優れたSOC

を構築するための
基本ガイド

splunk>
turn data into doing™

高度なサイバー脅威に先手を打つのは容易なことではありません。未知の脅威や隠れた脅威を見付けるのはさらに困難です。従来のポイントソリューションでは、高度なセキュリティ脅威の複雑さと 規模に対応できません。

旧来のソリューションでは、内部脅威、横展開するマルウェア、アカウント侵害がもたらすリスクを検出するのは困難です。問題は、開発時点で今日のサイバー脅威が想定されていなかったことだけでなく、これまでSOC(セキュリティオペレーションセンター)を支えていたソフトウェアソリューションが、アナリストが処理しきれない量のアラートを生成し、しかもその多くが誤検知であったりします。

これでは、セキュリティチームがいくら仕事熱心であったり優秀であったりしても、未処理のセキュリティインシデントが増え続け、状況は改善しません。現実には、そもそも優れたセキュリティ人材が不足しており(試算では350万人不足しています)、人材が見つかったとしても、高額の年収を求められます。

旧来のツールがセキュリティチームの足を引っ張っているのは事実です。今日多くのSOCが使用しているツールは、予算を浪費するだけでなく、異なるベンダーの製品とシームレスに連携しません。そして、シームレスに連携しないことが、プロセスの遅延とデータの喪失を引き起こします。

その結果、アナリストは組織内で起きているインシデントをしばしば見落としてしまいます。調査では、ビジネス部門およびIT部門の意思決定者による推定を平均すると、社内データの55%がダークデータである(把握されていない、または活用されていない)ことがわかりました。活用できるにもかかわらず実体が見えないデータがこれだけある中で、セキュリティチームがセキュリティを確実に維持するのは不可能でしょう。なぜなら、すべてのデータが最終的にはセキュリティにかかわるからです。

今日の問題を理解するには、SOCの原点を振り返る必要があります。SOCはそもそも、物理的にも役割的にも、セキュリティ運用の新たな中枢として誕生しました。そして、継続的に業務を見直し、役割を拡大して、かつてないスピードで知見や洞察を引き出すことが求められました。

SOCアナリストの日常業務はまもなく、アラートのトリアージと追跡調査が主になりました。しかし、アラートの量があまりに多いため、すぐにティア1アナリストの負荷が過大になり、現状から大きく後れを取っているという感覚が常につきまとうようになりました。

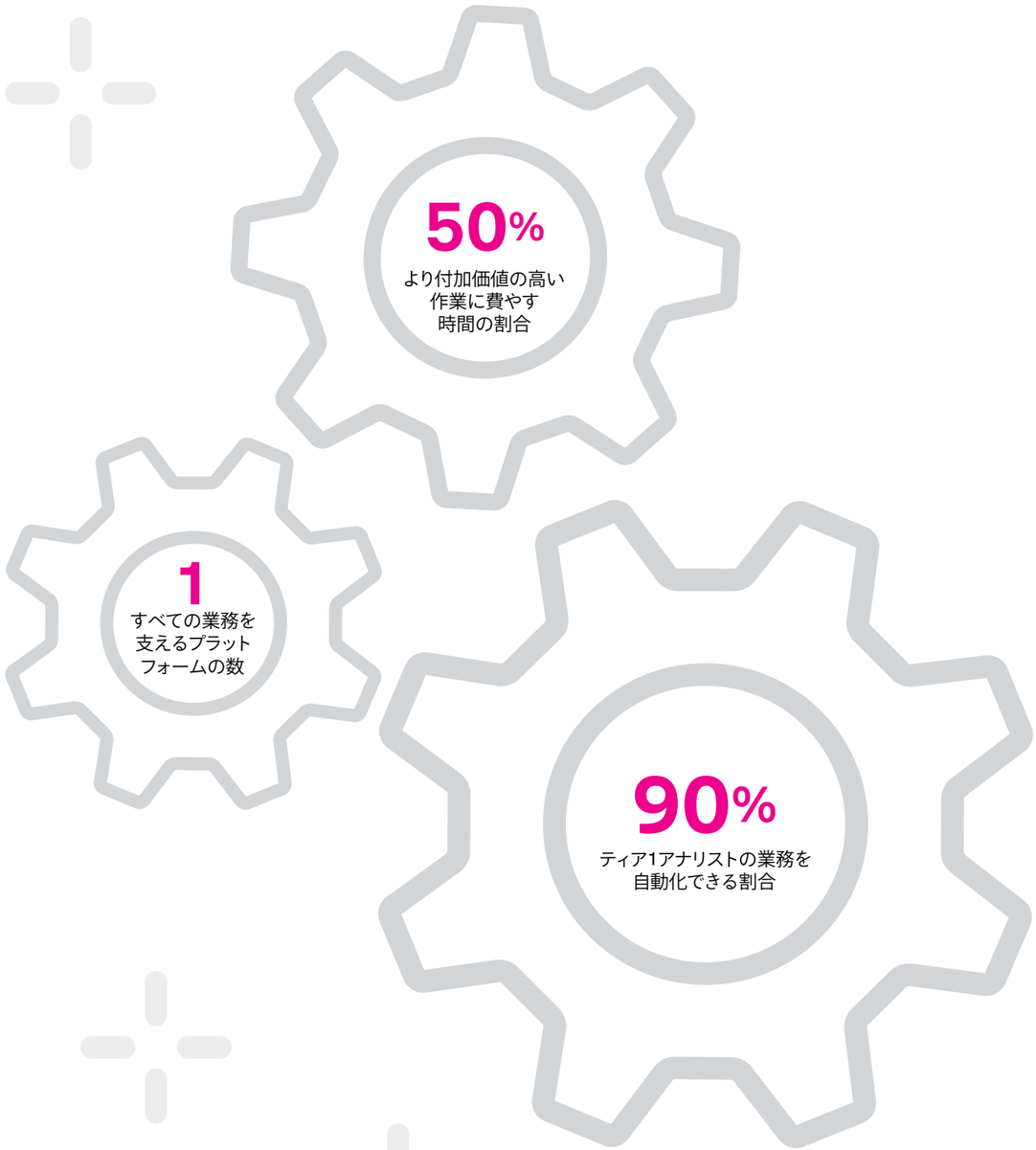
これほど過酷な状況になったのは、80%のSOCの基盤が、連携されていない個別のシステムを寄せ集めて構築されてきたためです。

