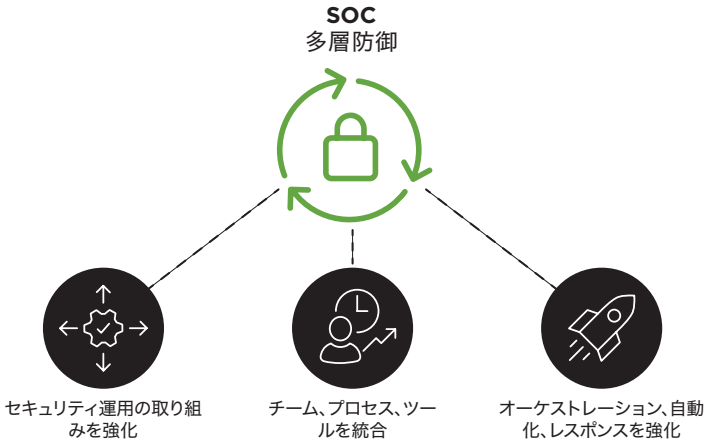
SPLUNK® PHANTOM

SOAR による SOC運用 の効率化を実現

- 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インシデントを分析するための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。

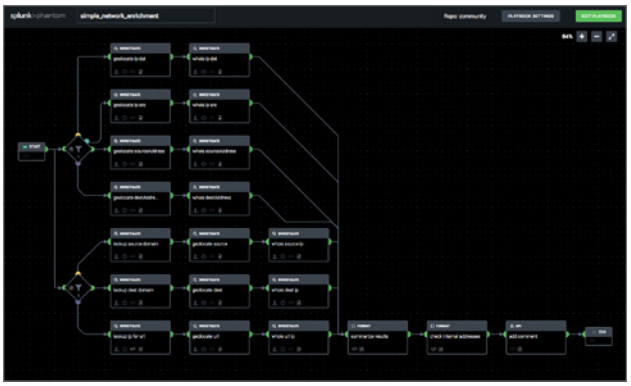
組織は、効率と拡張性を最大化するツールを導入しながら、機能を単に寄せ集めたよりも効果的な、統合された防御システムを構築することで、既存のリソースをより有効に活用したいと考えています。

Phantom はセキュリティチーム、プロセス、ツールを統合することによって、よりスマートな作業と脅威への迅速なレスポンス、防御体制の強化を実現します。

Splunk Phantom 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) 機能によって、アナリストを反復作業から解放し、最もミッションクリティカルな意思決定に集中できるようにします。チーム、プロセス、ツールが統合されるため、組織はセキュリティを強化し、リスクを効果的に管理できます。Phantom を使用すれば、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 SOC 機能をサポートできます。

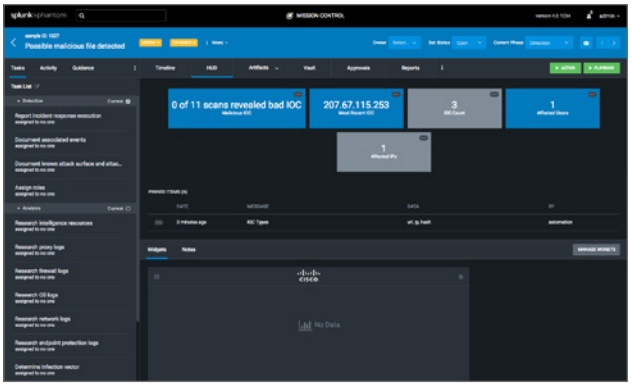
SOC を自動化

イベントのエンリッチメントやプログラムによるトリアージに Phantom を使用すれば、ノイズを排除し、脅威インテリジェンスをマシンスピードで事前に読み込んで、意思決定をサポートしながら、人手による分析が必要な最も重要なイベントを優先させることができます。また、フィッシングを調査して疑わしいフィッシングメールを数秒で処理できるほか、。マルウェア調査における反復作業を自動化することでセキュリティを強化し、全体的な平均復旧時間 (MTTR) を短縮できます。



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。サンドボックスにファイルを送信し、脅威インテリジェンスサービスに対してクエリを実行するといった調査のためのセキュリティアクションを、調査のコンテキストを失うことなくミッション コントロール インターフェイスから実行できます。



ケース管理に Phantom を使用すると、標準的な運用手順との整合性を高め、人間と機械のタスクのオーケストレーションを行い、ケースに関するすべてのデータとアクティビティを 1 つの場所に保管できます。また、イベントやケースについて他のチームメンバーとのチャット機能が提供されるため、コラボレーションが向上するほか、イベントのケースやタスクを適切なチームメンバーに割り当てることもできます。

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今すぐお試しください.

splunk>

詳細はこちら: www.splunk.com/asksales

www.splunk.com

PB-Splunk-Phantom-Maximize-Your-SOC-Efficiency-With-SOAR-106-JAPANESE