ホワイトペーパー

SOARに必要な10の機能

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)で脅威への対応を迅速化

splunk>
turn data into doing®

進化を続けるサイバーセキュリティ

セキュリティの担当者にサイバーセキュリティ業務で直面している問題をたずねたとしたら、その回答に共通のテーマが出てくることでしょう。たとえば以下のようなテーマです。

- スキルの高いサイバーセキュリティ人材の不足
- 大量のセキュリティアラート
- 管理しきれないほど多数の単体セキュリティ製品
- こうした製品間における統合の欠如
- 長期的にセキュリティ運用の規模拡大に対応できなくなる
- コストの増大、予算の縮小
- マルウェアの巧妙化
- 脅威の検出と対応の遅さ

こうした問題があることを考えると、セキュリティチームが絶えず苦慮を強いられているのも当然です。

その対策として、多くのセキュリティチームが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)ツールに注目しています。SOARソリューションを活用すると、チームが使用するさまざまなセキュリティ製品全体にわたって、セキュリティアクション(調査、トリアージ、対応など)のオーケストレーションを行い、手動で行うしかなかった反復的なセキュリティタスクを自動化することができます。

ただし、SOARといってもさまざまなものが存在します。理想的なSOARソリューションが持つ機能は、セキュリティ運用に対するチームのアプローチを一変させます。具体的には以下のことが可能になります。

- 手動の反復的なタスクを自動化することで業務を効率化
- 検出、調査、対応を自動化してレスポンスを迅速化し、脅威の潜伏時間を短縮
- セキュリティ運用を自動化し、セキュリティチームが他の戦略的な活動に取り組む時間を捻出

理想的なSOARソリューションには、以下のような必須の機能が10種類あります。これらの機能は、セキュリティチームが混乱から脱却してセキュリティ運用の秩序を取り戻すために役立ちます。

理想的なSOARに必要な機能	
オーケストレーション	オーケストレーションとは、複雑なITエコシステム全体で、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。すべてを相互に連携させ、複数の製品やワークフローに及ぶタスクを自動化します。
自動化	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。人手を介することなくプログラムによって脅威の検出、調査、修復を行います。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選別して手動で対応する必要がなくなります。
イベントおよびアラート管理	データをSOARソリューションに取り込んだら、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。
脅威インテリジェンス	セキュリティチームは、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利用できる必要があります。また、アナリストが注目すべき脅威インテリジェンスソースを判別できるように、スコアリング機能も備わっていると効果的です。
ケース管理とコラボレーション	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。複数のアラートやイベントを確認し、1つのケースとして集約し、エスカレーションできる必要があります。その結果、組織のセキュリティチーム全体でコラボレーションとコミュニケーションを効果的に行えるようになるため、セキュリティイベントの解決に要する時間を短縮できます。

メトリクスとレポート作成	何か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。メトリクスは、SOARソリューションの有効性を測定するだけでなく、ROIを向上させるためにできる対策を見つけることもできます。
モバイル対応	SOARソリューションでは、アナリストがモバイルデバイスから簡単にアクセスして管理、操作できることが重要です。これによってアナリストは、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、どこにいても常に通知を受け取ることができます。
拡張性	SOARソリューションは、組織とともに成長していく必要があります。ユースケースは次第に増えるため、プラットフォームは、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、環境をサポート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するように設計されている必要があります。
オープンかつ拡張可能	SOARソリューションは、オープンかつ拡張できるように設計されている必要があります。新しいセキュリティシナリオや製品、アクション、プレイブックを簡単に取り入れることができる必要があります。
コミュニティの充実度	SOARソリューションは、アプリケーション開発のオープンなエコシステムを採用し、コミュニティモデルをサポートしている必要があります。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マイナスの影響を与えることなく、テクノロジーの採用や廃止を自在に行えるため、長期的な成功につながります。

それぞれの機能を詳しく見てみましょう。

オーケストレーション

セキュリティチームがセキュリティインシデントに対応するときは、多種多様なセキュリティツールを使用します。その各ツールが所定のワークフローにおいて、それぞれの役割を果たします。たとえば、VirusTotalでファイルのレピュテーションを調べ、ファイアウォールでIPをブロックし、エンドポイントセキュリティツールで実行可能ファイルをブロックする、といった具合です。オーケストレーション機能が備わっていなければ、セキュリティチームはこういったワークフローを手動で実施することになります。SOARソリューションがあれば、すでに導入されているこれらのセキュリティツールをAPIを活用してすべて統合し、セキュリティツールの各ワークフローを調整して、それぞれのセキュリティインシデントに応じて検出、調査、対応することができます。たとえるなら、各種セキュリティツールは交響楽団を構成する楽器であり、SOARソリューションは指揮者として、すべての楽器が協調してタイミング良く演奏されるようにします。

