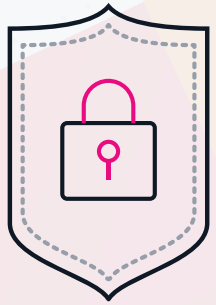
セキュリティ
エッセンシャルガイド

Splunkのセキュリティ製品で課題を解決する



splunk>
turn data into doing™

サイバーセキュリティの対策は万全ですか?

最悪の事態に備えただけで
最善の結果を期待していませんか?

目次

新たな攻撃者を追跡・検出し、組織を保護する最も効果的な方法とはどのようなものでしょうか。

組織全体の防御システムに対して部分的な対応でなく、包括的なアプローチをとるべきです。

はじめに

サイバーセキュリティの対策は万全でしょうか?最悪の事態に備えただけで最善の結果を期待していませんか?デジタルテクノロジーは日常生活のあらゆる場面に浸透しています。そして毎日のように新たな脅威が出現しています。このような状況で組織が資産を守り、攻撃者を検出するためには、情報を集めて適切な備えをすることが必要不可欠です。

メディアで取り上げられるような組織への侵害や世界中で多発したランサムウェア攻撃、クリプトマイニング(暗号通貨発掘)の被害を考えると、組織が適切にデータを収集、活用、分析しなければならないと考えるのは当然です。さらに、多様で急速に増え続けるマシンデータに対応するために適切なプロセスと手順を確立し、多くの場合それと並行して新しいテクノロジー、手法、要件を取り入れる必要があります。

では、組織を保護し、新たな攻撃者を追跡して検出する最も効果的な方法とはどのようなものでしょうか。組織全体の防御システムに対して部分的な対応でなく、包括的なアプローチをとるべきです。Splunkは、すべての組織がこのガイドで説明するセキュリティジャーニーの6つのステージを経て、セキュリティセンターの中枢、Nerve Centerを構築する必要があると考えます。

それでは、Nerve Centerとは何かを詳しく見ていきましょう。

Splunk製品が変革するセキュリティオペレーションセンター（SOC）

データ主導のビジネスは、調査、監視、分析、実行(IMAA)モデルを活用することで、人材、プロセス、テクノロジーが最適化され、セキュリティを強化できます。Nerve Centerモデルでは、セキュリティテクノロジースタックのデータをすべて使用するため、手動、半自動、あるいは全手を自動化させて脅威を調査、検出し、連携的な対応を迅速に実行することができます。また、セキュリティインフラストラクチャへの投資がセキュリティエコシステムとスキルの強化につながるため、セキュリティ対策を新しい領域に拡大して脅威にプロアクティブに対応できるようになります。

SplunkのData-to-Everythingプラットフォームと Splunkのセキュリティポートフォリオは、複数のサイバーセキュリティ領域とセキュリティ以外の領域を統合することで、コラボレーションを促進してデータ処理のベストプラクティスを実現します。セキュリティチームはSplunkソリューションを使用して統計分析、視覚的分析、行動分析、探査的分析を実行することにより、情報に基づいて意思決定を行い対策を実施できます。これを基盤として、データの収集から、サイバー脅威やセキュリティ課題への対応の実行まで、最先端のワークフローを確立できます。

図1：Splunk Enterprise Securityには、データのやり取りや処理の呼び出しを行うための共通フレームワークが含まれています。セキュリティチームはAdaptive Operations Frameworkを利用することで、迷いなく迅速に自社環境に変更を適用できます。Splunk Enterprise Securityではレスポンスを自動化することもできます。これによって各ドメインに適したさまざまな処理を使用し、セキュリティインフラを攻撃者に適応させることができます。

運用方法

では、Nerve Centerモデルによってセキュリティを強化するには具体的に何をすればよいでしょうか。

このガイドでは、その運用方法を計画するための足がかりとして、組織が直面する特に重要なセキュリティユースケースを紹介し、Splunkの分析主導型プラットフォームがセキュリティ課題の解決にどのように役立つかを説明します。このガイドは次の3つのセクションに大きく分けられます。

1. **基本を理解する**
   セキュリティジャーニーの概要を紹介し、セキュリティユースケースの概要および各ユースケースとSplunkソリューションの対応関係について説明します。

2. **分析主導型セキュリティジャーニーを始める**
   データ主導型セキュリティジャーニーの6つのステージについて説明し、各段階で何をどの程度実行できるかを紹介します。

3. **一般的なセキュリティ課題をSplunkで解決する**
   以下の領域に関する一般的なセキュリティ課題の解決例を紹介します。

- インシデント調査とフォレンジック
- セキュリティ監視
- 高度な脅威検出
- SOC自動化
- インシデントレスポンス、コンプライアンス
- 不正行為の分析と検出
- 内部脅威

今こそ徹底したセキュリティ対策を構築する時です。

基本を理解する

サイバー犯罪者はその活動を止めることはありません。そのため、常にセキュリティに関する新しいユースケースとインサイトを収集し、組織の保護レベルを高く維持する必要があります。

Splunkはそのお手伝いをします。

Splunkの分析主導型セキュリティジャーニー

「うちの組織は安全なのか」と始終尋ねられる立場にあるセキュリティチームは、サイバーセキュリティとは旅、ジャーニーであり、目的地ではないことを知っているでしょう。この旅に終着点はなく、常に挑戦を求められますが、それを乗り越える方法は必ずあります。

まず、自社の環境について理解して、どこから手をつけるのかを決める必要があります。考えるべきことは何か、何を守りたいのか、特に重要なデータはどれか、そして、脅威にどのように対応するかです。

6つのステージから成る分析主導型セキュリティジャーニー (図2)は、これらの疑問に対する答えを導き、徹底したセキュリティ対策を構築するために役立ちます。それを実現すれば、現在のセキュリティ対策の欠陥を把握し、次の課題を確認して、その課題に正面から取り組むというサイクルを確立できます。

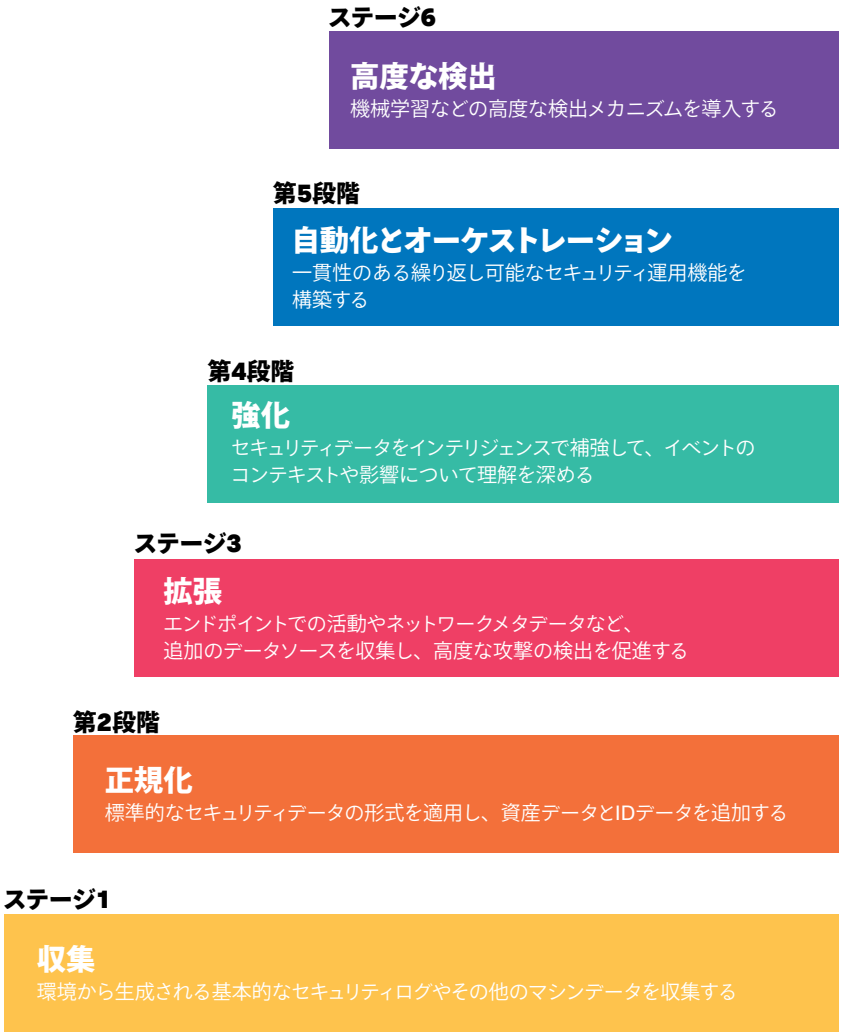


図2：Splunkの分析主導型セキュリティジャーニー

Splunkのセキュリティスイート

ハイキングをするときに、地図を確認せず、食糧や適切な装具を詰め込んだリュックサックも持たずに出発することはありますか？もちろんないでしょう。旅が適切な装備なしには成功しないのと同じように、セキュリティジャーニーも適切なテクノロジーがなければ成功しません。

Splunkのセキュリティスイートは、変化の激しいデジタルビジネス環境で、セキュリティチームが未知の領域を前進し、脅威を検出、調査して、それに対応し、適応できるように支援します。ティア1のアナリストは、Splunkソリューションを使って、期間、キーワード、IPアドレス、マシン名などに関する基本的な調査を実施できます。さらに、ティア2とティア3のアナリストは、同じ製品を使用して高度な相関付け、分析モデルの構築、詳細なフォレンジック調査などの作業を行うこともできます。

Splunkのセキュリティスイート	
Splunk Enterprise	幅広いセキュリティユースケースに対応し、あらゆるソースからのマシンデータを監視してすばやく分析し、行動につながるインサイトを提供する柔軟なプラットフォームです。セキュリティを包括的に強化するための分析主導型セキュリティの基盤にもなります。このソリューションはクラウドでも利用できます。
Splunk Enterprise Security	さまざまなセキュリティテクノロジーから生成されたマシンデータ(ネットワーク、エンドポイント、アクセス、マルウェア、脆弱性、ID情報など)に関するインサイトを提供する、SIEM(セキュリティ情報/イベント管理)ソリューションです。このソリューションはクラウドでも利用できます。
Splunk User Behavior Analytics	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に必要な情報を導き出す、機械学習を活用したソリューションです。
Splunk SOAR	既存のセキュリティテクノロジーと統合して、それらのテクノロジー間を結合するレイヤーとして機能し、セキュリティ環境をスマート化、高速化、強化する、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)プラットフォームです。
Apps	Appsは、Splunk、Splunkパートナー、Splunkコミュニティが開発した、Splunkプラットフォームの能力をさらに引き出す一連のアプリケーションです。たとえば、ペイメントカード業界のコンプライアンスに対応するためのSplunk App for PCI Complianceなどがあります。このソリューションはクラウドでも利用できます。
Splunk Security Essentials	Splunk Security Essentialsでは、新しいユースケースを参照して、Splunk Enterprise、Splunk Cloud、Splunk SIEM/SOAR製品へセキュリティの検出機能をデプロイできます。このAppはSplunk Cloudの有効なライセンスでフルサポートされており、セキュリティ体制の強化にすぐに着手して、価値実現までの時間を短縮できます。
Splunk Enterprise Security Content Update	Splunk Enterprise Security (ES)を利用するお客様向けに、「分析ストーリー」と呼ばれるセキュリティ分析ガイドを提供します。このガイドでは、環境内で新たに検出された脅威を調査してそれに対応するための、Splunk ESの最適な利用方法、実装すべきサーチ、達成できる成果を確認できます。

セキュリティに関するユースケース

次の表に、このジャーニーに対応する具体的なセキュリティユースケースを示します。これを確認し、自社の状況に合わせてセキュリティに関する課題を選択してください。このガイドの目的は、Splunkの分析主導型プラットフォームによってセキュリティの課題をどのように解決し、以下のようなセキュリティジャーニーをどのように進めることができるのかを示すことです。

