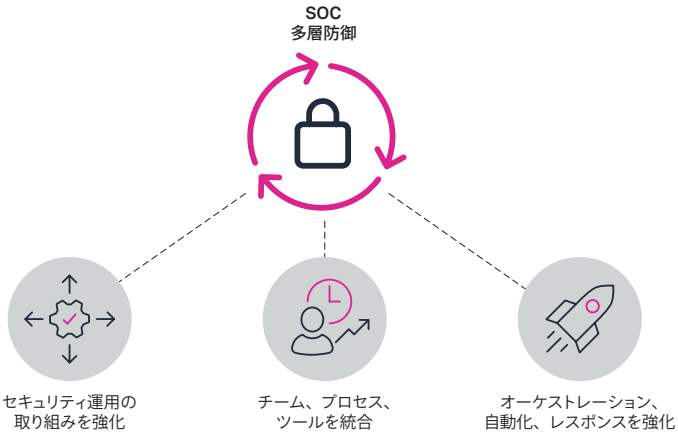
Splunk Phantom

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(SOAR)機能によって
SOCの効率を最大化

- **セキュリティ運用の取り組みを強化し、**セキュリティスキルのギャップを解消
- **チーム、ツール、プロセスを統合し、**SOC運用の効率化を実現
- 高度なオーケストレーション、自動化、レスポンスによって、**SOC運用を大幅に強化**

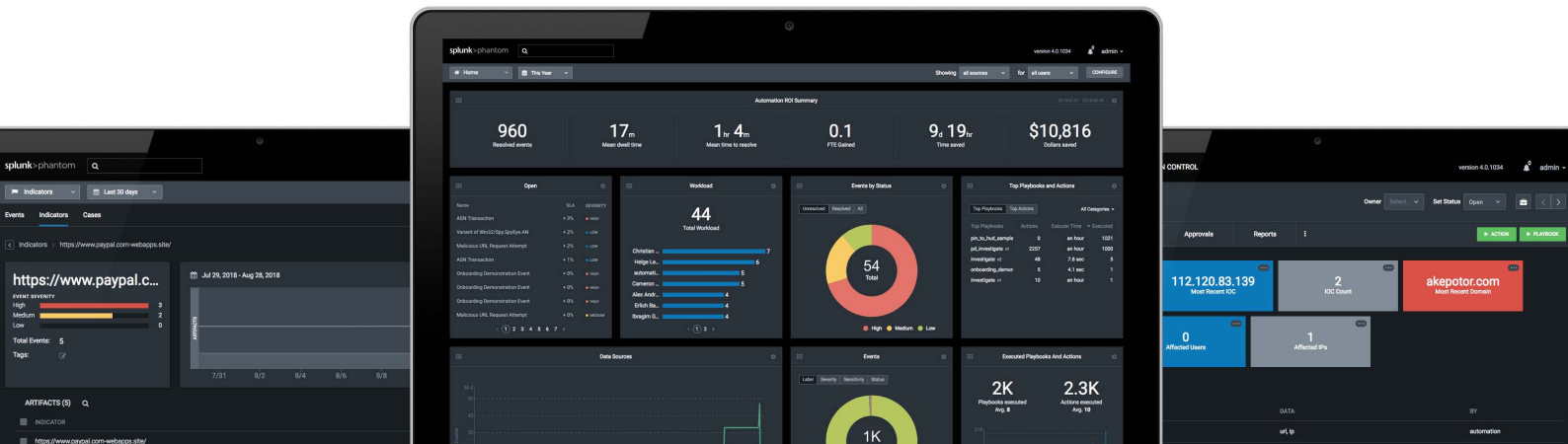


セキュリティチームは組織が直面する脅威を特定し、分析、軽減しようと懸命に取り組んでいます。

しかし、セキュリティ製品は独立して動いており、他のセキュリティ製品との連携がないため、全体としての対応策を考えなければならないという課題も抱えています。しかも、ほとんどの企業には日々発生する大量のセキュリティアラートを分析するために十分なセキュリティ担当者がいないため、結果として未処理のセキュリティインシデントが増え続けています。

組織は、効率と拡張性を最大化するツールを導入しながら、機能を単に寄せ集めたよりも効果的な、統合された防御システムを構築することで、既存のリソースをより有効に活用したいと考えています。

