Splunk SOAR
5つの自動化ユースケース

splunk>
turn data into doing™

SOC (セキュリティオペレーションセンター)は常に多忙を極めています。アナリストのもとには大量のセキュリティアラートが届き、脅威の調査と解決が追い付かないことも少なくありません。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、こうした単調で定型的な繰り返しのタスクに溢れています。

さらに、サイバーセキュリティ人材の深刻な人手不足が、日々発生する数千単位のアラートへの対応を一層難しくしています。結果として、脅威の検出と対応に顕著な遅れが出て、ビジネスに悪影響を及ぼすだけでなく、ユーザーや資産が危険にさらされるおそれもあります。

しかし、救いはあります。Splunk SOARを使用すれば、この混乱を抜け出して、秩序をもたらすことができます。ムダな業務を排除し、セキュリティ運用を合理化して、アラートをかつてないスピードで検出、トリアージし、対応できます。

SOAR (Security Orchestration, Automation and Response: セキュリティのオートメーションと自動化によるレスポンス)ソリューションによって定型的な日常業務を処理し、組織内で使用しているさまざまなITツールやセキュリティツールのオーケストレーションを実現して、検出、調査、封じ込めを含むあらゆるプロセス、さらにはチケットを通じたチーム間連携などのコミュニケーションを一元的に管理できます。さらに、処理を自動化して人手の介入をなくすこともできます。

この電子書籍では、SOARで一般的な5つのユースケース、各ユースケースを実現するための手順、Splunk SOARで事前構築済みのプレイブックを使ってこれらの手順を自動化する方法をご紹介します。

目次

1. アラートのエンリッチメント

セキュリティアラートの調査でまずやるべきは、IPアドレス、URL、ユーザー名、ドメイン、ハッシュなどから侵害の痕跡(IOC)を見付け出すことです。これは、アラートの重大度を判断するために役立ちます。多くの場合は次に、データを手動で調査して関連するコンテキストを探ることや、複数の脅威インテリジェンスプラットフォームを切り替えながら詳細情報を収集します。

SOARツールを使用すれば、SOC内の異なるツールからインテリジェンスを簡単に収集して統合し、アラートのデータをエンリッチして、1つの画面にまとめて表示できます。さまざまなソースからデータを収集してエンリッチするプロセスを自動化することで、アナリストはアラートを受け取ると同時に、重要な関連情報を確認できます。オーケストレーションと自動化は、セキュリティアラートの調査と対応の大幅な迅速化に役立つだけでなく、異なるソースからデータを収集して統合し、アラートをエンリッチできるメリットもあるのです。

Recorded Future Indicator Enrichmentプレイブックでは、調査対象のイベントに、ファイルハッシュ、IPアドレス、ドメイン名、URLの情報がエンリッチされます。これら関連する脅威インテリジェンスやIOCの詳細をコンテキストとして追加することで、調査を迅速化できます。Recorded Futureは、アナリストが脅威にすばやく対応するために役立つ追加コンテキストを提供するセキュリティインテリジェンスプラットフォームです。

このプレイブックには以下のアクションが用意されています。

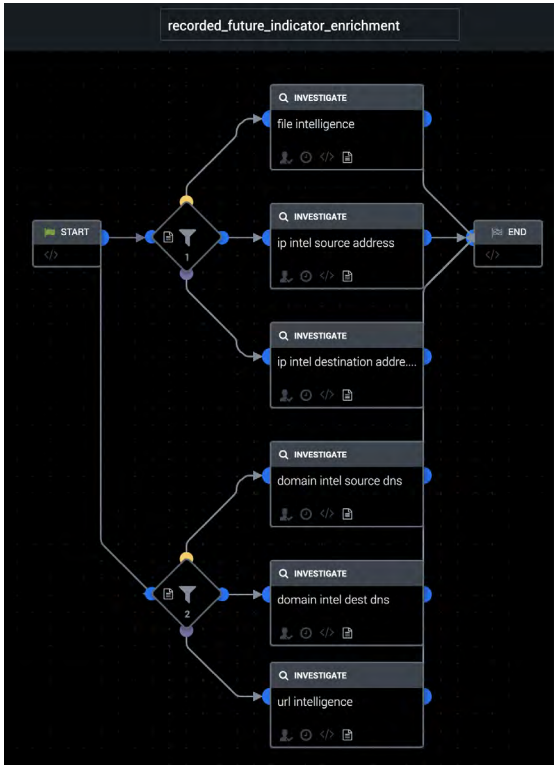
1. **ドメインインテリジェンス：**ドメインに関する脅威インテリジェンスを取得します
2. **ファイルインテリジェンス：**ハッシュによって特定されたファイルに関する脅威インテリジェンスを取得します
3. **IPインテリジェンス：**IPアドレスに関する脅威インテリジェンスを取得します
4. **URLインテリジェンス：**URLに関する脅威インテリジェンスを取得します