Splunkソリューションとセキュリティユースケースの対応関係

ユースケース	Splunkソリューション
インシデント調査とフォレンジック	Splunk Enterprise、Splunk Enterprise Security、Splunk SOAR
セキュリティ監視	Splunk Enterprise、Splunk Security Essentials App、Splunk Enterprise Security、Splunk SOAR
高度な脅威検出	Splunk Enterprise、Splunk Security Essentials App、Splunk Enterprise Security、Splunk User Behavior Analytics
SOC自動化	Splunk Enterprise、Splunk Enterprise Security、Splunk SOAR
インシデントレスポンス	Splunk Enterprise、Splunk Enterprise Security、Splunk SOAR
コンプライアンス	Splunk Enterprise、Splunk Security Essentials App、PCI、Splunk Enterprise Security
不正行為の分析と検出	Splunk Enterprise、Splunk Security Essentials App、Splunk Enterprise Security
内部脅威の検出	Splunk Enterprise、Splunk Security Essentials App、Splunk User Behavior Analytics

セキュリティに関するユースケースの定義

ここで、認識を合わせるためにユースケースについて簡単に説明します。

インシデント調査とフォレンジック

セキュリティインシデントは警告なく発生する可能性があり、多くの場合は長期間にわたって検出されないため、組織に深刻な脅威をもたらします。セキュリティチームが問題に気付く頃には、高い確率ですでに被害が発生しているのが一般的です。Splunkを使用すれば、セキュリティチームは「単一の情報源」からコンピューター、環境内にあるすべてのタイムスタンプ付きマシンデータを得ることができます。これを利用することで、より迅速で精度の高いセキュリティ調査を行い、長期間にわたって脅威が検出されずに残る確率を下げることができます。

セキュリティ監視

セキュリティ監視によって、ほぼリアルタイムで継続的に送られる、脅威やその他のセキュリティの問題の兆候を示すデータストリームを分析できます。監視対象となるデータソースには、ネットワークやエンドポイントシステムのほか、クラウドデバイス、データセンターシステム、アプリケーションが含まれます。セキュリティチームは、SplunkのData-to-Everythingプラットフォームを使用して、これらのソースから提供されるデータストリームから脅威を検出し、対応の優先順位を決めることができます。

高度な脅威検出

APT (Advanced Persistent Threat)とは、ステルス性の高い継続的なコンピューターハッキングプロセスであり、多くの場合は特定のエンティティを標的として1人以上の攻撃者が連携して行います。一般に、APTはビジネスまたは政治的な目的を達成するために民間組織や政府機関を標的として行われます。Splunk Enterpriseを使用すると、組織はデータを検索して相関付け、高度な脅威を追跡できます。Splunk Enterprise SecurityとSplunk User Behavior Analyticsでは、統計分析、異常検出、機械学習技術によって未知の脅威や高度な脅威を検出することで、既存の機能を拡張してキルチェーン手法を適用できます。

SOC自動化

セキュリティオペレーションチームは、Splunkソフトウェアを導入することで、情報の追加や対応策の実行、さらにはケース管理(インシデント管理)のオーケストレーションと自動化を実現できます。SplunkのSOC自動化ソリューションを活用すれば、運用範囲を拡大し、対応を迅速化して、脅威やその他のセキュリティの問題を修復できます。また、Splunkソリューションによって、分析主導型セキュリティ対策の実践や、セキュリティチームとその他の関係チームとのコラボレーションを促進することもできます。

インシデントレスポンス

インシデントレスポンス (IR)には、ITシステム上のセキュリティイベントの監視と検出、およびそれらのイベントへの対応計画の実行が含まれます。IRチームは「ブルーチーム」と呼ばれることが多くあります。ブルーチームは、脅威が検出されたときに組織のインフラを守る役割を担います。一方、「レッドチーム」は、インフラシステムで既存の設定の弱点を見付ける役割を担います。Splunkソリューションではそれぞれ、セキュリティポートフォリオに応じたIR機能が提供されています。各ソリューションには、検出したイベントの調査を実行するための仕組みが備わっています。インシデント担当者に標準的な対応手順を指示する機能を備えていることもあります。

コンプライアンス

ほぼすべての環境で、GDPR、HIPAA、PCI、SOXなどをはじめ、何らかの形の規制要件に対応する必要があります。CISによる20のクリティカルセキュリティコントロールのように、厳密にはコンプライアンスとみなされない一般的なガイドラインもあります。Splunkソリューションを使用すれば、さまざまな方法でコンプライアンスの課題を解決することができます。たとえば、相関ルールやレポートを作成し、これらを使用して機密性の高いデータや重要な従業員に迫る脅威を特定したり、コンプライアンスを自動的に実証したりできます。

不正行為の分析と検出

デジタル時代においてマシンデータは不正行為検出の要であり、きわめて重要な役割を果たします。Splunkソリューションでは新しいデータを取り込むことができるため、不正行為管理チームは異常の検出と調査の精度を向上させることができます。これにより、組織全体の金銭的損失を防ぎ、組織の評判を守って、事業効率を維持できます。

内部脅威の検出

内部脅威とは、社内ネットワークへのアクセス権を持つ現在の従業員または元従業員、請負業者、パートナーにより、機密性の高いデータが意図的または偶発的に流出するか、悪用または破壊されることを指します。多くの場合、このような内部脅威者はネットワークへの正当なアクセス権を持ち、機密性の高い資料のダウンロードが許可されているため、従来のセキュリティ製品を回避するのは簡単です。Splunkソリューションを使用すれば、セキュリティチームは他の製品では発見できないような内部者による脅威および侵害された内部者による脅威を検出し、優先順位を付けることができます。

分析主導型セキュリティジャーニーを始める

サイバーセキュリティ対策の効果を上げるには、対策を継続的に進化させる必要があります。問題は、多くの組織が対策の現状と改善方法について明確な意識を持っていない点です。セキュリティジャーニーのどの段階にいるのかがわかれば、時間とリソースをより効果的に利用できます。そして、次に何をすべきかを理解すれば、後の段階についてより的確な計画を立て、成功に導くことができます。

以下では、データを活用して常に攻撃の先手を取るための、分析主導型セキュリティジャーニーの6つのステージについて詳しく説明します。各段階について、以下の点を取り上げます。

- ユースケース別の適用度
- データソース
- マイルストーン
- 課題

ステージ1：**収集**

環境内の基本的なセキュリティログや
その他のマシンデータを収集します。

セキュリティユースケース別の適用度

インシデント調査とフォレンジック

セキュリティ監視

高度な脅威検出

SOC自動化

インシデントレスポンス

コンプライアンス

不正行為の分析と検出

内部脅威

説明

ステージ1では、防御すべき環境について理解を深めるための材料を集めることに集中します。

データソース
ステージ1のベストプラクティスは、セキュリティインフラの4つの基本コンポーネントで生成されるマシンデータを収集することです。

1. **ネットワーク**
   ネットワークトラフィックの可視化は、すべてのセキュリティチームにとって重要です。この初期段階での優先事項は、自社のネットワークから出入りするトラフィックの種類を把握することです。許可されたトラフィックとブロックされた通信の試行回数の両方を確認することが重要です。

   ソースの例：
   - 以下のベンダー製品のファイアウォールトラフィックログ
     - Palo Alto Networks
     - Cisco
     - Checkpoint
     - Fortinet

2. **エンドポイント(ホストベース)**
   エンドポイントのログからは、マルウェアの実行、許可されてない行為を実行する内部脅威者、ネットワーク内に潜む攻撃者などの悪質な活動に関するインサイトを得ることができ、ネットワークの可視性を補完します。このデータは、サーバー、ワークステーション、およびすべてのオペレーティングシステムから収集することが重要です。

   ソースの例：
   - Windowsイベントログ
   - Linuxシステムログ
   - Linux auditdログ
   - MacOSシステムログ

3. **認証**
   認証ログからは、ユーザーがいつどこからシステムやアプリケーションにアクセスしているのかがわかります。攻撃を成功させるために有効な資格情報が悪用される場合が多いため、正当なログインとアカウントの乗っ取りを見分けるためには以下のデータが必要です。

   ソースの例：
   - Windows Active Directory
   - ローカル認証
   - Cloud IAM (Identity & Access Management)
   - Linux auditdログ
   - MacOSシステムログ

4. **Webアクティビティ**
   多くの攻撃は、ユーザーが悪質なWebサイトにアクセスすることから始まり、攻撃者によって管理されるサイトに機密性の高いデータが流出することで終わります。調査においては、いつ誰がどのサイトにアクセスしているのかを可視化することが必要不可欠です。

ソースの例：
- 以下のベンダー製品の次世代ファイアウォール(NGFW)トラフィックフィルタまたはプロキシログ
  - Palo Alto Networks
  - Cisco
  - Checkpoint
  - Fortinet
  - Bluecoat
  - Websense

マイルストーン
この4つのカテゴリーのデータを取り込んで以下の状態になっていれば、このステージは完了です。

- 攻撃者が簡単に改ざんできない独立したシステムに、重要なアクティビティログが保存されている。
- 4つのカテゴリーのデータを基本的な調査に使用できる。

課題
異なるソースからデータを収集するのは手間がかかることが多く、データを正しく取り込む作業は単調になりがちです。ミスが生じたり、収集する情報が不十分だったりすると、無駄な時間を取られたり、調査が不完全になったりします。

ステージ2：**正規化**

標準的なセキュリティデータの形式を適用し、資産データとIDデータを追加します。

セキュリティユースケース別の適用度

インシデント調査とフォレンジック

セキュリティ監視

高度な脅威検出

SOC自動化

インシデントレスポンス

コンプライアンス

不正行為の分析と検出

内部脅威

説明

ステージ2では、標準的なセキュリティデータの形式に合わせてデータを調整します。つまり、イベント発生源のIPアドレス、ポート、ユーザー名などの共通の値を持つフィールドに、イベントを生成したデバイスを問わず共通の名前を持たせます。データを正規化することは、以下のことを実現する上で重要です。

- ベンダーやコミュニティが提供するさまざまな検出メカニズムに対応する。
- ネットワークに接続するシステムとユーザーを追跡するためのセキュリティオペレーションセンターの構築に着手する。
- セキュリティチームの能力を拡大する。

SOCを正式に構築する予定がない場合でも、データの正規化には以下のメリットがあります。

- ソースをまたいだデータの相関付けを容易にする。
- 調査を効率化する。
- 分析の有効性を高める。

データソース

ステージ2では、以下の参照情報を収集する必要があります。

- IT資産(システム、ネットワーク、デバイス、アプリケーション)
- Active Directory、LDAP、その他のIAM/SSOシステムに登録されたユーザー ID

マイルストーン

ステージ2のマイルストーンは以下のとおりです。

- 共通情報モデル(CIM)にデータが適切にマッピングされている。
- CIMに関連付けられた高速なデータモデルを使用することで、サーチパフォーマンスが飛躍的に向上する。
- 資産とユーザーの詳細情報がセキュリティログプラットフォームのイベントと相関付けられる。

課題

サーチ可能な基本データを揃えるだけでは、より高度なセキュリティ検出やエンドポイントの可視化に必要なインサイトや知見は得られません。

ステージ3：**拡張**

エンドポイントでの活動やネットワークメタデータなど、精度の高いデータソースを追加で収集し、高度な攻撃の検出を促進します。

セキュリティユースケース別の適用度

インシデント調査とフォレンジック

セキュリティ監視

高度な脅威検出

SOC自動化

インシデントレスポンス

コンプライアンス

不正行為の分析と検出

内部脅威

説明

DNS (Domain Name System)とエンドポイントのデータを使用すれば、多彩な検出機能を利用して、ネットワークに潜伏している侵入者を発見して追跡できます。