私たちはみな、この新しい現実を受け入れる必要があります。今日発生するインシデントの量に対して、それを分析できる技能を持ったアナリストの数は不足しており、その差を埋められるツールはほとんど行き渡っていないのです。

では、古いテクノロジーに頼っている企業は何をすべきでしょうか。現役のSOCアナリスト全員分のクローンを作製するか、何とかして巨万の富を手に入れるか、それらが無理であれば、アナリストが脅威に先手を打てるように支援するテクノロジーを導入するしかありません。

新しい脅威に対応するには、SOCに新しい分析機能を導入して、脅威が大損害をもたらす前にその存在に気付けるように、セキュリティチームがより多くのインサイトを得られるようにする必要があります。また、一部のプロセスをツールで自動化して、セキュリティチームが真のアラート、つまり実際の脅威への対応に集中できるようにすることも重要です。

今こそSOCを立て直すときです。そして現状に見合った、あるいは将来を見据えたSOCを構築しましょう。



今こそ構築すべき
未来志向のSOC

将来、ティア1アナリストの業務の90%は自動化されるでしょう。定型的で重要性が低い作業が多いため、自動化すれば、アナリストは本当に重要な問題だけに集中できます。

また、アラートのトリアージに時間をかける代わりに、検出や対応のロジックの微調整に時間を費やせるようになるでしょう。相関ルールとプレイブックを作成すれば、さらに多くのプロセスを自動化できます。これにより、アナリストの業務時間の50%が、より付加価値の高い作業に割り当てられると期待されます。

さらに、Splunkのような、イベントの監視と調査を連携する単一のプラットフォームが主流になるでしょう。これにより、多数の製品間を行き来する手間を省くことができます。