努力に頼るよりも、スマートに仕事をしましょう。Splunk SOARでアラートのエンリッチといった定型作業を自動化すれば、セキュリティアナリストはアラートについて必要な情報をすべて手に入れた状態で調査を開始できます。この事前構築済みのプレイブックをSplunk SOARで使用することにより、あらゆる調査に対応する分析情報をすばやく収集できます。

プレイブックを入手

Norlys社のセキュリティチームは、「面倒なことは自動化」と決めて業務にあたっています。その結果、現在では毎日20種類のプレイブックを使ってコストと時間を節約しています。

> **「Splunk SOARを使用することにより、週に35時間、1日あたりで5時間節約しています。おかげで重要な作業に集中できるようになりました」**
>
> — Norlys社セキュリティアナリスト、Tibor Földesi氏



2. フィッシングの調査と対応

Verizon社の『2021年度データ漏洩/侵害調査報告書』[1]によると、過去2年間に発生したデータ漏洩/侵害の原因にフィッシングは依然として上位に挙げられています。フィッシング攻撃は今日でも、組織が直面する主な脅威として蔓延しているのです。

フィッシングメールの調査は通常、初期データの分析とアーティファクトの調査から始まります。調査対象になるアーティファクトには、メールの添付ファイル、正規のURLに偽装したリンク、メールヘッダー、送信者のメールアドレス、メールの本文などがあります。メールが悪質だと判断されたら、組織内で被害が広がるのを防ぐため、セキュリティアナリストが封じ込めの措置を講じなければなりません。通常は、ユーザーがメールを開く前に、セキュリティアナリストがユーザーのメールボックスからそのメールを削除します。しかし、フィッシングメール1件1件についてこのすべての手順を手動で行うとしたら、想像するだけでも大変です。

Splunk SOARを利用しているあるお客様は[2]、フィッシングアラートの調査と封じ込めに、以前は1件あたり平均90分かかっていたそうです。その上、SOCに届くフィッシングメールの数は1日あたり最大300件にのぼります。この場合、セキュリティアナリストが大量のアラートの調査と対応に常時追われるだけでなく、その手順を1つずつ手動で行うために時間がかかり、脅威が組織全体に及んで、取り返しのつかない損害が生じるおそれがあることも問題です。

このユースケースでは、受信したフィッシングメールを自動的に調査して封じ込めるPhishing Investigate and Respondプレイブックが役立ちます。このプレイブックには合計15のアクションが用意されています。Splunk SOARが第三者ソースからのフィッシングメールアラートを受信すると(メールサーバーからメールを直接取得するなど)、プレイブックが自動的に開始され、以下のアーティファクトが分析されます。

1. **ファイルレピュテーション:** VirusTotalにファイルのレピュテーション情報を問い合わせます
2. **URLレピュテーション:** Webサイトのリンクを1件ずつWildFireに送信して評価を得ます
3. **ドメインレピュテーション:** 該当するドメインのリスクを評価します
4. **IPレピュテーション:** VirusTotalにIP情報を問い合わせます
5. **IPアドレスの位置情報検索:** MaxMindにIPの位置情報を問い合わせます
6. **Whoisドメイン検索:** 該当するドメインのWhois検索を実行します
7. **Whois IP検索:** 該当するIPのWhois検索を実行します

さらにメールに含まれる添付ファイルとURLに関する情報が収集され、次の2つのアクションが開始されます。

8. **ファイルのデトネーション:** ファイルをThreat Gridサンドボックスで実行して分析結果を取得します
9. **URLのデトネーション:** URLをThreat Gridサンドボックスで読み込んで分析結果を取得します

