インシデント

次のトピックでは、インシデント処理を設定する方法について説明します。

インシデント対応について

インシデント対応とは、セキュリティ ポリシーの違反が疑われる場合に組織が取る対応を指します。Firepower システムには、インシデントの調査に関連する情報の収集および処理をサポートする機能が含まれます。これらの機能を使用して、インシデントに関連する可能性のある侵入イベントおよびパケット データを収集することができます。攻撃の影響を軽減するために Firepower システムの外部で実行するアクティビティに関する記録のためのリポジトリとしてインシデントを使用できます。たとえば、セキュリティ ポリシーによって、ネットワークの安全性に問題のあるホストの検疫が要求される場合は、インシデントにそのことを記録できます。

Firepower システムはインシデントのライフ サイクルもサポートします。これにより、攻撃への対応を進めるごとに、インシデントのステータスを変更できます。インシデントを閉じるときに、学んだ教訓の結果としてセキュリティ ポリシーに加えた変更を記録できます。

インシデントの定義

一般的に、インシデントとは、セキュリティ ポリシー違反の可能性があることが疑われる、1 つ以上の侵入イベントと定義されます。Firepower システムでは、この用語は、インシデントへの応答を追跡するために使用できる機能について記述しています。

一部の侵入イベントは、ネットワーク資産の可用性、機密性、および整合性の点で他のイベントよりも重要になります。たとえば、ポート スキャン検出では、ネットワークでのポート スキャン アクティビティについて通知することができます。しかし、セキュリティ ポリシーでは、ポート スキャンが明確に禁止されていなかったり、優先度の高い脅威とは見なされていな

かったりすることがあります。それで、直接的なアクションの実行はしないで、代わりにすべてのポート スキャンのログを後の調査のために保持しておくことができます。

一方、ネットワーク内のホストが侵害されていることを示す、分散型サービス拒否（DDoS）攻撃に関係したイベントをシステムが生成する場合、そのアクティビティはセキュリティ ポリシーの明確な違反であると考えられます。それで、これらのイベントを調査して追跡できるように、Firepower システムでインシデントを作成する必要があります。

共通のインシデント対応プロセス

準備（Preparation）

インシデントの準備には次の 2 通りの方法があります。

- 明確で包括的なセキュリティ ポリシーと、それらを施行するためのハードウェアおよびソフトウェア リソースを配置する
- インシデントに対応するための明確に定義された計画と、その計画を実行できる適切なトレーニングを受けたチームを配置する

インシデント対応において重要なのは、ネットワークのどの部分が最も大きなリスクとなるかを理解することです。これらのネットワーク セグメントに Firepower システムを展開することで、インシデントがいつどのように発生するかについて理解を深めることができます。また、時間をかけて各管理対象デバイスに対する侵入ポリシーを慎重に調整することによって、生成されるイベントの品質を最大限に高めることができます。

検出と通知

インシデントを検出できなければ、インシデントに対応できません。インシデント対応プロセスでは、検出できるセキュリティ関連イベントのタイプと、それらを検出するために使用するメカニズム（ソフトウェアとハードウェアの両方）を識別する必要があります。また、セキュリティ ポリシーの違反を検出できるケースにも注意する必要があります。積極的あるいは受動的にモニタされないセグメントがネットワークに含まれている場合は、それらのセグメントにも注意する必要があります。

ユーザがネットワークに展開する管理対象デバイスは、それらがインストールされているセグメントのトラフィックの分析、侵入の検知、およびそれらを説明するイベントの生成を行う必要があります。各管理対象デバイスに展開するアクセス コントロール ポリシーが、検出するアクティビティの種類と優先度に影響を与えることに注意してください。インシデント チームが数百のイベントを取捨選択しなくてもよいように、特定のタイプの侵入イベントに対して通知オプションを設定することもできます。特定の優先順位の高い、重大度の高いイベントが検出されたときに自動的に通知するように指定できます。

調査と認定

インシデント対応プロセスでは、セキュリティ インシデントの検出後に、どのように調査を実施するかを指定する必要があります。一部の組織では、経験の浅いチーム メンバーがすべてのインシデントのトリアージを行い、重大度と優先度が比較的に低いケースは自分たちで処理

し、熟練のチーム メンバーが重大度と優先度が高いインシデントを処理しています。各チーム メンバーがインシデントの重要度を繰り上げる基準について理解するように、エスカレーション プロセスの概要を慎重にまとめる必要があります。

エスカレーションプロセスでは、検出されたイベントがネットワーク資産のセキュリティにどのような影響を与えるかについての理解が不可欠です。たとえば、Microsoft SQL Server を実行するホストに対する攻撃は、それとは異なるデータベース サーバを使用する組織にとって優先度は高くありません。同様に、ネットワークで SQL Server を使用しているものの、すべてのサーバにパッチを適用済みで、その攻撃に対する脆弱性がないことを確信している場合には、その攻撃の重要度は低くなります。しかし、最近誰かが脆弱性のあるバージョンのソフトウェア コピーを（テスト目的などで）インストールしていたりすれば、簡易調査で指摘されるよりも大きな問題が発生するおそれがあります。

