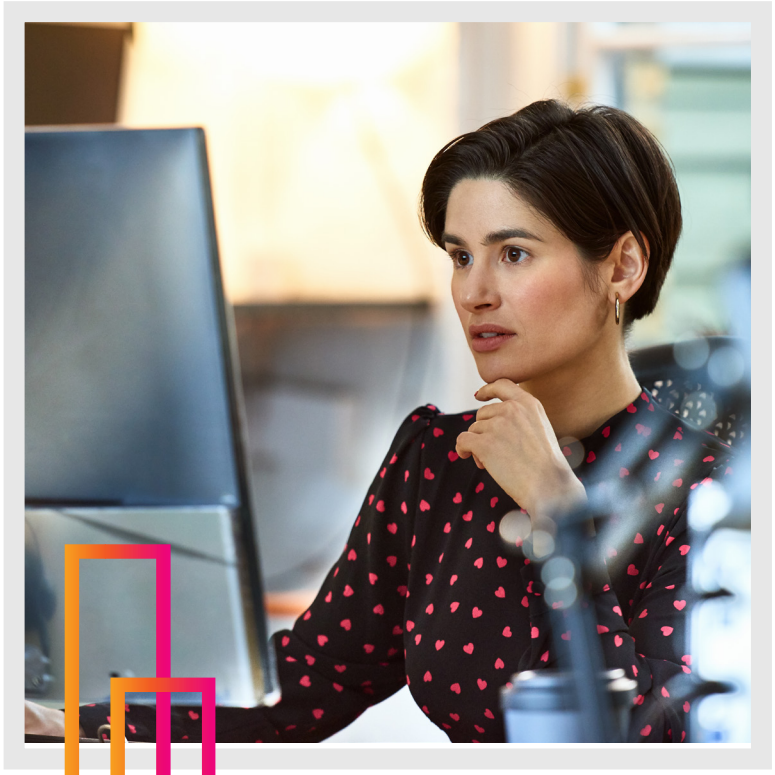
SOAR導入ガイド

セキュリティソリューションとして
SOARの評価基準を考える



splunk>
turn data into doing®

目次

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)ソリューションに投資するには今が絶好のタイミングです。セキュリティチームが手動でインシデントに対応する時代は終わりました。これからは、繰り返しの作業を自動化し、分析の生産性と精度を向上させて、もっとスマートに仕事をすることで、ビジネスをより強固に守る時代です。

セキュリティチームは、いつの間にか、退屈で負担の大きい分析作業に苦しめられがちです。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。一方で、SOC (セキュリティオペレーションセンター)の業務に必要な知識と経験を備えたサイバーセキュリティ人材は世界全体で100万人以上不足しています。

ほかにも以下の課題がよく挙げられます(もちろんこれらはごく一部です)。

- **過剰なアラート：**アナリストのもとには日々 (数千までとはいかなくても)数百件のセキュリティアラートが届きます。これだけ大量になると、セキュリティチームはすぐに追い詰められて、セキュリティインシデントのバックログが増え、「アラートの洪水」状態になりかねません。
- **サイロ化した単体製品の氾濫：**セキュリティチームは、ばらばらで連携の取れない、相互運用性ゼロのセキュリティツールを使いこなすことを求められます。ツールが連携していなければ、セキュリティに隙が生じることは避けられず、そこが防御の弱点になります(当然、攻撃者はそれを見逃しません)。
- **スキル不足：**SOCの人材確保は容易ではありません。適格なアナリストは供給不足で、市場で引く手あまたのセキュリティ人材は離職率も高いのが現状です。アナリストのトレーニングと体系的な知識の習得に費やした時間とリソースがいつの間にか無駄になっていることも珍しくありません。
- **プロセスの欠如：**ほとんどのセキュリティチームが、各種のセキュリティイベントに対応したワークフローと標準作業手順(SOP)を確立できていません。手順が厳密に定められていなければ、攻撃を受けたときにアナリストは適切な対応をすばやく取ることが難しくなります。
- **検出の遅さ：**MTTD (平均検出時間)があまりに長いと、攻撃者に、ネットワークに侵入してデータを盗み出す十分な時間を与えることになります。平均的なセキュリティ担当者がアラートに対応するまでの時間は、数分(最良のシナリオで)から数週間または数カ月(あるいはそれ以上)です。後者の対応時間では(ときには前者でも)、深刻な脅威の滞留時間としては長すぎます。

こうした数々の課題を抱えたままでいると、脅威の検出と対応はますます難しくなります。そこで必要になるのが、強力かつ柔軟で高速な、自動化を活用したソリューションです。

SOARを導入すれば、アナリストは、組織を脅かすあらゆる脅威に規模を問わず対応できます。強力なSOARソリューションなら、ワークフローをコード化し、自動化プレイブックを作成することにより、ファイルのデトネーション(仮想領域での実行)からデバイスの隔離まで、手作業で行えば数時間から数日以上かかるようなセキュリティインフラ全体のアクションを、わずか数秒で実行できます。

大切なのは、どのような組織でもSOARのメリットを享受できる点です。この『SOAR導入ガイド』では、製品を評価するうえで重要な基準をご紹介します。組織のセキュリティチームとセキュリティ運用体制に最適な製品を選べば、アナリストは無駄な作業から解放され、より付加価値の高い業務に集中する(そして十分な昼休みを取る)ことができます。

SOARとは？

SOARソリューションは、セキュリティチームの時間とリソースを奪いがちな日常業務を一掃します。SOARがあれば、セキュリティチームは、より多くのインシデントを処理し、問題を詳しく調査して、重要なセキュリティタスクに時間を割くことができます。それは最終的に、組織全体のセキュリティ態勢を強化することにもつながります。