1 『2021年度データ漏洩/侵害調査報告書』
2 お客様事例:Rackspace社でのフィッシング調査の自動化

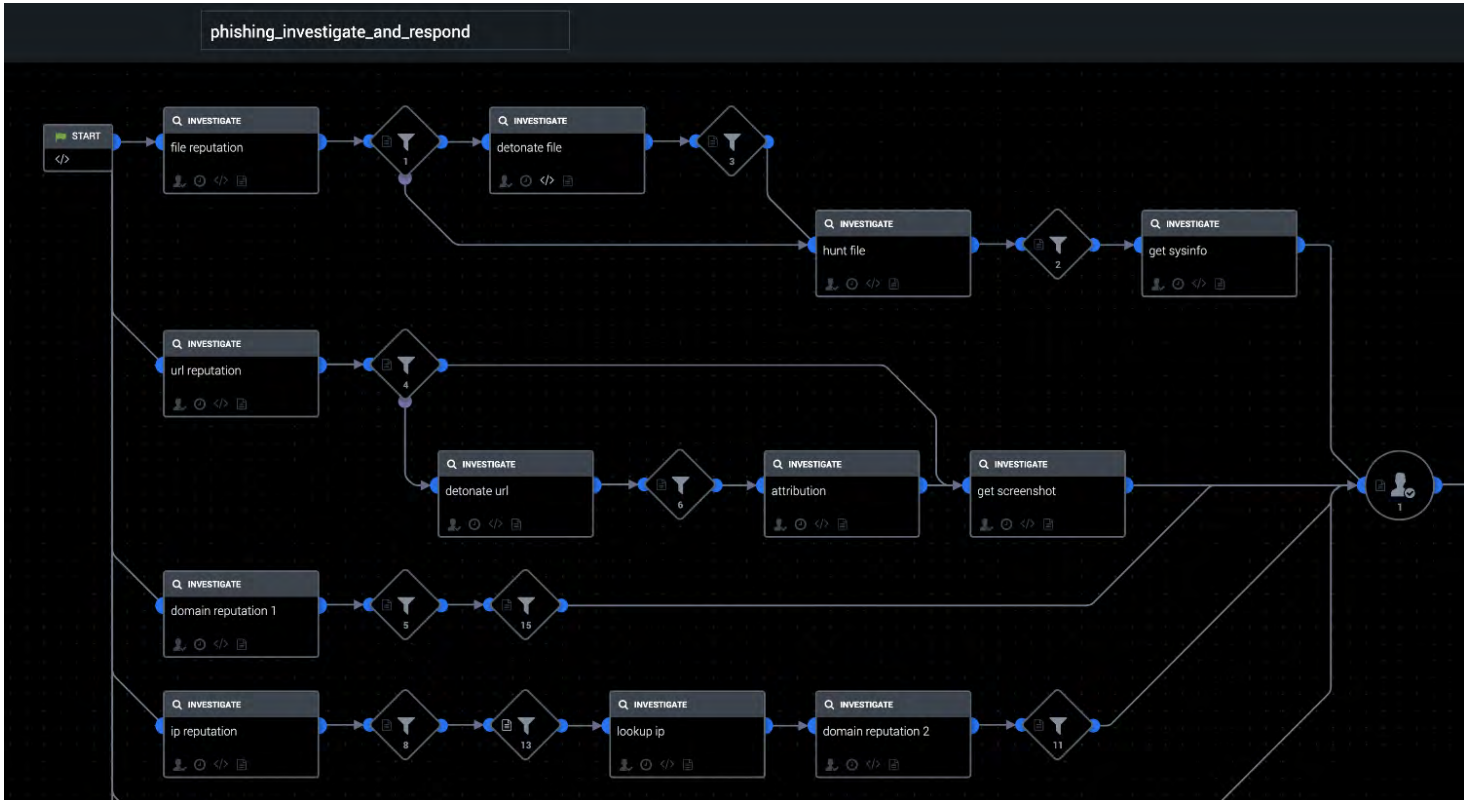
調査フェーズでファイル、URL、IPアドレス、またはドメインに不審な点が見付かった場合は、規定のパラメーターに基づいてフィッシングメールかどうかが判断され、必要に応じてユーザーの受信箱からメールを削除することで脅威が封じ込められます。