データソース
この段階で必要なデータソースには以下のものが含まれます。

1. **ネットワーク**
   多くの脅威ハンターや脅威インテリジェンスアナリストは、分析に使うデータソースを1つだけ選べるなら、それはDNSだと答えるはずです。

   ソースの例：

   - Splunk StreamやBroといったソースからのプロトコル固有のワイヤーデータ
   - デバッグレベルのログやワイヤーデータのソースからのDNSクエリーレベルのデータ
   - DHCPアクティビティ

2. **エンドポイント**
   プロセスの生成、ファイルの変更、レジストリの修正、ネットワーク接続など、エンドポイントの活動に関する豊富な情報を入手すれば、エンドポイントで発生している重要なイベントに関する履歴を明確に把握できます。

   ソースの例：

   - sysmon
   - Osquery
   - Carbon Black Defense

マイルストーン
精度の高いデータソースを収集することで、以下の状態を目指します。

- 高度な検出を実行するための基盤が構築される。
- 一般的な侵害の痕跡をいくつか照合できるようになる。

課題
収集するネットワークデータとエンドポイントデータには詳細な情報が含まれていますが、コンテキストが不十分であり、相手側の組織が認識している侵害の痕跡が自社の環境内に未検出のまま残っている可能性があります。

ステージ4：**強化**

セキュリティデータをインテリジェンスで補強して、
イベントのコンテキストや影響について理解を深めます。

セキュリティユースケース別の適用度

インシデント調査とフォレンジック

セキュリティ監視

高度な脅威検出

SOC自動化

インシデントレスポンス

コンプライアンス

不正行為の分析と検出

内部脅威

説明

セキュリティチームとしてのパフォーマンスを高めるには、必要不可欠なマシンデータを収集するだけでなく、社内外のソースから得たインテリジェンスを活用してデータを補強することが重要です。脅威インテリジェンスのフィード、オープンソースのインテリジェンス(OSINT)ソース、社内からの情報など、コンテキストを把握して調査に役立つ情報があれば、収集したデータからより多くの価値を引き出し、セキュリティイベントやインシデントを迅速に検出できます。

データソース

データソースには以下のものが含まれます。

- ローカルIP/URLのブロックリスト
- オープンソースの脅威インテリジェンスフィード
- 商用の脅威インテリジェンスフィード

マイルストーン

コンテキストを把握するためのインテリジェンスを活用してデータを補強することにより、以下の状態を目指します。

- 資産の重要度に基づいて、アラートの緊急性を理解できる。
- アラートを脅威インテリジェンスフィードと照合し、他のシステムにピボットして、追加のコンテキスト収集作業を開始することで、アラートに情報を補完できる。

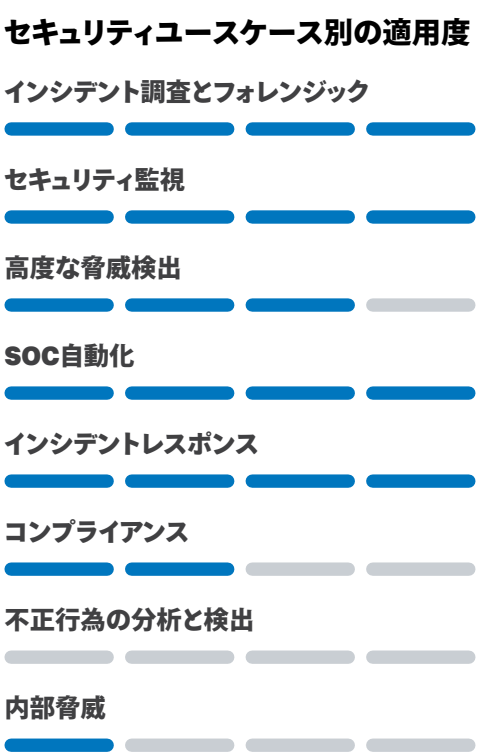
課題

高度な検出機能が揃っていても、セキュリティチームがその場しのぎの運用を続けたり、データのコンテキストと社外情報との相関付けを怠ったりしていては意味がありません。また、リクエストを追跡したりパフォーマンスを測定したりせず、コラボレーションが場当たり的で、教訓は蓄積されず、将来に活用されないこともあります。

ステージ5：**自動化とオーケストレーション**

一貫性のある繰り返し可能なセキュリティ運用機能を構築します。

セキュリティユースケース別の適用度



説明

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)ソリューションを利用すれば、数多くのより高度な方法でリスクを低減できます。自動化とオーケストレーションを取り入れる主なメリットには、既存のセキュリティツールや脅威インテリジェンスソースの統合による防御力の強化、セキュリティイベントへの対応の迅速化、調査プロセスの効率化、攻撃による損害の最小化などが挙げられます。さらにレベルアップして、受信アラートの自動トリアージと優先順位付けを継続的に行うことで、セキュリティチームの作業負担を減らし、人手による確認が必要となる特に重要な問題に集中させることもできます。さらに、対応計画を手動で実行する代わりに、標準化された自動化プレイブックを実行すれば、一貫性と再現性を向上させることができます。

データソース

この段階で使用するデータソースの1つは、Splunk Enterpriseのようなデータプラットフォームで生成された、精度の高いイベントです。自動化/オーケストレーションシステムでは、高度なアクションを実行するために、相関サーチ、重要なイベント、その他の高精度イベントを取り込みます。

マイルストーン

ステージ5のマイルストーンでは、以下の状態を目指します。

- インシデントを追跡する。
- アナリストの効率を定期的に測定する。
- あらかじめ定められたプレイブックに従って対応を実行する。
- シンプルなレスポンスを自動化し、それらを組み合わせることで、より高度なオーケストレーションを実現する。

課題

セキュリティチームは普段、可能な限り脅威を検出、分析、緩和しようと最前線で全力を尽くしています。それでも、調査や既知の脅威への対応に時間を取られ、セキュリティインシデントのバックログは増えるばかりです。(現実には、多くの組織で、日々直面する大量のインシデントを分析できる熟練の担当者が不足しています。)

ステージ6：**高度な検出**

機械学習などの高度な検出メカニズムを導入します。

セキュリティユースケース別の適用度

説明

機械学習、データサイエンス、高度な統計を導入して、環境内のユーザー、エンドポイントデバイス、アプリケーションを分析すれば、活動の痕跡をごくわずかしか残さない攻撃者、未知の脅威、内部脅威でも検出できる可能性が高まります。

データソース

攻撃を追跡するには、エンドポイントからより詳細なデータを収集する必要があります。プロセスの生成、ファイルの変更、レジストリの修正、ネットワーク接続など、エンドポイントの活動に関する豊富な情報を入手すれば、エンドポイントで発生している重要なイベントに関する履歴を明確に把握できます。

データソースには以下のものが含まれます。

- Microsoft sysmon
- Osquery
- Carbon Black Defense

マイルストーン

ステージ6では、以下の状態を目指します。

- 先進的な技術を使用して、未知の脅威を特定する。
- 新たな検出メカニズムが利用可能になり次第すぐに導入し、チームに蓄積された専門知識と外部の調査機関を活用する。

課題

この段階では、セキュリティ体制を継続的に改善し、新しい機能を取り入れることが要求されます。また、新しい調査を実施しなければならない可能性もありますが、セキュリティジャーニーに従い、能力を高め続けることで、最善の防御を実現できます。攻撃は次々に発生しますが、現代の組織が直面する既知の脅威や未知の脅威の数々を検出して阻止できる最適な体制が整います。

一般的なセキュリティ課題をSplunk Security Operationsスイートで解決する

セキュリティジャーには困難がつきものです。これから直面するかもしれない問題をまとめたハンドブックがあって、それらが実際に発生したときに、ハンドブックに従って目の前の状況に対処し、進路を守り続けることができたらすばらしいと思いませんか?

心配ありません。このセキュリティジャーをSplunkがサポートします。

以下に、16の一般的なセキュリティ課題の解決例をご紹介します(Splunk Security Essentials AppやSplunk Securityオンラインデモではさらに多くの例をご紹介しています)。各例では、課題の概要、データソース、ユースケース、Splunkソリューション、プログラミングの難易度、実装方法、アラートの量、既知の誤検知、対応方法のベストプラクティスについて説明します。

以下の例をご紹介します。

- インシデント調査とフォレンジック
  - WMIを介した横方向移動の検出
  - 複数回の不正アクセス試行の特定
- セキュリティ監視
  - AWSのパブリックS3バケットの検出
  - ホストの複数感染の検出
- 高度な脅威検出
  - 新しいドメインへの接続の検出
  - 類似ドメインからのメールの検出
- SOC自動化
  - マルウェア調査の自動化
  - フィッシング調査の自動化
- インシデントレスポンス
  - ユーザーに対するデータ流出DLPアラートの検出
  - 基本的なダイナミックDNS検索の検出
- コンプライアンス
  - 新しいローカル管理者アカウントの検出
  - 本来許可されないシステムへのユーザーログインの検出
- 不正行為の分析と検出
  - 侵害されたユーザーアカウントの検出
  - 異常な行動をとる医療提供者の特定
- 内部脅威の検出
  - Webへの大量アップロードの検出
  - 元従業員のアカウントへのログイン成功の検出

インシデント調査とフォレンジック

WMIを介した横方向移動の検出

ステージ3

MITRE ATT&CK戦術

横方向移動　実行

MITRE ATT&CK技法

リモートサービス　Windows Management Instrumentation

データソース

Windowsセキュリティ　エンドポイント検出/対応

セキュリティの課題

Windows Management Instrumentation (WMI)は攻撃者にとって、システムの偵察、ウイルス対策や仮想マシンの検出、コードの実行、横方向移動、長期の潜伏、データの盗み出しに悪用できる格好の踏み台になっています。

ユースケース

高度な脅威検出

カテゴリー

横方向移動

必要なSplunkソリューション

Simple Search Assistant

SPLの難易度

低

実装方法

このユースケースでは、監視するエンドポイントにsysmonをインストールし、フォワーダーとサーチヘッドにsysmonアドオンをインストールする必要があります。

アラートの量

少ない

既知の誤検知

既知の誤検知なし

対応方法

この問題を検出したら、インシデントレスポンスプロセスを開始して、このプロセスで行われる活動を調査します。

WMIを介した横方向移動の検出に関するヘルプ

Splunkで、WMIを介した横方向移動を検出するには、まず、sysmonのEDRデータを読み込みます。代わりに、その他のプロセス起動ログを完全な形式のコマンドラインで書き出すこともできます。起動されているWindows Management Instrumentationコマンドライン(WMIC)インスタンスを調べ(EventCode 1はプロセス起動を示します)、フィルタを使って、CommandLine文字列に不審なフィールドが含まれていないかどうかを確認します。

```
index=* sourcetype=XmlWinEventLog:Microsoft-Windows-sysmon/
Operational EventCode=1 Image=*wmic* CommandLine=*node*
CommandLine="*process call create*"
| table _time host Image CommandLine
```


複数回の不正アクセス試行の特定

ステージ1

MITRE ATT&CK戦術

資格情報によるアクセス

MITRE ATT&CK技法

ブルートフォース

データソース

認証　Windowsセキュリティ

セキュリティの課題

ログイン失敗の多くは、パスワードの入力ミスが原因です。ただし、ユーザーがアクセスを許可されていない機密性の高いシステムでログインの失敗が繰り返される場合は不正が疑われます。多くの組織では、リスクの低い状況(プロキシログなど)以外でユーザーの不正操作を知らせるメッセージが発生することはめったにありません。リスクの高いアクティビティ(システムログインやファイル共有アクセスなど)でこの状況が発生し、かつ、その状況が繰り返し起こる場合は、常に調査を行うのが妥当です。

