

インシデントカテゴリと定義により、対応チームメンバーとその他の組織の人材全員が、用語、概念、説明の意味を理解するための共通基盤を得ることができます。カテゴリ、タイプ、定義は業界によって異なる場合があります。米国連邦機関のインシデントカテゴリのリストは、us-cert.cisa.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdfから入手できます。

インシデント管理における課題の1つとして、リソースを効果的に割り当てることができます。これは、特定されたインシデントの重度を評価し、修復に向けた優先順位を付けることを意味しています。このプロセスに影響を与える可能性がある要因はいくつかあります。

- データの完全性 - インシデントの優先順位付けで最も重要な要素は多くの場合、リスクにさらされたデータの価値です。
- ダウンタイム - もう1つの重要な要素は、インシデントがビジネスのプロセスを中断する度合いです。インシデントは、資産、システム、またはビジネスプロセスの可用性のグレードの低下（パフォーマンスの低下）または中断（完全停止）のいずれかをもたらす可能性があります。アセットのインベントリと、ビジネスプロセスの徹底したリスク評価（アセットとコンピューターシステムが各プロセスをどのようにサポートするかを示す）を完了した場合、重要なプロセスを簡単に特定し、ダウンタイムのコストの観点からインシデントの影響を定量化できます。
- 財務/評判 - データの完全性とダウンタイムの両方は、短期および長期に渡り重要な経済的影響をもたらします。短期的なコストには、インシデント対応そのものと、損失したビジネスの機会が含まれます。長期的な経済的コストとして、評判や市場での地位の失墜が含まれる場合があります。
- 範囲 - インシデントの範囲（大まかには影響を受けるシステムの数）は、優先順位を直接示すものではありません。数多くのシステムのパフォーマンスが低下しますが、データ侵害の危険がないタイプのマルウェアに感染する可能性があります。これは、脅威アクターがトップシークレットの情報が保存される単一データベースサーバーのデータを侵害する際のマスキング攻撃の可能性もあります。
- 検知時間 - 調査によると、データ侵害の存在の半数以上が、侵入が発生してから何週間も何か月も発見されませんが、侵入に成功すると、数分以内にデータが危険にさらされると一般的には言われています。これは、侵入の検索に使用されるシステムが完璧で、検知への対応が迅速である必要があることを示しています。
- 復旧時間 - 一部のインシデントでは、必要なシステムの変更の実装が複雑なため、修復に時間がかかる場合があります。この長引く復旧期間を、継続的な攻撃や新たな攻撃に対する警戒を強めるきっかけにしてください。

サイバーキルチェーン攻撃のフレームワーク

有効なインシデント対応は、脅威インテリジェンスに依存します。脅威リサーチは、特定の敵の戦術、技術、手順(TTP)に関する知見を提供します。脅威リサーチからの知見を使用して、イベントのシナリオに対処する特定のツールやプレイブックを作成できます。脅威リサーチの主なツールは、攻撃の段階を説明するために使用するフレームワークです。これらの段階はしばしばサイバー・キルチェーンと呼ばれ、ロッキーード・マーティンが委託した影響力のあるホワイトペーパー Intelligence-Driven Computer Network Defense (インテリジェンスに基づくコンピューターネットワーク防御) (lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf)に従っています。



キルチェーンの段階。

Lockheed Martinのキルチェーンでは次の段階を特定します。

1. 勘査 - この段階では、脅威アクターは攻撃の段階を完了するために使用する方法を決定し、ターゲットの人材、コンピューターシステム、サプライチェーンに関する情報を集めます。
2. 武器化 - 脅威アクターはアクセスを可能にするペイロードコードと、脆弱性を使用してターゲットシステムで実行するエクスプロイトコードを結合します。
3. 配布 - 脅威アクターは、武器化されたコードをターゲットの環境に送信するベクトル（メールの添付ファイルやUSBドライブなど）を特定します。
4. エクスプロイト - 武器化されたコードは、このメカニズムによってターゲットシステムで実行されます。例えばフィッシングメールでは、ユーザーをだましてコードを実行させようとしたり、ドライブバイダウンロードでは、ユーザーが介入することなく脆弱なシステムで実行されたりします。
5. インストール - このメカニズムにより、武器化されたコードはリモートアクセスツールを実行し、ターゲットシステムで持続性を持つようになります。
6. コマンドと制御 (C2またはC&C) - 武器化されたコードは、リモートサーバーにアウトバウンドチャネルを確立します。このリモートサーバーを使用してリモートアクセスツールを制御したり、別のツールをダウンロードして攻撃をさらに進める可能性があります。
7. 目的に対するアクション - この段階では、脅威アクターは通常、取得したアクセスを利用してターゲットシステムから情報を密かに収集し、リモートシステムに転送します（データ流出）。ただし、脅威アクターには別の目標または動機がある可能性があります。

その他の攻撃フレームワーク

脅威アクターの行動の特徴を分類し、攻撃のインジケーターを見つけやすくするために、他の攻撃フレームワークも導入されています。

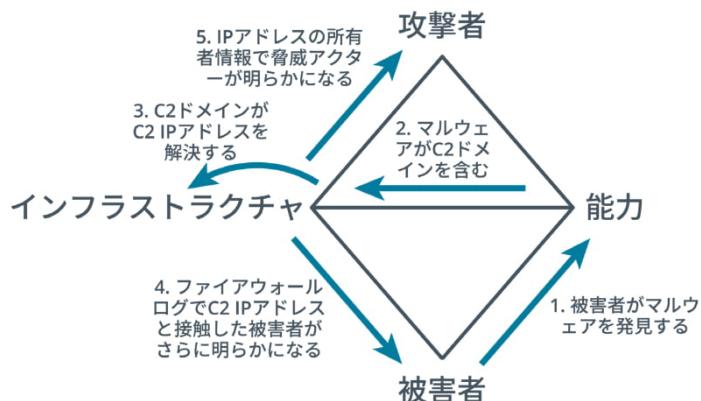
MITRE ATT&CK

キルチェーンによるライフサイクル分析の代わりに、**MITRE Corporationの敵対的戦術、技術、および共有知識(ATT&CK, Adversarial Tactics, Techniques, and Common Knowledge)**マトリックスにより、既知のTTPのデータベースを利用することができます。この無料で利用できるリソース(attack.mitre.org)では、各手法を一意のIDでタグ付けし、1つ以上の戦術カテゴリ（初期アクセス、持続性、ラテラルムーブメント、コマンドと制御など）に配置します。脅威アクターが特定の戦術カテゴリを展開する順序は明らかにされません。これは、アナリストは局所的な証拠から各攻撃のライフサイクルを解釈する必要があることを意味しています。このフレームワークにより、特定の脅威アクターが戦略レベルでキャンペーンを実行する方法を推測することなく、さまざまな脅威アクターグループが使用するTTPを直接比較できます。

