# Splunkによる高度な分析と脅威の検出

Splunk Enterprise SecurityとSplunk User Behavior Analyticsの活用

セキュリティの脅威は、規模も巧妙さも進化を続けています。未知の脅威、隠れた脅威、内部脅威を早期に発見して高度な攻撃者に先手を打つことは、ますます難しくなっています。判明している既知のルールセットとシグネチャに頼った従来のセキュリティツールは、既知の脅威を検出することには長けています。しかし、内部脅威、ゼロデイ攻撃、横移動するマルウェア、アカウント侵害をはじめとする高度なセキュリティ脅威は複雑であり、従来のツールでは完全には対応できません。また、SOCでは常に大量のアラートが発生しており、その多くは誤検知です。脅威が進化し続ける状況では、セキュリティチームに新しい分析機能を導入し、潜在的な脅威を見つける新たな視野を獲得する必要があります。

## 攻撃の早期検出の自動化により高度な脅威の調査を迅速化

Splunk Enterprise Security (ES)は業界屈指の分析主導型SIEMソリューションです。全社を網羅して脅威、攻撃、その他の異常なアクティビティを検出、監視、調査し、対応、レポート生成を行います。ビッグデータプラットフォームを基盤としており、あらゆるセキュリティ関連データに対応できる優れた拡張性と可視性を提供します。さらに、ビジネスのコンテキストを補完し、強力かつ実用的なインサイトを提供します。Splunk User Behavior Analytics (UBA)は機械学習ベースのソリューションです。未知の脅威やユーザー、エンドポイントデバイス、アプリケーションによる異常な行動を検出します。

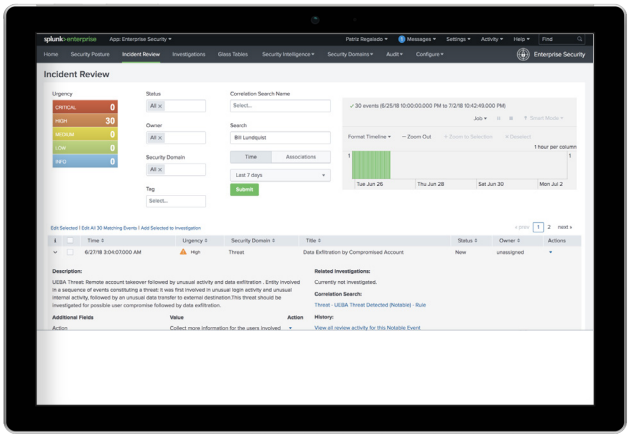
Splunk ESとSplunk UBAを組み合わせることで、きわめて巧妙な脅威にも速やかに対応できます。ワークフローの一環として異常や脅威の共有と相関付けが行われるため、インシデントの統合ビューに表示されたリスクスコアを見ながら、優先度を付けて迅速に調査を進めることができます。Splunk UBAは脅威の情報をSplunk ESに自動的にプッシュし、Splunk ESはその情報を重要なイベント

## 機械学習のメリットをSOCで活用

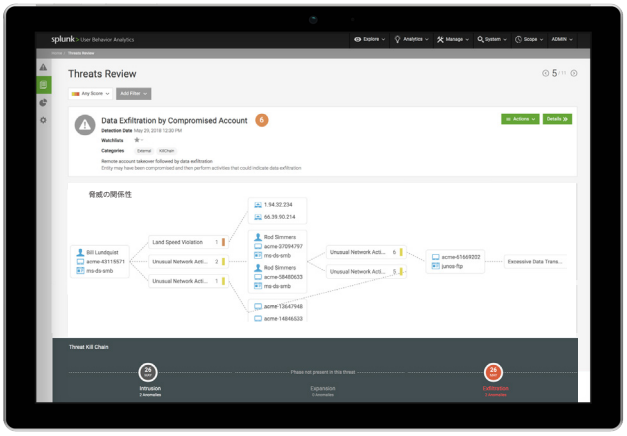
セキュリティにおける機械学習のメリットは明らかです。機械学習を利用することで、セキュリティインシデントに対する分析、対応能力を高め、脅威への体制を強化するとともに、リスク全体を最小化できるようになります。しかも、コストの削減や、限られたリソースへの負担の軽減も同時に実現できます。