ユースケース

内部脅威

カテゴリー

内部脅威

必要なSplunkソリューション
Simple Search Assistant

SPLの難易度
中

実装方法
ユニバーサルフォワーダーとSplunkテクノロジーアドオンから取り込まれたデータがあること、およびすべてが自動的に機能していることを確認します。

アラートの量
少ない

既知の誤検知
この問題が検出された場合、最も可能性が高いのは、単にユーザーのアクセスに混乱が生じて発生した誤検知です。たとえば、前日にADグループの変更があり、ユーザーが誤って「dev_system_access」セキュリティグループから削除された場合などです。それ以外は、誤検知が発生する標準的なパターンはありません。

対応方法
このアラートが発生したら、以下の手順を実行します。

1. ユーザーが以前に対象のリソースにアクセスしたことがあるかを調べます。
2. 最近、職務などの変更がなかったかどうかを調べます。
3. 最近、ADグループに関する変更がなかったかどうかを調べます。

多くの組織では、エスカレーションの次のステップとして、リソースのオーナーやユーザーの上司に、この行為が適切なものかどうかを確認します。さらに、悪質な意図を示す兆候がないかどうか、およびアカウント乗っ取りの可能性がないかどうかも確認します。

複数回の不正アクセス試行の特定に関するヘルプ
Splunkで、ライブデータに基づいて複数回の不正アクセス試行を特定するには、シンプルサーチと以下のサーチ処理言語を使用します。Windowsセキュリティログを取り込んで、ステータスコード「0xC000015B」を調べます。このステータスコードは、要求されたログオンタイプがユーザーに許可されていないことを示します。この失敗の多くが特定のユーザーで1日あたりに発生していないかどうかを確認します。発生している場合は、ユーザーが機密リソースにアクセスしようとしている可能性があります。下のスクリーンショットは、デモデータに対するサーチ結果を示します。

```
index=* source=win*security user=* EventCode=* action=failure
Logon_Type=* Failure Reason Logon Type Status=0xC000015B
```

セキュリティ監視

AWSのパブリックS3バケットの検出

ステージ3

データソース

監査証跡 AWS

セキュリティの課題
これはよくありがちな問題です。ファイルを簡単に転送するために利用者がAWS S3バケットにファイルを保存したまま削除するのを忘れたり、S3バケットに機密性の高いデータをバックアップして、アクセス許可を誤って設定してしまうことがあります。誤って設定したパブリックS3バケットは、機密データを必要以上に外部にさらして悪用のリスクを高め、情報漏えいの大きな原因になるため、パブリックに設定された新しいS3バケットまたは既存のS3バケットを検出することが重要です。

ユースケース
セキュリティ監視
高度な脅威検出

カテゴリー
データ流出、SaaS

必要なSplunkソリューション
Splunk Security Essentials
Splunk Add-On for Amazon Web Services
Splunk Simple Search Assistant

SPLの難易度
中

実装方法
パブリックS3バケットのサーチでは、共通情報モデル(CIM)にマッピングした正規化済みのデータを使用すると効率的です。Splunk Add-On for Amazon Web Servicesを使用すると、CloudTrailサービスやS3バケットを含むさまざまなAWSサービスコンポーネントを可視化できます。Splunk Add-on for AWSでこれらのログを取り込めば、サーチを問題なく自動化できます。実装時には、ベストプラクティスに従ってデータにインデックスを指定します。

アラートの量
非常に少ない

既知の誤検知
このサーチで発生する可能性がある不要なアラートには、以下の2種類があります。いずれもユーザーによる操作が原因です。

1. パブリックバケットを意図的に作成した場合。このアラートを防ぐには、この操作をよく行うマーケティング担当者をホワイトリストに追加するか、パブリックバケットの作成方法に関するポリシーを作成して、意図的なパブリックバケットの作成をサーチから除外します。
2. パブリックのバケットを作成した後すぐにプライベートモードに切り替えた場合。

対応方法
この問題を検出したら、インシデントレスポンスプロセスを開始して、このプロセスで行われる活動を調査します。

WMIを介した横方向移動の検出に関するヘルプ

Splunkで、WMIを介した横方向移動を検出するには、まず、sysmonのEDRデータを読み込みます。代わりに、その他のプロセス起動ログを完全な形式のコマンドラインで書き出すこともできます。起動されているWindows Management Instrumentationコマンドライン(WMIC)インスタンスを調べ(EventCode 1はプロセス起動を示します)、フィルタを使って、CommandLine文字列に不審なフィールドが含まれていないかどうかを確認します。

対応方法

パブリックS3バケットに関するアラートが発生したときは、以下の3点を確認します。

1. そのS3バケット今もパブリックの状態か。
2. 該当するファイルはパブリックなものか。
3. バケット内に何が保存されているか。

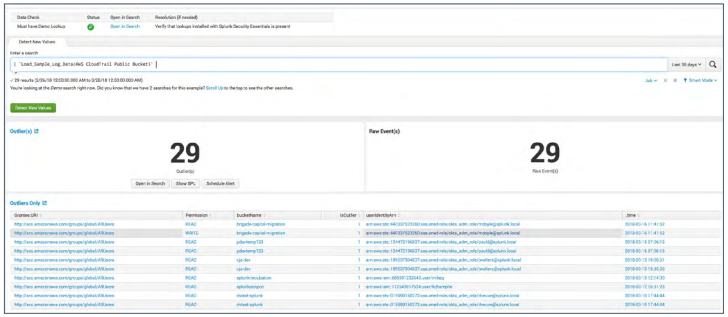
1つ目の点は簡単にわかります。ログでバケット名と「PutBucketACL.」を調べ、以降にACLが変更されているかどうかを確認します。2つ目と3つ目の点は少し難しく、S3バケットに対するサーバーアクセスのログ記録を有効にしておく必要があります(少し面倒ですが、デフォルトでは有効になっていないため、確認を怠らないようにしましょう)。

組織全体でAWS環境を使用している場合は、オープンなS3バケットを最優先で分析する必要があります。さらに、AWSの機能を使用してそのようなバケットの修復を自動化することもできます。

AWSのパブリックS3バケットの検出に関するヘルプ

Splunkで、ライブデータに基づいてパブリックS3バケットをサーチするには、シンプルサーチと以下のサーチ処理言語を使用します。AWS Cloudtrailログに対してライブサーチを実行し、パケットの権限が変更されたときに発生する「PutBucketAcl」イベントと、「AllUsers」を含むすべての項目を抽出します。スクリーンショットは、デモデータに対するサーチ結果を示します。

```
index=* sourcetype=aws:cloudtrail AllUsers
eventName=PutBucketAcl
| spath output=userIdentityArn
path=userIdentity.arn
| spath output=bucketName
path="requestParameters.bucketName"
| spath output=aclControlList path="requestParameters.
AccessControlPolicy.AccessControlList"
| spath input=aclControlList output=grantee path=Grant{}
| mvexpand grantee
| spath input=grantee
| search "Grantee.URI"=*AllUsers
| table _time, Permission, Grantee.URI, bucketName,
userIdentityArn | sort - _time
```



ホストの複数感染の検出

ステージ1

MITRE ATT&CK戦術

初回アクセス　実行

MITRE ATT&CK技法

ドライブバイ攻撃　スピアフィッシング添付ファイル

スピアフィッシングリンク　ユーザー実行

データソース

ウイルス対策　マルウェア対策

セキュリティの課題

ウイルス感染は常に問題ですが、1つのホストが複数のウイルスに同時に感染した場合は特に深刻です。この問題が発生した場合は、複数の手口を試みていずれかの成功を狙うエクスプロイトキットによる攻撃を受けたか、無関係の複数のウイルスにホストが感染した可能性があります。従来のマルウェア対策製品は一般的に、既知のマルウェアの検出には効果がありますが、未知のタイプや進化するタイプのマルウェアは検出できません。マルウェアの亜種が社内システムへのバックドアを仕込み、長期の潜伏やデータの流出を可能にすることがあるため、マルウェアに感染したホストは最優先でただちに調査して、他にも問題がないかどうかを確認する必要があります。

ユースケース

セキュリティ監視

カテゴリー

エンドポイントの侵害

必要なSplunkソリューション

Splunk Security Essentials
Splunk Common Information Modelアドオン
Splunk Simple Search Assistant

SPLの難易度

低

実装方法

ホストの複数感染を検出するには、ウイルス対策ソリューションのログを収集する必要があります。Symantecログであればこのサーチは簡単です。他のアンチウイルス製品を使用している場合でも、その製品のフィールド名とソースタイプをサーチ条件に簡単に適合することができます。特に、CIMにマッピングするSplunkアドオンを使えば簡単です(アドオンについてはSplunkbaseを検索してください)。

アラートの量

少ない

既知の誤検知

既知の誤検知なし

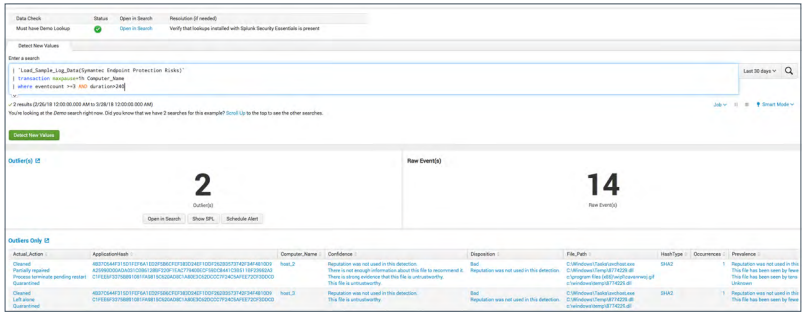
対応方法

1つのホストで複数の感染が発生した場合、他のマルウェアイベントと同様に対応しますが、緊急度は高くします。

ホストの複数感染の検出に関するヘルプ

Splunkで、ライブデータに基づいて短期間に複数の感染が確認されたホストを検出するには、シンプルサーチと以下のサーチ処理言語を使用します。まずは、基本のデータセットとして、過去24時間分のSymantec Endpoint Protectionのリスクイベントを取り込みます。イベントをグループ化する方法はいくつかありますが、最も速いのは統計を使用する方法です。ここでは最も簡単な方法として、トランザクションを使用しています。これにより、すべてのイベントが「Computer_Name」に基づいてグループ化されます。最後に、数分以内に3つ以上のイベントが発生しているかどうかでフィルタリングします。下のスクリーンショットは、デモデータに対するサーチ結果を示します。

```
index=* sourcetype=symantec:* earliest=-24h
| transaction maxpause=1h Computer_Name
| where eventcount >=3 AND duration>240
```



高度な脅威検出

新しいドメインへの接続の検出

ステージ2

MITRE ATT&CK戦術

データ流出　コマンドアンドコントロール

MITRE ATT&CK技法

コマンドアンドコントロールを介したデータ流出

代替プロトコルを介したデータ流出

標準アプリケーション層プロトコル

データソース

Webプロキシ　NGFW

セキュリティの課題

多くの組織で、ユーザーがアクセスするドメインは毎日ほぼ同じです。しかし、社内ネットワークから要求されたドメインのうち、以前にアクセスしたことのないものも多少はあるはずです。もちろん、その中には正当なドメインへのトラフィックもありますが、全体から見ればごくわずかです。重要なのは、初めてアクセスするドメインは脅威の発生を示している可能性があることです。

ユーザーが新しいドメインにアクセスした場合、その理由はさまざまですが、まず疑うべきは、攻撃者がコマンドアンドコントロール通信の拠点として使用しているドメイン、またはデータ流出やマルウェア攻撃のステージングサーバーのドメインにシステムが接続しているかもしれないということです。ホストが感染したと疑われる場合、それを確認する良い方法は、そのホストが新しいドメインにアクセスしていないかどうかを調査することです。

ユースケース

高度な脅威検出

カテゴリー

コマンドアンドコントロール、データ流出

必要なSplunkソリューション

Splunk Enterprise
Splunk Security Essentials
Splunk URL Toolbox
Splunk Simple Search Assistant