Linux、macOS、Windowsのホストに対するTTPともいえるエンタープライズ向けのマトリックスと、モバイル向けのマトリックスがあります。例えば、Drive by Compromise（ドライブバイコンプロマイズ）には、ID T1189が与えられ、Windows、Linux、およびmacOSホストを標的とするInitial Access（初期アクセス型）の戦術に分類されます。このページをクリックすると、検知方法、緩和手段、過去の使用例と分析などの情報にアクセスできます。

侵入分析のダイヤモンドモデル

侵入分析のダイヤモンドモデルでは、脅威アクター、能力、インフラストラクチャ、被害者の4つの中核的な特徴の関係を模索することで、侵入イベント(E)を分析するフレームワークを提案します。この4つの特徴はダイヤモンド形の4つの頂点によって表されます。また各イベントは、日時、キルチェーンの段階、結果などのメタ機能によって説明される場合もあります。各特徴には、信頼水準(C)が割り当てられ、データの精度または分析によって値に割り当てられた結果や仮定の信頼性を示します。



ダイヤモンドモデルに表される侵入イベント。（画像：Sergio Caltagirone、Andrew Pendergast、Christopher Betzによってパブリックドメインに公開
[activeresponse.org/wp-content/uploads/2013/07/diamond.pdf] ）

インシデント対応の演習

インシデント対応に使用される手順やツールは、習得して効果的に実行するのが難しいものです。実際のインシデントというプレッシャーの高い環境で、初めてのスタッフがそれらを実践しているような状況は避けたいでしょう。テスト演習を実施することは、スタッフの能力開発を助け、手順やツールの欠陥を特定するのに役立ちます。特定のインシデント対応シナリオにおけるトレーニングでは、次の3つの形式が使用できます。

- 机上** - これは最もコストがかからないタイプのトレーニングです。ファシリテーターがシナリオを提示して、対応者は脅威を識別、封じ込め、根絶するための措置を説明します。このトレーニングではコンピューターシステムは使用しません。シナリオのデータはフラッシュカードとして提示されます。
- ウォークスルー** - このモデルでは、机上演習と同じようにファシリテーターがシナリオを提示し、インシデント対応者は対応措置を実演します。机上演習とは違って、対応者はスキャンを実行したり、サンプルファイルを分析するなどの措置を、通常は企業の実際の対応と復旧ツールのサンドボックスバージョンで実施します。

- シミュレーション - シミュレーションとはチームベースの演習で、レッドチームが侵入を試み、ブルーチームが対応と復旧管理にあたり、ホワイトチームは演習を管理し、評価します。このタイプのトレーニングには、かなりの投資と計画が必要になります。



ネットワーク攻撃シミュレーション練習に参加するケンタッキー州とアラバマ州の州兵および対空警戒員。
(画像: © 2017 Kentucky National Guard)



MITREは、インシデント対応演習の準備と進行について説明したホワイトペーパーを発行しています(mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf)。

インシデント対応、災害復旧、保持ポリシー

インシデント対応は、エンタープライズリスク管理とサイバーセキュリティの耐性（レジリエンス）に関する全体的な計画に適合します。

インシデント対応と災害復旧および事業継続性

特定のインシデント対応計画は、その他の災害復旧と事業継続の計画と区別されるべきです。

- 災害復旧計画 - 災害**は、組織の主要な業務機能が中断される特別な種類のインシデントと見なすことができます。災害復旧では、プロセスをセカンダリサイトにシフトするなど、多大なリソースが必要になります。災害復旧には、それほど深刻ではないインシデントよりも広範なステークホルダーが関与します。
- 事業継続計画(BCP)** - これは、ビジネスプロセスがマイナーな中断と災害レベルの中止の両方にどのように対処すべきかを特定します。インシデント発生時、システムは分離する必要がある可能性があります。継続計画により、ワークフローをサポートする処理の冗長性が確保されるため、セキュリティの修復のためにサーバーがオフラインになった場合に、処理を別のシステムにフェイルオーバーできます。システムにこの種の計画された耐性（レジリエンス）がない場合、インシデント対応はさらに混乱します。
- オペレーション継続計画(COOP)** - この用語は政府機関に使用されますが、機能的には事業継続計画に似ています。一部の定義では、COOPは特に、ITサポートのない任務機能を実行するバックアップ方法を指します。

インシデント対応、フォレンジクス、保持ポリシー

インシデント対応プロセスは、封じ込め、根絶、復旧に重点を置いています。これらの目的は、フォレンジクスの目的と完全には一致しません。デジタルフォレンジクスでは、改ざんや操作がないことを示す証拠を収集し、保存する手法を説明します。フォレンジクス手順は詳細で時間がかかり、インシデント対応の狙いは通常、緊急を要します。調査で証拠が保持されるようにフォレンジクス収集方法を使用する必要がある場合、これは対応プロセスの早期に特定される必要があります。

保持ポリシーも、遡及的なインシデント対応または脅威ハンティングにとって重要です。過去のログとデータ取得の保持ポリシーでは、それらが保持される期間が設定されます。イベントの発生から数か月または数年後に侵害のインジケーターを発見する場合があります。ログやその他のデジタル証拠を保管するための保持ポリシーがなければ、それ以上の調査を行うことはできません。

レビュー アク ティビティ： インシデント対応手順

次の質問にお答えください。

1. インシデント対応ライフサイクルの6つの段階とは何ですか？
2. 次の記述は正しいですか、誤りですか？すべてのセキュリティアラートをスタッフ全員に公開するのは重要です。
3. あなたは、ある企業にインシデント対応手順を改善するためのセキュリティコンサルティングを行っています。ビジネスマネージャーは、対応者向けのアウトオブバンドの連絡先メカニズムがなぜ必要なのか尋ねています。何と答えますか？
4. 特定のTTPの説明を提供する攻撃フレームワークはどれですか？
5. あなたのコンサルティングにはトレーニングセグメントが含まれます。実際のインシデント処理シナリオを最もよく表しているのはどのインシデント対応演習ですか？

トピック17B

インシデント対応に適切なデータソースを活用する



対象試験範囲

4.3 与えられたインシデントに基づいて、適切なデータソースを使用して調査をサポートすることができます

セキュリティ監視では、大量のデータが生成され、自動検知システムでは、大量のアラートが生成される可能性があります。最も急を要するイベントをインシデントとして優先して調査し、素早く解決することは、あらゆるタイプの組織にとって重要な課題になっています。あなたはセキュリティの専門家として、適切なデータソースを活用し、インシデントの識別をできる限り効率的に実行できる必要があります。

インシデントの識別

識別はイベントの照合プロセスで、イベントがインシデント、またはインシデントへの前兆の可能性（インシデントが発生する可能性が高いイベント）として管理されるべきかどうかを決定します。イベントや前兆が記録できるチャネルは複数あります。

- ログファイル、エラーメッセージ、IDSアラート、ファイアウォールアラート、その他のリソースを使用し、ベースラインを確立して、セキュリティインシデントの可能性を示すパラメータを特定する。
- 偏差を確立された指標と比較し、インシデントとその範囲を認識する。
- サイト、施設、ネットワーク、ホストの手動または物理的な検査。
- 従業員、顧客、またはサプライヤーによる通知。
- システムベンダー、監督機関、メディア、その他の外部当事者による新しい脆弱性や脅威の公開レポート。