自動化は多くの業界でもはや常識になっていますが、サイバーセキュリティの領域では遅れていると言わざるを得ません。しかし、この数年の間に目覚ましい進歩が見られます。企業の間でSOARへの関心が高まり、それに伴って、隣接するセキュリティ市場のベンダーが既存の製品を再構築してSOAR市場に参入する例が増えています。

一方で、新規参入したベンダーは、それぞれ得意な機能を前面に押し出しているため、SOARに関する市場定義がわかりづらくなり、製品の比較が難しくなっている面もあります。定義をわかりやすくするために、ここでは次のカテゴリに分けて説明します。

セキュリティオーケストレーション

セキュリティオーケストレーションとは、複雑なインフラを横断して相互に依存する一連のセキュリティアクションを機械的に調整することです。

セキュリティの自動化

セキュリティの自動化とは、セキュリティに関連するアクションを機械によって実行することです。

セキュリティレスポンス

セキュリティレスポンスとは、イベント、ケース、インシデントの対応ワークフローで、人間のアクティビティと機械のアクティビティをポリシーに基づいて調整することです。

セキュリティオーケストレーションとは？

セキュリティオーケストレーションとは、複雑なITエコシステムを横断する一連のセキュリティアクションを機械的に調整することです。これにより、タイプの異なる個別のセキュリティツールを連携させると同時に、製品やワークフローをまたぐタスクを自動化できます。単体製品をまたぐ複雑なプロセスを自動化することで、セキュリティ担当者の作業を効率化し、プロセスやツールの価値を最大限に引き出すことができます。

セキュリティオーケストレーションには以下の機能があります。

- 複数のツールをまたぐワークフローを統合して自動的に調整する。
- 異なるソースのデータを集約して、セキュリティインシデントに関するコンテキストを提供する。
- 深く掘り下げた有意義な調査を実行できるようにする。

セキュリティの自動化とは？

セキュリティの自動化とは、セキュリティに関連するアクションを機械によって実行することです。脅威の調査、対応、修復を、人手を介することなくプログラムによって行います。セキュリティの自動化によってほとんどの作業を実行できるため、アナリストはアラートが発生するたびに手動で選別して対応したり、アクションやタスクを手動で1つずつ処理したりする必要がなくなります。

セキュリティの自動化には以下の機能があります。

- 環境内の脅威を調査する。
- セキュリティアナリストが行っていた手順、指示、判断のワークフローに従って潜在的な脅威を選別し、イベントを調査して、それが本当にインシデントであるかどうかを判断する。
- インシデントに対してアクションを取るべきかどうかを判断する。
- 問題を封じ込め、解決する。
- 脆弱性の調査とパッチの適用を自動化する。

セキュリティレスポンスとは？

セキュリティレスポンスとは、機械によって自動化されたアクションと、イベント、ケース、インシデントのワークフローに関して人間が行うアクションを、ポリシーに基づいて調整することです。セキュリティイベントやアラートの技術的な詳細を体系化することで、アナリストは手元の情報をすばやく理解することができ、セキュリティシナリオの範囲全体を的確に把握して、適切な対応が取れるようになります。これにより、セキュリティアナリストは、提供されるデータに基づいて調査、封じ込め、対応のアクションをシームレスに実行できます。

アラートやイベントを確認してエスカレーションしたら、ケース管理コンポーネントがそれを引き継いで、ケースの作成から解決まで、広範囲にわたる部門横断的なライフサイクルが進められます。

セキュリティレスポンスには以下の機能があります。

- 複数のイベントを1つのケースに集約し、エスカレーションする。
- インシデントを組織の既存のプロセスにシームレスにマッピングする。
- 特定の技術データに基づいて調査、封じ込め、対応のアクションを実行する。
- イベントやアラートに対して実行されたすべてのアクションをアクティビティログに記録する。
- ケースの作成から解決まで、広範囲にわたる部門横断的なセキュリティライフサイクルを推進する。

SOARの一般的なセキュリティシナリオ

以下のユースケースは、既存の手動ワークフローを基にモデル化したもので、運用上の一般的な課題についても触れています。これらのワークフローには、通常、単体の製品間で連携が必要な数多くの手動タスクが含まれます。

評価を始める前に、まずは自分の組織に該当しそうなユースケースを具体的に洗い出す必要があります。その際には、セキュリティ運用の関係者はもちろん、関係部署のリーダーの意見も取り入れるのが理想的です。重要なユースケースを特定しておくことは、たとえすぐには対応しないとしても、効果的なセキュリティ戦略を策定するために不可欠です。