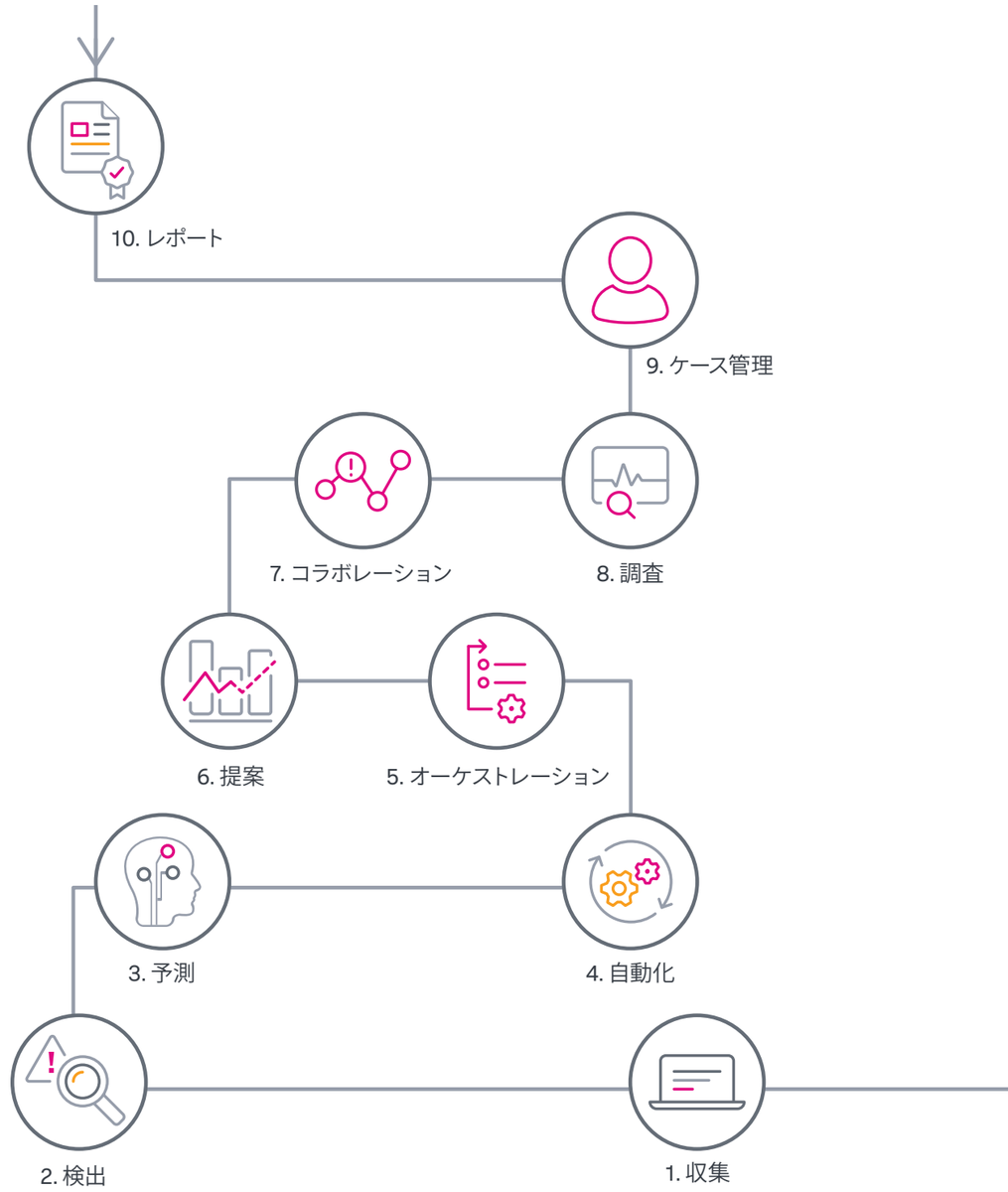
必要なテクノロジーはすでにある

未来志向のSOC構築の第一歩は、入念に設計されたプラットフォームを導入してSOCの機能を強化した上で、必要に応じて自動化や機械学習のためのツールを加えればよいという考え方を受け入れることです。自分がSOCを率いることになってもかまわないという心持ちが大切です。

次世代型、将来を見据えたSOCの基盤には、異なるベンダーのソリューションをシームレスに統合して既存の機能を補強できる単一スイートを導入します。その場しのぎで継ぎ合わせるソリューションでは効果がありません。

また、セキュリティチームが誤検知のアラートへの対応で時間を無駄にすることのないよう、脅威の兆候に関するインサイトを提供して、少人数でも能力を最大限に引き出せる、強力な分析機能を備えていることも重要です。その上で高度な機械学習、自動化、オーケストレーションテクノロジーを活用できることも欠かせません。

未来志向のSOCを今すぐ構築するには、以下の10の機能をサポートするセキュリティ運用プラットフォームが必要です。



1. 収集

すべてはデータから始まります。データこそSOCに活力をもたらす酸素です。分析機能やアルゴリズムはデータなしには動きません。データと同じくらい重要なのが、構造化データであるか非構造化データであるかを問わず、あらゆるソースからデータを大規模に取り込む機能です。また、データをコンピューターまたは人間が利用できるように整理する機能も必要です。