機械学習は高度な脅威検出や内部脅威への対策などのセキュリティユースケースに最適です。こうした場面では、監視と対応を行うためのより繊細なシステムが必要とされるためです。ネットワーク内での横展開移動や、特権ユーザーの侵害、意図しないユーザーの機密情報へのアクセスなどを含む高度な攻撃も、機械学習を利用した異常の自動検出機能があればすべて対応できます。

分析チームやSOCチームは、機械学習を組み込むことで、迅速な調査の実施や有意義なインサイトの取得、インシデントの根本原因の判断、過去のトレンドの活用、検出内容の共有が可能になり、何千ものアラートや誤検知によって忙殺されることがなくなります。つまり、どのようなセキュリティインシデントであっても、よりスピーディーに検出し、影響を分析して迅速に対応できるようになります。



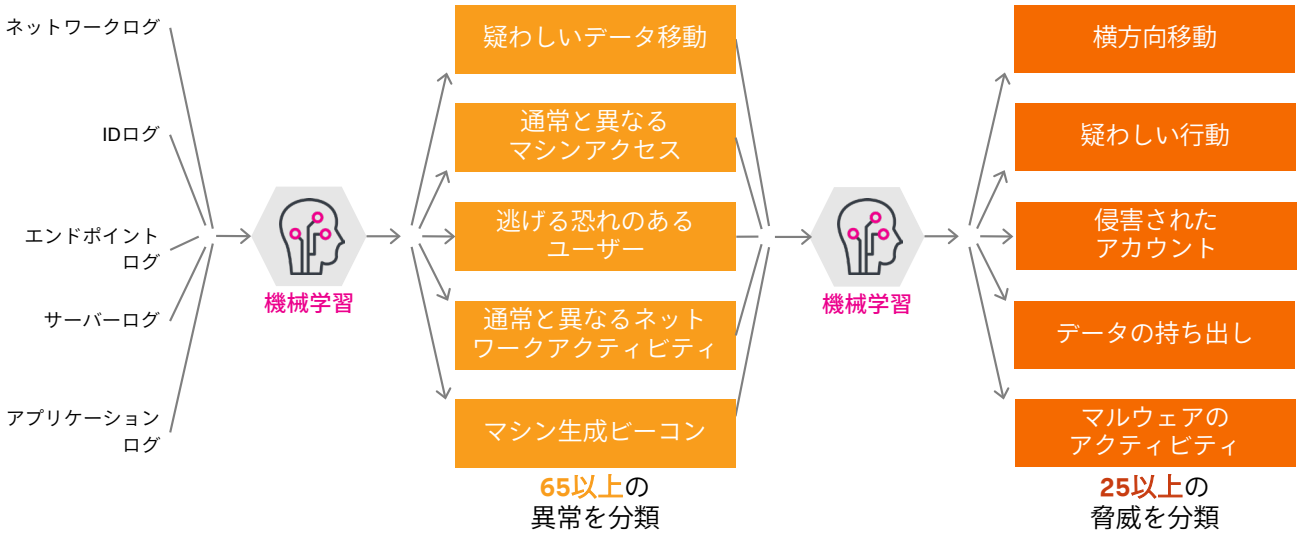
として処理します。Splunk UBAが検出した脅威はSplunk ESのリスクスコアアルゴリズムによって処理されるため、Splunk ESのリスクスコアフレームワークとインシデントレビューのワークフローで脅威の管理を継続できます。Splunk ESでの人間による相関付けルールやサーチに、Splunk UBAの教師なし機械学習をベースとした脅威相関付けによる未知の脅威の検出を組み合わせることで、脅威をいち早く検出できます。




## 機械学習を活用してSIEMを補完し、SOCの作業を効率化

Splunk ESの人間主導の脅威検出と、Splunk UBAの機械主導の脅威検出という強力な組み合わせにより、ルールベースの相関付けでは検出できなかった脅威も機械学習で速やかに検出できるようになり、アナリストの作業時間を短縮できます。Splunk UBAは、収集した異常に対して2階層の機械学習システムを適用します。これによって重要度の高い脅威のみを検出できるため、SOCの効率が向上します。

Splunk UBAが検出した行動の異常をSplunk ESに取り込めるようにすることで、Splunk ESの重要なイベントに既知および未知の脅威に関するコンテキストを付加して、脅威に関する精度と忠実度を向上させることができます。Splunk UBAの強力な機械学習アルゴリズムを使用すると、多くの異常を自動的に関連付けて1つの脅威にたどり着くことができます。アラートはSOCチームが見る前にフィルタリングされるため、緊急性の高い脅威や複雑な脅威に多くの時間を割けるようになります。高いスキルを持ったセキュリティ担当者やデータサイエンスのプロフェッショナルチームを大量に採用する必要もありません。