SPLの難易度

中

実装方法

この異常検出方法では、任意の組み合わせの値について最も古い日時と最も新しい日時を追跡します(ユーザーとサーバーの各組み合わせの最初のログオン、コードリポジトリとユーザーの各組み合わせの最初の閲覧、各システムのUSBキー使用を示す最初のWindowsイベントIDなど)。通常は、最も新しい日時が過去24時間以内であるかどうかを確認して、その場合はアラートを生成します。これは市販されている数多くのセキュリティデータサイエンスツールの主要機能であり(Splunk UBAを除く)、Splunk Enterpriseを使用すれば簡単に実行できます。

このサーチではCIMに準拠するデータを使用するため、実装は比較的簡単です。まず、プロキシのデータ(またはstream:httpやbroなどのWebブラウジングを可視化したデータ)を取り込んで、URIフィールドがあることを確認します。あとは、Splunkでドメインを解析するためのURL Toolbox Appをインストールするだけです。サーチの規模を拡大してより大量のデータを扱う(または実行頻度を増やす)場合は、アクセラレーション機能を利用することをお勧めします。

アラートの量

非常に多い

既知の誤検知

多くの組織では、新しいドメインの割合はわずかです。ただし、「新しいドメイン」アラートの大半は正当なトラフィックによって生成されるため、これらのアラートすべてを調査のためにアナリストに送ると負担が大きくなります。本質的に既知の誤検知はなくても、「新しいドメイン」アラートはいずれも値が非常に小さいため、これらのアラートを大部分の相関サーチとは別に処理することもできます。ほとんどの場合、相関サーチは、コンテキストデータを対象とする場合や他の指標と相関付ける場合に適しています。

対応方法

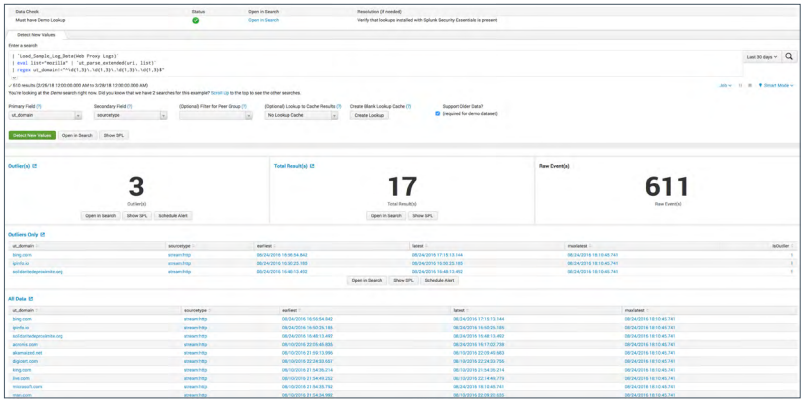
「新しいドメイン」イベントは基本的に、完全には除去されていないマルウェア、新しいサービス、異常なログインなど、別のイベントのコンテキストデータと考えるのが最善です。これを最も簡単に実現するには、サマリーインデックスにイベントを記録し、調査活動にこのインデックスのサーチを組み込みます。Splunk Enterprise Securityを使用している場合は、リスク管理フレームワークで簡単に組み込むことができます。このサーチを保存するときにリスク指標のアダプティブレスポンスアクションを作成すると、関連する資産のリスクスコアが調整されて、資産の分析時に調査ワークベンチに表示されます。最後に、ここで任意のアラートの有効性を分析できるように、VirusTotalやThreatCrowdなどのオープンソースのインテリジェンスリソースでこれらのドメインを検索することをお勧めします。

新しいドメインへの接続の検出に関するヘルプ

Splunkで、ライブデータに基づいて新しいドメインへの接続を検出するには、シンプルサーチと以下のサーチ処理言語を使用します。まず、プロキシのデータセットを読み込み、CIMフィールドを使って、URLが実際に含まれるイベントだけを抽出します。

次に、URL Toolboxを使って、URLからドメインを抜き出します。さらに、regexフィルタリングコマンドを使って、サーチからIPアドレスを除外します。この手順はオプションですが、一部のアプリケーションは正常な操作の中で多くの一時的なAWSインスタンスIPに接続するため、IPアドレスを含めると、値に対するノイズの比率が非常に高くなることがあります。最後に、statsコマンドを使って、このフィールドの組み合わせで最も古い日時と最も新しい日時を算出し、このイベントが確認された最も古い日時が過去24時間以内(つまり最新)であるかどうかを調べます。下のスクリーンショットは、デモデータに対するサーチ結果を示します。

```
tag=web url=*
| eval list="mozilla" | `ut_parse_extended(url,list)`
| regex ut_domain!="^\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}$"
| stats earliest(_time) as earliest latest(_time) as
latest by ut_domain, sourcetype
| where earliest >= relative_time(now(), "-1d@d")
```



類似ドメインからのメールの検出

ステージ4

MITRE ATT&CK戦術

初回アクセス

MITRE ATT&CK技法

スピアフィッシングリンク

データソース

電子メール

セキュリティの課題
類似ドメインからのメールはフィッシングでよく使われます。一部の攻撃者は、「spiunk.com」のドメインでsplunk.comからのメールを装うなど、見間違えやすい文字を使ってドメインを偽装します。また、.help.comや.supportなど、もっともらしいサブドメインが使われることもあります。問題は、ユーザーがそれを正規のソースから送られたメールだと考えて開いてしまうことです。スプーフィング攻撃によるメールは正規のものとほとんど見分けがつきません。

ユースケース
高度な脅威検出

カテゴリー
エンドポイントの侵害、SaaS

必要なSplunkソリューション
Splunkサーチアシスタント
初回検出アシスタント
URL Toolbox App

SPLの難易度
高

実装方法
このサーチの実装は、基本的には比較的簡単です。CIMに準拠したデータを使用する場合は、特別な設定は必要ありません。それでも、メールログのソースが複数ある場合は特に(境界に設置したメールセキュリティアプライアンスと基幹Exchange環境など)、メールデータのインデックスとソースタイプを指定することをお勧めします。URL Toolboxをインストールして、適切なインデックス、ソースタイプ、src_userフィールドを設定すると、効率が大幅に向上します。

アラートの量
非常に少ない

既知の誤検知
このサーチでは、ドメイン名でdnstwistを実行する場合と同様に、組織内でよく要求するドメイン名と類似するあらゆるドメインからの受信メールが精査されます。よく使用するドメインと似ているが同じではないソースドメイン名からメールを受信する場合、誤検知によるアラートが生成される可能性があります。たとえば、海賊船用の木材を製造しているplank.com社がsplunk.comの営業担当者にメールを送信するシナリオを考えてみましょう。この2つの文字列がどの程度異なっているかを示すレーベンシュタイン距離は「2」であるため(plankの「a」を「u」に置き換えて「s」を追加するとsplunkになります)、アラートが生成されます。誤検知によるアラートを減らすには、既知の事例をサーチから除外するか、初回検出にパイプして過去の事例を自動的に排除します。

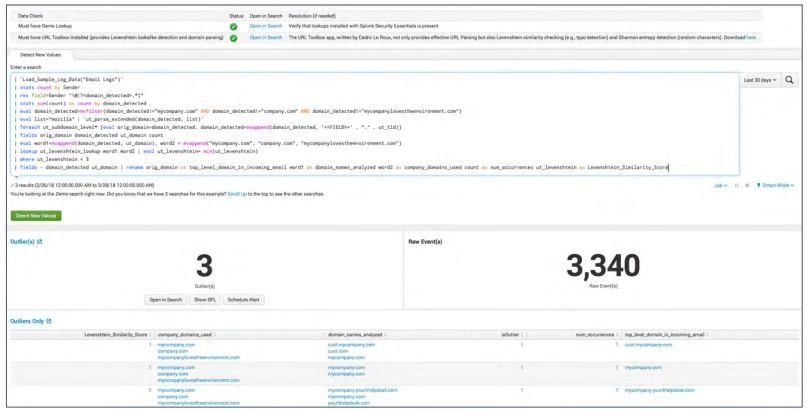
対応方法

このサーチから値が返されたら、インシデントレスポンスプロセスを開始し、イベントの発生時間、送信者、受信者、件名、またはメールと添付ファイル(ある場合)を確認します。そして送信者に連絡をとります。このメール送信が許可された行為であれば、その旨を実行者名とともに記録に残します。そうでなければ、ユーザーの資格情報が他者に利用された可能性があるため、追加の調査が必要になります。

類似ドメインからのメールの検出に関するヘルプ

Splunkで、ライブデータに基づいて類似ドメインからのメールを検出するには、Simple Search Assistant、URL Toolbox、および以下のサーチ処理言語を使用します。まず、ソースアドレスが記録されたメールログを取り込み、ソースアドレスごとにまとめます。次に、ドメインを抽出して、分析対象となる実際のドメインごとにまとめます。また、自社のすべてのドメインと、メールを受信することがわかっているすべてのドメインを除外します。さらに、無料のURL Toolbox Appを使って、トップレベルドメインからサブドメインを抜き出します。レーベンシュタインアルゴリズムに送るフィールドは「domain_detected」なので、複数値フィールドの「domain_detected」に各サブドメインを追加します。URL Toolboxに2つの複数値フィールドが渡され、そこで各組み合わせが照合されてレーベンシュタインスコアが計算されます。このグループから最も低いスコアを取り出します。最後に、レーベンシュタインスコアが3未満のものを抽出します。下のスクリーンショットは、デモデータに対するサーチ結果を示します。

```
index=* sourcetype=cisco:esa* OR sourcetype=ms:o365:*:messaget
race OR sourcetype=MSExchange*:MessageTracking OR
tag=email src_user=*
| stats count by src_user
| rex field=src_user "\@(?.*)"
| stats sum(count) as count by domain_detected
| eval domain_detected=mvfilter(domain_detected!=
"mycompany.com" AND domain_detected!="company.com" AND
domain_detected!="mycompanylovestheenvironment.com")
| eval list="mozilla" | `ut_parse_extended(domain_detected,
list)`
| foreach ut_subdomain_level* [eval orig_domain=domain_
detected, domain_detected=mvappend(domain_detected, '<>'
."."." ut_tld)]
| fields orig_domain domain_detected ut_domain count
| eval word1=mvappend(domain_detected, ut_domain),
word2 = mvappend("mycompany.com", "company.com",
"mycompanylovestheenvironment.com")
| lookup ut_levenshtein_lookup word1 word2 | eval ut_
levenshtein= min(ut_levenshtein)
| where ut_levenshtein < 3
| fields - domain_detected ut_domain | rename orig_domain
as top_level_domain_in_incoming_email word1 as domain_
names_analyzed word2 as company_domains_used count as num_
occurrences ut_levenshtein as Levenshtein_Similarity_Score
```



SOC自動化

マルウェア調査の自動化

ステージ5

データソース

認証　Windowsセキュリティ

セキュリティの課題
複数のシステムで同じマルウェアが検出された場合、それは大規模インシデントに発展する瀬戸際かもしれません(このような攻撃は多くの場合、ワーム、ランサムウェア、広範に及ぶフィッシングを伴います)。マルウェアのアラートを調査して対応するには、通常、各アラートにつき30分以上かかります。Splunk SOARは、この調査と対応を自動化して、プロセスが悪質であるかどうかを検証し、対応策をすばやく実行して、感染したエンドポイントでハッシュをブロックします。