Firepower システムは、調査および認定のプロセスをサポートするのに特に適しています。独自のイベント分類を作成し、ネットワークの脆弱性を最も適切に示す方法で、それらを適用することができます。ネットワークのトラフィックによってイベントがトリガーされると、自動的に、そのイベントの優先度判別と認定が行われ、脆弱性があることが判明しているホストに対してどのような攻撃が行われるかを示す特別なインジケータが付けられます。

Firepower システムのインシデント トラッキング機能には、エスカレーションされたインシデントを示すためにユーザが変更できるステータス インジケータも含まれています。

コミュニケーション（Communication）

すべてのインシデント対応プロセスでは、インシデント対応チームと内部および外部の対象者の間でのインシデントについての連絡の方法が指定されている必要があります。たとえば、どの種類のインシデントが管理介入を必要とし、どのレベルでの介入が必要かを考慮する必要があります。また、プロセスでは、組織の外部との連絡の方法とタイミングが説明されている必要があります。次の点に注意してください。

- あるインシデントについて、法執行機関に通知する必要がありますか。
- ホストがリモート サイトに対する分散型サービス妨害（DDoS）に関与している場合、そのことを通知しますか。
- CERT 調整センター（CERT/CC）や FIRST などの組織と情報を共有する必要があるでしょうか。

Firepower システムには、HTML、PDF、CSV（カンマ区切り値）などの標準形式で侵入データを収集するために使用できる機能があり、侵入データを他のユーザと簡単に共有できます。

たとえば、CERT/CC は Web サイトのセキュリティ インシデントに関する標準情報を収集します。CERT/CC は、Firepower システムから簡単に抽出できる次のような情報を探します。

- 影響を受けるマシンに関する次のような情報
  - ホスト名および IP
  - タイム ゾーン
  - ホストの目的や機能

- 攻撃元に関する次のような情報
  - ホスト名および IP
  - タイム ゾーン
  - 攻撃者と接触したことがあるかどうか
  - インシデント処理の概算コスト
- 次のようなインシデントの説明
  - 日付
  - 侵入方法
  - 使用された侵入者ツール
  - ソフトウェア バージョンとパッチ レベル
  - 侵入者ツールの出力
  - 悪用された脆弱性の詳細
  - 攻撃元
  - その他の関連情報

また、インシデントのコメントセクションを使用して、問題を伝えた日時と相手を記録することができます。

封じ込めとリカバリ

インシデント対応プロセスでは、ホストまたはその他のネットワーク コンポーネントが侵害された場合に、どのような手順を実行するかを明確に示す必要があります。封じ込めとリカバリの方法には、脆弱性のあるホストへのパッチの適用から、ターゲットのシャットダウンとネットワークからの除去まで、さまざまな選択肢があります。攻撃の性質と重大度によっては、刑事責任を追求する場合に備えて証拠を保存しておくことの重要性を考慮する必要もあります。

Firepower システムのインシデント機能を使用して、インシデントの封じ込めとリカバリのフェーズ中に実行するアクションを記録しておくことができます。

学んだ教訓

それぞれのセキュリティ インシデントは、攻撃が成功したかどうかに関わりなく、セキュリティ ポリシーを見直す機会となります。ファイアウォール ルールを更新する必要はありますか。パッチ管理に対するより構造化されたアプローチが必要ですか。不正なワイヤレスアクセスポイントは新しいセキュリティ問題となりますか。それぞれの学んだ教訓は、セキュリティ ポリシーにフィードバックし、次のインシデントへのより良い対処のために役立てる必要があります。

Firepower システムのインシデント タイプ

作成する各インシデントにインシデント タイプを割り当てることができます。Firepower システムでは、以下のタイプがデフォルトでサポートされます。

- 侵入（Intrusion）
- サービス妨害（DoS）
- 不正な管理者アクセス
- Web サイトの改変
- システム整合性の侵害
- デマ ウイルス
- 盗難
- ダメージ
- 不明

独自のインシデント タイプを作成することもできます。

カスタム インシデント タイプの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

手順

ステップ 1 **[分析（Analysis）] > [侵入（Intrusions）] > [インシデント（Incidents）]**を選択します。

ステップ 2 [インシデントの作成（Create Incident）] をクリックします。

ステップ 3 [タイプ（Type）] エリアで、[タイプ（Types）] をクリックします。

デフォルトのインシデント タイプがページの下部に表示されます。

ステップ 4 [インシデント タイプ名（Incident Type Name）] フィールドに、新しいインシデント タイプの名前を入力します。

ステップ 5 [追加（Add）] をクリックします。

ステップ 6 [完了（Done）] をクリックします。
次にインシデントを作成または編集するときに、新しいインシデント タイプを使用できます。

インシデントの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

マルチドメイン導入では、現在のドメインで作成されたインシデントのみを表示および変更できます。先祖ドメインでは、任意の子孫ドメインからのインシデントにイベントを追加できます。