Splunk SOARを活用して潜在的な脅威から組織を守れば、フィッシングアラートの調査と対応の迅速化にもつながります。

プレイブックを入手

「漏洩/侵害の原因としてフィッシングは36%を占め、昨年の25%から増加しています」

— Verizon社『2021年度データ漏洩/侵害調査報告書』

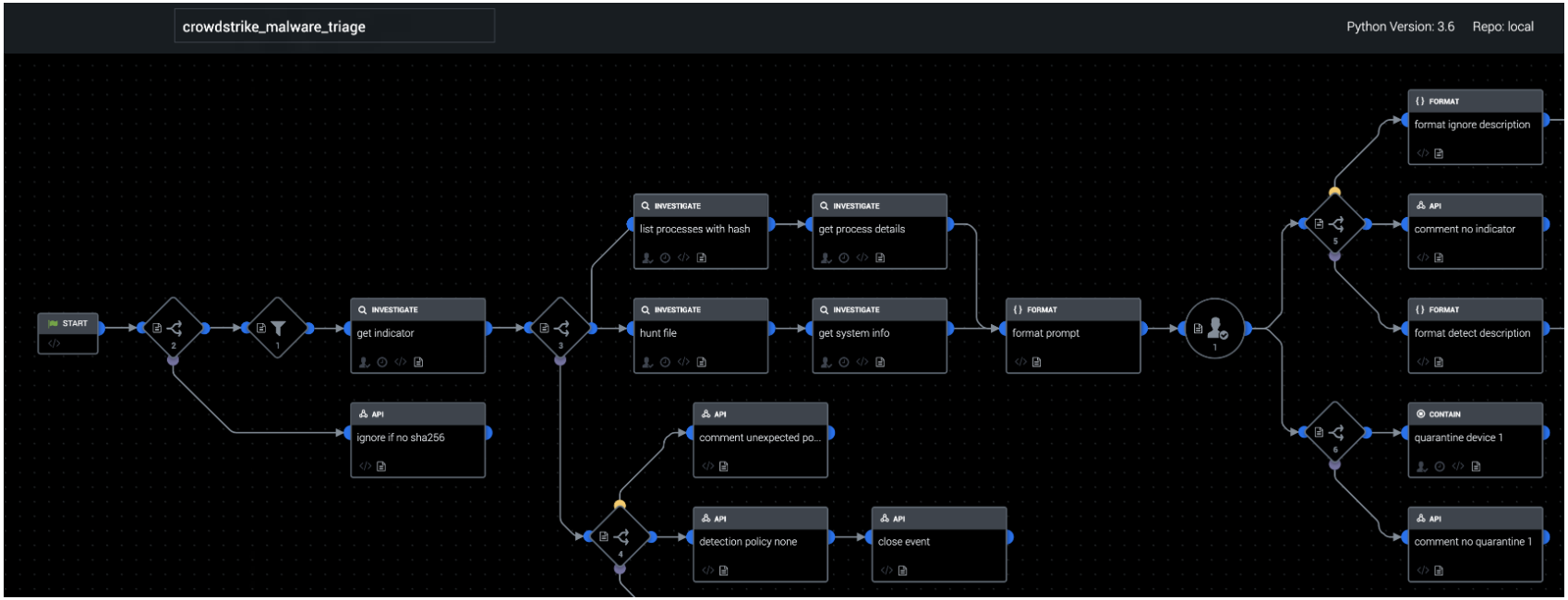


3. エンドポイントでのマルウェアトリアージ

EDR (エンドポイント検出/対応)ツールは、ネットワーク内のエンドポイントを監視し、そのアクティビティデータを収集するために役立ちます。世の中がより柔軟なリモート・ワークの状況へと移行し、クラウドベースのインフラが普及する中で、エンドポイントの可視化はどの組織でもセキュリティチームにとって大きな課題です。