ユースケース
セキュリティ監視
高度な脅威検出
SOC自動化

カテゴリー
エンドポイントの侵害、横方向移動

必要なSplunkソリューション
Splunk SOAR

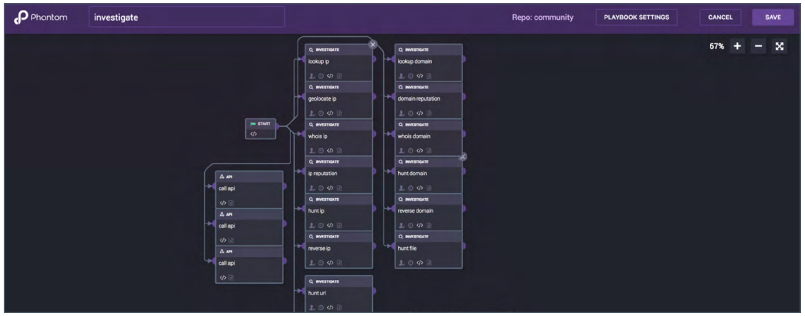
SPLの難易度
該当せず

実装方法
データソースからSOARプラットフォームにマルウェアイベントを取り込みます。対象のIP、URL、ファイルなどに関するレピュテーションインテリジェンスを検索するなど、判断の迅速化に役立つ調査を行います。こうしたコンテキスト収集活動は、自動化の有力候補です。判断に基づいて、手動で、または自動化プレイブックを使用して、隔離手順や修復手順を実行します。

アラートの量
非常に少ない

既知の誤検知
該当せず

対応方法
プレイブックを使用して、エンドポイントのマルウェア感染を調査および修復します。これらの対応を自動化すれば、手動で対応する時間を節約し、感染したエンドポイントをよりすばやくブロックできます。調査と検出の自動化対象として、まずは、ファイルやディレクトリの非表示、shimデータベースファイルの作成、複数の拡張子を持つファイルの実行、エンドポイントの1文字の処理などのユースケースから始めるとよいでしょう。



アラートのコンテキスト補強に関するヘルプ

フィッシング調査と対応の自動化

ステージ5

データソース

監査証跡　AWS

セキュリティの課題

フィッシングメールを検出し損ねると、組織全体に被害が及ぶ可能性があります。メールを調査するには、本文だけでなく、添付ファイルや、受信者と考えられるユーザーまで調べる必要があるため、手動で1件ずつ調査すると時間がかかります。調査を自動化すれば、フィッシング攻撃に対して迅速に対応できます。

ユースケース

セキュリティ監視
高度な脅威検出
SOC自動化

カテゴリー

フィッシング、攻撃手口、アカウントの侵害

必要なSplunkソリューション

Splunk SOAR

SPLの難易度

該当せず

実装方法

不審なメールをSOARプラットフォームに取り込みます。対象のIP、URL、ファイルなどに関するレピュテーションインテリジェンスを検索するなど、判断の迅速化に役立つ調査を行います。こうしたコンテキスト収集活動は、自動化の有力候補です。判断に基づいて、自動化プレイブックを使用して対応策を実行し、メールシステムからすべてのフィッシングメールを削除します。

アラートの量

非常に少ない

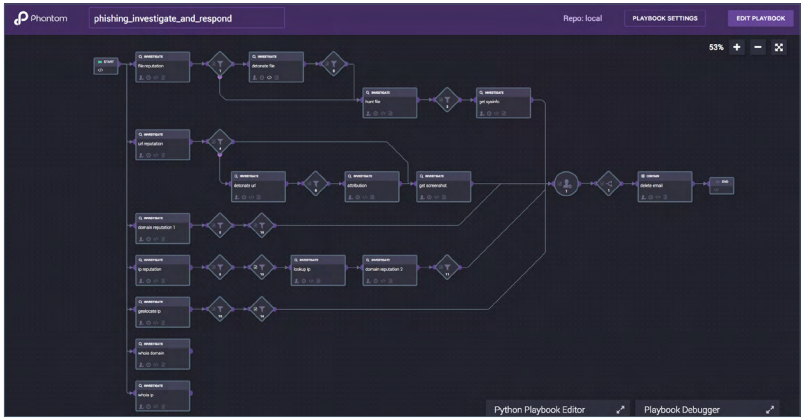
既知の誤検知

該当せず

対応方法

プレイブックの作成時に適切な調査を実装して自動化すれば、対応策の実行に必要な手作業を減らすことができます。プレイブックによって対応を自動化することで、フィッシング調査を効率化して、修復などの対応策を迅速に実行できます。

フィッシング調査の自動化



インシデントレスポンス

ユーザーに対する初めてのデータ流出 DLPアラートの検出

ステージ3

MITRE ATT&CK戦術

データ流出

MITRE ATT&CK技法

データ流出

データソース

DLP

セキュリティの課題
データ流出のDLPアラートが通常は発生しないユーザーに対して突如発生するようになった場合、従来のアラートよりも事態は深刻です。特に、該当するルールの重要性が高い場合やユーザーが高い権限を持つ場合は、これらのイベントを調査して、社内の機密情報が流出していないかどうかを確認する必要があります。

ユースケース
内部脅威

カテゴリー
内部脅威

必要なSplunkソリューション
Simple Search Assistant

SPLの難易度
中

実装方法
このルールの実装は簡単です。データ流出を示すDLPアラートを記録できるようにするだけです。関連する用語や設定は組織によってかなり異なるため、DLPチームと協力して作業する必要があります。その上で、ユーザーフィールドとシグネチャフィールドを定義すれば、サーチが機能します。

アラートの量
多い

既知の誤検知
これは厳密には行動検出であるため、この場合の「誤検知」の意味は通常とやや異なります。発生するアラートは常に、サーチ対象期間中の最初の発生(ルックアップキャッシュ機能を使用する場合はルックアップ構築期間中の最初の発生)を正確に反映します。そのため、従来の意味での「誤検知」は実際にはありませんが、ノイズはかなり多くなります。

対応方法
これは行動に関するアラートであるため、通常は、このアラートのみで対応を実行する必要はありません。ただし、以下の場合は例外です。

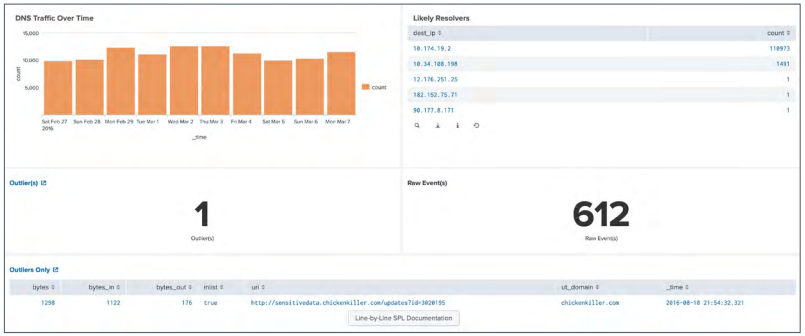
- アラートの重要度またはユーザーの優先度から、このアラートのみで調査を行う必要があると判断される場合
- このアラートができるだけ発生しないようにDLPが細かく調整されている場合

それ以外は、Splunk ESのリスク集約機能やSplunk UBAの脅威モデルを利用して、他のアラートと併せて検討するのが最善です。

ユーザーに対する初めてのデータ流出DLPアラートの検出に関するヘルプ

この例では、Simple Search Assistantを使用します。使用しているデータセットは、DLPイベントの基本データセットです。分析のために、データ流出のアラートを抽出しています。下のスクリーンショットは、デモデータに対するサーチ結果を示します。

```
index=* tag=dlp tag=incident
| stats earliest(_time) as earliest latest(_time) as latest
by user, signature
| where earliest >= relative_time(now(), “-1d@d”)
```



基本的なダイナミックDNS検索の検出

ステージ1

MITRE ATT&CK戦術

コマンドアンドコントロール　攻撃に対するOPSEC　インフラの確立と保守

MITRE ATT&CK技法

ダイナミックDNS　標準アプリケーション層プロトコル

データソース

Webプロキシ　NGFW　DNS

セキュリティの課題

攻撃者は、コマンドアンドコントロール機能の柔軟性を持たせるため、ダイナミックDNSを悪用することがあります。ダイナミックDNSは正当な目的でも使われますが(IT担当者が自宅のネットワークにアクセスするために使用することがよくあります)、そのアクセスを監視しないと大きなリスクにつながります。SplunkとMalware Domains Listを利用すれば、環境内のダイナミックDNSアクセスを簡単に検出できます。

ユースケース

セキュリティ監視、高度な脅威検出

カテゴリー

コマンドアンドコントロール

必要なSplunkソリューション
Simple Search Assistant
URL Toolbox

SPLの難易度
低

実装方法
まずは、ダイナミックDNSプロバイダーのリストを入手します。リストをダウンロードしたら、Splunkルックアップフォーマットに合わせて形式を変換します。ファイルを準備すれば、後は簡単に手順を進めることができます。

アラートの量
中

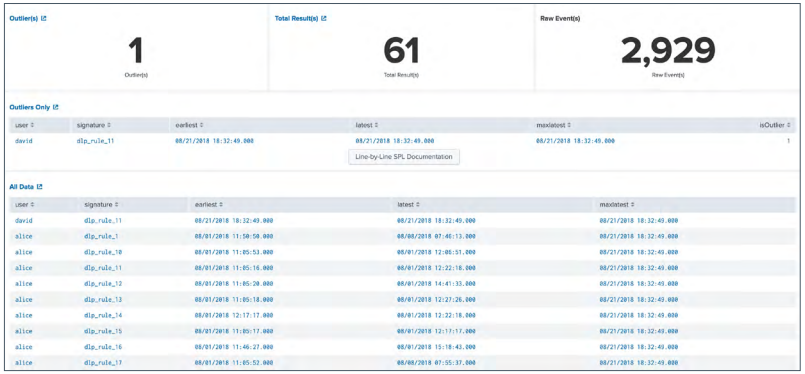
既知の誤検知
本番環境でダイナミックDNSを使用するサービスはまれですが、ないわけではありません。それらのサービスは、多少の誤検知の原因になりますが、通常、ビジネスクリティカルなサービスではありません。ダイナミックDNSがよく使われるのは、ユーザーが自宅に設置したWebカメラにアクセスして飼い犬の様子を確認するといった例です。こうした行為を許可し、それに応じて設定を調整するか、またはこうした行為を一切禁止するかは、最終的にはポリシー上の判断になります。

対応方法
このアラートが発生したときは、ユーザーが自宅のネットワークにアクセスしたなど、一般的に許容できる事例であるかどうかを確認します。そうでない場合は、以下の対応をとります。

1. Splunk Streamまたはパケットキャプチャからのデータを調べて、送信されたデータのタイプを確認します。
2. オープンソースのインテリジェンスデータベースでDNS名とIPを調べて、危険があるかどうかを確認します(ただし、このシナリオではその判断が難しい場合がほとんどです)。
3. 該当するホストが危険だと考えられる場合は、Microsoft sysmonやその他のエンドポイント対応機能でエンドポイントのログを取得して、そのホストにアクセスしているプロセスを特定します。

基本的なダイナミックDNS検索の検出に関するヘルプ
この例では、シンプルサーチと以下のサーチ処理言語を使用し、ライブデータに基づいて、ダイナミックDNSサーバーへのアウトバウンド通信を検出します。まず、プロキシログのデータセットを取り込みます。ダイナミックDNSプロバイダーを特定するため、URL Toolboxを使用して登録ドメインからサブドメインを抜き出します。次に、ダイナミックDNSドメインのルックアップを実行します。これにより、一致するものに「true」の値が設定された「inlist」という名前のフィールドが追加されます。最後に、一致するレコードを探します。下のスクリーンショットは、デモデータに対するサーチ結果を示します。

```
index=* sourcetype=pan:threat OR (tag=web tag=proxy)
earliest=-20m@m earliest=-5m@m
| eval list="mozilla" | `ut_parse_extended(url,list)`
| lookup dynamic_dns_lookup domain as ut_domain OUTPUT inlist
| search inlist=true
| table _time ut_domain inlist bytes* uri
```



コンプライアンス

ユーザーに対する初めてのデータ流出 DLPアラートの検出

ステージ1

MITRE ATT&CK戦術

防御回避　持続性

MITRE ATT&CK技法

有効なアカウント　アカウントの作成

データソース

監査証跡　Windowsセキュリティ

セキュリティの課題
ローカル管理者アカウントは正当な技術者が使用するものですが、攻撃者に悪用される場合もあります。攻撃者は、ネットワークの侵入に成功すると、多くの場合、目的のアカウントや資産に誰にも気付かれず自由にアクセスできるように、管理者権限を手に入れようとします。そのための簡単な方法の1つは、既存のアカウントを盗んで権限を昇格させることです。

