

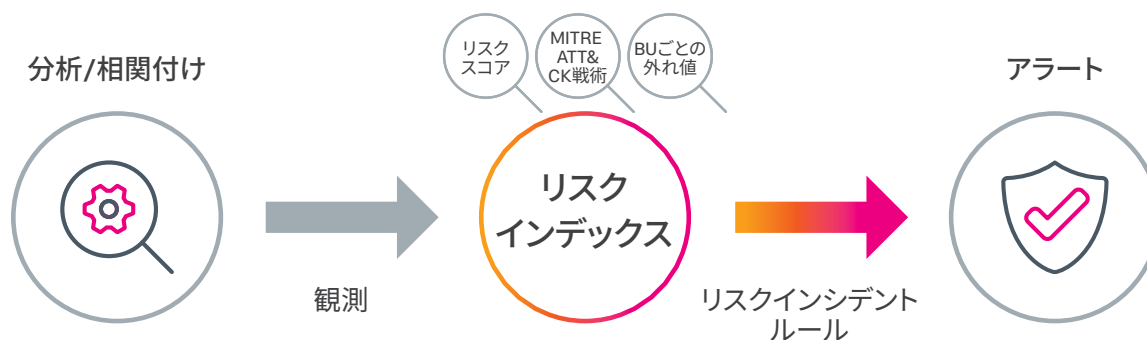
Splunkによるリスクベースアラートの導入

アラートの量を削減しセキュリティ運用を強化

メリット

- **検出の強化**：従来のSIEMでは見逃していた高度な脅威(ローアンドスロー攻撃など)の検出を強化できます。
- **シームレスな連携**：MITRE ATT&CK、キルチェーン、CIS 20、NISTなどのサイバーセキュリティフレームワークとシームレスに連携できます。
- **アナリストリソースの拡大**：アナリストのリソースを拡大して、SOCの生産性と効率を最適化できます。

RBAがアラート量を削減する仕組み



SOC（セキュリティオペレーションセンター）は大量のノイズで溢れており、毎日何万件ものアラートに対して限られたリソースで対応しています。そのため、最も優先度の高いアラートのみが調査され、そのほとんどが後で偽陽性と判断されるか、もしくはそのまま放置されています。このような状況を改善しようと相関サーチの「徹底」にリソースを費やしても、皮肉にもさらなるノイズを生み出してしまいます。また、もう1つの方法であるアラートの抑制でも、セキュリティの対象範囲に意図しない盲点が生じ、脅威の検出と調査を一層困難なものにしています。しかし、もっと良い方法があるはずで

Splunk® Enterprise Security (ES)は、SOCの運用に必要な新しいリスクベースアラート機能を提供します。これによってSOCは、重要な課題である「過剰なアラート」に対処できます。何らかの不審なアクティビティが発生した場合、アナリストはエンティティ（ユーザーやシステムなど）のリスク属性を作成します。その属性は、アラートをトリガーするのではなく、リスクインデックスに送信されます。チームは、関連するMITRE ATT&CK技法に照らして注釈

を付けたり、リスクスコアを適用したりするなど、関連するコンテキストを追加することでリスク属性を補完することができます。エンティティのリスクスコアや行動パターンが定義済みのしきい値に達すると重要なイベントが起動され、調査プロセスの開始時にはアナリストに有用なコンテキストが提供され、脅威を迅速に無力化することができます。RBAのメリットは、こうした機能強化だけではありません。

リスクベースのアプローチは、SOCのリソースを従来の事後対応型から事前対応型へと転換するためのまたとない機会をチームにもたらします。アラートの忠実度と真陽性率が上がるにつれて、アナリストのリソースを脅威ハンティングや攻撃手法シミュレーションなど、より影響力の大きいタスクに移行できるようになるため、SOCはアナリストのスキルセットを強化して未知の脅威に備えることができます。また、アナリストが多くのセキュリティ調査を効率的に行えるようになるため、ストレスが軽減し生産性も向上します。

