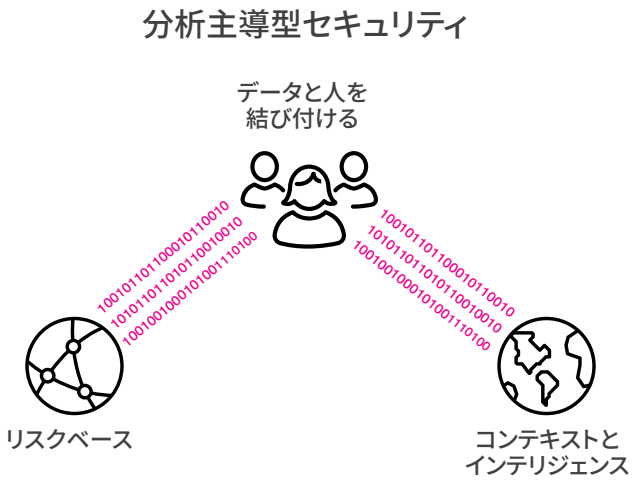
# Splunk® Enterprise Security

最新の脅威に対応するための分析主導型セキュリティと継続的な監視

- アダプティブレスポンスアクションと調査ワークベンチを使用してインシデントレスポンス時間を短縮し、**セキュリティ運用を最適化**
- マルチクラウドとオンプレミスから収集したマシンデータを活用して環境をエンドツーエンドで可視化し、**セキュリティ体制を強化**
- ユーザー行動分析、異常や脅威の検出、分析ストーリーを使用して、**調査能力を向上**
- 脅威インテリジェンスを活用して、**情報に基づいた的確な意思決定を実現**




今日の企業は動的な脅威の状況、進化する攻撃手口、高度な脅威、変化するビジネス需要への適応を迫られていますが、既存のセキュリティ技術では対応しきれません。これらの新たな課題に対応するため、セキュリティチームには、分析能力に加えて、コンテキストに即したインシデント対応が求められています。また、脅威への対応時間を短縮し、ビジネス中心の意思決定を下すには、新しい脅威検出技術を迅速に実装できる必要があります。すべてのマシンデータを一元化して活用することで、セキュリティチームは、攻撃を迅速に検出して対応し、阻止することができます。

**Splunk Enterprise Security** (Splunk ES)は、**セキュリティ情報イベント管理(SIEM)ソリューション**です。セキュリティチームは、内部と外部からの攻撃を迅速に検出して対応し、脅威管理を簡素化するとともに、リスクを最小限に抑え、ビジネスを保護することができます。**Splunk ES**を使用すれば、セキュリティチームはすべてのデータを利用して、組織全体を可視化し、セキュリティインテリジェンスを獲得できます。デプロイモデルがオンプレミス、パブリックまたはプライベートクラウド、SaaS、これらの組み合わせのいずれでも、**Splunk ES**はご利用いただけます。どの場合でも、継続的な監視、インシデント対応、セキュリティオペレーションセンターの運営が可能になるほか、企業の幹部がビジネスリスクを把握できるようになります。**Splunk ES**は、**Splunk Enterprise**ではソフトウェアとして、または**Splunk Cloud**ではクラウドサービスとしてデプロイできます。

**Splunk ES**を使用すると、組織の規模や成熟度に関係なく、セキュリティチームはセキュリティ運用を効率化することができます。特長は次のとおりです。

- **データを元にしたインサイト：**ネットワーク、エンドポイント、アクセス、マルウェア、アノマリ(UBAで検出)、脆弱性、IDから情報を自動的に取得し、事前に定義されたルールまたはアドホックサーチによって相関付けます。
- **すぐに使える相関サーチルール：**アラート監視、動的な検出、コンテキストに即したサーチ、迅速な検出、**高度な脅威の分析**を実行します。
- **柔軟なカスタマイズ：**継続的なセキュリティ監視、インシデント対応、セキュリティオペレーションセンター (SOC)のサポート、経営層によるビジネスリスクの把握など、デプロイの目的に合わせて相関サーチ、アラート、レポート、ダッシュボードをカスタマイズできます。
- **運用効率の向上：**ワークフローベースのコンテキストと自動化された意思決定(人による支援もあり)によって運用を効率化できます。