従業員が内部関係者による詐欺行為や不正行為などの脅威を報告することに恐怖心を抱くことがないよう、内密に報告する手段を提供することが推奨されます。侵入者に攻撃が検知されたことが気付かれないように、「アウトオブバンド」の通信手段を使用しなければならない可能性もあります。

第一対応者

疑わしいイベントが検知される場合、その状況を把握して適切な対応策を練ることができるよう、CIRTの適切な人員に通知することが最重要です。この人員は、**第一対応者**と呼ばれます。これは、組織のすべてのレベルの従業員が、実際のセキュリティインシデントまたはその疑いがある状況を適切に認識し、それに対応できるようトレーニングをする必要があることを意味しています。組織全体でセキュリティに関する認識が適切であれば、誤検知や検知漏れは減ります。最も重大なインシデントでは、CIRT全体が関与し、効果的な対応を考案する場合があります。

分析とインシデントの識別

通知が行われると、CIRTまたは他の責任者はイベントを分析し、本物のインシデントが特定されたかどうかと、どのレベルの優先度を割り当てる必要があるかを判断する必要があります。分析は、インシデントのタイプと影響を受けたデータやリソース（その範囲と影響）の特定によって異なります。この時点では、インシデント管理データベースにイベントインジケーター、インシデントの性質、インパクト、インシデント調査担当者の記録があるはずです。インシデント管理の次の段階は、適切な対応を決定することになります。

セキュリティ情報イベント管理

攻撃フレームワークと組み合わせることで、通知は、悪意のあるアクティビティや、予測するインジケーターの場所を提供します。インシデント分析は、セキュリティ情報イベント管理(SIEM)システムにより、大幅に容易になります。SIEMでは複数のセンサー、アプライアンス、ホストからのネットワークトラフィックとログデータを解析し、情報を標準フィールドタイプに正規化します。

相関

SIEMでは次に、データソースから抽出したインジケーターで相関ルールを実行し、潜在的なインシデントとして調査するべきイベントを検知できます。また報告されたインシデントのタイプに基づいて、データをフィルタリングまたはクエリできます。

相関とは、個別のデータポイント間の関係を解釈し、セキュリティチームにとって重要なインシデントを診断することです。SIEM相関ルールとは、特定の条件に一致するステートメントです。これらのルールでは、ANDやORなどの論理式と、`=` (等しい)、`<` (小なり)、`>` (大なり)、`in` (含む)などの演算子を使用します。例えば、1度のユーザーログインの失敗はアラートが発生すべき条件ではありません。1時間以内に同じアカウントで複数回のユーザーログインの失敗が発生する場合は、調査が必要な可能性が高く、相関ルールによる検知の候補になります。

```
Error.LogonFailure > 3 AND LogonFailure.User AND Duration < 1 hour
```

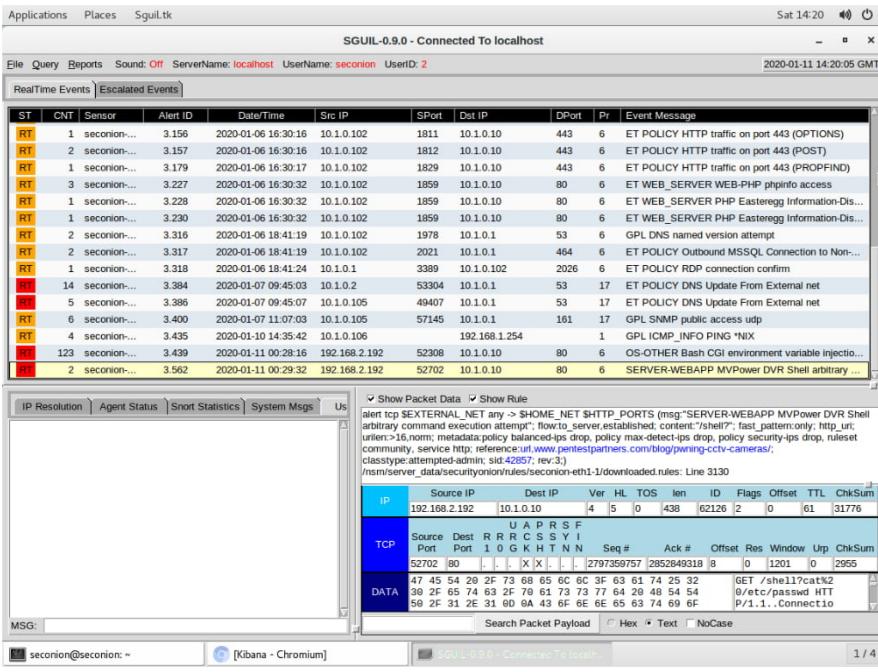
ネットワークで観察されるインジケーター間の相関と同じく、SIEMは脅威インテリジェンスフィードで構成されている可能性があります。これは、ネットワークで観察されたデータポイントが、IPアドレスやドメイン名などの既知の脅威アクターインジケーターに関連している可能性があることを意味しています。AIアシスト分析により、より高度なアラートと異常な動作の検知が可能になります。

保持

SIEMでは保持ポリシーを規定し、履歴ログとネットワークトラフィックのデータが定義された期間保管されるようにできます。これにより、遡及的なインシデントと脅威ハンティングが可能になり、フォレンジックな証拠の貴重なソースとなります。

SIEMダッシュボード

SIEMダッシュボードは、自動アラートの主なソースの1つです。SIEMダッシュボードでは、日常のインシデント対応のために機能するコンソールを提供します。さまざまな目的に合わせて、個別のダッシュボードが作成できます。インシデント対応者のダッシュボードには、アカウントに割り当てられた未分類のイベントと、主なステータス指標が表示される視覚化情報（図表）が含まれます。マネージャーのダッシュボードでは、イベント対応者全員の未分類イベントの数など、全体的なステータスインジケーターが表示されます。



Security OnionのSGUILコンソール。SIEMでは、優先度と調査のために手動で評価する必要がある膨大な数のアラートを生成できます。
(スクリーンショットはSecurity Onion securityonion.net提供)

感度とアラート

SIEMの運用における最大の困難の1つは、システムの感度を調整し、誤検知インジケーターがイベントとして報告されることを減らすことです。これが困難なのは、第一に全体的な感度を調整するための単純なダイヤルがなく、第二に、イベントを生成するルールの数を減らすと検知漏れのリスクが高まるからです。検知漏れとは、イベントとして関係付けられ、アラートを発生させるべきインジケーターが無視されることです。

相関ルールは、それぞれに一致するそれぞれに一致する重要度レベルを割り当てます。例：

- ログのみ - イベントが生成され、SIEMのデータベースに追加されますが、自動的に分類されます。
- アラート - イベントは、対応者が評価できるようにダッシュボードまたはインシデント対応システムに一覧表示されます。対応者はイベントを分類し、ログに送るか、インシデントとしてエスカレーションします。
- 警報 - イベントは自動的に重要と分類され、優先アラームが発生します。これは、インシデント対応者に電子メールやテキストメッセージが送信されることを意味する場合があります。