ユースケース
高度な脅威検出、セキュリティ監視、コンプライアンス

カテゴリー
エンドポイントの侵害

必要なSplunkソリューション
Splunk Security Essentials
Splunk Enterprise

SPLの難易度
中

実装方法
まずは、Windowsセキュリティログが取得されていること、およびアカウント変更時に監査が行われていることを確認します。Windowsセキュリティについて不明な点がある場合は、Windowsセキュリティのデータソースに関するドキュメントを参照してください。

ログを取り込んだら、「sourcetype="WinEventLog:Security" EventCode=4720 OR EventCode=4732」を検索して、アカウントの作成イベントや変更イベントを確認します。最後に、グループのメンバーシップの変更を適切に探せるように、ローカル管理者グループ名が「administrators」になっていることを確認します。

アラートの量
中

既知の誤検知
このサーチで誤検知の唯一の原因となるのは、ヘルプデスク管理者がローカル管理者アカウントを作成した場合です。自社の環境でこのような操作がよく行われる場合、これらの管理者のユーザー名をベースサーチの対象から除外することで、該当する管理者アカウント作成メッセージをフィルタリングする必要があります。ローカル管理者グループに「administrators」が含まれていない場合、誤検知の原因となる可能性があります。

対応方法
このサーチで値が返されたら、インシデントレスポンスプロセスを開始して、以下の情報を確認します。

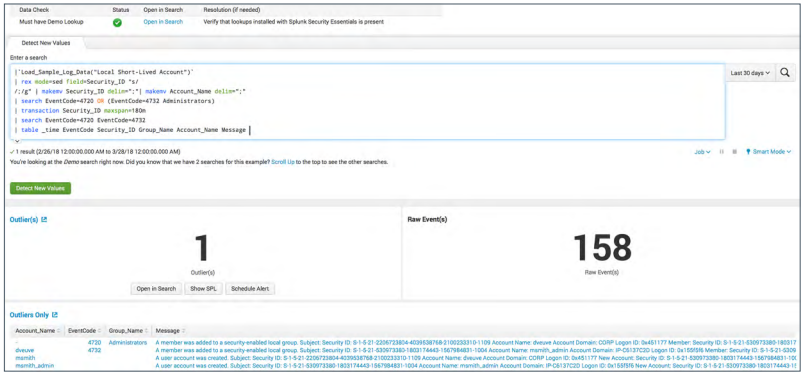
- 新しいアカウントの名前
- 作成日時
- アカウントを作成したユーザーアカウント
- 要求を出したシステム
- その他の関連情報

そしてシステムの所有者に連絡をとります。このイベントが正当な行為であれば、その旨を実行者名とともに記録に残します。そうでなければ、ユーザーの資格情報が他者に利用された可能性があるため、追加の調査が必要になります。調査を行うと同時に、正規の管理者アカウントについて、現在割り当てられている権限が本当に必要かどうか、および複雑で長いパスワードが使われているかどうかを確認することもお勧めします。

新しいローカル管理者アカウントの検出に関するヘルプ

この例では、シンプルサーチと以下のサーチ処理言語を使用して、新しく作成されてローカル管理者のステータスに昇格されたアカウントを特定します。使用するデータセットは、アカウント作成イベントまたはアカウントのグループメンバーシップ変更イベントを含む一連のWindowsセキュリティログです。下のスクリーンショットは、デモデータに対するサーチ結果を示します。

```
index=* source="winEventLog:Security" EventCode=4720 OR
(EventCode=4732 Administrators)
| transaction Security_ID maxspan=180m
| search EventCode=4720 (EventCode=4732 Administrators)
| table _time EventCode Account_Name Target_Account_Name
Message
```



本来許可されないシステムへのユーザーログインの検出

ステージ4

MITRE ATT&CK戦術

資格情報によるアクセス　権限のエスカレーション　収集

MITRE ATT&CK技法

有効なアカウント　情報リポジトリのデータ　アカウント操作

データソース

認証　Windowsセキュリティ

セキュリティの課題

一般データ保護規則(GDPR)の下では、個人データを処理するシステムやアプリケーションに対する権限を持つ従業員、ベンダー、処理者によるアクセスについて、完全な監査証跡を保持することが組織に求められています。また、欧州連合各国および欧州経済領域に居住する個人が組織に対して、自らのデータがどこに保存され、そのデータに誰がアクセスするかについて開示を求める権利が保証されます。

これらの要求を満たすため、組織は、該当する個人データにアクセスした従業員、ベンダー、処理者を特定するとともに、それらの個人データを定期的に処理するその他のサービスを特定し、報告できるようにする必要があります。管理者以外が個人データを処理する場合は、権限のある個人のみがそのデータにアクセスしたことを証明する必要もあります。不正アクセスを示す監査証跡がある場合は、文書化した上で、データ保護監督機関に報告しなければなりません。

違反を検出するように補強されたデータマッピングを使用すれば、以下の情報を特定できます。

- データにアクセスした従業員、ベンダー、処理者
- データが保存されている可能性がある場所
- データを定期的に処理するその他のサービス

管理者に代わってデータを処理している場合、このサーチによって、権限のある個人のみがデータにアクセスしたことを証明できます。

ユースケース
内部脅威、コンプライアンス

カテゴリー
GDPR、IAM分析、横方向移動、運用

必要なSplunkソリューション
Splunk Enterprise

SPLの難易度
低

実装方法
まず、データマッピングの結果を使用して、システムをGDPRカテゴリーに関連付けるルックアップを作成します。次に、同じ処理をユーザーに対しても行います。この時点で、CIMに準拠したデータを使用していれば、あとの操作は簡単です。

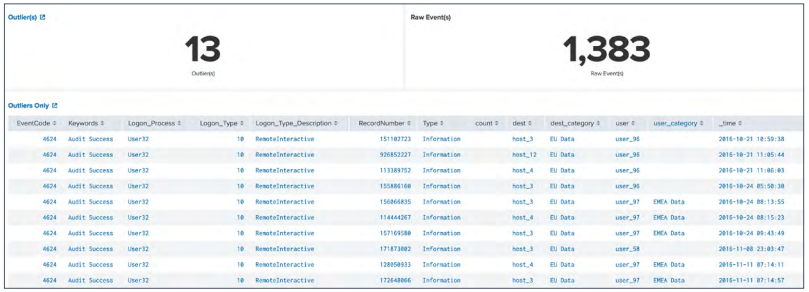
アラートの量
多い

既知の誤検知
このサーチでは、指定したリストに記載されていないユーザーがデータにアクセスするとアラートが生成されます。誤検知が発生する原因として最も多いのは、権限のあるユーザーのリストが更新されていないことです。

対応方法
文書に追加すべきユーザーがいないかヒントを探します。ただし、変更を行う前は必ず、データ保護責任者(DPO)またはそのチームに確認してください。権限のあるユーザーのリストの更新を自動化することも検討しましょう。その際は、リストのソースとして、DPOが管理する、権限のあるユーザーについての信頼できる記録を使用します。また、ユーザー名に部門名を補足して、アクセスが許可されているかどうかを部門単位で判断する方法もあります。

本来許可されないシステムへのユーザーログインの検出に関するヘルプ
この例では、シンプルサーチと以下のサーチ処理言語を使用し、ライブデータに基づいて、対象となるシステムへのユーザーの未許可ログインを検出します。使用するデータセットは、Windowsセキュリティログによるログイン情報を含む一連のWindows認証ログです。このサーチでは、GDPRカテゴリーのルックアップでホストを検索し、GDPRの対象になるホストのみを抽出します。次に、GDPRカテゴリーのルックアップでユーザーを検索し、最後に、一致するGDPRカテゴリーがないユーザー、またはいずれのGDPR情報も許可されていないユーザーを検出します。下のスクリーンショットは、デモデータに対するサーチ結果を示します。

```
index=* source=win*security user=* dest=* action=success
| bucket _time span=1d
| stats count by user, dest
| lookup gdpr_system_category.csv host as dest OUTPUT
category as dest_category | search dest_category=*
| lookup gdpr_user_category user OUTPUT category as
user_category
| makemv delim="|" dest_category | makemv delim="|"
user_category
| where isnull(user_category) OR user_category !=
dest_category
```



不正行為の分析と検出

侵害されたユーザーアカウントの検出

ステージ1

データソース

アプリケーションログ　Webアクセスログ

セキュリティの課題
詐欺師は、オンラインバンキング、クレジットカード、メール、医療サービスなど、さまざまなサービスプロバイダーのオンラインアカウントを、ユーザーに気付かれないように乗っ取ろうとします。フィッシング、スパイウェア、マルウェアなどを駆使して、アカウントへのアクセスに必要な資格情報を盗みます。乗っ取ったアカウントの主な用途には、クレジットカード詐欺、アカウントに与えられた権利の悪用、アカウントのサブスクリプションの悪用などがあります。詐欺師はユーザーになりすまして、アカウント情報を変更する、買い物をする、現金を引き出す、さらには盗んだ情報を使いほかのアカウントにアクセスしてより機密性の高いデータを盗むなどの悪事を働きます。場合によっては、アカウントには変更を加えず、ユーザーが使える状態にしたまま悪用し続けることもあります。

ユースケース
不正行為の分析と検出

カテゴリー
アカウントの乗っ取り、パスワードリスト攻撃(クレデンシャルスタッフィング)

必要なSplunkソリューション
Splunk Enterprise

SPLの難易度
中〜高程度

実装方法
重要なユーザーアカウントのデータを特定して、フィールドが適切に抽出されていることを確認します。同時に、セキュリティを強化するための機能を実装することも検討します。たとえば、不正認証のブロック、2要素認証、認証時のCAPTCHAの常時使用、機械学習、生体認証などがあります。熟慮した強化策を導入して攻撃を難しくし、回避しなければならないセキュリティ対策を増やすことで、不正アクセスをより効果的に防ぐことができます。帯域制限、IPブロック、不正要求のブロックなどの対策も、攻撃の規模の拡大を防ぐのに役立ちます。

アラートの量
中

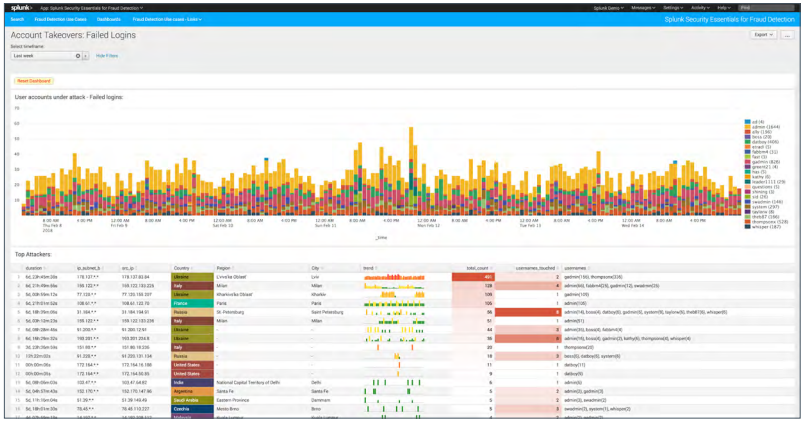
既知の誤検知
なし

対応方法
大半は、ユーザーアカウントの乗っ取りを狙う総当たり攻撃です。攻撃元のIPアドレスとサブネットを調査し、それに従ってファイアウォールのルールを調整して、アカウントが乗っ取られる可能性を最小限に抑えます。タイムチャートでスパイクを特定し、大量の攻撃を受けているアカウントを調査します。