EDRツールやEPP (エンドポイント保護プラットフォーム)ツールを使用すれば、組織のシステム内のエンドポイントで不審なアクティビティが発生していないかどうかを監視できます。一方、これらのツールでは大量のアラートが生成され、その中には実際に脅威を示すものもありますが、誤検知もある程度含まれます。SOARツールを使用すれば、EDR/EPPツールによる判定とアクションを一元的に管理して、誤検知を取り除き、リスクレベルを判断して、適切な対策を講じることで、大量アラートの調査、トリアージ、対応を迅速化できます。

これらの作業に対応するのがCrowdstrike Malware Triageプレイブックです。このプレイブックでは、Crowdstrikeで検出されたアラートをエンリッチし、重要度を判断するためのコンテキストが追加されます。すべての情報が収集されたら、アナリストに確認を求める通知が送られます。そしてアナリストの判断に応じて、問題のファイルをCrowdstrikeのカスタムインジケーターリストに「detect」または「none」の検出ポリシーで追加し、必要に応じてエンドポイントをネットワークから隔離できます。このプレイブックのもう1つのメリットは、過去のアラートと一致するアラートを検出し、ファイルハッシュを分類することで、将来同じアラートが発生したときに、アナリストによる確認を省いて同じ対応策を自動的に実行できる点です。



このプレイブックには以下のアクションが用意されています。

1. **インジケーターの取得：**タイプと値を提供してIOCを取得します
2. **プロセス詳細の取得：**該当するプロセスIDで実行中か以前に実行されたプロセスの詳細を取得します
3. **システム情報の取得：**該当するデバイスIDを持つデバイスの詳細を取得します
4. **ファイルの追跡：**ハッシュを問い合わせてネットワーク上でそのファイルを追跡します
5. **プロセスのリスト：**特定のデバイス上でIOCを最近使用したプロセスをリストします
6. **デバイスの隔離：**デバイスをブロックします
7. **インジケーターのアップロード：**CrowdStrikeで監視したい1つ以上のインジケーターをアップロードします

「Splunk SOARによる自動化によって、マルウェアに関するメールアラートにこれまで30分以上かかっていたのが、たった約40秒で処理できるようになりました」

— Blackstone社CISO、Adam Fletcher氏

Ponemon Instituteの調査によると、組織が1日に受信するマルウェアアラートは平均1万7,000件に及びます[3]。これほど大量のアラートを受信すると、対応の優先順位を判断することは極めて困難です。大手投資会社のBlackstone社は、Splunk SOARを使用することで、受信アラートのトリアージと処理にかかる時間を1分以内に短縮しました。このお客様事例はこちらからご覧いただけます。

