技術概要

Splunk® User Behavior Analytics の使用

Caspida によって強化

製品特長

- 既知の/未知の/隠れたサイバー攻撃とインサイダー脅威の検出を改善
- 誤検出を回避し脅威の優先順位を決めることによって、セキュリティアナリストの効率を向上
- SOC アナリストとインシデント対応者、SIEM 管理者にとって使いやすい

変わりつつある脅威検出の状況

サイバー攻撃は高度化しているため、機密の企業/顧客データの損失を防止できるほど早期に、隠れた脅威を見つけることは困難です。Splunk Enterprise には、脅威に関する隠された情報を含むセキュリティデータが豊富に含まれています。APT やインサイダー攻撃のような高度化した脅威が企業内に隠れている間に、データを分析することによって違反の兆候を探り出すことができます。このような脅威を突き止めたり理解するには、動的で多様な形態の脅威パターンを発見し、数週間/数か月間/数年間にわたる脅威主体の行動を特定する先進的な検出ソフトウェアが必要です。

自動早期違反検出

Splunk Enterprise はオペレーショナルインテリジェンスのためにマシンデータを集約・分析します。そのデータの中に、隠れた脅威を示す兆候が散らばっているのです。Splunk User Behavior Analytics は、Splunk プラットフォームのリポジトリを分析し、以前には検出できなかった脅威(サーバー攻撃とインサイダー脅威を含む)の兆候を突き止めることによって、Splunk プラットフォームを拡張します。

脅威を検出するための機械学習と行動分析

Splunk User Behavior Analytics は、Splunk Enterprise 内の数十億ものイベントを分析します。その際、行動モデリング、ピアグループ分析、グラフマイニング、その他の各種技術を利用して、隠れた脅威を発見し、異常を特定し、次にそれらをつなぎ合わせて実用的な脅威パターンを形成します。Splunk User Behavior Analytics はキルチェーンを介して脅威を可視化し、完全な裏付け証拠を提供します。そのため、セキュリティアナリストは直ちに対策を講じることができます。Splunk User Behavior Analytics はその結果を Splunk App for Enterprise Security (Splunk ES)に送り返します。

Splunk User Behavior Analytics は、時間の経過とともに多くのデータソースにまたがって攻撃と脅威に関する独自の相関とパターン検出を提供します(図 1 参照)。Splunk User Behavior Analytics の相関分析では、機械学習とグラフ分析を利用します。そして、行動分析とともに、以下を自動的に検出する機能によって Splunk Enterprise と Splunk ES を強化します。

- APT、マルウェア、インサイダー脅威
- アカウント情報の漏洩と特権アカウントの不正利用
- ボットネットとマルウェアのビーコニング
- Lateral Movement
- データの不正転送

Splunk User Behavior Analytics は、調査すべき重大な脅威の優先順位リストを提供することによってセキュリティアナリストの生産性を高めます。この手法により、現在のセキュリティソリューションを悩ませている大量のアラートと誤検出を回避することができます。また、分析ワークフローにより、ハンターが異常を調べ、ポリシー違反やデータ不正転送の潜在的意図を探すことが可能になります。

図 1：Splunk User Behavior Analytics ダッシュボード。

Splunk Enterprise Security

Splunk User Behavior Analytics は Splunk ES とシームレスに統合します(図 2 参照)。また、自動的に脅威情報を Splunk ES に入れ、次にその情報が重要なイベントになります。Splunk ES Risk Scoring Framework と Splunk ES Incident Review ワークフローを脅威管理に利用することができます。さらには、Splunk User Behavior Analytics によって発見された脅威によって Splunk ES 内で、改良されたリスク点数が生成されます。この組み合わされたソリューションにより、高度化した脅威(APT、マルウェア、インサイダー脅威など)にも対処できる、完全な脅威検出機能と脅威防止機能が得られます。

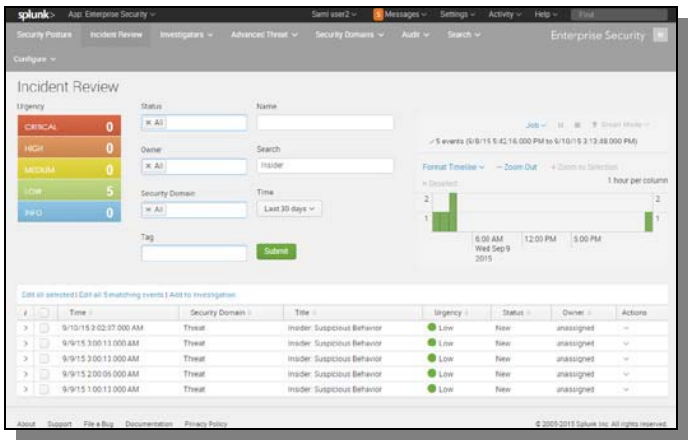

図 2：Splunk Enterprise における Splunk User Behavior Analytics の脅威情報。

Splunk が行動分析を提供する理由？

機械学習と統計的プロファイリング、その他の異常検出技術には基盤が必要です。高度な分析をサポートするには、拡張性が非常に高く容易に利用できるデータプラットフォームが必要です。それは、広範なセキュリティシステムと企業システムから、ユーザーにアクセス性と品質、データカバレッジを提供するようなプラットフォームです。セキュリティ運用のライフサイクル全体（予防、検出、対応、緩和を始め、継続的なフィードバックループまで）を、コンテキストを意識したインテリジェンスを提供するために、連続監視と高度な分析によって統一する必要があります。Behavioral Analytics の脅威検出機能は、脅威を検出するために Splunk および Splunk ES で現在用いられている、サーチ/パターン/表現(ルール)に基づいたアプローチを拡張します。

組織の規模や技能のレベルに関係なく、組織が既知/未知の脅威を監視・警告・分析・調査・対応・共有・検出できるようにする、データプラットフォームとセキュリティ分析機能を Splunk は提供することができます。

Splunk User Behavioral Analytics の詳細につきましては、ubainfo@splunk.com でお問い合わせください。

〒100-6334 東京都千代田区丸の内 2-4-1 丸の内ビルディング 34F　splunkjp@splunk.com　03-6206-3780　splunkbase.splunk.com

Item # TB-Splunk-UBA-108-A4