

# セキュリティのためのSplunk®

分析主導型セキュリティを活用

- セキュリティとセキュリティ以外のデータソースから**セキュリティ分析を包括的に実行**
- キルチェーン手法を使用して**高度な脅威調査を効率化**
- 回答までの時間の短縮とプロアクティブな脅威ハンティングにより**インシデント分析を迅速化**
- **機械学習ベースの高度な分析**を使用し、異常と脅威を迅速に検出して、内部および外部の脅威を軽減
- **アダプティブレスポンスのアクションとPhantomのプレイブック**により意思決定を自動(または人による支援)で行い、運用効率を改善



サイバー攻撃の巧妙化が進み、高度な脅威の持続性が増し、ビジネスリスクの継続的な管理が重視される状況下で、企業はセキュリティエコシステム全体を再評価する必要に迫られています。現在のセキュリティ分析では、ID、エンドポイント、サーバー、アプリケーション、Webサーバーとメールサーバー、さらに従来とは異なるシステムから取得した、ユーザー、攻撃、コンテキスト、時刻と場所に関する情報を詳細に分析することが重要です。

また、クラウド、モバイルワークロード、ハイブリッド環境の導入により、クラウドサービスとアプリケーションの可視化のニーズも高まっています。このニーズに対応するには、内部および外部の脅威をリアルタイムで特定、調査して対応するための動的なインフラと、アプリケーション全体のアクティビティを表示する機能が必要です。

Splunkの分析主導型セキュリティソリューションを利用すれば、機械学習や行動分析などの高度な技術を含む包括的なアプローチでサイバーセキュリティを実現できます。これらの手法により、セキュリティチームは従来のセキュリティ製品よりも幅広いセキュリティコンテキストに基づいて、脅威を迅速に特定、調査して対応できます。Splunkのソリューションは、オンプレミス、クラウド、またはハイブリッドクラウド環境に導入できます。

## セキュリティの中核として機能するSplunk

**Splunk Adaptive Operations Framework (AOF)**では、Splunkの主要なセキュリティテクノロジーとのインテグレーションを構築および開発してきたセキュリティベンダーのオープンエコシステムを活用し、サイバー防御とセキュリティ運用を強化します。

これらのインテグレーションにより、セキュリティチームはマルチベンダーのセキュリティ環境でもマシン並みのスピードで脅威を適切に検出、調査して対応できるようになり、「セキュリティの中核」を実現できます。



### 内部脅威の検出

機械学習、行動ベースライン、ピアグループ分析、行動分析を使用して、内部脅威を自動的に検出します。

### 高度な脅威検出

キルチェーン分析を使用して、高度な脅威のさまざまな段階を追跡し、一連のイベントをリンクさせ、対象を絞って修復できます。

### 不正行為の検出と調査

さまざまな不正行為、窃盗、悪用をリアルタイムで検出、調査、報告します。Splunkを使用すれば、イベントデータをインデックスして企業全体の不正行為を可視化したり、1つのトランザクションの不正行為スコアを集計することで、既存の不正行為対策ツールを補完できます。

### SIEM

Splunkは、インシデントレビュー、インシデント管理サポート、分析と行動プロファイリング、脅威インテリジェンス、アドホックサーチなど、エンタープライズ向けのSIEMユースケースで活用できます。大規模な企業では、セキュリティ体制の評価、監視、アラートとインシデントへの対応、CSIRT、侵害の分析と対応、イベント相関など、情報セキュリティオペレーション全般にSplunkを使用しています。Splunkは、あらゆる規模のSOC(セキュリティオペレーションセンター)を運用するためのSIEMとして使用できます。

### 迅速なインシデント調査

組織のSOCアナリストと脅威ハンターは、コラボレーション機能を活用し、既存の相関ルールを使用したアドホック検索をセキュリティ関連のすべてのデータに対して実行して、インシデントを迅速に調査できます。一元的なビューによってSIEMワークフロー内の潜在的な攻撃者の行動をアナリストとハンターの両方が調査できるため、インシデント対応の時間を短縮できます。また、過去の履歴を使用することで、根本原因を究明して次のステップを判断できます。

### コンプライアンスレポートの作成

相関ルールとレポートを作成して、機密データまたは主要な従業員に対する脅威を特定し、コンプライアンスを自動的に証明したり、PCI、HIPAA、FISMA、GLBA、NERC、SOX、GDPR、ISO、COBIT、CIS Top 20などの技術的規制に関するコンプライアンス違反を特定できます。

### ログ管理

セキュリティ関連のマシンデータを統合、収集、保存し、インデックス、検索、相関付け、可視化、分析、レポート作成を行うことで、セキュリティの問題を特定して迅速に解決します。サードパーティのレポートソフトウェアを使用することなく、履歴データに対してアドホッククエリーを実行してレポートを作成できます。Splunkソフトウェアでは、リレーショナルデータベース、コンマ区切り値(CSV)ファイル内のフィールド区切りデータ、HadoopやNoSQLなどの他のエンタープライズデータストアに柔軟にアクセスして、ログデータを補強できます。

**今すぐSplunk Enterprise Securityをお試しください。** Splunk Enterprise Securityの機能をぜひお試しください。ダウンロード、ハードウェアのセットアップ、設定は不要です。Splunk Enterprise Security Online Sandboxは7日間利用できる評価環境です。クラウドでプロビジョニングされ、データは予め用意されています。この環境を使用して、データの検索、可視化、分析に加えて、セキュリティ関連のさまざまなユースケースにわたるインシデントの綿密な調査を行うことができます。詳細な手順を記載したチュートリアルが用意されており、Splunkソフトウェアが実現する効果的な可視化と分析をご紹介します。[詳細についてはこちらをご覧ください。](#)