以下に、調査、エンリッチメント、封じ込め、修復に関するセキュリティユースケースの一部をご紹介します。

アラートのトリアージ	受信したアラートを検証し、優先順位を付けて、イベントのコンテキストを追加します。後に続く処理での負担を軽減するために、何らかの技法やモデルを使用して誤検出のアラートを排除することも必要です。
インシデント対応	インシデントへの対応方法は、対象となるインシデントのタイプによって異なります。たとえば、フィッシング攻撃の試行への対応と、ランサムウェア攻撃の被害への対応はまったく異なります。
IOC (侵害の痕跡)の検出	IOCの検出を自動化して、チームのリソースを消耗することなく、最新の脅威インテリジェンスを活用できます。参照すべき脅威インテリジェンスソースを判断できるように、インテリジェンススコアリングを取り入れることもできます。
脆弱性管理	脆弱性の特定、分類、修復、軽減のサイクルを自動化(続いて標準化)して、効率と一貫性を大幅に向上させることができます。
NAC (ネットワークアクセスコントロール)	SOARでは、動的アクセス制御戦略を強化できます。たとえば、以前はNACの意思決定には含まれなかった検出システムの統合などが考えられます。
ユーザー管理	特定のアカウントの有効化/無効化を体系的にすばやく行うことにより、内部脅威、アカウントの乗っ取り、認証情報の悪用を阻止します。
侵入テスト	資産の検出、分類、ターゲットの優先順位付けといったアクティビティを自動化して、侵入テストチームの作業効率を向上させます。
インテリジェンスの共有	インテリジェンスの共有に取り組んでいる企業では、自動化を支援するプレイブックから大きなメリットを得ることができます。また自動化によって、アナリストの生産性を高め、一刻を争う情報を手動プロセスよりもはるかに速く提供できます。

これら以外にも、SOARのユースケースとなるさまざまな課題が考えられ、セキュリティチームは検出や自動化の基準をコード化する必要があります。その他のユースケースについては、『Splunk SOARの5つの自動化ユースケース』を参照してください。

SOARの基本

評価の基準

ここでは、SOARソリューションの評価基準について、**コア機能**、**プラットフォームの特性**、**ビジネス上の考慮事項**の3つの基本カテゴリに分けて説明します。

コア機能

コア機能は、SOARソリューションの中核を成す基本機能です。以下では、各機能とコンポーネントに加えて、ソリューションを評価するうえでの重要な考慮事項も示します。

オーケストレーター

- **データの取り込み**
  まずはセキュリティデータを取り込む必要があります。オーケストレーターがあれば、あらゆるソースからあらゆる形式のデータを取り込み、集約すると同時に、論理的な分類を維持できます。非構造化データについては、データの解釈とアクセスを可能にするために、データハンドラーを使用できる必要があります。
- **意思決定**
  データソースに自動化プレイブックを適用できるようにする必要があります。たとえば、メールデータを取り込む場合はフィッシングメールを検出するプレイブックを、SIEM (セキュリティインシデント/イベント管理)のアラートに対してはマルウェアを調査するプレイブックを各ソースに適用するなどが考えられます。
- **タスク実行**
  自動化タスクを適切かつ最適なタイミングで呼び出し、実行のために自動化エンジンに送ります。
- **人間による監視**
  機械による自動化を活用しながら、必要な場面では人間による監視ができることが重要です。一般的に、人間の介入が必要な状況は3つあります。1つ目は、資産に対してセキュリティアクションを実行するためにそのオーナーの承認が必要な場合、2つ目は、セキュリティの確保とビジネスの継続性のバランスをとるためにアナリストの考慮が必要な場合、3つ目は、コード化された意思決定ロジックをアナリストがさらに強化する必要がある場合(エラーの発生など)です。
- **データ管理**
  各アクションから出力されたデータを適切に解析、正規化、構造化して、後続のアクションで利用できるようにします。他のリソースに負荷をかけないために、関連データのキャッシュがサポートされているかどうかも重要なポイントです。
- **フォールトトレランス**
  SOARは多数の単体製品やサービスと頻繁に交信しますが、交信先の可用性が保証されているとは限りません。外部サービスへのアクセスは、中断されたり、利用できなくなったりすることがあります。このような状況をオーケストレーターが想定し、事前の設定に従ってシームレスに運用を復旧、再開できるかどうかが重要なポイントです。

自動化エンジン

自動化エンジンは、ほとんどのSOARソリューションの中核であり、オーケストレーターからアクションやタスクを受け取って、それぞれに応じた処理を実行します。自動化プロセスでは処理の実行に人間が介入しないため、プラットフォームの拡張性や柔軟性といった基準が重要な考慮事項になります。

- **拡張性**
  SOARの導入後は、時間とともに適用するユースケースが増え、自動化の範囲が拡大します。処理負荷の増大に対応するため、自動化エンジンにはスケールアップとスケールアウトの両方の拡張性が求められます。
- **柔軟性**
  セキュリティは急速に進化しているため、大がかりな再構築を行わずに新しい機能をサポートできることが重要です。自動化エンジンに、環境独自の機能に適応できる柔軟性があるかどうかを確認しましょう。

アラート管理

データを取り込んだ後は、受信したアラートを対応待ちリストに入れて優先順位を付けます。その後、生産性と精度を最大限に高められるよう、手動または自動のアクションで調査します。

適切な情報を適切なタイミングで把握できるよう、画面にアラートがわかりやすく整理、選別されて表示されると便利です。これにより、アナリストは広い範囲を検索したり複数の画面を頻繁に切り替えたりせず、重要なイベントの内容をすばやく理解できます。

