重要ポイントのまとめ

Splunk Enterprise Securityのユースケーストップ5

splunk>
a CISCO company

セキュリティイベントを迅速に検出して対応するのは簡単なことではありません。セキュリティアナリストが1件のアラートを処理するのに、数日とまではいかなくても数分はかかることがあります。これでアラートの数が数千に及ぶとなると、チケットが多すぎるのに対してアナリストが少なすぎることがわかります。問題が見えてきたのではないでしょうか。

発生するアラートの数を減らすとともに、セキュリティチームが対応時間を短縮できるようにすることが必要です。その第一歩となるのは、チームが脅威をより迅速に検出して対応できるように、環境に対する可視性を向上させることです。さらに、アラートのトリアージに自動的に対応すれば、数分かかっていた時間を数秒に、また数時間を数分に短縮することができます。

これにより、マルウェアのような検出が困難で巧妙な脅威が隠れたり拡散したりする場所を減らし、脅威がもたらす損害額を減らすことができます。ストレスのたまったセキュリティアナリストもずっと楽になります。

つまり、アラートの数を減らし、統合された効率的な作業プロセスを構築することが重要です。そのためには、AIエージェントを活用して調査を迅速化し、クラウド、オンプレミス、ハイブリッド環境全体を包括的に可視化する必要があります。適切なソリューションを導入すれば、アラートの量を最大で80%削減し、アナリストの生産性を大幅に向上させ、自信を持ってイベントに対応できるようになります。

それを実現するのが、市場をリードするSplunkのSIEM (セキュリティ情報/イベント管理)ソリューション、**Splunk Enterprise Security** (ES)です。Splunk ESは、SIEM、**SOAR** (セキュリティのオーケストレーションと自動化によるレスポンス)、**UEBA** (ユーザーとエンティティの行動分析)、脅威インテリジェンス、検知エンジニアリングの機能を統合し、組み込みのAIによって脅威の検出、調査、対応(**TDIR**)ワークフローを効率化して、AIを活用したセキュリティ運用を支える最高峰のプラットフォームです。

適切な基盤を確立すれば、成果の実現を加速させ、リスクを低減し、エージェント型AIの時代に求められるレジリエンスを構築できます。このクイックガイドでは、Splunkのお客様が課題解決のために実践している5つの主要なユースケースをご紹介します。アラートの削減から、統合的な可視化、自動化の拡大まで、これらのユースケースは、セキュリティチームがセキュリティ強化のどの段階にあってもすばやく成果を達成するために参考になるはずです。

1. リスクベースアラートとエージェント型AIでアラートを削減

多くのSOC (セキュリティオペレーションセンター)は大量のアラートに圧倒されています。アラートの中には誤検知や重複するシグナルが数多く含まれ、膨大なノイズによって真の脅威を見落としてしまうこともあります。アナリストは複数の異なるツールを行き来し、行き詰まりを繰り返すことを余儀なくされ、やがて疲労が限界に達することも少なくありません。

Splunk Enterprise Securityのリスクベースアラートは、アナリストの効率を低下させる手作業を削減します。リスクの原因をユーザーやエンティティに関連付け、特定のリスクや行動のしきい値を超えたときにアラートをトリガーすることで、誤検知を最大で80%削減します。

アラートの量が減れば、脅威検出を最適化して、真陽性率を高めることにつながります。また、リスクベースアラートなら、従来の相関サーチでは見逃されていたローアンドスロー攻撃などの高度な脅威も検出できます。さらに、時間とリソースを実際の複雑な脅威に費やせるようになり、業界標準のサイバーセキュリティフレームワークに沿って運用できるようになります。

そこにエージェント型AIを取り入れれば、ノイズへの対応を短期間でさらに効率化できます。エージェント型AIは、セキュリティの自動化の新たな段階を示し、アナリストを支援するだけでなく、アナリストに代わって作業を行います。これにより、アナリストは本当に重要な業務に集中でき、調査が加速するため、大規模な増員を行うことなく効率的に対応能力を強化できます。AIを最新のSOARソリューションに組み込めば、定型的なタスクを自動化し、アラートにリアルタイムで情報を補強して、TDIRワークフロー全体をスピードアップできます。

SOC全体で、AIは、膨大な量のテレメトリを数秒で分析し、リスクスコアに基づいてアラートに優先順位を付け、推奨される修復手順を提案して、複数のツール間でワークフローを連携させます。そのため、AIドリブンの自動化を取り入れれば、MTTD (平均検出時間)とMTTR (平均対応時間)を大幅に短縮できます。