2. 検出

セキュリティ運用スイートには、システムに取り込まれたイベントを検出する機能が不可欠です。この場合、検出対象はあくまでイベントであり、この点が、ファイルやネットワークトラフィックを対象としていた従来のソリューションとは異なります。検出時に、相関ルール、機械学習、分析ストーリーなどの高度な機能を組み合わせるセキュリティ運用スイートもあります。

3. 予測

セキュリティイベントが実際に検出される30分前にアラートを受け取れたら、SOCにとってどれだけ有益でしょうか。セキュリティイベントの予測機能があれば、インシデントを早期にエスカレーションしたり、あらかじめ定められたプロセスに従ってインシデントに効率的に対応したりできます。大規模攻撃の兆候を早い段階で警告する技術や、未知のインシデントを大きなリスクにつながる前に特定する技術など、非常に有望な予測技術も次々と登場しています。

4. 自動化

自動化はSOCアナリストを支援する新しいテクノロジーのひとつです。それを示す良い例が、近年のSplunkによるPhantomの買収です。自動化ツールは、標準的な運用手順をデジタルプレイブックの形にまとめて、調査、データ補強、追跡、隔離、修復作業を迅速化します。

自動化機能を取り入れれば、従来は30分かかっていたプロセスを40秒で実行するなど、時間を大幅に短縮して、より多くのイベントを処理できます。SOCの進化の中で自動化は、もはや選択肢ではなく必須機能と言えます。

5. オーケストレーション

これまで、セキュリティを強化するために必要に迫られ、予算に余裕があることも手伝って、多くの製品を購入してきたSOCも少なくないでしょう。こうしたツールの大半は、特定の機能を提供することで防御力を高めますが、進化することはありません。問題は、脅威の方が進化することです。今日、脅威を追跡するための製品は、API主導の潮流に合わせることが求められます。そこで注目されるのがオーケストレーションです。オーケストレーションは、SOC内外のあらゆる製品をつなぎます。ブラウザーで製品ごとにタブを開いたり、ソリューション間でコピー＆ペーストしたりする必要はありません。すべての製品をオーケストレーションでつなげば、オーバーヘッドを削減し、ストレスを解消して、アナリストのエネルギーを有意義な作業に集中させることができます。

6. 提案

この時点で、イベントは必要なものだけに絞り込まれています。SOCの基盤となるプラットフォームがアナリストに、次にすべきことを教えてくれたら便利だと思いませんか？次世代型SOCは、提案機能によってこれを実現します。提案は、個々のアクションまたはプレイブックの形で示されます。この機能は2つの点で役立ちます。第1に、経験の浅いアナリストにとっては、同じような脅威に直面したときに何をすべきかを学ぶことができます。第2に、ベテランのアナリストにとっては、すでにわかっている対応手順の正当性チェックやリマインダー代わりになります。

7. 調査

先ほど、ティア1アナリストの業務の90%が近い将来に自動化されるという予測をご紹介しました。では、その他の業務はどうでしょうか。残念ながら、最終的には人間による詳細な分析が欠かせません。しかし、直感的に使用できるセキュリティツールがあれば、アナリストの作業を効率化し、調査が必要なイベントの優先順位を判断できます。

8. コラボレーション

セキュリティは、協調とコミュニケーションが求められるチームスポーツです。つまり、コラボレーションが重要です。SOC環境では、見落としは許されず、イベントを総合的に処理する必要があります。そのため、ChatOps機能やコラボレーション体制を整備して、ツール、人、プロセス、自動化機能をつなぎ、作業環境の透明性を高めることが重要です。これにより、情報、アイデア、データを共有し、コラボレーションを促進できます。さらに、アラートの処理について外部の専門家に支援を仰いだり、一刻を争う状況で重要情報を同業他社と共有したり、最終的には業界全体でコラボレーションしたりできるようにもなるでしょう。

9. ケース管理

防止に最善を尽くしてもインシデントは起こるものです。重要なのは、インシデントが起きたときに、対応プロセスの管理体制がすでに整っていることです。セキュリティチームが、対応計画、ワークフロー、証拠収集、コミュニケーション、関連文書、タイムラインをすばやく入手できるようにすることが大切です。そのため、次世代型SOCのコア機能としてケース管理に注目が集まっています。

10. レポート

計測できないものは管理できません。ビジネス界ではデータ主導型モデルへの移行が進んでいますが、セキュリティも例外ではありません。今日では、セキュリティプロセスのあらゆる側面を測定できます。適切なレポートツールがあれば、プロセスの進捗を簡単に報告して、チーム全体でより正確に状況を把握し、次に実行すべきアクションを判断できます。SOCが今日直面している課題は、使用しているツールが多すぎることであり、その状態では正確なレポートを作成するのは困難です。