- **アラートの詳細**
  アナリストがセキュリティイベントをすばやく把握して内容を理解できるように、セキュリティアラートの詳細がわかりやすく表示されることを確認します。たとえば、IPアドレス、ドメイン名、ファイルハッシュ、ユーザー名、メールアドレスなど、関連する技術データをすばやく確認できると便利です。また、CEF (Common Event Format)などの標準形式や同等の形式が採用されていると、データ交換の際に役立ちます。
- **アクションの実行**
  セキュリティアナリストがアラートの調査、問題の封じ込め、修正を行うときに手動でアクションを実行できることを確認します。画面上で操作対象のデータを選択してアクションを実行できる機能も必要です。また、アラートの受信時に一連のアクション(プレイブック)を自動実行できることも重要です。
- **アクションの結果**
  サマリー形式(表など)だけでなく、より総合的な形式(JSONなどの標準形式)でアクションの結果を利用できれば、結果をすばやく簡単に確認できます。
- **アクティビティログ**
  アラートに対して手動または自動プレイブックで実行されたすべてのアクションを記録する包括的なアクティビティログを備えていることを確認します。各アクションについて成否を含む結果も記録されれば、アクションが最後まで実行されたかどうかを把握できます。
- **アラートのステータス、重大度、機密度**
  アラートに、ステータスインジケーター (新規、オープン、クローズなど)や、重大度と機密度に関するインジケーター (TLP (Traffic Light Protocol)の設定など)が含まれるかどうかを確認します。また、各インジケーターは、アラート管理インターフェイスやプレイブック内から変更できる必要があります。
- **アラートに関するコラボレーション**
  画面内に、アナリストがコラボレーションしたり、コメントしたり、アラートやその関連データなどに関してさまざまな情報を提供できる領域が必要です。

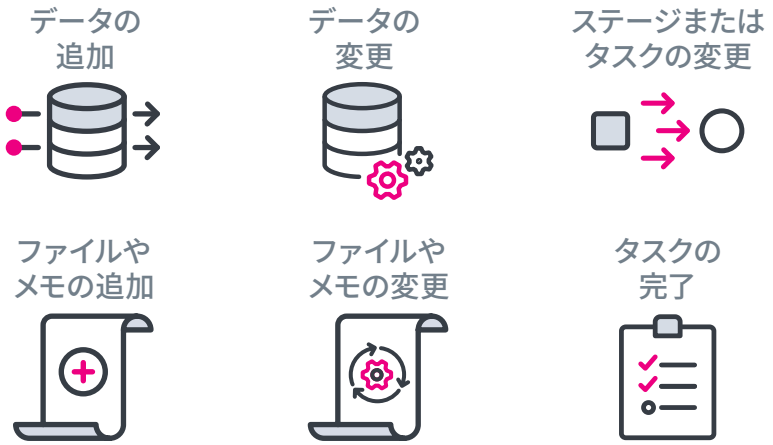
ケース管理

ケース管理には、ケースの作成から解決までのインシデントライフサイクルについて、広範囲にわたる部門横断的な視点が必要です。ケース管理機能があれば、複数のアラートやイベントを効率的に確認し、1つのケースとして集約してエスカレーションできます。通常、アラート管理では個別の技術的な対応が中心になりますが、ケース管理では、技術以外の手順もプロセスに組み込むことがあります。

また、ケースの全体量はアラートよりもはるかに少ないのが普通で、10件にも満たないことが一般的です。

- **ケースデータの整理**
  個々のケースに関連するすべてのデータは、ケース管理コンポーネントに集約されます。その情報を1カ所で表示できれば、画面を切り替えずに全体を把握するのに役立ちます。
- **ケースへのデータの追加**
  ソースデータやアクションの結果など、関連する技術データをケースに添付する必要があります。技術以外の関連データ(注釈、メモ、メール、スクリーンショット、録音など)も添付できるとさらに便利です。
- **ケースとアラートの関連付け**
  各アラートについて、ケース管理画面とアラート管理画面をリンクできれば理想的です。この機能は特に、データを詳しく調査するときや、封じ込めアクションを実行するときに便利です。
- **既存のプロセスへのマッピング**
  多くの組織は、インシデント対応時、緊急時、災害発生時などの重大な状況で実施する標準作業手順書を作成しています。ケース管理で、複数のステージを含むプロセスやワークフローを定義し、各ステージに1つ以上のタスクを含めて、各タスクに担当者を割り当てることができ、さらにそれをテンプレートとして保存できると便利です。
- **アクティビティの監査**
  ステータスの更新など、新しい情報や更新された情報が監査証跡に記録され、簡単にエクスポートできる機能が必要です。

ケースに加えられる変更には、次のようなものがあります。

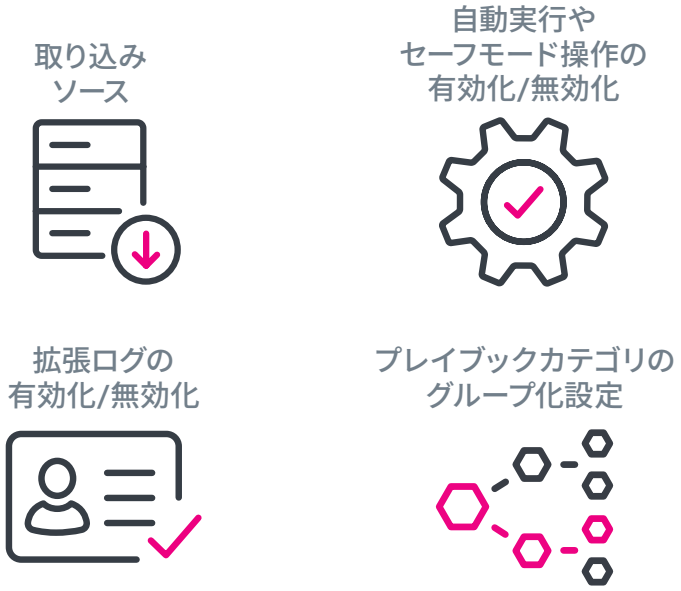


プレイブック管理

プレイブック管理は、組織全体(場合によってはさらに広い範囲)の標準の作業手順の実装と保守に役立ちます。このコンポーネントには改訂/バージョン管理とシンジケーション管理機能があると理想的です。