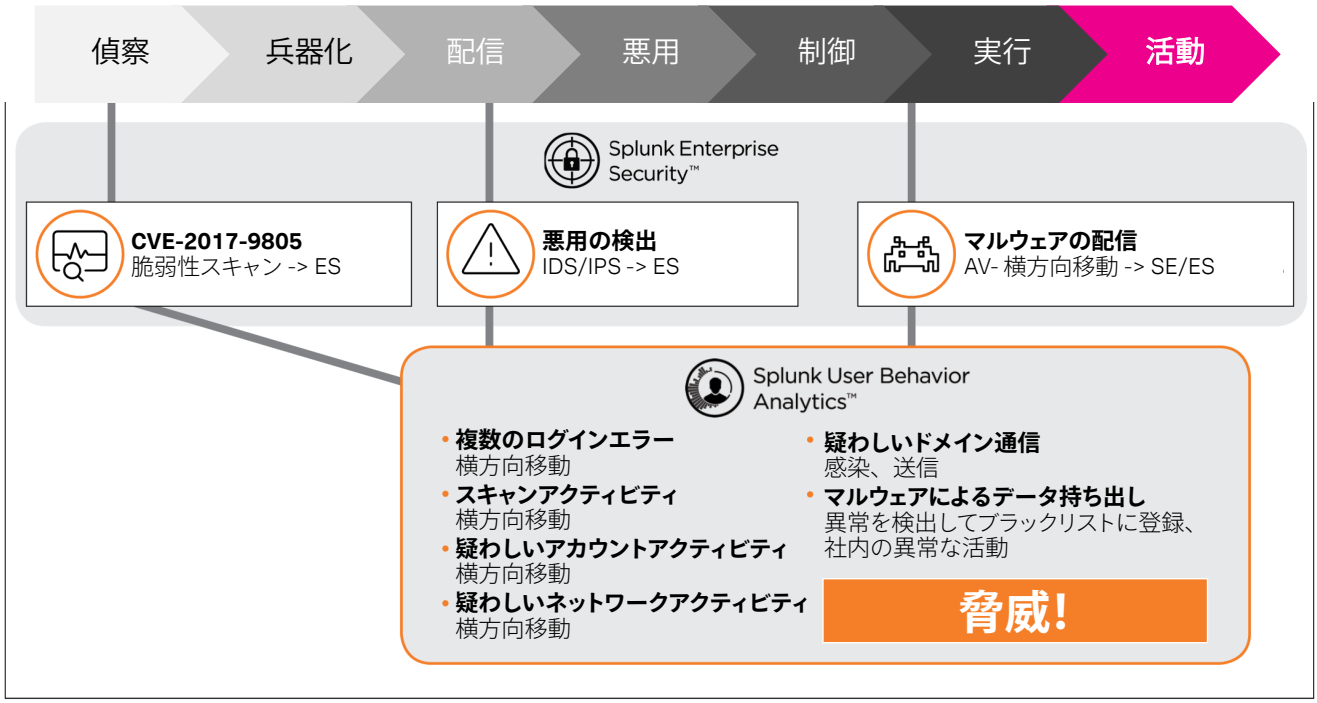
## SIEMとUBAの脅威インテリジェンスを統合し、内部脅威検出の最適化と未知の脅威の検出を実現

未来の攻撃は、現在の攻撃手法とは異なるかもしれません。そのためSplunk UBAは、内部脅威に対する防御と高度な脅威の検出に有効なデータサイエンスや教師なし機械学習を駆使して、隠れた脅威や未知の脅威を自動的に検出します。Splunk UBAの複数エンティティに関する異常行動および脅威情報をSplunk ESに取り込むことで、両製品の強みを活かすことができます。ユーザー、デバイス、アプリケーション関連の異常について、より詳細なコンテキストが得られるようになり、脅威に対する検出と対応が向上します。Splunk UBAの脅威検出機能は、Splunk ESが脅威検出に使用しているサーチ、パターン、ルールベースのアプローチを拡張します。さらに機械学習を使用したSplunk UBA独自の相関付けとパターン検出、グラフ分析、行動分析が加わることで、Splunk ESでは内部脅威、アカウント侵害、特権アカウント悪用、横方向移動、データ流出など多岐にわたる高度な脅威を自動的に検出できます。