Splunk SOARでこの事前構築済みのプレイブックを使用すれば、アラートをトリアージして、特に大きな損害につながる可能性のあるアラートを抽出できます。

プレイブックを入手
デモを見る

3 Ponemon Institute『The Cost of Malware Containment』

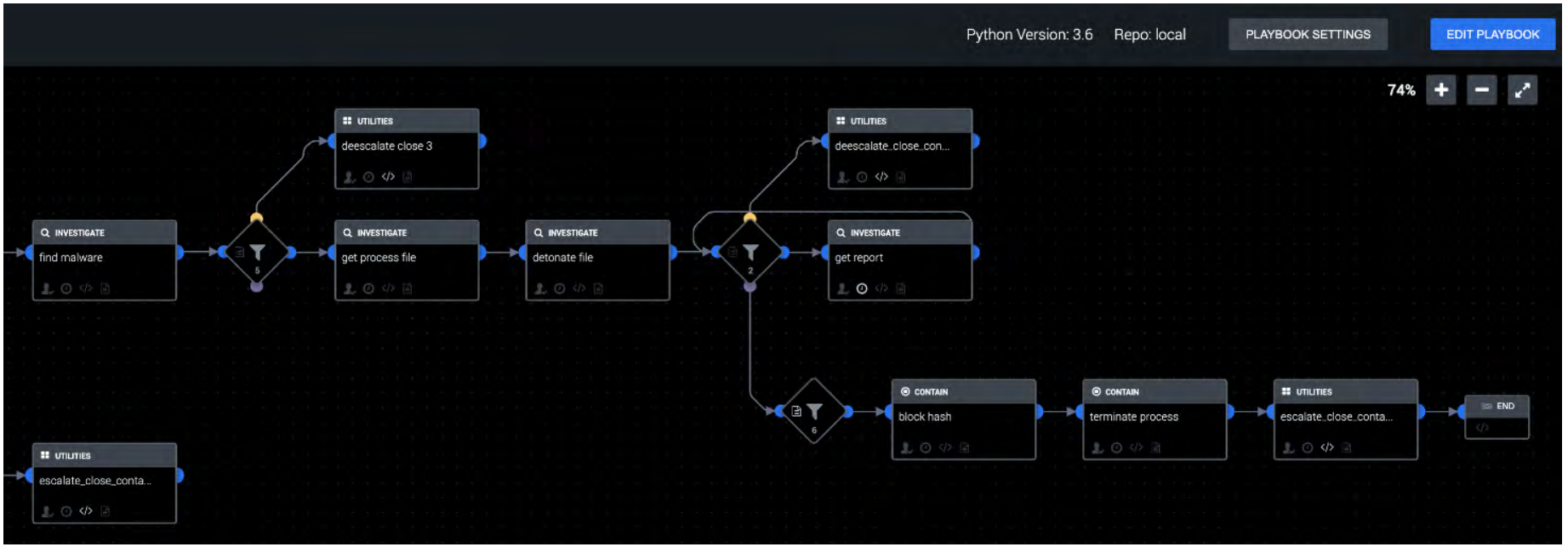
4. コマンドアンドコントロール：調査と封じ込め

コマンドアンドコントロール(C&CまたはC2)攻撃では、攻撃者がコンピューターに侵入した後、そのコンピューターに指令(コマンド)を送ります。まず、ソフトウェアアプリケーションの脆弱性を突くか、フィッシングメールで偽のURLまたは添付ファイルをユーザーに開かせて悪質なコードを実行することで、コンピューターに侵入します。

次に、侵入したコンピューターと攻撃者のサーバー間で接続を確立し、サーバーからコマンドを送ることでそのコンピューターを乗っ取ります。その後、いくつかの攻撃を実行して、ネットワーク上の他のコンピューターに侵入したり、機密ファイルを盗み出したり、システムを停止させたりします。

Splunk SOARを使用すれば、C2攻撃シナリオの調査と封じ込めにかかる時間を数時間から数分に短縮できます。

Splunk SOARでは、C2攻撃のアラートを受信すると、C2 Investigate and Containプレイブックが開始されます。このプレイブックでは、C2攻撃シナリオに適切に対応するための調査手順と必要に応じて封じ込め手順が実行されます。侵入を受けたVMからファイルと接続情報が抽出され、情報がエンリッチされた後、重大度に応じて封じ込め措置が実行されます。重大度は、脅威スコアが50を超えるファイルや、レピュテーションステータスが「MALICIOUS(悪質)」のIPアドレスなどを基準に判断されます。



このプレイブックには以下のアクションが用意されています。

1. **ハッシュのブロック：**ハッシュをCarbon Blackのブラックリストに追加します
2. **IPのブロック：**IPをブロックします
3. **マルウェアの検出：**Volatility Malfindプラグインを実行して、ユーザーモードのメモリーに挿入されたコード/dllを検出します
4. **IPの位置情報検索：**MaxMindにIPの位置情報を問い合わせます
5. **プロセスファイルの取得：**メモリーダンプからプロセスファイルを抽出します
6. **レポートの取得：**AutoFocusタグに関する詳細を取得します
7. **IPの追跡：**IPを追跡して関連タグのリストを取得します
8. **VMのリスト：**登録済みのVMのリストを取得します
9. **メールの送信：**メールを送信します
10. **VMのスナップショット：**VMのスナップショットを作成します
11. **プロセスの終了：**マシンで実行中のプロセスを終了します
12. **Whois IP検索：**該当するIPのWhois検索を実行します

この事前構築済みのプレイブックをSplunk SOARで使用すれば、C2攻撃シナリオを調査して封じ込めることができます。

プレイブックを入手

「SolarWinds攻撃について私が最も驚いたのは、そのスパイ技術の高さです。攻撃自体が完璧であっただけでなく、地理的に正しいかターゲットにうまく偽装したIP、VPS、ドメインを使用して痕跡を隠す手法も非常に巧みでした」