センサー

センサーは、パケットキャプチャと侵入検知を実行するネットワークタップまたはポートミラーです。SIEMの主な使用法の1つは、複数のセンサーとログソースからデータを集約することですが、1つのセンサーまたはソースホストからの出力を表示するダッシュボードを構成することが適切な場合もあります。

傾向分析

傾向分析は、時系列においてデータセット内でパターンやインジケーターを検知し、そうしたパターンを使用して将来のイベントを予測するプロセスです。傾向は、ログファイルの各イベントを調べるだけで特定することは困難です。代わりに、イベントの種類の発生率を視覚化し、そうしたイベントの数や頻度が時間とともにどのように変化するかを示すソフトウェアが必要になります。傾向分析は、頻度、ボリューム、統計偏差に適用できます。

- 頻度ベースの傾向分析では、1日の1時間あたりのNXERROR DNSログイベント数など、メトリックのベースラインを確立します。頻度がベースラインのしきい値を超える（場合によっては下回る）場合、アラートが発生します。
- ボリュームベースの傾向分析では、より単純なインジケーターで実行できます。例えば、脅威レベルを判断する1つの単純なメトリックは、ログボリュームです。ログが増えるペースが以前よりも速い場合、調査する必要がある可能性があります。ボリュームベースの分析は、ネットワークトラフィックにも適用されます。また、エンドポイントディスク使用量も計測できます。通常、クライアントのワークステーションではローカルでデータを保存する必要はありません。よってホストのディスク容量が突然減少する場合、データ流出の計画に使用されていることを示している可能性があります。
- 統計的偏差分析では、データポイントが疑わしいものとして処理される必要がある場合を示すことができます。例えばクラスターのグラフでは、標準ユーザーと特権ユーザーによるアクティビティを示し、それぞれのタイプが実行するプロセスや、アクセスするシステムなどの動作メトリックの分析を呼び出すことができます。標準ユーザーと特権ユーザーの2つのクラスターの外に表示されるデータポイントは、そのアカウントによる疑わしいアクティビティが示される可能性があります。

ロギングプラットフォーム

ネットワークアプライアンスとホストからのログデータは、ローカルエージェントをインストールしてログデータを収集・解析するか、転送システムを使用してログを直接SIEMサーバーに送信することで、SIEMによって集約できます。また組織でSIEMを利用していない場合でも、ロギングプラットフォームを使用して、中心的な場所にログデータを集約できます。

Syslog

Syslog (tools.ietf.org/html/rfc3164)では、イベントメッセージのログにオープンフォーマットのプロトコルとサーバーソフトウェアを提供します。これはさまざまなホストタイプによって使用されています。例えば、syslogメッセージはCiscoのルーター、スイッチ、サーバー、ワークステーションで生成できます。これには通常UDPポート514が使用されます。

syslogメッセージはPRIコード、タイムスタンプとホスト名が含まれるヘッダー、メッセージ部で構成されます。PRIコードは、ファシリティと重要度のレベルから計算されます。メッセージ部には、ソースプロセスとコンテンツを示すタグが含まれます。コンテンツの形式は、アプリケーションによって異なります。スペース区切りまたはコンマ区切りのフィールドや、JSONデータなどの名前/値ペアが使用される可能性があります。

 [RFC 5424](http://tools.ietf.org/html/rfc5424) (tools.ietf.org/html/rfc5424)では、構造をわずかに調整し、タグをアプリ名、プロセスID、メッセージIDフィールドに分割し、それらをヘッダーの一部にします。

RsyslogとSyslog-ng

元のsyslogの仕様には2つの更新があります。

- Rsyslogでは同じ構成ファイル構文を使用しますが、TCPを介して機能し、セキュアな接続を使用できます。また、構成ファイルでより多くの種類のフィルター式を使用し、メッセージの処理をカスタマイズできます。

- Syslog-ngでは、異なる構成ファイル構文を使用しますが、TCP/セキュア通信とより詳細なメッセージのフィルタリングオプションも使用できます。

journalctl

Linuxでは、syslogによって管理される種類のテキストベースのログファイルが、cat、tail、headなどのコマンドを使用して表示できます。最新のLinuxディストリビューションでは、systemdを使用してシステムを起動したり、バックグラウンドサービスを開始・管理できるようになりました。イベントをsyslog形式のテキストファイルに書き込む代わりに、systemdによって管理されるプロセスからのログが、journaldと呼ばれるバイナリ形式ファイルに書き込まれます。journaldによってキャプチャされたイベントはsyslogに転送できます。journaldで直接イベントを表示させるには、journalctlコマンドを使用してジャーナルログ全体を印刷するか、コマンドでさまざまなオプションを発行して、サービス名の一致や指定した重大度レベルに一致するメッセージのみを印刷するなど、さまざまな方法でログをフィルター処理できます。

NXlog

NXlog (nxlog.co)はオープンソースのログ正規化ツールです。その主な用途の1つは、XMLベースの形式を使用するWindowsログを収集し、syslog形式に正規化することです。

ネットワーク、OS、セキュリティログファイル

ログファイルデータは、セキュリティインシデントの調査において重要なリソースになります。ログ形式だけでなく、ログファイルのソースの範囲も考慮し、特定の調査シナリオをサポートするのに最適なログファイルの種類を決定する方法を把握している必要があります。

システムログとセキュリティログ

セキュリティ情報のソースの1つは、各ネットワークサーバーやクライアントからのイベントログになります。Microsoft Windows、Apple macOS、Linuxなどのシステムでは、さまざまなログを保存し、ユーザーとソフトウェアがシステムとやり取りをする際のイベントを記録します。ログの形式は、システムによって異なります。またログ内に含まれる情報もシステムによって異なり、多くの場合は取得する情報のタイプが設定できます。

イベントが生成されると、ログカテゴリに配置されます。これらのカテゴリは、イベントの一般的な性質や、影響を及ぼすOSの領域を表しています。Windowsイベントログの5つの主要カテゴリは次のとおりです。

- アプリケーション - サービスが起動できないなど、アプリケーションやサービスによって生成されるイベント。
- セキュリティ - 失敗したログイン、拒否されたファイルへのアクセスなどの監査イベント。
- システム - ストレージボリュームの稼働状況チェックなど、オペレーティングシステムやそのサービスによって生成されるイベント。
- 設定 - Windowsのインストール中に生成されるイベント。
- 転送イベント - 別のホストからローカルログに送信されるイベント。

ネットワークログ

ネットワークログはルーター、ファイアウォール、スイッチ、アクセスポイントなどのアプライアンスによって生成されます。ログファイルには、アプライアンス自体の動作や状態（アプライアンスのシステムログ）に加え、ファイアウォールでブロックされたポートの使用を試みるホストや、スイッチに接続する際に複数のMACアドレスを使おうとするエンドポイントなど、ネットワークの動作を記録するトラフィックログやアクセスログが記録されます。