サイバーセキュリティフレームワークの運用化

Splunk Enterprise Securityでは、MITRE ATT&CK、CIS 20、NISTコントロールなどの主要なサイバーセキュリティフレームワークをすぐに使用できます。選択したフレームワークを検出プロセスに組み込むことで、セキュリティの重要な概念をセキュリティ運用の基盤と統合することができます。こうしたフレームワークに基づいて、攻撃手法のシミュレーションなどのプロアクティブな演習を実施できます。

また、必要なフレームワークを使用して、セキュリティの対象範囲内におけるギャップ(MITREのどの検出方法でカバーしているかなど)を定量化し、セキュリティ強化のためにどのようなデータソースを追加する必要があるかを判断できます。

複雑な脅威の検出

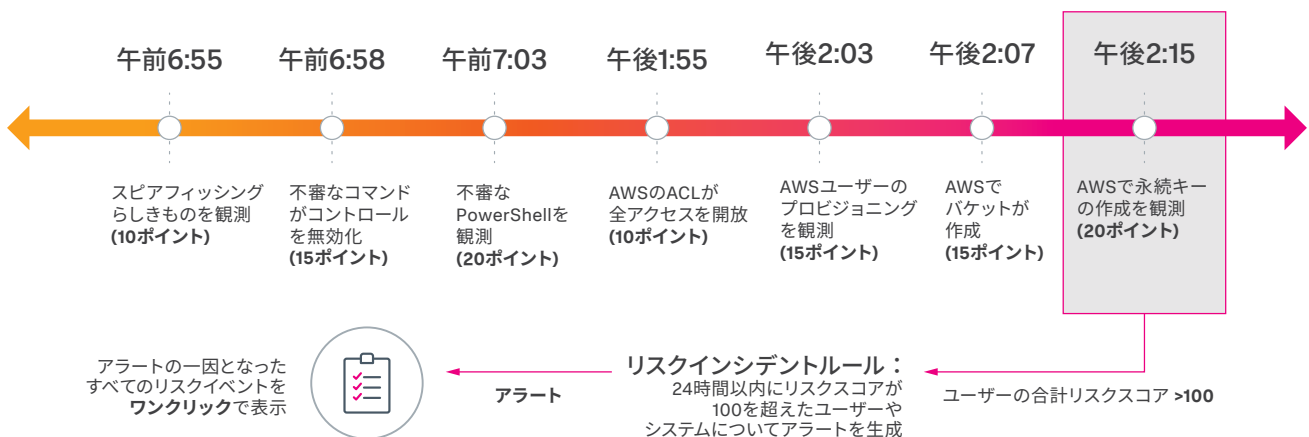
従来型のSIEMにとって、複雑な脅威の検出は大きな課題でした。さまざまなアラートが大量に発生するため、ローアンドスローのような攻撃を検出するのは至難の業です。また、生成されたトラフィックと通常のトラフィックを区別するのも容易なことではありません。しかし、リスク属性の包括的なコレクションを作成することで、長期間にわたる検出を簡単に実現できるだけでなく、攻撃者がローアンドスロー手法を使用することも極めて難しくなります。たとえば、あるエンティティの行動が2週間にわたって3つ以上のMITRE ATT&CK戦術に該当した場合にアラートを発生させるといった設定ができるため、攻撃対象の保護範囲を効果的に拡大できます。

調査と修復の効率化

Splunk® Phantomの自動化機能を使用すると、セキュリティインシデントのトリージア作業に必要な時間を短縮できるほか、調査プロセスに詳細なコンテキストを取得できます。SOCは、侵害の痕跡(IOC)をはじめとした忠実度の高い重要なイベントをSplunk Enterprise SecurityからSplunk Phantomへとシームレスに共有できます。そのため、Phantomは関連する属性をすべて同時に自動で調査することができます。IP、ドメイン、URL、ハッシュなどをキューに追加し、自動的にブロックすることも可能です。こうした機能により、環境内に存在するリスクの高いデバイスやユーザーを、人手を介さずに確実かつ瞬時に検疫したり無効化したりすることができます。また、セキュリティチームは時間に余裕が生まれ、SOC内の付加価値の高いほかの作業に注力できるようになります。

実際の流れ

リスクベースアラートでは、これらのイベントがコンテキストとなり、忠実度の高いアラートを生成



RBA が組織のセキュリティ運用の強化にどのように役立つかをご覧ください。 [デモを見る](#)