— Splunkディスティングイッシュドセキュリティストラテジスト、Ryan Kovar

5. 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、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。

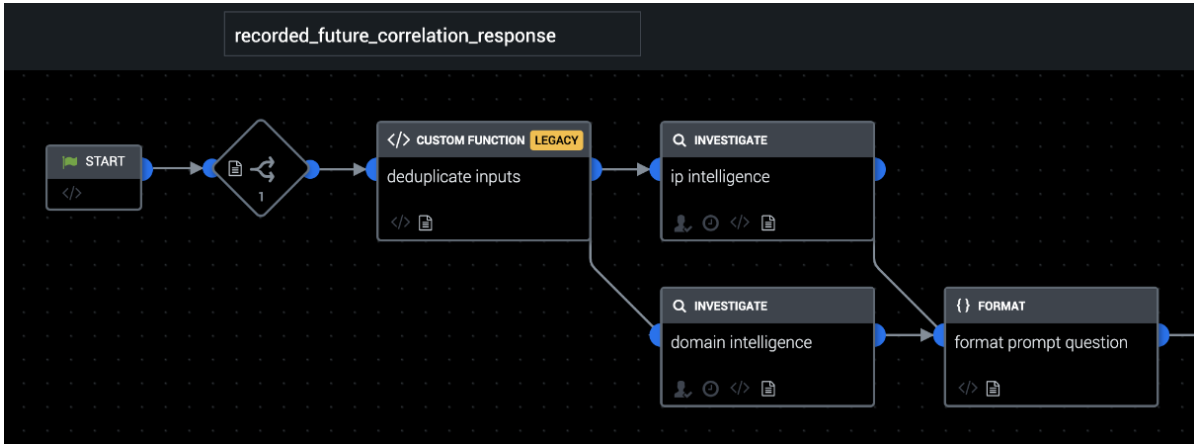
今日、多くのセキュリティチームが脅威インテリジェンスプラットフォームを使用して、脅威をすばやく理解するために役立つ関連コンテキストやインテリジェンスを収集しています。しかし、異なる情報の関連性を把握するために、さまざまな製品の画面を行き来しながら作業しなければならないことがよくあります。また、インテリジェンスフィードを使用する場合でも、送られてくるインジケーターがあまりにも多くて手動では追跡しきれないこともあります。オーケストレーションと自動化機能を備えたプラットフォームなら、集約した情報を1カ所で確認し、情報に基づく判断をすばやく行うことができます。さらに、判断を人手に頼らずに自動化すること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

このユースケースでは、Recorded Future Correlation Responseプレイブックを使用することで、Splunkの相関サーチに役立つ関連ネットワークインジケーターについてより多くのコンテキストを収集できます。このプレイリストでは、十分なコンテキストが収集されて、アナリストが承認し次第、アクセスが自動的にブロックされます。まず、トラフィックの監視データをRecorded Futureのバルク脅威フィードと照合して、リスクの高いネットワーク接続を特定し、その情報をSplunk SOARに転送します。Splunk SOARは、そのネットワークインジケーターが脅威リストに含まれる詳しい理由をRecorded Futureに問い合わせて、該当するIPアドレスとドメイン名をブロックするかどうかの判断をアナリストに提示します。この例では、ネットワーク監視データのソースとしてCisco WSAの「レイヤ4トラフィックモニタ」を使用しています。この場合、Cisco Firepower NGFWによって境界でのブロック措置を実行し、Cisco UmbrellaによってDNSシンクホールを設定できます。

このプレイブックには以下のアクションが用意されています。

1. **IPのブロック：**IPネットワークをブロックします
2. **ドメインインテリジェンス：**ドメインに関する脅威インテリジェンスを取得します
3. **IPインテリジェンス：**IPアドレスに関する脅威インテリジェンスを取得します

プレイブックを入手



Recorded Future Correlation Responseプレイブックでネットワークアクセスをブロックした後、Splunk SOARが第2のプレイブックを実行することによって、URLを調査、追跡、ブロックできます。さまざまなセキュリティ製品のアクションを一元管理できるだけでなく、1つのインシデントを解決するために複数のプレイブックを実行できることもSplunk SOARの利点です。