Splunkのメリット

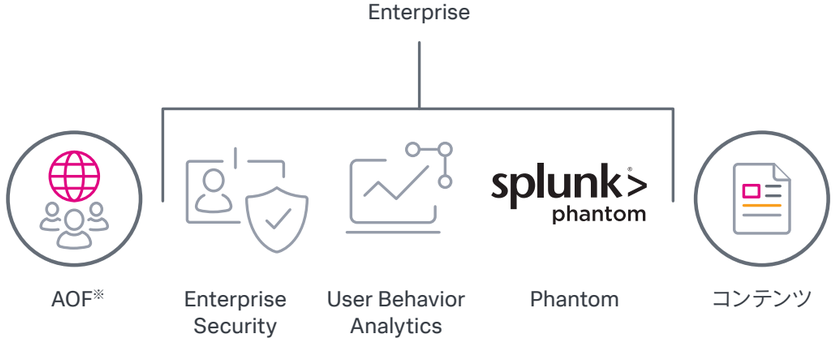
Splunk Security Operationsスイートは、最先端のSIEM、UEBA、SOARテクノロジーを単一プラットフォーム上に統合して、次世代型SOCの実現を後押しします。これらすべてのソリューションを1つのプラットフォームで提供するベンダーはSplunkだけです。

Splunkは、これらの機能をネイティブでサポートするだけでなく、次のユースケースもサポートします。

リアルタイム監視	Splunk Enterprise、Splunk Cloud、またはSplunk Enterprise Security
調査	Splunk Enterprise、Splunk Cloud、またはSplunk Enterprise Security
自動化とオーケストレーション	Splunk Phantom
高度な脅威と内部脅威の検出	Splunk User Behavior AnalyticsまたはSplunk Enterprise Security
インシデント対応	Splunk PhantomまたはSplunk Enterprise Security
コンプライアンス	Splunk Enterprise、Splunk Cloud、またはSplunk Enterprise Security

Splunk CloudまたはSplunk Enterpriseとも呼ばれるSplunkプラットフォームは、出発点として最適です。まず、データを取り込むことができます。そして、カスタマイズ可能なデータ分析プラットフォームとして、マシンデータを具体的なビジネス成果につなげます。SaaSやその他のオープンソースソリューションとは異なり、Splunk CloudとSplunk Enterpriseでは、既存のテクノロジー資産を活用できるだけでなく、IT部門、セキュリティ部門、業務部門のシステム、アプリケーション、デバイスから生成される膨大でさらに増え続けるデータをほぼリアルタイムで調査、監視、分析し、行動につなげることができます。

Splunk Security Operationsスイート



Splunk Security Operationsスイートに含まれるコンポーネント

Splunk Enterprise Security (ES)：リアルタイムのセキュリティ監視、高度な脅威の検出、インシデントの調査とフォレンジック、インシデント対応の各機能を提供してより効率的な脅威対策を実現する、分析主導型のSIEMソリューションです。

Splunk ESを導入すれば、脅威の検出、調査、対応を迅速化できます。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。その後、SaaSやオンプレミスのソースと相関付けることで、ユーザー、ネットワーク、エンドポイント、アクセスのアクティビティや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。

※ Adaptive Operations Framework

Splunk User Behavior Analytics (UBA)：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。

Splunk UBAを導入すれば、可視性を高め、脅威検出の精度を向上できます。従来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。キルチェーンの十分な可視化により、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ます。これにより、行動に基づく精度の高いアラートが生成されるため、脅威の調査よりも追跡により多くの時間をかけることができます。また、コンテンツサブスクリプションが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。

Splunk Phantom：チームのプロセスと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するSOARプラットフォームです。

Phantomを導入することで、SOCのセキュリティ運用能力を最大限に高めることができます。定型業務を自動化して作業量を最適化し、本当に人間による判断が必要な問題にのみ人手を集中させることができます。検出と調査の自動化によって脅威の潜伏時間を短縮し、マシン速度で実行されるプレイブックを活用して対応を迅速化できます。さらに、既存のセキュリティインフラストラクチャを統合して、各製品をSOCの防御戦略で積極的に活用することもできます。

Splunkについて

Splunk Inc.は、データを、すべての人がアクセスできる便利なものに、そして価値あるものに変えます。

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。

2020-Splunk-SEC-Fundamental-Guide-to-Building-a-Better-Security-Operations-Center-JA-202004

splunk> turn data into doing™