侵害されたユーザーアカウントの検出に関するヘルプ

Webのログを使用して、ユーザーまたはIPアドレスの動作を確認します。さらに認証ログを使用すると、侵害されたアカウントの特定に役立ちます。これらの情報に基づいて、失敗回数が多いものを抽出します。その他のアカウントログも、メールアドレスの変更など、何らかの変更が行われたかどうかを把握するために役立ちます。データには、ログイン試行に関する情報と試行の成否を示すフラグが含まれているはずです。この例のサーチ処理言語を以下に示します。下のスクリーンショットは、デモデータに対するサーチ結果を示します。

```
index=web-logs action=login result=failure
| stats count, sparkline as trend by src_ip | where count>5
| sort - count
| table _time src_ip trend count
```



異常な医療トランザクションの特定

ステージ1

データソース

アプリケーションログ

セキュリティの課題

米国ではこれまでに、処方薬を不正に請求した疑いで400人以上が訴追されています。このような詐欺が規制や要件に影響を与えると、医師の日々の業務が難しくなり、患者が本当に必要な処方を簡単に入手できなくなる恐れがあります。このサーチでは、国または州全体で処方薬の請求に関する異常な行動を特定します。

ユースケース

不正行為の分析と検出

カテゴリー

アカウントの乗っ取り

必要なSplunkソリューション

Splunk Enterprise
Splunk Machine Learning Toolkit (MLTK)
Splunk Stream

SPLの難易度

中

実装方法

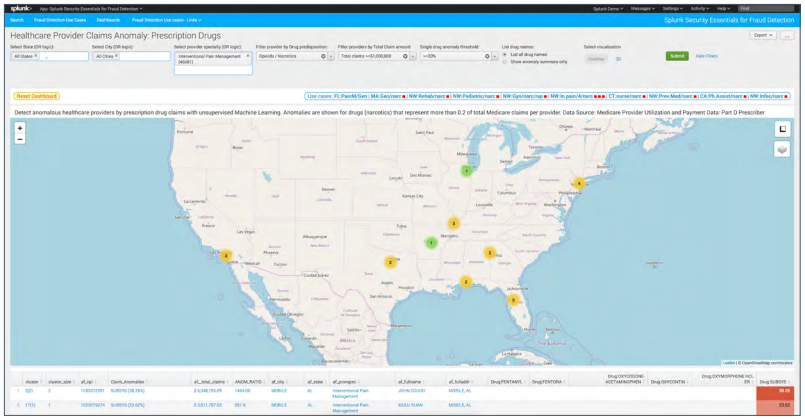
データセットはhttps://data.cms.gov/からダウンロードできます。このデータはCSV形式で提供されるため、簡単に取り込めます。ダッシュボードを表示したり、データをドリルダウンしてソースSPLを確認したりするためのAppをダウンロードすることもできます。このAppにはCMSデータセットがあらかじめ含まれています。

アラートの量
中

既知の誤検知
結果は異常値および外れ値として表示されます。表示される医療提供者の行動が不正であるかどうかの決定的な証拠はありません。それでも、詳細な調査から、異常な行動(特にオピオイドの大量処方)をとる医療提供者は多くの場合、データセットが公開された後も数年にわたって疑わしいビジネス慣行に関与していたことがわかっています。

対応方法
医療提供者の名前をクリックすると、詳細なプロファイル分析ダッシュボードが開きます。このダッシュボードで、詳細な処方データを調査し、全国の提供者のプロファイルとこの提供者のプロファイルを比較するチャートで、提供者の処方行動がピアグループの行動と一致しないことを確認できます。

異常な行動をとる医療提供者の特定に関するヘルプ
地図にアノマリが表示されます。黄色い丸をクリックすると、特定のアノマリに関する概要データが表示されます。医療提供者名をクリックすると、詳細なプロファイル分析ダッシュボードが開き、この提供者に関する固有のデータが表示されます。



内部脅威の検出

Webへの大量アップロードの検出

ステージ1

MITRE ATT&CK戦術
データ流出

MITRE ATT&CK技法
コマンドアンドコントロールを介したデータ流出

代替プロトコルを介したデータ流出

データソース
Webプロキシ　NGFW

セキュリティの課題
最近では、標準的な経路からのデータ流出が一般的になっており、内部脅威者はGoogle、Dropbox、Box、小規模なファイル共有サイト、さらにはリストに載っていないドロップサイトにデータをアップロードします。HTTPSの送信は常に許可されるため、ほとんどの組織ではデータの持ち出しが比較的容易に行えます。

ユースケース
セキュリティ監視、内部脅威

カテゴリー
データ流出

必要なSplunkソリューション
Splunk Enterprise
Splunk UBA
Splunk Simple Search

SPLの難易度
低

実装方法
このサーチは、Palo Alto Networks環境ではただちに機能します。プロキシを可視化するその他のソースに適用する場合でも簡単に導入できます。たとえば、専用のプロキシと、Splunk StreamやBroなどのネットワーク可視化ツールを組み合わせる場合などです。ソースタイプとフィールドを一致するように調整するだけで使用できるようになります。

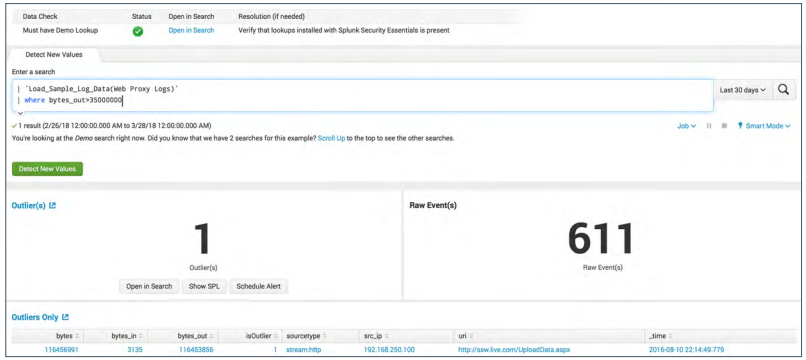
アラートの量
中

既知の誤検知
このサーチでは、大量の誤検知が発生する可能性があります(休暇中の写真がアップロードされた場合など)。多くの組織では、監視リストに含まれるユーザーに焦点を当てて絞り込みを試みます。対象となるのは、機密性の高いデータへのアクセス権を持つユーザーか(経営層、サイエンティストなど)、雇用上の理由があるユーザーです(パフォーマンスプラン、解雇予告済み、契約満了など)。これらの監視リストは、ルックアップを使用して実装できます。

対応方法
このアラートが発生するのは、多くの場合、完全に正当な理由(休暇中の写真のアップロードなど)からです。対応手順では、通常、データの送信先や、ユーザーが以前にもそのサイトにデータをアップロードしていないかを確認します。ユーザーに直接問い合わせて理由を確認することもあります。その際は、その従業員の組織内での状況を事前に調べておくことをお勧めします。たとえば、従業員がパフォーマンスプランの対象であるか、契約の満了間近であるかなどです。これらはいずれも、データ流出が大いに懸念される状況です。アクセス先サイトに対してNGFWまたはDLPシステム経由でSSLインスペクションを有効化すると、実際に転送したファイルを閲覧できる場合があり、コンテキストの把握に役立ちます。

Webへの大量アップロードの検出に関するヘルプ
この例では、シンプルサーチと以下のサーチ処理言語を使用します。このライブサーチでは、プロキシログのデータセットを使用して、35 MBを超えるイベントを調べます。下のスクリーンショットは、デモデータに対するサーチ結果を示します。

```
index=* sourcetype=pan:traffic OR (tag=web
tag=proxy) OR (sourcetype=opsec URL Filtering) OR
sourcetype=bluecoat:proxysg* OR sourcetype=websense*
earliest=-10m
| where bytes_out>35000000
| table _time src_ip user bytes* app uri
```



元従業員のアカウントへのログイン成功の検出

ステージ4

MITRE ATT&CK戦術

権限のエスカレーション　資格情報によるアクセス

MITRE ATT&CK技法

有効なアカウント　アカウント操作

データソース

認証　Windowsセキュリティ

セキュリティの課題
基本的に、退職したユーザーはログインすべきではありません。そのような状況が発生した場合、以前に資格情報が漏えいしたか、元従業員が不適切なアクションをとるためにログインを試みている可能性があります。いずれの場合でも検出すべきです。

ユースケース
セキュリティ監視、内部脅威

カテゴリー
アカウントの侵害、内部脅威

必要なSplunkソリューション
Splunk Simple Search Assistant

SPLの難易度
低

実装方法
Splunk Security Essentials Appでデータのオンボーディングガイドに従っていれば、このサーチをすぐに使用できます。通常は、Windowsセキュリティログを保存するインデックスを指定する必要があります(index=oswinsecなど)。Splunkユニバーサルフォワーダー以外の方法でデータを取り込む場合は、使用するソースタイプとフィールドを確認してください。その後の作業は簡単です。

アラートの量
少ない

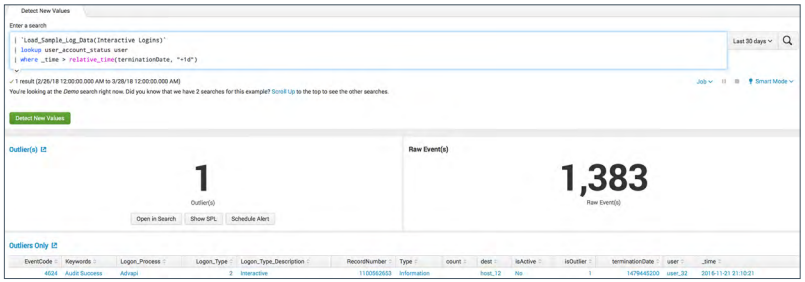
既知の誤検知
組織の方針としてアカウントを無効化または削除しない場合、このサーチが実用的にならない可能性があります。該当する場合は、退職後でも許容できるアクティビティが発生する可能性があるシステム(メール環境など)を指定することで、この行動に境界を設定することを検討してください。また、従業員のステータスが有効から無効に変わったときにパスワードを変更するための検出管理機能を実装するのもよいでしょう。さらに、従業員の退職後はアカウントに使用制限をかけるようにしてください。

対応方法
このアラートが発生したときにまず把握すべきことは、これがシステムの通常動作が何らかの形で続いていることを示すのか(机の下のデスクトップがまだログイン状態である、iPhoneアカウントがアクティブのままである、など)、それとも故意のアクションなのかということです。もちろん、成功したのか失敗したのかも重要です。最後に、組織体制が整っていない企業でシステム管理者の業務を行っていた従業員に関しては、当該アカウントの下でサービスやスケジュール設定されたジョブが実行されていないことを確認します。実行されている場合、アカウントを完全に無効化すると運用に影響を与える可能性があります。

元従業員のアカウントへのログイン成功の検出に関するヘルプ

この例では、シンプルサーチと以下のサーチ処理言語を使用し、ライブデータに基づいて、元従業員のアカウントでの認証成功アクティビティを検出します。使用するデータセットは、ログイン成功情報を含む、一連の匿名化済みWindows認証ログです。ルックアップでは、ユーザーのステータスを確認して、有効期限が1日以上前であるか無効であるユーザーを抽出しています。下のスクリーンショットは、デモデータに対するサーチ結果を示します。

```
index=* (source=win*security OR sourcetype=linux_secure OR
tag=authentication) user=* user!="" action=success
| lookup user_account_status.csv user
| where _time > relative_time(terminationDate, "+1d")
```



最後に

Splunkの分析主導型セキュリティを活用してセキュリティ体制を強化する方法について興味をお持ちの場合は、SplunkbaseからSplunk Security Essentials Appをぜひダウンロードしてください。300種類以上に及ぶセキュリティ上の課題の解決方法を無料で学ぶことができます。情報を収集したら、Splunkのセキュリティ担当者やパートナーと協力して、貴社の環境にもユースケースを導入しましょう。今すぐお問い合わせください。

© 2021 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。

21-13315-Splunk-Essential Guide to Security-EB-JA-202202