SOARソリューションを評価する場合、オーケストレーション機能は、特定のセキュリティシナリオに関連するすべてのアクティビティを始めから終わりまで指示、監視できる必要があります。また、あらゆるデータソースからあらゆる形式のセキュリティデータを取り込める必要もあります。また、オーケストレーターは、1つのアクションから出力されたデータの解析、正規化、構造化が適切に行われ、そのデータを後続のアクションで利用できるようにする必要があります。

自動化

セキュリティアナリストの多くは、反復的で単調なセキュリティタスクやセキュリティアクションを1日では処理できないほど大量に抱えており、これらのアクションを手動で行っています。数分から数時間、ときには数日から数週間かかるこれらのアクションを、プレイブックによる自動化では数秒で実行できる必要があります。たとえば、フィッシングの調査では、複数のアクションを4～5種類のセキュリティツールで行う必要があるかもしれません。手動で約40分かかるとしても、自動化プレイブックでは1分未満で終えられると良いでしょう。このようにSOARツールを使用すると、MTTD (平均検出時間)とMTTR (平均対応時間)を劇的に短縮できます。

プレイブックは容易に作成して変更できることが重要です。SOARソリューションに内蔵されている自動化エディターは、アナリストやマネージャーがプロセスを自動化

プレイブックに体系化する際に使用します。このエディターでは、ソースコードの編集と視覚的な編集の両方を実行できる必要があります。そうすれば、セキュリティチームのメンバーの好みやコーディングスキルを問わず、誰でも包括的で高度なプレイブックを作成できます。プレイブックを視覚的なエディターで作成した場合でも、その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、作成者がそれにアクセスして、視覚的なエディターとソースコードエディターをシームレスに切り替えて編集できる必要があります。

イベントおよびアラート管理

データを取り込んだら、イベントおよびアラート管理機能を使用して、受信したイベントとアラートを対応待ちリストに入れて優先順位付けを行います。そうすれば、大がかりな検索をしたり、コンテキストを切り替えたりすることなく、アラートを迅速に処理して効率的に対応することができます。情報を速やかに処理するには、イベントとアラートに、ステータスインジケーター (新規、オープン、クローズなど)、重大度に関するインジケーター、機密度に関する色分けされたインジケーターも必要です。セキュリティシナリオをすばやく把握できるように、セキュリティイベントやアラートの技術的な属性を整理しておく必要があります。たとえば、IP、ドメイン、ファイルのハッシュ値、ユーザー名、メールアドレスなどがわかりやすく表示されることが重要です。さらに、セキュリティアナリストがこのようなデータに対して、調査、封じ込め、対応のアクション(または、プレイブックのような一連のアクション)をシームレスに実行できる必要があります。

そしてSOARソリューションは、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の記録を表示する、包括的なアクティビティログ機能を備えている必要があります。これは、アクションが手動で開始されたかプレイブックを介して開始されたかを問いません。アクションごとに結果が表示され、アクションが成功したか失敗したかを示すインジケーターも含まれている必要があります。

脅威インテリジェンス

脅威インテリジェンスは、攻撃の手口を理解し、組織の被害を抑えるために重要です。インテリジェンスには戦略、戦術、手順の3種類があり、これらを外部ソースと内部ソースから収集し、統合します。インテリジェンスを1カ所に集約したら、ソースと信頼度の観点でデータを評価、分析して、すばやく効果的な判断に必要なデータを特定します。

今日、多くのセキュリティチームが脅威インテリジェンスを使用して、脅威を理解するために役立つ関連コンテキストやインテリジェンスを収集しています。しかし、異なる情報の関連性を把握するために、いくつもの製品の画面を切り替えながら作業しなければならないことがよくあります。また、インテリジェンスフィードを使用する場合でも、送られてくるインジケーターがあまりにも多くて手動では追跡しきれないこともあります。オーケストレーションと自動化機能を備えたプラットフォームなら、集約した情報を1カ所で確認し、情報に基づく判断をすばやく行うことができます。さらに、判断を人手に頼らずに自動化することもできます。

ケース管理とコラボレーション

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を使用して、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を進める必要があります。SOARは複数のイベントをまとめて確認し、1つのケースに集約してエスカレーションします。ケース管理インターフェイスは、アラートのソースデータや、ケースに対するアクションの結果といった、関連する技術データを添付できる必要があります。また、注釈やメモ、メール、スクリーンショット、録音、ケースに関連するあらゆるファイルなど、技術以外の関連データも添付できる機能が必要です。ケースに加えられたあらゆる変更は、監査証跡として記録され、エクスポートできなければなりません。

ケース管理では、組織の既存プロセスに簡単にマッピングできる必要もあります。多くの組織は、インシデント対応時に実施するSOP (標準運用手順書)を用意しています。そのため、ケース管理コンポーネントには、組織のプロセスに沿ってステージを定義し、それをテンプレートとして保存できる機能が必要です。また、SOPを複数のステージに分け、各ステージにタスクを1つ以上振り分けて、それぞれのタスクを担当者に割り当てられる機能も必要です。インターフェイスには、ケースの進捗に関するインジケーターと、ケースのステータスに関するインジケーターが備わっている必要もあります。