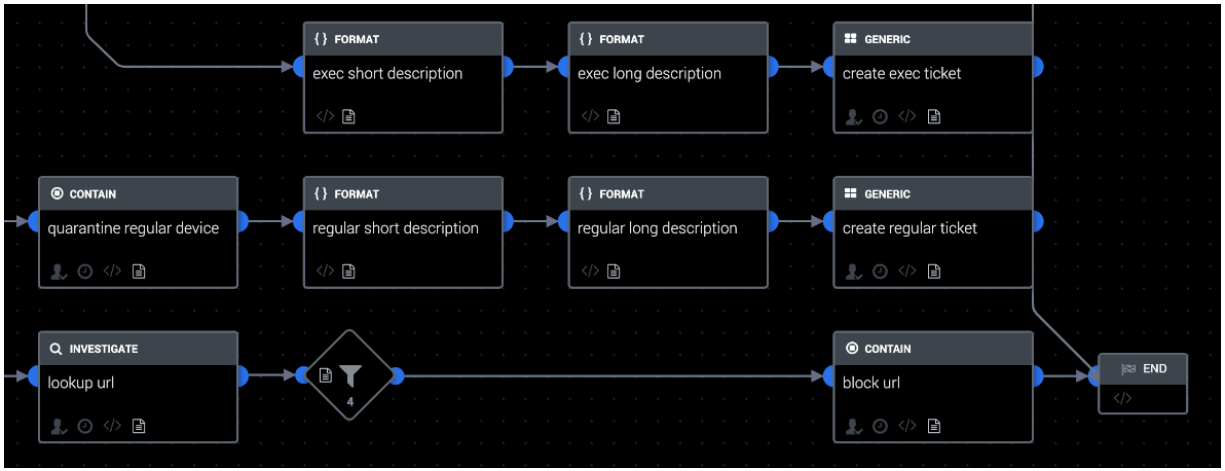
不審なURLが検出されたら、Zscaler Hunt and Block URLプレイブックを使用して、そのURLにアクセスしたデバイスを特定し、組織内での重要度に基づいてトリアージできます。続いて、URLの危険度と、影響のあるデバイスの使用者が経営幹部かどうかに基づいて、URLをブロックし、適切なServiceNowチケットを作成できます。このプレイブックは、VirusTotal、Zscaler、Microsoft Exchange、ServiceNow、Splunk、Carbon Blackでサポートされます。

このプレイブックには以下のアクションが用意されています。

1. **URLのブロック：**URLをブロックします
2. **チケットの作成：**インシデントを作成します
3. **ユーザー属性の取得：**ユーザーの属性を取得します
4. **URLのルックアップ：**URLに関連するカテゴリを検索します
5. **デバイスの隔離：**エンドポイントを隔離します
6. **クエリーの実行：**指定のクエリーに従ってオブジェクトデータを取得します
7. **URLレピュテーション：**VirusTotalにURL情報を問い合わせます

脅威インテリジェンスを活用してさまざまなユースケースを補強すれば、セキュリティチームがアラートを調査する際の重要なリソースとして役立ちます。事前構築済みのこれらのプレイブックを活用すれば、脅威のインジケータの追跡にかかる時間を短縮して、より重要な作業に集中できます。

プレイブックを入手



セキュリティ運用を強化する

SOARの概要といくつかの一般的なユースケースについて紹介しました。ぜひ自動化とオーケストレーションを取り入れて、セキュリティチームを強化し、大量アラートの克服と生産性の向上を目指してください。最後にまとめると、SOARには以下のメリットがあります。

- 脅威の調査と対応を迅速化する
- SOCの効率と生産性を向上させる
- アナリストの単純作業をなくし、負担を軽減してスマートに仕事ができるようにする
- 手に負えなくなっていたセキュリティ業務を適切に管理する

無料のコミュニティエディションと事前構築済みのプレイブックをお試しいただけます。

詳細はこちら

21-19396-Splunk-Five Automation Use Cases For Splunk SOAR-EB-JA-202109

splunk> turn data into doing™