手順

ステップ 1 **[分析（Analysis）] > [侵入（Intrusions）] > [インシデント（Incidents）]**を選択します。

ステップ 2 [インシデントの作成（Create Incident）] をクリックします。

ステップ 3 [タイプ（Type）] ドロップダウン メニューから、インシデントを最も適切に説明するオプションを選択します。

ステップ 4 [滞留時間（Time Spent）] フィールドに、インシデントで費やした時間の合計を #d #h #m #s の形式で入力します。ここで、# は日数、時間数、分数、秒数を表します。

ステップ 5 [概要（Summary）] テキスト ボックスに、インシデントの簡単な説明（最大 255 文字の英数字、スペース、記号）を入力します。

ステップ 6 [コメントを追加（Add Comment）] テキスト ボックスに、インシデントのより詳細な説明（最大 8191 文字の英数字、スペース、記号）を入力します。

ステップ 7 インシデントにイベントを追加します。

- 選択したイベントを追加するには、クリップボードのイベントを選択して、[インシデントに追加（Add to Incident）] をクリックします。
- クリップボードからすべてのイベントを追加するには、[すべてをインシデントに追加（Add All to Incident）] をクリックします。

（注） クリップボードの複数のページにある個々のイベントを追加する場合は、1 つのページのイベントを追加してから、他のページのイベントを追加します（ページごとに追加します）。

ステップ 8 [保存（Save）] をクリックします。

インシデントの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

マルチドメイン導入では、現在のドメインで作成されたインシデントのみを表示および変更できます。先祖ドメインでは、すべての子孫ドメインからインシデントにイベントを追加できます。

手順

ステップ 1 **[分析（Analysis）] > [侵入（Intrusions）] > [インシデント（Incidents）]**を選択します。

ステップ 2 編集するインシデントの横にある編集アイコン（  ）をクリックします。

ステップ 3 インシデントの以下の側面を編集できます。

- ステータスの変更
- タイプの変更
- クリップボードからのイベントの追加
- イベントの削除

ステップ 4 [滞留時間（Time Spent）] フィールドに、インシデントに費やした追加の時間の合計を入力します。

ステップ 5 [コメントを追加（Add Comment）] テキスト ボックスで、インシデントに対する変更点（最大 8191 文字の英数字、スペース、および記号）を示します。

ステップ 6 オプションで、インシデントにイベントを追加したり、削除したりすることができます。

- クリップボードからイベントを追加するには、クリップボードのイベントを選択して、[インシデントに追加（Add to Incident）] をクリックします。
- クリップボードからすべてのイベントを追加するには、[インシデントにすべてを追加（Add All to Incident）] をクリックします。
- インシデントから特定のイベントを削除するには、イベントを選択し、[削除（Delete）] をクリックします。
- インシデントからすべてのイベントを削除するには、[すべて削除（Delete All）] をクリックします。
- イベントを追加または削除せずにインシデントを更新するには、[保存（Save）] をクリックします。

インシデント レポートの生成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

Firepower システムを使用して、インシデント レポートを生成できます。このレポートには、インシデントの概要、インシデントのステータス、およびコメントに加えて、インシデントに追加するイベントの情報を含めることができます。また、レポートにイベントの概要情報を含めるかどうかも指定できます。

手順

ステップ 1 **[分析（Analysis）] > [侵入（Intrusions）] > [インシデント（Incidents）]**を選択します。

ステップ 2 レポートに含めるインシデントの横にある編集アイコン（  ）をクリックします。

ステップ 3 次の 2 つの対処法があります。

- レポートにインシデントのすべてのイベントを含める場合は、[すべてのレポートの生成（Generate Report All）] をクリックします。
- レポートにインシデントの特定のイベントを含める場合は、目的のイベントの横にあるチェックボックスをオンにしてから、[レポートの生成（Generate Report）] をクリックします。

ステップ 4 レポートの名前を入力します。

ステップ 5 [インシデント レポートのセクション（Incident Report Sections）] で、レポートに含めるインシデントの部分（[ステータス（status）]、[概要（summary）]、および [コメント（comments）] のチェックボックスをオンにします。

ステップ 6 レポートにイベント情報を含める場合は、使用するワークフローを選択し、[レポートのセクション（Report Sections）] で、イベントの概要情報を含めるかどうかを指定します。

ステップ 7 レポートに含めるワークフロー ページの横にあるチェックボックスをオンにします。

ステップ 8 レポートに使用する出力形式（[PDF]、[HTML]、および [CSV]）の横にあるチェックボックスをオンにします。

（注） CSV ベースのインシデント レポートには、イベント情報のみが含まれます。インシデントのステータス、概要、コメントは含まれ**ません**。

ステップ 9 [レポートの生成（Generate Report）] をクリックして、レポート プロファイルの更新を確認します。