理想的なSOARソリューションにはコラボレーション機能も必要です。調査や対応のワークフローでは、コンテキストに即したコラボレーションを実現するために、チャットが組み込まれていたり、ケースのメモを添付して共有できるなどのコラボレーション機能を利用できる必要があります。イベント、アラート、ケースの情報とともに、リアルタイムで使用できるチャットとメモ機能があれば、状況を認識してセキュリティインシデントを効率的かつ迅速に解決できます。また、監査証跡の生成も容易になります。このコラボレーションの記録を取得し、取得した関連イベントデータやアクションとともに整理しておくことが理想的です。SOARソリューション内のワークフロー情報から切り離された外部ツールでコミュニケーションが行われていたら、これは簡単なことではありません。

メトリクスとレポート作成

セキュリティチームにとっては、セキュリティ運用の状態を簡単に測定し、継続的に改善できることも重要です。そのため、強力なメトリクスとレポート作成機能も必須です。これらの機能は、自動化がもたらす効果を把握し、ROIを向上させるためにどのような改善が可能かを見極めるために役立ちます。

自動化は、SOC (セキュリティオペレーションセンター) の部門間を横断して効率を高めるために使用されます。自動化によってパフォーマンスがどのくらい向上し、リソースをどのくらい節約できたかを定量的に把握でき、ダッシュボードでこの情報をいつでも参照できることが重要です。

SOARで把握すべき主なパフォーマンスメトリクスの例としては、MTTR (平均解決時間)、MDT (平均滞留時間)、実行を自動化することで節約できたアナリストの作業時間、実行を自動化することで節約できたFTE (フルタイム当量)、各プレイブックの実行によって短縮できた平均時間、削減できたコスト(FTEあたりのコスト x 節約できたFTE)、オープンとなっているアラートの総数、1日(時間、週、月)あたりのオープン/クローズされたアラート数、SLA (サービスレベル契約)に照らしたパフォーマンスなどがあります。上層部やCISOに、セキュリティ運用の概況とSOARによる改善効果を速やかに理解してもらえるよう、以上の情報をすべて整理してレポートにまとめることが簡単にできる必要があるでしょう。

モバイル対応

SOARソリューションの目的は、対応の迅速化です。迅速な対応を可能にするには、人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連絡する必要があります。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簡単にアクセスして管理、操作できることが重要です。これによってアナリストは、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、どこにいても常に通知を受け取ることができます。

拡張性

SOARソリューションは、組織とともに成長していく必要があります。必要に駆られてユースケースを追加し続けると、時間とともにプラットフォームにかかる処理負荷も高くなります。

自動化エンジンは、スケールアップ(CPUやRAMリソースの追加など)とスケールアウト(サーバーインスタンスの追加など)が可能で、パフォーマンスを最適化し、自動化のROIを確保できるように設計されている必要があります。

オープンかつ拡張可能

SOARソリューションは、新しいセキュリティシナリオや製品、アクション、プレイブックを簡単に取り入れられるように、オープンかつ拡張可能である必要があります。そうでなければ、そのSOARの価値は次第に失われるかもしれません。

共通の基準とプログラミングモデルに従ったオープンなエコシステムがあれば、セキュリティチームはいくつかのメリットを享受できるでしょう。中核のプラットフォームを変更することも、自動化プレイブックに悪影響を及ぼすこともなく、ソリューションに新しいテクノロジーを短時間で統合できます。SOARベンダーの許可や開発サイクルにとらわれずに、統合機能を開発することが可能になります。たとえば、統合用のコードを自分たちで作成したり、自社製アプリケーションを開発したり、ベンダーの早期アクセスAPIを作成したりすることができます。

コミュニティの充実度

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に、専門家たちが連携してプレイブックやベストプラクティス、戦略を共有する必要性が高まっています。SOARソリューションは、活発なコミュニティモデルをサポートし、アプリケーションの統合やプレイブックを容易に共有できる必要があります。

SOARソリューションのインストールベースを評価することで、関連するコミュニティがどの程度コラボレーションの可能性を持っているかを把握できます。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は、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することができ、アイデアをブレインストーミングする機会をもたらします。また、コミュニティにベンダーが参加していれば、そのベンダーはコミュニティとコラボレーションの両方に力を入れていることを示しています。

SOARでセキュリティ運用を改善したいとお考えですか？ Splunkが提供する理想的なSOARテクノロジーを活用すれば、セキュリティチームの効率性と有効性を大幅に強化できます。ぜひ詳細をご覧ください。

営業への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

22-23997-Splunk-10EssentialCapabilitiesofaBest-of-BreedSOAR-WP-A4-JA-202208