- **プレイブックの整理**
  アナリストが独自のカテゴリを設定してプレイブックをグループ分けできる機能が必要です。この機能があれば、機密度、部門、資産のタイプ、主題など、それぞれの組織にとって有意義で最適な分類ができます。
- **カスタム関数**
  あらかじめ用意されている機能以外に、独自に記述したコードや関数を使用できるかどうかも重要なポイントです。記述した関数を複数のプレイブック間で共有でき、一元的なコード/バージョン管理機能が提供されているとさらに便利です。
- **改訂管理と配布**
  プレイブックを効果的に管理するには、バージョン管理システム(VCS)と統合できるソリューションを強くお勧めします。VCSを使用すると、デプロイ時にプレイブックを組織的に配布することができます。また、開発プロセスで、変更を追跡したり、問題のあるアップデートをロールバックしたりするためにも重要です。
- **プレイブックの一括編集**
  通常、プレイブックごとに内部構造が異なっていても、管理レベルでは多くのプレイブックに共通点があります。

プレイブック管理システムで複数のプレイブックに対して以下の指定の一括編集ができると便利です。



自動化エディター

自動化エディターは、アナリストがプロセスをコード化してプレイブックに書き込むためのエディターです。テキスト主体のソースコードエディターでは面倒な作業も、視覚的に操作できる自動化エディターなら、プログラミング経験の有無を問わずセキュリティチームの誰もがソースコードレベルで機能を組み立てて、包括的で高度なプレイブックを作成できます。

視覚的な自動化エディターについて考慮すべき点は、ビジネスプロセスを指定するグラフィカルな表記法であるビジネスプロセスモデリング表記法(BPMN)に準拠しているかどうかです。BPMNは、ビジネスユーザーにとってわかりやすい記法をサポートしている一方で、技術ユーザーが極めて複雑なプロセスを表現できる別の記法も用意されています。

- **ユーザーインターフェイスの要素**
  ユーザーインターフェイスには、プレイブックを視覚的に作成するためのキャンバスが最初に表示されるべきです。そこには、実行するアクション(block_ipやfile_reputationなど)を選択する領域が必要になります。アクションを選択したら、アクションを設定するためのパラメーターを指定します(手動で入力するか、リストから選択します)。編集モードとテストモード、さらにソースコード表示をシームレスに切り替えて、同じ画面でテストやデバッグを実行できればさらに便利です。

- **コードをブロックで表現する機能**
  特定の機能を持つステップをブロックで表現できれば、その実際のソースコードを意識せずに、包括的で複雑なプレイブックを作成できます。ブロックは、1対1、1対多、多対1の関係で結び付けて、実行の順番を指定できることも重要です。

- **意思決定プロセスへの人間の介入**
  一般的には、人間による監視の下で自動化を行う必要があります。自動化のプロセスに人間が介入して、プレイブック実行の確認、補完、続行の承認を行います。そのためには、プレイブックの作成者が、介入する担当者、通知のタイプ、必要な承認レベル、サービスに障害が発生した場合にアラートすべきエラーのタイプなどを指定できる必要があります。

- **アクションの結果の共有**
  ユーザーインターフェイスには、入力、パラメーター、下流のアクション、判断ブロックなどの形で新しい情報を追加できる機能が必要です。上流のアクションのパラメーターを使用するときは、前のアクションの結果を視覚的に操作したりドロップダウンメニューから選択したりできると便利です。

- **プレイブックのソースコードへのアクセス**
  視覚的なエディターでプレイブックを作成するときに、プレイブックのソースコードがリアルタイムで生成され、作成者がアクセスできるかどうかも重要なポイントです。従来のようにソースコードを記述することでプレイブック全体やその一部を作成したい作成者もいるかもしれません。視覚的なエディターの代わりにソースコードを表示でき、視覚的な編集モードとソースコードモードをシームレスに切り替えられることも確認しましょう。

- **視覚的な編集とソースコードによる編集を同時に使用したプレイブックの構築**
  作成者がプレイブックのソースコードを編集する際に、ソースコードからだけでなく視覚的なブロックからも変更ができると便利です。個々のブロック(アクションブロックや判断ブロックなど)で、視覚的なエディターではできないカスタマイズを行うためにソースコードレベルでの変更が必要になる場合があるためです。また、ソースコードでの変更を行った後も引き続き視覚的な変更ができることが必要です。

- **内蔵のテスト/デバッグ/実行ログ機能**
  統合開発環境(IDE)には実行機能とデバッグ機能が備わっているのが一般的です。自動化エディターでも、セキュリティアラートに対応してプレイブックを実行し、実行の状況と結果を確認できる機能があると便利です。これにより、作成者が1つの画面ですばやくプレイブックを編集、テスト、デバッグできます。

- **セーフモード**
  新しいプレイブックを本番運用前にテストする際には、セーフモードを使用できることが重要です。セーフモードでは、変更を実際には反映せずに、自動化対象の実行をシミュレーションできます。

アプリケーションフレームワーク

アプリケーションフレームワークは、市販されているさまざまな単体製品とSOARプラットフォームをつないで統合を拡張するためのインターフェイスを提供します。

- **オープンエコシステム**
  市販の新しい製品や人気の製品と統合できなければ、SOARソリューションの価値はしだいに低下していきます。他の製品との統合性を確保するには、アプリケーション開発を促進するオープンなエコシステムを採用していることが重要です。ソリューション本体を変更することなく新しいテクノロジーをすばやく統合できるかどうかも確認しましょう。
- **アプリケーション開発**
  アプリケーション開発はオープンエコシステムの重要な要素です。開発機能が充実していれば、複数のテクノロジーを統合してプレイブックで使用できます。既存のアプリケーションのソースコード表示、テスト、拡張、編集と新しいアプリケーションの開発を1つの画面で効率的に行えるSOARソリューションがお勧めです。