認証ログ

各ホストにおける認証の試行はセキュリティログに書き込まれる可能性があります。また、RADIUSサーバーとTACACS+サーバー、Windows Active Directory (AD)サーバーなど、ログインを認証するサーバーからのログを調べる必要がある場合があります。

脆弱性スキャン出力

脆弱性スキャンレポートは、攻撃がどのようにしてなされたかを判断する際のもう1つの重要なソースです。スキャンエンジンでは、スキャンレポートに脆弱性が含まれる場合にログに記録したり、アラートを出すことがあります。レポートを分析し、パッチ適用されていない脆弱性や、修復されていない構成の弱点を特定できます。これらは、最近開発されたエクスプロイトに関連付けられます。

アプリケーションログファイル

アプリケーションログファイルは、OSではなくアプリケーションによって管理される単純なもので、アプリケーションでは、イベントビューアまたはsyslogを使用して、標準形式でイベントデータを書き込むか、開発者が選択した形式で独自のアプリケーションディレクトリにログファイルを書き込む可能性があります。

DNSイベントログ

DNSサーバーでは、ドメイン名とIPアドレス間を変換するリクエストを処理するたびにイベントをログに記録する可能性があります。DNSイベントログでは、次のような、有用なセキュリティインテリジェンスを提供するさまざまな情報を保持できます。

- ホストがDNSに行ったクエリの種類。
- 疑わしいIPアドレス範囲やドメインと通信しているホスト。
- スパイクや一貫して多いDNSルックアップの失敗などの統計的異常。これはマルウェアに感染しているか、構成が間違っている、または廃止されたアプリケーションや障害のあるアプリケーションを実行しているコンピューターを示している可能性があります。

Web/HTTPアクセスログ

Webサーバーは通常、エラーが発生するHTTPトラフィックや、事前定義されたルールセットの一部に一致するトラフィックをログに記録するように構成します。ほとんどのWebサーバーでは、共通ログ形式(CLF)またはW3C拡張ログファイル形式を使用して、関連情報を記録します。

レスポンスのステータスコードでは、リクエストとサーバーの動作の両方についてかなりの情報を明らかにできます。400の範囲のコードは、クライアントベースのエラー、500の範囲のコードは、サーバーベースのエラーを示します。例えば、403（「Forbidden」）レスポンスが繰り返される場合、クライアントによる認証されていないリソースへのアクセスの試みを、サーバーが拒否していることを示している可能性があります。502（「Bad Gateway」）レスポンスは、ターゲットサーバーとそのアップストリームサーバー間の通信がブロックされているか、アップストリームサーバーがダウンしていることを示している可能性があります。

またステータスコードに加えて、一部のWebサーバーソフトウェアでは、リクエストとレスポンスの両方のHTTPヘッダー情報をログに記録します。これにより、Cookie情報やMIMEタイプなど、各リクエストやレスポンスの構成をより正確に把握できるようになります。もう1つの注目すべきヘッダーフィールドは、リクエストを行うアプリケーションの種類を特定するUser-Agentフィールドです。これはリクエストを行うアプリケーションの種類を特定します。ほとんどの場合、これはクライアントがサイトへのアクセスに使用しているブラウザのバージョンと、クライアントのオペレーティングシステムになりますが、Microsoft Edgeなどのブラウザには、ユーザーエージェント文字列にGoogle ChromeとSafariのバージョンが含まれるため、誤解が生じる可能性があります。従ってユーザーエージェントフィールドは、クライアントの環境についての信頼できるインジケーターではない場合があります。

VoIPとコールマネージャーおよびセッションイニシエーションプロトコル(SIP) トラフィック

多くのVoIPシステムでは、セッションイニシエーションプロトコル(SIP)を使用してエンドポイントを特定し、呼び出しを設定します。通話内容は別のプロトコル（通常はRTP (Real Time Protocol)）を使用して転送されます。VoIPプロトコルは、Web通信と同様の脆弱性とエクスプロイトのほとんどに対して脆弱です。SIPとRTPの両方で、トランスポートレイヤーセキュリティ(TLS)によってエンドポイントが認証され、通信が保護されるセキュアなプロトコル形式を使用してください。

コールマネージャーは、ローカルネットワーク内で、またインターネットを介してエンドポイントを接続するゲートウェイです。コールマネージャーでは、VoIPコールを携帯電話と固定電話のネットワークに接続するメディアゲートウェイも実装される可能性があります。SIPは、SMTPのログと同様のログが、通常は共通ログ形式で生成されます。SIPログは、コールリクエストに関するエンドポイントと、接続のタイプ（音声のみや動画付き音声など）、メッセージのステータスを特定します。リクエストを処理する場合、コールマネージャーとその他の中間サーバーでは、ホップごとのSMTPヘッダーと同様に、ViaヘッダーにIPアドレスを追加します。ログを調べることで、認証されていないプロキシがトラフィックを傍受する中間者攻撃の証拠が明らかになる可能性があります。電話網に接続されているVoIPシステムも、料金詐欺のターゲットになります。コールマネージャーのアクセスログで疑わしい接続を監査できます。

ダンプファイル

システムメモリには揮発性データが含まれます。システムメモリのダンプでは、実行しているプロセス、一時ファイルシステムの内容、レジストリデータ、ネットワーク接続、暗号化キーなどを特定するために分析できるイメージファイルを作成します。また、マスストレージデバイスに保存される場合に暗号化されるデータにアクセスする方法にもなります。

メタデータ

メタデータは、アプリケーションによって作成され、メディアに保存され、またはネットワーク上で送信されるデータの特性です。多くのメタデータソースは、いつ、どこで、といった時系列の質問に解を与え、他のタイプの証拠も含むことができるため、インシデントを調査する際に役立つ可能性があります。

ファイル

ファイルのメタデータは属性として保存されます。ファイルシステムは、ファイルが作成、アクセス、変更されたときにそれを追跡します。ファイルは読み取り専用としてマークしたり、非表示またはシステムファイルとしてマークするなどのセキュリティ属性が割り当てられる可能性があります。アクセス許可を示すファイルに添付されたACLは、また別のタイプの属性を表します。最後に、ファイルには作成者、著作権情報、インデックス/検索用のタグを記録する拡張属性が含まれる場合があります。Linuxの場合、lsコマンドを使用してファイルシステムのメタデータをレポートできます。

Web

クライアントがWebサーバーからのリソースを要求する場合、サーバーはリソースと、そのプロパティを設定または説明するヘッダーを返します。また、クライアントでは要求にヘッダーを含めることができます。ヘッダーの主な使用法の1つは、認可情報をCookieの形式で送信することです。返されるデータの種類（テキストやバイナリなど）を説明するヘッダーも重要な場合があります。ヘッダーのコンテンツは、Webブラウザに組み込まれた標準ツールで調べることができます。またヘッダー情報は、Webサーバーによってログに記録される場合があります。

