunkが提供するデータプラットフォームとセキュリティ分析機能を使用すれば、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の監視、アラート生成、分析、調査、対応、共有、検出を実行できます。





Splunk User Behavior Analytics のユーザーダッシュボード

Splunk User Behavior Analyticsの詳細については、ubainfo@splunk.comまでお問い合わせください。

splunk>
営業へのお問い合わせはこちら：https://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

20-13552-Splunk-UBA to Detect Insider Threats-A4-JA-202012