Splunk SOAR

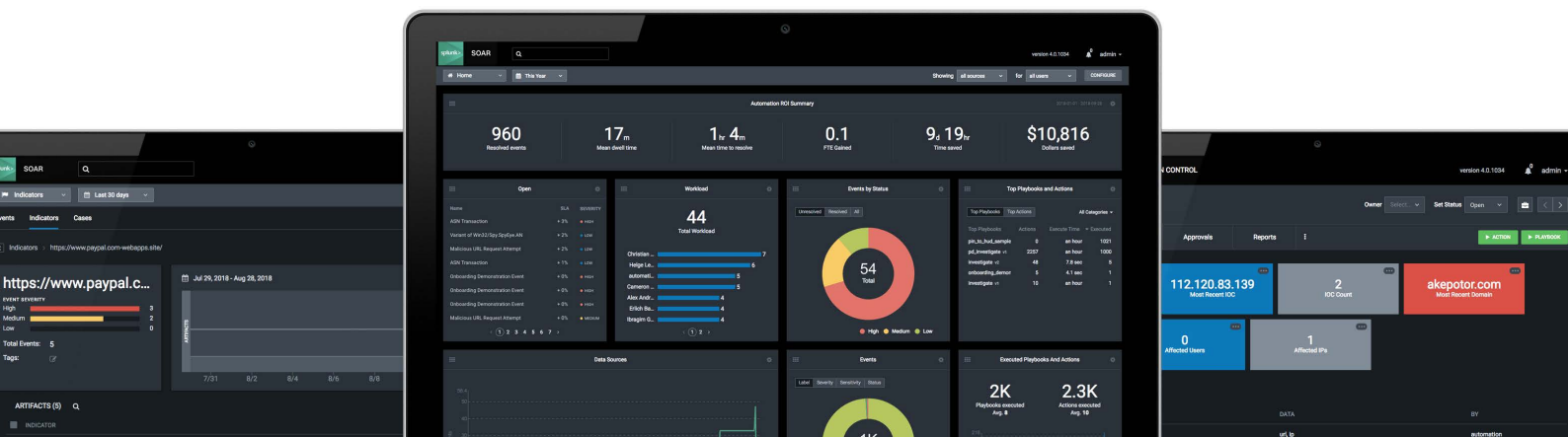
最新のSOCに最適なSOAR(セキュリティのオーケストレーションと自動化によるレスポンス)機能を提供

- アラートのトリアージと繰り返し行うセキュリティタスクの自動化によって業務を効率化し、ミッションクリティカルな目標に注力できます
- 数時間かかっていたセキュリティインシデントの調査と対応を数秒に短縮します
- ツールとチームの垣根を超えて統合(オーケストレート)したワークフローはSOCの効果と生産性を向上させます

SOC業務を自動化して生産性を向上させ、脅威への対応を迅速化

SOC (セキュリティオペレーションセンター)は今、混乱状態に陥っています。アナリストのもとには日々大量のセキュリティアラートが届き、十分な調査と解決ができないことも少なくありません。セキュリティ運用業務は、特にTier-1アナリストレベルの対応において、単調で定型的な繰り返しのタスクに溢れています。世界中のSOCに十分な人材を供給するには、必要な知識と経験のあるサイバーセキュリティのプロフェッショナルが100万人以上足りません。そして、脅威の検出、トリアージ、対応に時間がかかりすぎています。

混乱から脱却し、秩序を取り戻す必要があります。Splunk SOAR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対応を可能にし、SOCを支援します。Splunk SOARを使用すれば、繰り返し行うタスクのほか、検出、調査、対応を自動化することでセキュリティインシデントのトリアージを迅速化し、セキュリティアナリストの負荷を軽減して効率を向上させます。また、生産性、効率、正確性が向上します。さらには、ツールとチーム間の複雑なワークフローを連携させ、協調させていくことで防御を強化することができます。また、Splunk SOARには、イベントおよびケース管理、脅威インテリジェンスの統合、コラボレーションツール、レポートなど、幅広いセキュリティ機能が備わっています。