電子メール

電子メールのインターネットヘッダーには、受信者と送信者のアドレス情報のほか、双方間におけるメッセージの送信を処理するサーバーの詳細が含まれます。電子メールが作成される

と、メールユーザーエージェント(MUA)で最初のヘッダーを作成し、メール配送エージェント(MDA)にメッセージが転送されます。MDAは、送信者がドメインからメッセージを送信することを許可されていることが確認されるはずです。電子メールが同じドメインでローカルに配送されていないと仮定すると、MDAは、独自のヘッダーを追加または修正してから、メッセージをメッセージ転送エージェント(MTA)に送信します。MTAは、メッセージを受信者にルーティングします。メッセージはISPによって運用されるSMTPサーバーやメールセキュリティゲートウェイなど1つ以上の追加のMTAを経由して渡されます。各MTAではヘッダーに情報を追加します。

ほとんどの電子メールアプリケーションではヘッダーがユーザーに公開されないため、通常ヘッダーは平均的なユーザーの判断の要因にはなりません。メッセージのプロパティ / オプション / ソースコマンドを使用して、メールクライアントからヘッダーを表示したり、コピーできます。MTAは、スパムの確認結果など、受信した各ヘッダーにたくさんの情報を追加できます。平文エディタを使用してヘッダーを表示する場合、各パートの開始位置と終了位置を特定するのが困難なことがあります。幸いなことに、ヘッダーを解析し、より構造化された形式で表示するために利用できるツールはたくさんあります。その一例は、Microsoft Remote Connectivity Analyzer (testconnectivity.microsoft.com/tests/o365) の一部として利用できる Message Analyzer ツールです。これにより、メッセージが通過するホップはより明確にレイアウトされ、各MTAによって追加されたヘッダーは分割されます。

モバイル

携帯電話メタデータは、着信、発信、試行された通話の通話詳細レコード(CDR)と、SMSテキストの時間、期間、相手側の番号で構成されます。またメタデータでは、データ転送量を記録します。デバイスの場所の履歴は、ネットワークへの接続に使用された基地局のリストによって追跡できます。疑わしいインサイダー攻撃を調査している場合、このメタデータで被疑者の所在を証明できる可能性があります。さらにAI対応の分析（または根気強い調査）によって、他の公開記録を通じて相手側の番号を企業や個人に関連付けることができます。

CDRは携帯電話事業者によって生成され、保存されます。CDRの保持期間は、国および州の法令によって決定されますが、通常は約18か月になります。CDRは、企業所有デバイスで直接利用でき、デバイスの所有者として通信プロバイダーに要求できます。個人的に所有しているデバイスのメタデータについては、通常は法執行機関が召喚状によって、またはアカウント所有者の同意がある場合のみアクセスできます。雇用契約では、従業員が職場で使用するデバイス持ち込み(BYOD)に対しこの許可を付与する必要がある場合があります。



現在の場所と時間などのメタデータも写真や動画に追加されますが、これはすべてのタイプのコンピューティングデバイスに当てはまります。これらのファイルがソーシャルメディアサイトにアップロードされると、アップロードした人の意図よりも多くの情報が明らかになる可能性があります。

ネットワークデータソース

ネットワークデータは通常、個々のフレームのレベルで詳細に分析されるか、トラフィックフローやプロトコルの使用状況に関する集約統計値を使用して分析されます。

プロトコルアナライザ出力

SIEMでは、ネットワークのさまざまなポイントでセンサーからの詳細を保存します。ネットワークパケットから取得された情報は、全体的なプロトコルの使用とエンドポイントのアクティビティを表示するように集約して、要約できます。またパケットのコンテンツは、分析用に記録できます。各パケットの全データの記録（遡及的ネットワーク分析(RNA)とも呼ばれる）はほとんどの組織にとってコストがかかり過ぎます。通常、パケットのコンテンツはトラフィックからのインジケーターがイベントとして関連付けられる場合にのみ保持されます。SIEMソフトウェアを使用すると、イベントまたはアラートの要約から基になるパケットヘビポットさせることができます。パケットコンテンツの詳細な分析により、攻撃に使用されるツールを明らかにできるようになります。また潜在的なマルウェアなどのバイナリファイルを抽出して分析できます。

Netflow/IPFIX

フローコレクターは、各フレームを記録するのではなく、ネットワークトラフィックに関するメタデータと統計を記録する手段です。ネットワークトラフィックとフローデータは、スイッチ、ルーター、ファイアウォール、Webプロキシなど、さまざまなソース（またはプローブ）から取得される可能性があります。フロー分析ツールでは、次のような機能が使用できます。

- 特定のアプリケーション、ホスト、ポートによって生成されたトラフィックで傾向とパターンをハイライト表示する。
- 異常検知、フロー分析パターン、またはカスタムトリガーに基づいてアラートする。
- 速やかにネットワーク接続のマップを作成し、トラフィックとフローデータのパターンを解釈できる視覚化ツール。
- 不正なユーザーの行動、転送中のマルウェア、トンネリング、割り当てられた帯域幅を超えるアプリケーションなどを明らかにするトラフィックパターンの識別。
- マルウェアによるハンドラーまたはコマンドと制御(C&C)チャネルへの接続の試みの識別。

NetFlowはCiscoが開発した、ネットワークフロー情報を構造化データベースに報告する手段です。NetFlowはIPフロー情報エクスポート(IPFIX) IETF標準(tools.ietf.org/html/rfc7011)として再開発されています。特定のトラフィックフローは、IPの送信元アドレスと宛先アドレス、プロトコルタイプなど、キーと呼ばれる同じ特性を共有するパケットにより定義できます。キーの選択はフローラベルと呼ばれ、フローラベルに一致するトラフィックは、フローレコードと呼ばれます。

さまざまなNetFlow監視ツールを使用して、ポイントインタイム分析用のデータを取得したり、ネットワークで発生しているセキュリティまたは運用上の問題を診断できます。数多くの商用NetFlowスイートと、NetFlowと同様の機能を提供する製品が市販されています。SiLKスイート(tools.netsa.cert.org/silk/)とnfdump/nfSEN (nfSEN.sourceforge.net/)は、オープンソースの実装の例です。評判が高いツールには他にArgus (openargus.org)があります。これは、NetFlowとは異なるデータ形式が使用されますが、クライアントツールではNetFlowデータを読み込み、解釈できます。

sFlow

HPによって開発され、後にWeb標準として採用された**sFlow** (tools.ietf.org/html/rfc3176)では、サンプリングを使用して、IPベースのNetflowよりも幅広いプロトコルタイプのOSIモデルの任意のレイヤーでトラフィック統計を計測します。またsFlowでは、サンプルのパケットヘッダー全体を取得できます。

帯域幅モニター

比較用に信頼できるベースラインがある場合、帯域幅の使用は、疑いのある動作の主なインジケーターになり得ます。予想外の帯域幅の消費は、データの流出攻撃などの証拠になる可能性があります。帯域幅の使用は、フローコレクターによってレポートできます。またファイアウォールやWebセキュリティゲートウェイでも帯域幅のモニターとアラートをサポートできる可能性があります。