また、Splunk ESとSplunk UBAでは動的かつ継続的にセキュリティコンテンツが更新されます。そのため、常に最新の脅威検出方法でプロアクティブな体制を維持できます。Splunk ESとSplunk UBAを組み合わせることで、隠れた潜在的なインシデントを明らかにし、高度な脅威に先手を打って速やかに対応できます。

### UBAが脅威の調査の精度を高め、調査範囲を拡大

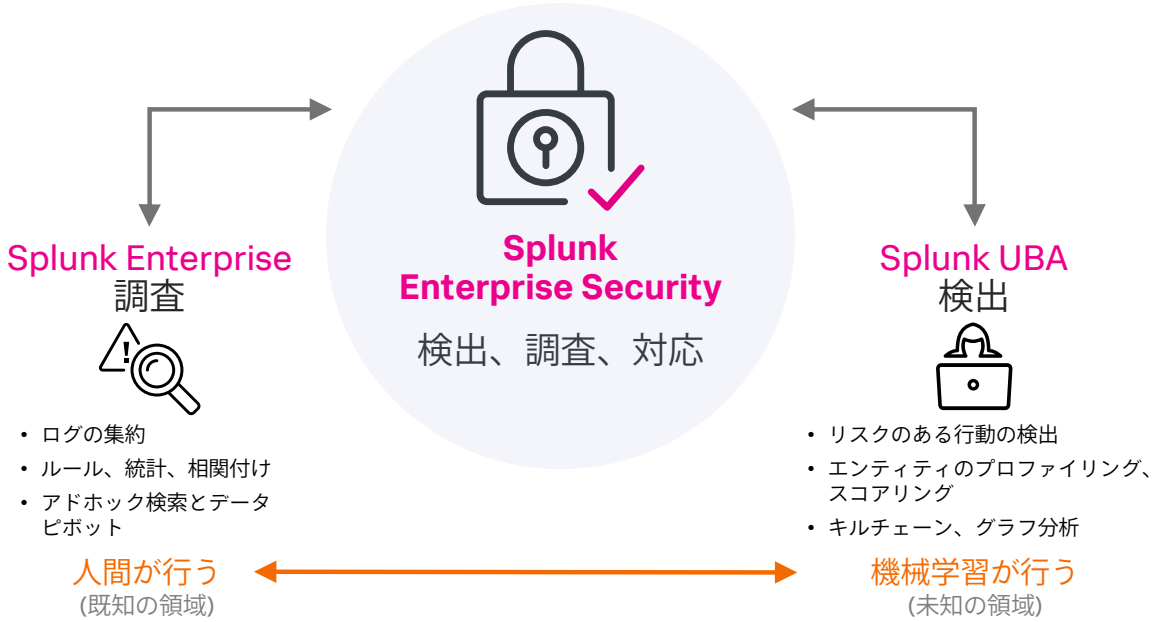
攻撃のキルチェーン



## 機械学習と行動分析を搭載した、実績ある分析主導型SIEM

Splunk ESは従来のSIEMテクノロジーのはるか先を行くソリューションです。詳細な調査と迅速な対応を可能にするだけでなく、重要なイベント、リスクスコア、脅威インテリジェンスなど、情報に基づいた意思決定を支援するセキュリティフレームワークを提供します。このフレームワークによってデータがコンテキストで補完され、調査を速やかに進める上で必要なインサイトが得られるようになるため、検出と対応を迅速化できます。Splunk ESをSplunk UBAで強化すれば、データサイエンスの力をイベントベースの相関付けと臨機応変な検索とともに活用して、会社全体で優れたインサイトを得ることができます。

また、Splunk ESとSplunk UBAを組み合わせることで、機械学習、異常なユーザー行動の検出、コンテキストで補強した相関付け、迅速な調査機能が統合されて効果を発揮します。この統合ソリューションにより、インシデントの調査と管理を一元的に可視化できるため、SOCチームは優先度付けされた精度の高い脅威に速やかに対応できます。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(検出、調査、防止、対応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。このビジョンを実現するには、Splunk ESとSplunk UBAを組み合わせたソリューションが最適です。




既存の投資に含まれるSplunk ESとSplunk UBA機能を使用してセキュリティ成熟度を高めることにご興味をお持ちいただけましたか？詳しくは、**Splunkの営業担当者**にお問い合わせください。セキュリティエキスパートがご相談に対応します。

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



20-13551-Splunk-Advanced Analytics and Threat Detection-A4-JA-202012