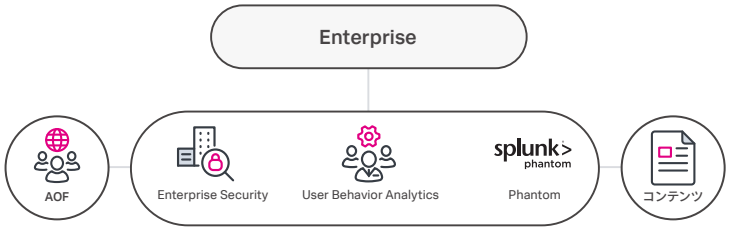
Splunk Security Operations

- 脅威の検出、調査、対応能力を強化
- リスクを低減
- セキュリティ運用のROIを向上



セキュリティチームは、脅威を特定、分析し、軽減しようと懸命に取り組んでいます。それでも多くの組織では、大量のインシデントが発生し、それらを分析できるスキルを持った人材が不足しているため、セキュリティインシデントのバックログは増えるばかりです。

この状況をさらに悪化させるのが、セキュリティオペレーションセンター (SOC)内の異なるツールから発せられる大量のアラートです。誤検知のアラートに対応してしまい、真の脅威に気付くのが遅れれば、早期に対応していた場合よりも問題解決に時間がかかることになりかねません。

Splunk Security Operationsスイートは、先進的なSIEM (セキュリティ情報/イベント管理)、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)ソリューションを統合して、セキュリティ運用のモダナイゼーションと最適化、サイバー防御の強化、リスクの低減を実現します。セキュリティの中枢として機能し、データをインサイトに変え、インサイトを行動に変えます。セキュリティスタックを最適化すれば、チームが最高のパフォーマンスを発揮できるようになります。さらに、その基盤には、高い実績があり拡張性に優れたData-to-Everythingプラットフォームが使用されています。このスイートは、最新の脅威に対応するための実用的なユースケースコンテンツを追加して拡張を続けています。

Splunk Security Operationsスイートは、監視、調査、自動化、オーケストレーション、高度な脅威、内部脅威の検出、インシデント対応、コンプライアンスなど、セキュリティに関する幅広い課題に対応します。ターゲット別のコンテンツが用意されているため、継続的な脅威や新しい脅威にすばやく対応できます。

SIEM（セキュリティ情報/イベント管理）

Splunk Enterprise Security (ES)は、分析主導型のSIEMソリューションです。リアルタイムのセキュリティ監視、高度な脅威の検出、インシデント調査とフォレンジックなど、脅威に効率的に対応するためのさまざまな機能を備えています。

UEBA（ユーザーとエンティティの行動分析)/UBA（ユーザー行動分析）

Splunk User Behavior Analytics (UBA)は、機械学習を利用して、ユーザー、エンドポイント、デバイス、アプリケーションでの未知の脅威や異常な行動を検出するためのソリューションです。従来であれば要員、リソース、時間不足によって見逃してしまうような脅威を検出することで、セキュリティチームを支援し、生産性を向上させます。

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）

Splunk Phantomは、SOARプラットフォームを提供します。チーム、プロセス、ツールを統合して、業務の効率化、対応の迅速化、防御力の強化を実現します。

統合のメリット

Splunk Security Operationsスイートでは、特定用途に特化したフレームワークとワークフローを利用して、検出、調査、インシデント対応にかかる時間を短縮できます。また、組み込みのダッシュボード、レポート、調査機能、ユースケースカテゴリ、分析機能、相関サーチ、セキュリティ指標を使って、脅威対策とインシデント管理を効率化することもできます。

さらに、SaaSやオンプレミスの区別なくデータを相関付けることで、ユーザー、ネットワーク、エンドポイント、アクセス、異常なアクティビティを検出し、その範囲を特定できます。

このスイートでは、従来のほとんどのセキュリティ製品にはない教師なし機械学習アルゴリズムによって、内部脅威や未知の脅威も検出できます。キルチェーンの高度な可視化により、異常行動と精度の高い脅威インテリジェンスが自動的に関連付けられるため、セキュリティアナリストは、より忠実な行動ベースのアラートに基づく脅威の捕獲に集中できます。

コンテンツサブスクリプションは動的にアップデートされるため、最新の脅威検出技術をプロアクティブに活用して、業務を停止することなく最新の脅威に対応できます。

セキュリティチームは、定型業務を自動化することで、優先度が高い脅威に集中し、パフォーマンスを最大限に発揮できます。Splunk Security Operationsスイートなら、検出と調査の自動化によって脅威の潜伏時間を短縮し、マシン速度でアクションを実行するプレイブックを活用して対応を迅速化できます。

SplunkのSecurity Operationsスイートは、今日のSOCの最新化を支援します。**詳しくはこちらをご覧ください。**

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

2020-Splunk-SEC-Security-Operations-Suite-A4-JA-202010