Splunk® Phantomでは、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(SOAR)機能を使用してアナリストの業務効率を向上し、インシデントの対応時間を短縮できます。1時間あたり5万件のセキュリティイベントを処理できるため、セキュリティの自動化における拡張性、パフォーマンス、スピードが大幅に向上します。また、チーム、プロセス、ツールを統合することで、セキュリティを強化し、リスクをより効果的に管理できます。セキュリティチームは、タスクを自動化し、ワークフローをオーケストレーションするとともに、イベントやケースの管理、コラボレーション、レポート作成などの幅広いセキュリティオペレーションセンター (SOC)機能をサポートできます。



SOC自動化

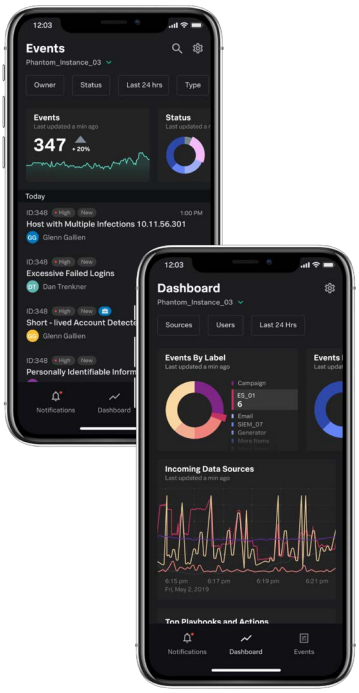
Phantomを使用すれば、作業を自動化して業務を効率化できます。セキュリティインフラストラクチャ全体で、手作業で行うと数時間以上かかる作業をわずか数秒で実行できます。コーディングが不要な視覚的なエディターまたは内蔵のPython開発環境を使用して、ワークフローをPhantomの自動化プレイブックにコード化することもできます。このように定型作業の負担を軽減すれば、チームはより中核的な業務に集中できます。

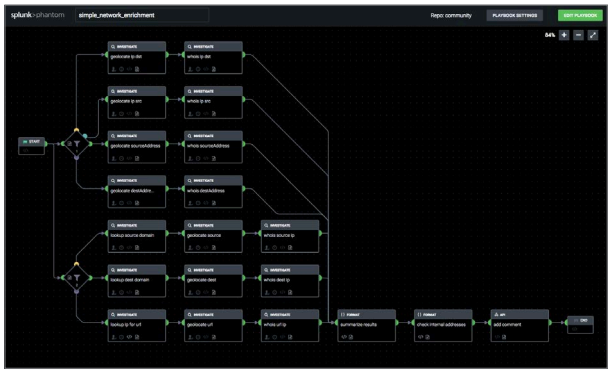
オーケストレーション

Phantomを導入すれば、既存のセキュリティツールを統合してより効果的に連携させることができます。SOCの複数のメンバーやツールがかかわる複雑なワークフロー間の連携と調整を強化することにより、SOCの多層防御の各部を総合的な防御戦略に密接に統合できます。また、高度な抽象化によって、チームの目標がツール固有のアクションに変換されるため、チームは目標達成に集中できます。

インシデント対応

Phantomを使用すれば、セキュリティチームは脅威を迅速に調査して対応できます。Phantomの自動検出、調査、対応機能によって、対応アクションをマシン並みのスピードで実行し、マルウェアの潜伏時間を減らして、全体的な平均復旧時間(MTTR)を短縮できます。さらに、Splunk MobileのPhantomを使用すれば、アナリストは外出中でもモバイルデバイスからセキュリティインシデントに対応できます。Phantomのイベントおよびケース管理機能では、セキュリティ運用を一層効率化できます。一元的な中央リポジトリから、ケースに関連するデータやアクティビティに簡単にアクセスできます。イベントやケースについて他のチームメンバーとチャットしたり、イベントやタスクを適切なチームメンバーに割り当てたりするのも簡単です。





さらに詳しい情報が必要な場合
Splunk Phantomの無料のコミュニティエディションをダウンロードしてお試しください。

splunk>
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

20-14148-splunk-phantom-maximize-your-soc-efficiency-with-soar-PB-A4-JA-202010