レビュー アク ティビティ：

インシデント対応に適切なデータソース

次の質問にお答えください。

1. 次の記述は正しいですか、誤りですか？「第一対応者」とは、CIRTにインシデントを報告する最初の人員です。
2. あなたは、侵入検知データをWebサーバーログファイルと関連付ける必要があります。SIEMでIDSアラートを収集するために配置する必要があるコンポーネントはどれですか？
3. Windowsイベントログをsyslog互換サーバーに転送する際に最適なソフトウェアツールはどれですか？
4. ある技術者は、ログに大量の403 Forbiddenエラーがあることに気付きました。このログを生成しているネットワークアプライアンスまたはサーバーの種類は何ですか？
5. 疑わしいMTAの証拠は、どのタイプのデータソースで探せますか？
6. あなたは顧客の施設でSIEMの展開をサポートしています。顧客は、フローレコードが統合できるかどうか尋ねています。どのデータソースの種類がフローレコードになりますか？

トピック17C

緩和策を適用する



対象試験範囲

- 1.2 与えられたシナリオに基づいて、可能性あるインジケーターを分析して攻撃のタイプを特定することができる
- 4.4 与えられたインシデントに基づいて、緩和技術や制御を適用して、環境の安全を維持することができる

緩和策は、最初に封じ込めるために適用され、次に悪意のある活動の影響を根絶して回復するため適用されます。インシデント対応は、ビジネスのワークフローを中断することなく、侵入を排除するという相反する課題がある、非常にプレッシャーの高い作業です。あなたは特定のシナリオに最適な手法を選択して、適用できるようになる必要があります。

インシデントの封じ込め

インシデントにはさまざまなシナリオ、技術、動機、深刻度があるため、インシデントの封じ込めや分離に対する標準的なアプローチは存在しません。CIRTが直面している多くの複雑な問題の一部は次のとおりです。

- どのような損害や盗難がすでに発生しているのか？今後どの程度のものが、どのような時間枠で発生する可能性があるか（損失管理）？
- 利用可能な対策は何か？そのコストと影響は何か？
- 攻撃が検知されたことを脅威アクターに警告してしまうアクションは何か？どのような攻撃の証拠を集め、保持する必要があるか？

インシデントが特定、分類され、優先順位が付けられると、インシデント対応の次の段階は封じ込めになります。封じ込めの手法は、分離ベースまたはセグメンテーションベースのいずれかで分類できます。

分離ベースの封じ込め

分離とは、影響を受けたコンポーネントを、より大きな環境から取り除くことです。これは、DoS攻撃のターゲットになった後にネットワークからサーバーを取り除くことから、通常実行されているホスト環境の外部のサンドボックスVMにアプリケーションを配置することまで、すべてが当てはまります。状況に関わらず、影響を受けたコンポーネントと本番ネットワークやインターネットとの間にもはやインターフェイスがないことを確認する必要があります。

単純なオプションは、ネットワークのプラグを外す（エアギャップを作る）か、スイッチポートを無効にして、ネットワークからホストを完全に切断することです。これはステルス性が最もないオプションで、攻撃やマルウェアを分析する機会は減ります。複数のホストに影響する場合、ルーティングインフラストラクチャを使用して、感染しているひとつまたは複数のLAN (VLAN)を、ネットワークの他の部分からは到達できない**ブラックホール**に分離できます。また、ファイアウォールやその他のセキュリティフィルターを使用して、感染したホストが通信できないようにすることもできます。

最後の手段として、ユーザー アカウントやアプリケーションサービスを無効化して分離することもあります。ネットワーク内に侵入者を発見した場合、ユーザーのネットワークアカウントを一時的に無効化することで、被害を封じ込めることができる可能性があります。侵入者はリソースへのアクセス権限がなければ、さらなる攻撃や組織から情報を盗むことはできなくなります。ほとんどのホストでアプリケーションが実行できないようになれば、攻撃のベクトルになる可能性が疑われるアプリケーションは、脅威アクターにとってあまり有用ではなくなります。

セグメンテーションベースの封じ込め

セグメンテーションベースの封じ込めは、ネットワーク技術やアーキテクチャを使用して単一または複数のホストを分離する手段です。セグメンテーションではVLAN、ルーティング/サブネット、ファイアウォールACLを使用して、単一または複数のホストが保護されたセグメント外と通信できないようにします。ホストを完全に分離するのではなく、保護されたセグメントをシンクホールまたはハニーネットとして構成し、脅威アクターがC&Cチャネルを介してフィルタリングされた（場合によっては変更された）出力を引き続き受信できるようにして、攻撃が正常に進行していると思わせることができます。リバースエンジニアリングによるマルウェアコードの分析により、強力な偽装能力を得ることができます。マルウェアによって行われた関数呼び出しを傍受して、脅威アクターに攻撃が進行していると信じさせながら、戦術と（できれば）身元に関する詳細な知識を得られるようにします。攻撃を特定のグループに関連付けることで、敵対者の能力を推定することができます。

インシデントの根絶と復旧

インシデントを封じ込めた後、緩和策と制御を適用して、侵入ツールと不正な構成の変更をシステムから根絶できます。マルウェア、バックドア、侵害されたアカウントを個別のホストから根絶するのは、インシデント対応の最後の手順ではありません。また、機能やサービスの回復を目標とする復旧フェーズも考慮する必要があります。これは、ホストが完全に再構成され、インシデント発生前のようにビジネスワークフローが運用できるようになることを意味しています。復旧における重要な部分は、同じ攻撃ベクトルによってシステムが侵害されないようにするプロセスです（それができない場合は、そのベクトルを綿密に監視して、別の攻撃を事前に警告できるようにします）。

マルウェアやその他の侵入メカニズムの根絶と攻撃からの復旧には、いくつかの手順があります。

- 影響を受けたシステムの再構成 - 悪意のあるファイルやツールを感染したシステムから削除するか、セキュアなバックアップ/イメージからシステムを復元します。

! ベースラインテンプレート構成またはイメージから再インストールする場合、ベースラインにインシデントの発生を許可したものがないことを確認してください！その場合は、テンプレートを更新してから、再度ロールアウトしてください。

- セキュリティ管理の再監査 - 別の攻撃に脆弱でないようにします。これは同じ攻撃の場合や、脅威アクターがネットワークについて取得した情報を通じて起動できる新しい攻撃の場合があります。

! 組織が標的型攻撃にさらされている場合は、インシデントの直後に別のインシデントが発生する可能性があることに注意してください。

- 影響を受けた関係者に通知し、彼らのシステムを修復する方法が提供されるようにします。例えば、顧客のパスワードが盗まれた場合は、同じパスワードが使用されているかもしれない（良い慣習ではありませんがほとんどの人がそうしています）別のアカウントの認証情報を変更するように通達されるべきです。

ファイアウォール構成の変更

攻撃の分析では、脅威アクターによって悪用されたベクトルを特定できるべきです。この分析は、その攻撃ベクトルをブロックする構成の変更を特定するために使用されます。構成の変更には、新しい種類のセキュリティ管理の導入や、既存の管理設定を変更し、有効性を高めることがあります。