2. データを完全忠実に可視化

クラウドへの移行は柔軟性を高めますが、同時にデータ環境の分散とサイロ化を生みます。そこでセキュリティチームは、非常に難しい選択を迫られます。アマゾン ウェブ サービス、Azure、GCP、SaaS、オンプレミスにわたって、コストを度外視してでも重複するストレージを持つのか、危険な盲点を生むことになってもストレージを分散させるのかという問題です。Splunk Enterprise Securityは、これらのギャップを解消し、データの柔軟な転送、階層化、アクセスを可能にします。さらに、1つの統合的なプラットフォームで、ハイブリッド環境やマルチクラウド環境のテレメトリを横断的に相関付けることができます。これにより、包括的な可視化とTCO (総所有コスト)の削減を両立し、M&A、新しいアプリケーションの導入、インフラの進化など、ビジネス環境の変化に適応するための俊敏性を向上させることができます。Splunkは、あらゆるシグナルを可視化し、コンテキストを提供し、実用的なインサイトを導出することで、SOCが将来の変化にも対応できる安心感をもたらします。

3. AIドリブンのワークフローで調査を加速

連携しないツールや手動の作業が重荷になって調査が停滞することがよくあります。アナリストが、さまざまな証拠をつなぎ合わせ、クエリーをゼロから書き、レポートの草案を練るのに時間を取られている間にも、攻撃者はシステム内で活動を続けています。Splunk Enterprise Securityは、TDIRワークフローにAIを直接組み込むことで、プロセスに変革をもたらします。

アナリストは、平易な言葉で複雑なSPLサーチを生成し、結果を自動的に要約できます。さらに、次のステップに関する提案を受け取ることもできます。また、統合されたケース管理機能によって、メモ、ファイル、脅威インテリジェンスを1カ所に集約できるため、コンテキストを維持したまま、シームレスに引き継ぐことができます。これにより、数日かかっていた作業が数分で完了します。アナリストの生産性が向上し、ドキュメントの一貫性が保たれ、SOC全体で、最も必要なときに可視性とスピードを発揮できます。

4. 自動化とコンテキスト補強をSOC全体で活用

多くのSOCでは、自動化が強力な武器になるにもかかわらず、十分に活用しているのは複雑なSOAR環境を運用できる上級者に限定されがちで、それ以外のメンバーは手作業に追われ、ボトルネックを抱えて、燃え尽き症候群に陥っています。Splunk Enterprise Security Premierは、SOARをネイティブに組み込むことでこの状況を一変させ、あらゆるアナリストが自動化の恩恵を受けられるようにします。

AIを活用したプレイブックの作成では、ワークフローを自然言語で説明するだけで、テスト済みの実行可能なプレイブックを誰でも作成できます。また、自律型の対応エージェントでは、脅威を自動ですばやく封じ込めながら、人間の関与を維持できます。このように、SOC全体で自動化を民主化し、対応手順を標準化することで、脅威を迅速に封じ込め、すべてのアナリストが効果的に対応できるようになります。そして最終的に、手作業をなくし、対応の一貫性、スピード、規模を向上させて、セキュリティ態勢を強化できます。

5. 検出のギャップを埋めてMTTD（平均検出時間）を短縮

サイバー攻撃は絶えず進化しており、検出がほとんど追い付かない状況です。多くのSOCは、自分たちがどのような攻撃戦術に対応できるかを十分に把握していません。その結果、盲点が生まれ、脅威のリスクが大きく高まります。Splunk Enterprise Securityは、脅威に先手を打つために必要な可視性と精度を実現します。

検知エンジニアリングのライフサイクル全体をカバーするDetection Studioでは、完全忠実な検出ルールを自信を持ってテスト、デプロイ、監視できます。リアルタイムのMITRE ATT&CKマッピングには、十分にカバーできている領域と強化が必要な領域が正確に示されます。また、Splunk脅威調査チーム(STRT)とCisco Talosが提供する厳選されたコンテンツにより、新たな戦術、技法、手順(TTP)に対応した最新の検出ルールを構築することもできます。これによって、SOCは、攻撃が起きてから対応するのではなく、プロアクティブにギャップを解消し、カバー範囲を拡大して、見落とされがちな攻撃のリスクを低減できます。

侵害への対策を万全にしましょう

こちらから、AIを活用したSplunkのセキュリティ運用プラットフォームの詳細をご確認ください。

splunk> a cisco company

26_CMP_listicle_The-top-5-use-cases-for-splunk-enterprise-security_v4-JA-202603