人間の介在なしに膨大な量のアラートと繰り返しのタスクを処理

Splunk SOARは、手動で行うと数分もしくは数時間かかるアラートのトリアージ、対応、繰り返しのタスクを自動化し、数秒で処理します。自動化プレイブックの使用により、異なるポイント製品のアクションをオーケストレーションして実行できるため、セキュリティアナリストの単純作業をなくして効率を向上させるとともに、ミッションクリティカルなタスクに取り組む時間の余裕を生み出します。もう、過剰なアラートに振り回されることはありません。混乱から脱却し、秩序を取り戻すことができます。

チームの力を強化

SOCには人が足りません。というのも、サイバーセキュリティ人材が枯渇しているからです。しかしSplunk SOARがあれば、3人のチームが10人分の力を発揮できます。繰り返しのタスク、調査、対応を自動化できるため、セキュリティチームの生産性が向上し、今のチームでより多くの作業を処理できるようになります。

ツールの連携を強化

Splunk SOARにより、ITおよびセキュリティスタック全体のワークフローと対応がオーケストレーションされ、防御戦略の中で各製品を有効活用できるようになります。その結果、既存のセキュリティインフラを統合して防御体制を強化し、侵入の難しい保護対策を構築できます。Splunk SOARでは、350を超えるサードパーティ製ツールと2,400を超えるアクションがサポートされており、チームやツールの垣根を越えてワークフローを接続して連携させることが可能です。調査と対応を迅速化するだけでなく、これまでの投資から価値を引き出すこともできます。

30分を30秒に

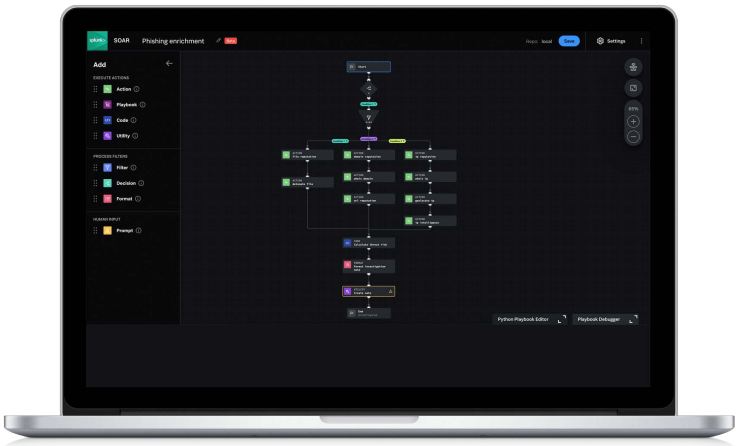
脅威の検出、トリアージ、対応には、時間がかかりすぎています。Splunk SOARを導入すれば、数分や数時間ではなく、数秒で脅威に対応できるようになります。自動化プレイブックを使用し、多くのツールのセキュリティタスクを自動化してマシンスピードで処理することで、脅威に対する平均検出時間(MTTD)と平均対応時間(MTTR)を短縮します。

それぞれに合ったSOAR

ビジネスのニーズに合わせてSOARを導入すれば、セキュリティ運用を合理化し、デジタルトランスフォーメーションを促進できます。Splunk SOARは、オンプレミス、クラウド、ハイブリッド環境に導入できます。

自動化を簡単に実現

Visual Playbook Editorでは、これまでよりも簡単に自動化プレイブックの作成、編集、実装ができるようになりました。コーディングの必要がなく、ドラッグアンドドロップで操作できるため、誰でも自動化を実現できます。担当チームがビジネスのニーズに合わせて、大規模な自動化に対応することも可能です。



Splunk SOARの特長と機能の詳細はこちらをご覧ください。

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

21-19335-Splunk-Splunk SOAR-A4-PB-JA-202111