これまで多くの組織では、インターネットからのローカルネットワークの侵入を防ぐように設計された進入方向のフィルタリングルールに焦点を合わせていました。現在の脅威の状況では、他の手段で内部ホストに感染したマルウェアが外部のC&Cサーバーに通信しないように、厳密な退出方向のフィルタリングルールを適用することも不可欠です。エグレスフィルタリングは、許可されたネットワークアクティビティを中断するという点で問題になる可能性がありますが、最新ネットワーク防御の重要なコンポーネントです。エグレスフィルタリングの構成における一般的なガイドラインの一部は次のとおりです。

- 認証されたアプリケーションポートのみを許可し、可能な場合は、宛先アドレスを承認済みインターネットホストに制限します。認証済みホストが特定できない場合や、デフォルトの拒否が厳しすぎる場合、URLとコンテンツフィルタリングを使用して、認証済みプロトコルにおける悪意のあるトラフィックの検知を試みます。
- DNSレックアップを独自またはISPのDNSサービスや、GoogleまたはQuad9のDNSサービスなどの認定済みパブリックリゾルバーに制限します。
- ルート禁止またはピア禁止(DROP)フィルタリストの記載に従い、「既知の不正な」IPアドレス範囲へのアクセスをブロックします。
- ローカルネットワークで使用が認められていないIPアドレス空間からのアクセスをブロックします。
- インターネットに接続する必要のないホストサブネットからのすべてのインターネットアクセスをブロックします。これにはほとんどの種類の内部サーバー、産業用制御システム(ICS)の管理に使用されるワークステーションなどがあります。

これらのルールの範囲内であっても、脅威アクターがコマンドの発信や流出を実行する余地は多くあります。例えば、コンテンツ配信ネットワークやソーシャルメディアプラットフォームなどのクラウドサービスを使用して、スクリプトとマルウェアのコマンドを通信し、HTTPSを介してデータを持ち出すことができます(rhinosecuritylabs.com/aws/hiding-cloudcobalt-strike-beacon-c2-using-amazon-apis)。

コンテンツフィルター構成の変更

基本的なパケットフィルタリング方式のファイアウォールでは（たとえステートフルであっても）限界があるため、ある種のコンテンツフィルタリング方式のアプリケーションプロキシが、より優れたセキュリティを提供する可能性があります。この種のアプライアンスは通常、セキュアWebゲートウェイ(SWG)と呼ばれます。SWGでは、インターネットサービスへのユーザーアクセスを仲介し、定期的に更新されるURL/ドメイン/IPブラックリストからのコンテンツをブロックして、アプリケーション層プロトコルヘッダーとペイロードで一致するコンテンツに基づいてトラフィックの侵入検知/防止を実行します。

SWGがすでに導入されている場合、脅威アクターはある種のバックドアを介してSWGを回避する方法を見つけています。ネットワーク構成を確認・更新し、インターネットへのクライアントアクセスはすべて、必ずSWGを通じて行うようにします。また、脅威アクターはフィルタリングされていないプロトコルまたはC&Cメソッドを使用している可能性もあります。SWGは、エクスプロイトをブロックするスクリプトとデータ、ドメインとIPアドレスで更新する必要があります。

データ損失防止(DLP)

データ損失防止(DLP)でも同様の機能が実行されますが、ユーザーアクセスの代わりに、タグ付けされたデータのコピーを仲介して、認可済みのメディアとサービスに制限します。まだ実装されていない場合、攻撃によりセキュリティ管理としてDLPに投資する必要性が明らかになる可能性が

あります。DLPが有効になっており、ポリシーを適用する正しい方法で構成されている場合、脅威アクターはDLPソフトウェアでスキャンできないバックドア方式を使用してDLPを回避できる可能性があります。また脅威アクターは、データを認識されないように偽装している可能性があります。

モバイルデバイス管理(MDM)

モバイルデバイス管理(MDM)では、スマートフォンのアプリと機能の実行制御を提供します。機能にはGPS、カメラ、マイクが含まれます。DLPと同様に、侵入によって、脅威アクター者が登録を回避するためのベクトルやMDMのポリシー・テンプレートの設定ミスが見つかるかもしれません。

証明書の更新または失効

デジタル証明書で表される秘密鍵の侵害やスプーフィングされた証明書を信頼できるものとして提示する機能は、脅威アクターが信頼できるリソースになりすまして、セキュアなシステムへの不正アクセスを取得できる可能性があるため、重大なセキュリティの脆弱性になります。

- 侵害されたルート証明書を削除 - 脅威アクターがルート証明書をインストール出来た場合、悪意のあるホストとサービスを信頼できるもののように見せかけることができます。疑いのあるルート証明書はクライアントのキャッシュから削除する必要があります。
- 侵害されたホストの証明書を失効 - ホストが侵害された場合、デジタル署名やデジタルエンベロープに使用された秘密鍵は安全ではなくなります。鍵に関連付けられる証明書は「鍵の侵害」プロパティを使用して失効させてください。証明書は、新しい鍵ペアで鍵を再生成できますが、対象と有効期限情報は同じになります。

エンドポイント構成の変更

エンドポイントセキュリティが侵害された場合、緩和策を検討するためのいくつかのクラスのベクトルがあります。

- ソーシャルエンジニアリング - マルウェアがユーザーによって実行された場合、セキュリティ教育と啓蒙活動を使用して、将来的に攻撃が実行されるリスクを低減します。アクセス許可をレビューして、アカウントが低い権限レベルで運用されているかどうか確認します。
- 脆弱性 - マルウェアがソフトウェアの不具合を悪用した場合、パッチをインストールするか、パッチが開発されるまでシステムを分離します。
- セキュリティ管理の欠如 - 攻撃がエンドポイント保護/ウイルス対策、ホストファイアウォール、コンテンツのフィルタリング、DLP、MDMで防げた可能性がある場合、エンドポイントにそれらを導入できる可能性について調査します。これが実用的でない場合は、同じベクトルによって悪用されないようにシステムを分離します。
- 構成ドリフト - マルウェアが文書化されていない構成の変更を悪用した場合（シャドーITソフトウェアまたは不正なサービス/ポートなど）、ベースライン構成を再び適用して、構成管理手順を調査し、この種の一時的な変更を防ぎます。
- 構成上の弱点 - 構成が正しく適用されているのに悪用された場合は、テンプレートをレビューしてよりセキュアな設定を考案します。テンプレートは同様のホストに適用されるようにします。

アプリケーションの許可/ブロックリスト

エンドポイント構成の要素の1つは、実行できるまたは実行できないアプリケーションを定義する実行制御ポリシーになります。

- 許可リスト（または承認済みリスト）では、プロセスが明らかに承認されている場合を除き、実行を拒否します。
- ブロックリスト（または拒否リスト）では、通常は実行を許可しますが、リストに記載されるプロセスは明確に禁止します。