## 分析主導型セキュリティとは

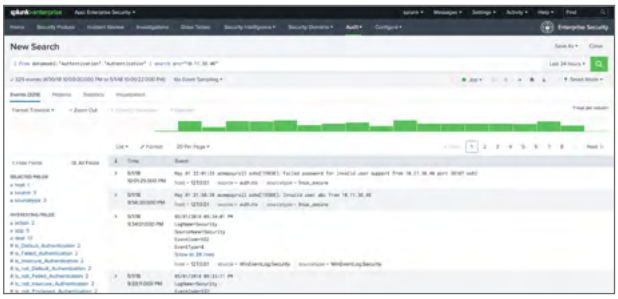
変化する脅威の状況に迅速に適応するために、**ITインフラストラクチャ、単体セキュリティ製品**からのデータ、すべてのマシン生成データを含むあらゆるセキュリティ関連データ間の関係を見つけ出すプロセスを指します。

### セキュリティ体制の継続的な監視

組織のセキュリティをより明確に可視化するために、事前に定義されたダッシュボード、主要セキュリティ指標、主要業績評価指標、静的および動的なしきい値とトレンド指標でカスタマイズしたグラステーブルビューを利用します。ユースケースライブラリを使用して、新たに発見された脅威や既存の脅威をすばやく検出し、迅速にインシデント対応を行うことで、組織全体のリスクを軽減します。

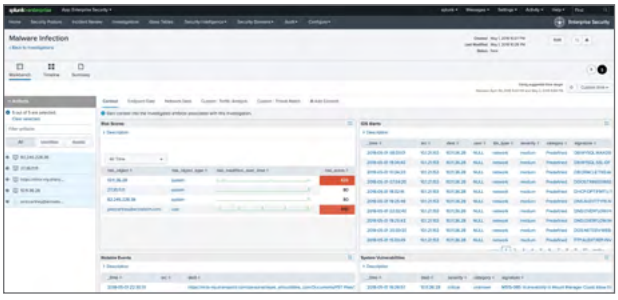
### インシデントに対する優先順位付けと行動

分析担当者や調査チームが使うインシデント対応ワークフローを最適化するために、一元化されたログ、アラートとインシデント、UBAで検出された異常、事前定義されたレポートと相関付け、インシデント対応ワークフロー (リスクスコア使用)、セキュリティに特化した相関付けを活用します。1つまたは複数の重要なイベントを1つのビューで調査する調査ワークベンチを使用して、調査を効率化し、インシデントに迅速に対応します。




### 迅速な脅威調査

アドホックサーチ、および静的、動的、視覚的な関連付けを使用して調査を迅速に行い、インシデント対応時間を短縮します。セキュリティおよびITスタックから自動的に取得されるデータを元にフィールドを調査してピボットすることで、脅威コンテキストをすばやく構築して攻撃者の行動を追跡し、証拠を検証します。アダプティブレスポンスアクションを使用して脅威の検出と修復を自動化および最適化することで、マルチベンダー環境における取得、共有、対応を自動化します。イベントの順序付けによって、脅威の検出に集中し、インシデント調査を迅速化します。




### 複数ステップでの調査を実行

**侵害と調査の分析**を行うことで、侵害されたシステムに関するアクティビティを追跡します。アドホックサーチとESのすべての機能を、イベントの順位付け、調査タイムライン、および調査ワークベンチと組み合わせて使用し、キルチェーン手法を適用して攻撃のライフサイクルを調査します。さらに、ユースケースライブラリを使用して、新たに発見された脅威や既存の脅威をすばやく検出し、迅速にインシデント対応を行うことで、リスクを軽減します。

**今すぐSplunk Enterprise Securityを試す**Splunk Enterprise Securityの機能をお試しください。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、データのサーチ、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案内します。**詳細についてはこちらをご覧ください。**

splunk> a CISCO company

お問い合わせはこちら：https://www.splunk.com/ja_jp/talk-to-sales.html

www.splunk.com/ja_jp
splunkjp@splunk.com

© 2020 Splunk Inc. 無断複写・転載を禁じます。 Splunk, Splunk>, Data-to-Everything, D2EおよびTurn Data Into Doingは、米国およびその他の国における Splunk Inc.の商標または登録商標です。他のすべてのブランド名、製品名、もしくは商標は、それぞれの所有者に帰属します。

2020-Splunk-SEC-Enterprise Security-A4-PB-JA-202512