Splunk UBAを使用したサイバー攻撃の検出

ハイライト

- マルウェア、APT攻撃、隠れた攻撃を検出
- 外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

企業は常に、ハクティビスト、サイバー犯罪者、国家などの外部からの攻撃にさらされています。これらの攻撃の多くは、マルウェア、APT、ゼロデイ攻撃の形態をとり、Webコンテンツ、フィッシング、リムーバブルメディアを介して仕掛けられます。

課題

外部攻撃が成功してしまうのは、攻撃者たちのスキルが高度になったためです。マルウェアはポリモーフィック型となり、一般的なシグネチャやルール、境界ベースの防御メカニズムを突破するようプログラムされています。さらに、いったんネットワークに入り込んだら、ひそかにネットワークを探索し、アカウントを侵害して、価値ある資産を発見するとデータを少しずつ流出させます。画期的な次世代マルウェア対策ソリューションが開発され、脅威インテリジェンスフィードが提供され、さらにはFS-ISACのような連携も行われていますが、こうした「レーダーに映らない」攻撃手法は現代のきわめて高度なセキュリティツールさえも突破します。

解決策

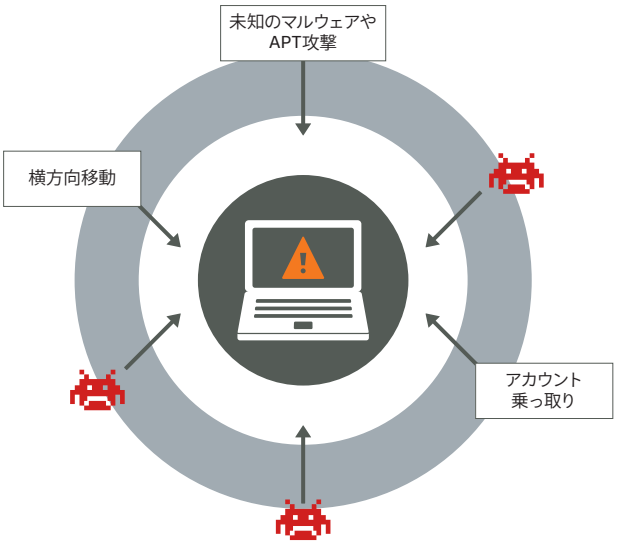
サイバー攻撃にはさまざまな形態がありますが、侵害されたユーザーの行動や資産の動きが過去の履歴や同種のグループの行動から逸脱する、という点は共通です。こうしたエンティティの行動の変化から侵害の指標(IoC)を検出して、脅威の識別に役立てることができます。

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、速やかに対応に活かすことができます。

キルチェーンとは、最終的に侵害を引き起こす、悪意ある一連のアクティビティからなるシーケンスです。多くの場合、シーケンスの各段階において、攻撃者がたどったルートや行動がわかる複数のイベントがあります。既知のしきい値の違反に対するアラートとは対照的に、行動ベースの脅威検出アプローチではコンテキストを重視した機械学習を使用します。そのため、真の隠れた脅威の発見率を最大限に高めながら、誤検出率を最低限に抑えられます。つまりキルチェーンとは攻撃の真の姿を示すものなのです。



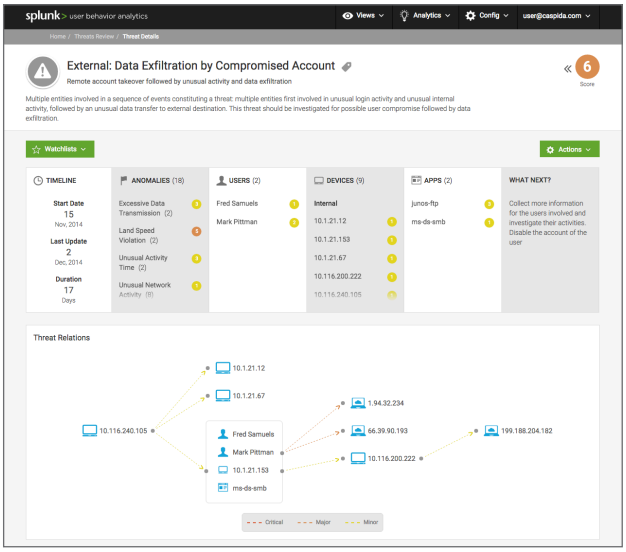
脅威検出の例

- **アカウントの乗っ取り(ATO)** – 悪意ある外部エンティティによる特権アカウントまたは通常アカウントの侵害
- **横方向移動** – ネットワーク内でのマルウェアの動き
- **コマンドアンドコントロール(CnC)アクティビティ** – マルウェアがCnCインフラと通信するために行う周期的なビーコンアクティビティ
- **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
- **ブラウザーのエクスプロイトやマルウェアのアクティビティ** – ポリモーフィック型攻撃とAPT攻撃の感染を検出

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 - 脅威の確認

「大手B2C企業である当社にとって、アカウント乗っ取りは特に厄介な問題です。サイバー詐欺に関するコストは数百万ドルに及び、現在のセキュリティツールではもはや最近の巧妙な攻撃者に太刀打ちできません。必要なのは、新しい行動ベースのパラダイムです」

— 消費者向け大手金融会社、
最高情報セキュリティ責任者

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

20-13557-Splunk-UBA to Detect Cyberattacks-A4-JA-202012