メトリクスとレポート作成

状況を把握したり定量化したりするには、メトリクスとレポートが必要です。SOARソリューションも例外ではありません。自動化によってパフォーマンスと生産性が向上したら、メトリクスによってその効果を具体的に測定することで、さらなる改善点を探ることができます。

- **柔軟性に優れたダッシュボード**
  成否を判定するためのメトリクスはさまざまで、通常は組織や個人によって異なり、多くの要因に左右されます。そのため、組織に最適なメトリクスとしてKPI (主要業績指標)を定めるのが一般的です。SOARソリューションでも、KPIに応じてメトリクスをカスタマイズおよび体系化できることが重要です。
- **パフォーマンスレポート**
  自動化を進める主な目的は効率化です。投資の妥当性を見極めるには、どのくらいパフォーマンスが向上しリソースを節約できたかを定量的に把握することが欠かせません。

  レポート対象として重要なメトリクスには以下のものがあります。
  - 平均解決時間(MTTR)
  - MDT(平均滞留時間)：攻撃者に侵入されてから適切な対応を取るまでにかかった時間
  - 自動化によって節約できたアナリストの作業時間
  - 自動化によって節約できたFTE (フルタイム当量)
  - プレイブックの実行によって節約できた平均時間
  - 削減できたコスト(FTEあたりのコスト×節約できたFTE)

- **セキュリティ効果レポート**
  自動化によってどのくらいセキュリティが向上し組織全体のセキュリティ態勢が強化されたかを把握することも重要です。対応すべきセキュリティアラートの総数とその対応率も、投資の妥当性を示す説得力のあるメトリクスです。

  レポート対象として重要なメトリクスには以下のものがあります。
  - MTTRとMDT
  - 未処理のアラートの総数
  - 1日/1時間/1週間/1カ月あたりのアラート発生数
  - 1日/1時間/1週間/1カ月あたりのアラート処理数
  - サービスレベル契約(SLA)に照らしたパフォーマンス

- **アプリケーションインテグレーションとプレイブックのパフォーマンス**
  どのプレイブックが頻繁に呼び出されているかを知れば、今後どの領域への投資を強化すべきかがわかります。偽陽性のアラートを自動的にクローズし、信頼性の高い真陽性のアラートに注力できるようにプレイブックを設計できれば理想的です。

  自動化が不足している領域とツール統合の効果を把握するためにレポート対象として重要なメトリクスには以下のものがあります。
  - 自動化によって処理されたアラート数(1時間/1日/1週間/1カ月/その他の期間あたり)
  - 使用頻度の高いアプリケーションインテグレーション
  - 使用頻度の高い手動/自動アクション
  - 使用頻度の高い自動化プレイブック
  - プレイブックの実行時間
  - アクションの実行時間

- **人間の作業量**
  自動化は人手不足を補うことを目的としていますが、SOARソリューションの通常のプロセスでは、アナリストの関与が必要な状況もまだたくさんあります。たとえば、アラートに対して手動のトリアージなどのアクションが必要なケースや、「人間による監視の下での自動化」を実現するために、人間による承認をプレイブックに組み込むケースなどです。

  自動化プロセスにおける人間の作業量を把握するために重要なメトリクスには以下のものがあります。
  - 担当者1人あたりに割り当てられたアラート数
  - 担当者1人あたりが処理したアラート数
  - 平均承認時間
  - 未了の承認数
  - 必要な承認数(1時間/1日/1週間/1カ月/その他の期間あたり)

プラットフォームの特性

プラットフォームの特性は、定量的には評価しにくいものです。そのため、以下の基準は、プラットフォームのデモを見たり実際に操作してみたりしなければ評価できない部分が多くあります。

導入オプション

SOARソリューションが、オンプレミス、クラウド、ハイブリッド環境のいずれに対応しているかを確認します。オンプレミスで導入したい組織もあれば、全面的にクラウドに展開したい組織もあるでしょう。どの提供方法や導入形態が最適かは、予算、データ保存やセキュリティに関する要件といった組織の主なニーズによって決まります。また、セキュリティ運用をどのように効率化するか、既存のフレームワークの範囲内でどうやってデジタルトランスフォーメーションを進めるかなども判断基準になります。

コミュニティの充実度

アプリケーション開発のためのオープンなエコシステムを採用して、コミュニティモデルをサポートしているSOARソリューションがお勧めです。そのようなソリューションであれば、ベンダーロックインを回避できるだけでなく、自動化プレイブックに悪影響を及ぼさずにテクノロジーを簡単に移行できるので、長期にわたって価値を引き出すことができます。セキュリティの世界は急速に変化するため、最新の脅威に対応できるよう、専門家が協力してプレイブック、ベストプラクティス、戦略を構築して共有する必要性も高まっています。

大規模かつアクティブなコミュニティ

多くのユーザーが、同じ目的を持つ他のユーザーの経験を参考にしたいと考えます。大規模かつアクティブなユーザーコミュニティに参加すれば、自動化の新しいユースケースのプレイブックやアプリケーションを共有したり、アイデアをブレインストーミングしたりする機会が得られます。アイデアの交換を活発にするには、コミュニティでユーザー同士を結び付けることが重要です。特にメッセージング/コミュニケーションツールは、疑問の答えを見つけたり自動化のユースケースについて意見を出し合ったりするなど、技術や設計に関する支援を得るための効果的な手段です。

コラボレーション

コラボレーションを行うことで、機能の完成度を高め、アプリケーションの統合を進め、自動化プレイブックを改良してシナリオの進化に対応することができます。

- **コミュニティ全体でのコラボレーション**
  ユーザーとベンダーのコンテンツが1つのリポジトリから一元的にアクセスできると便利です。対象となるコンテンツには、プレイブックやアプリケーションインテグレーションといった技術的な投稿や、プレゼンテーション、技術メモ、ブログ、その他の文書といった技術以外の投稿などがあります。
- **プラットフォーム全体でのコラボレーション**
  信頼できる複数のユーザーグループがグループの垣根を越えてコラボレーションできるSOARソリューションがお勧めです。特に、組織内のセキュリティチーム全体で、特権を持つ複数のグループが機密情報を共有できることが重要です。

認識能力

コグニティブなSOARソリューションなら、人間の知識と過去の観測を将来の判断に活かすことができます。この機能は、プレイブックの形でシステムに組み込まれます。情報源としては、実行の統計、取り込んだデータの特性、アクションの結果が使用されます。

これらの情報に基づいて、個々のアクションやプレイブック、またはプレイブックを構成する一連のアクションが提案されます。SOARソリューションを評価する際は、現在の認識能力だけでなく、認識能力に関する将来的な戦略とロードマップを確認することも重要です。

自動化への人間の介在

自動化を導入する際は、通常、ユースケースを一度に1つずつ取り入れて、時間をかけてシステムに対する信頼を高めていきます。自動化プレイブックに人間が選択的に介入できる機能があるSOARソリューションなら、このプロセスを効果的に進めることができます。ワークフローへの人間の介入は、資産単位(単体のセキュリティツールやテクノロジー)またはアクション単位で行えるのが理想的です。

資産単位の場合は、資産に対してアクションが実行されるたびに資産の管理者に通知できること、アクション単位の場合は、自動化プレイブックの任意の時点でプロンプトを挿入できることが重要です。後者の場合は、プロンプトによって、実行を継続するか、一時停止するか、中止するかをユーザーが選択できるようにします。このレベルの管理機能があれば、ステップが自動化されていてもユーザーは安心して利用できます。

セキュリティ

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)ソリューションである以上、最も重要なのはもちろんセキュリティです。SOARソリューションでは認証情報などの極めて機密性の高い情報が保持されるため、機密情報の暗号化やロールベースの堅牢なアクセス制御機能は必須です。

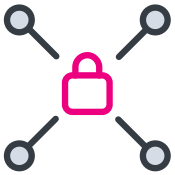
SOARソリューションのセキュリティのベストプラクティスには以下のものがあります。

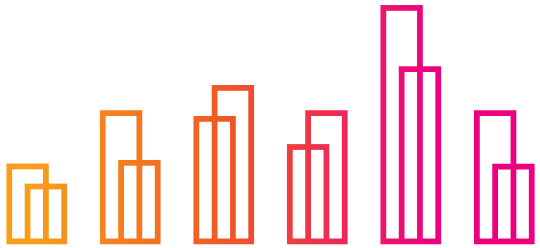
セキュリティ認証情報を暗号化する

メモリーに認証情報を残さない

認証管理システムをサポートする

多要素認証をサポートする





拡張性

SOARソリューションには、スケールアップとスケールアウトの両方の拡張性が求められます。将来ユースケースを追加するにつれて処理負荷も増えることを考慮する必要があります。ソリューションを評価する際は、ハードウェアリソース(CPUやRAMなど)を増やすことによるスケールアップと、導入環境を構成するサーバーインスタンスの数を増やすことによるスケールアウトの両方に対応していることを確認しましょう。

オープン性と柔軟性

単体製品の種類が増えていることからもわかるように、セキュリティを巡る状況は常に変化しています。そのため、オープンで柔軟性の高いSOARソリューションがお勧めです。そのようなソリューションであれば、新しいセキュリティシナリオや製品、アクション、プレイブックに簡単に対応できます。

オープンな統合フレームワーク

オープンな統合フレームワークのメリットは、プラットフォーム内のテクノロジーを入れ替えても自動化した運用に悪影響が及ばない点です。また、SOARベンダーに頼らずに新たなインテグレーションを社内開発できるメリットもあります。

これらのメリットが特に重要なのは、アプリケーションを自社開発する場合、ベンダーが提供するカスタムAPIやリリース前のAPIを利用する場合、あるいは自動化プラットフォームの機能を拡張する場合などです。オープンなフレームワークは、一般的な基準やプログラミングモデルに従っていることが重要です。また、ドキュメントやサンプルが豊富に提供されているかどうかも確認しましょう。

インターフェイスの制約がないこと

テクノロジーの中には、REST API、SSH、syslog、カスタムAPIなどのプロトコルやメソッドを使用したインターフェイスを公開しているものがあります。柔軟な統合フレームワークであれば、インターフェイスの種類による制約を回避できます。自動化プラットフォームから単体製品やアプリケーションに接続する場合、アプリケーションインテグレーションがインターフェイスの制約を受けず、どのような方法でも接続できることが重要です。

モバイル

SOARソリューションの目的の1つは、対応を迅速化して滞留時間と平均解決時間を短縮することです。対応を迅速化するには、人間による介入が必要になったときにセキュリティアナリストにすばやく対応してもらう必要があります。しかし、通知時点で必ずしもアナリストがPCの前にいて対応できる状態にあるとは限りません。

そのため、アナリストがモバイルデバイスからSOARソリューションに簡単にアクセスして管理や操作ができることが重要です。これにより、アナリストは、外出先からプレイブックを実行したり、ノートPCがなくてもセキュリティアーティファクトを確認してイベントをトリアージしたり、その場ですばやく通知に対応したり、席を外しているときでも常に通知を受け取ることができます。

使いやすさ

企業向けのソフトウェアは複雑であるのが常ですが、SOARソリューションの導入と使用時の負担を減らすことは可能です。

- **導入とセットアップ**
  多くの組織では、すでに他のインフラで仮想化を活用しているため、フォームファクタが仮想アプライアンスであれば導入が簡単です。
- **オンボーディング**
  システムの設定や、データソースへの接続、いくつかのプレイブックの有効化を支援するオンボーディングプロセスを備えたSOARソリューションなら、初期の習熟までにかかる時間を短縮できます。
- **早期の自動化**
  SOARソリューションを導入したら、早く自動化を開始したいと考えるでしょう。これは、難しい設定なしで使用できる自動化プレイブックが多数提供されていれば可能です。また、ユーザーが自動化プレイブックを短時間で設計してテストし、導入できるような機能を備えていることも、自動化までにかかる時間を大幅に短縮する要素です。

ビジネス上の考慮事項

提供されているコア機能がいかにすばらしくても、製品に対する従来の考え方以外にも考慮すべき事項があり、購入の判断に大きな影響を与える場合があります。十分に考慮しなければならない事項の1つは、製品を販売しているベンダーの特性です。また、ベンダーが提供しているサービスも重要です。コア機能とそれを補完するサービスの組み合わせこそが製品の全体像であり、購入後の使用感を左右するからです。

ベンダーの特性

製品購入の判断をするときは、ベンダーの特徴や質、将来性を考慮することが重要です。現実には、新規参入するベンダーの多くが市場から撤退することになります。期待を裏切らない、実力のあるベンダーを選ぶことが大切です。

経歴

セキュリティソリューションの開発における豊富な経験を持ったベンダーを選びましょう。SOARは、市場セグメントとしては比較的新しいものの、その起源はかなり前まで遡ります。ベンダーの沿革とSOAR市場への参入を決めた経緯を知ることが重要です。

実行力

経験豊富な専門家による精鋭チームがいることも重要な点です。ほとんどの場合、ベンダーの実行力はチームメンバーの実績と直結しています。

顧客基盤

ベンダーの顧客基盤の特徴や質は、ベンダーの特性を反映しています。優秀な企業は、製品の購入前に、候補となるベンダーをさまざまな視点から徹底的に調査します。

受賞歴と評価

ベンダーの受賞歴やその他の評価にも目を向けましょう。これらは、ベンダーとその製品が宣伝に違わない実力を持っていることを証明するものです。ただし、ベンダーの質と同様に、賞の質もさまざまである点には注意してください。

付帯的なサービス

ベンダーが提供する付帯的なサービスは、製品の導入とプロジェクトの成功に大きく影響します。

プロフェッショナルサービス

セキュリティ運用の成熟度は組織によって大きく異なります。そのため、導入の成功を支援するプロフェッショナルサービスをベンダーが提供しているかどうかも重要なポイントです。また、プロセスの構築(プロセスがまだ整備されていない場合)や手動ワークフローから自動化プレイブックへの移行についてSME (特定分野の専門家)の支援を受けられるサービスがあるかどうかも確認しましょう。

ポストセールスサポート

スタートアップの中には、製品とプリセールスサポートは優れていても、ポストセールスサポートには力を入れていないベンダーが少なくありません。すべてのサポートオプションを調べて、自社にとって必要なサポートを提供しているかどうかを確認しましょう。

Splunk製品のご紹介

Splunkは、セキュリティチームを混乱から秩序へと導きます。

Splunk SOARは、セキュリティチームの作業の効率化、対応の迅速化、組織全体のセキュリティ態勢の強化を支援します。Splunk SOARにより、繰り返し行うタスクの自動化、セキュリティインシデントの迅速なトリアージと、検出、調査、対応の自動化、セキュリティチームの生産性、効率、正確性の向上、さらに、複数のチームやツールをまたぐ複雑なワークフローの連携と調整による防御力の強化を実現できます。

Splunk SOARは、イベント管理とケース管理、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も備えています。既存のセキュリティインフラを統合して連携させながら、個々の製品の強みを防御戦略に活かすこともできます。

統合の強化

Splunkbaseでは、Splunk SOARと連携および統合できる何千ものサードパーティ製のセキュリティ Appが公開されています。 これらのインテグレーションを使用すれば、Splunk SOARから既存のセキュリティツールにさまざまなアクションの実行を指示できます(たとえばVirusTotalにファイルのレピュテーションチェックを指示したり、CiscoファイアウォールにIPのブロックを指示したりするなど)。Splunk SOARのAppモデルでは350以上のツールと2,100以上のアクションのインテグレーションがサポートされています。これらはすべて、Splunkbaseからダウンロードできます。すぐに使えるこれらのApp、ユーティリティ、アドオンを活用すれば、セキュリティ監視の強化、次世代ファイアウォールの実現、高度な脅威管理など、さまざまな目標を達成できます。

始めましょう

Splunk SOARについて詳しくは、Splunk SOARの無料のコミュニティエディションをダウンロードするか、Splunkの営業窓口にお問い合わせください。

22-23828-Splunk-SOAR Buyers Guide-EB-JA-202208

splunk> turn data into doing