インシデント対応

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。FireSIGHT 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 FireSIGHT 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。

FireSIGHT 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。

FireSIGHT システムでのインシデントの対応に関する詳細については、以下のセクションを参照してください。

インシデント対応の基本

ライセンス：Protection

各組織には、セキュリティ ポリシーの違反を検出し、定義し、対応するための独自のプロセスがある場合があります。続くセクションでは、インシデント対応の基本、および FireSIGHT システムをインシデント対応計画にどのように組み込むことができるかについて説明します。

インシデントの定義

ライセンス：Protection

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。シスコではまた、インシデントへの対応を追跡するのに FireSIGHT システムで使用される機能を説明するためにこの用語を使用しています。

侵入イベントの操作（41-1 ページ）で説明されているように、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、FireSIGHT システムによって提供されるポート スキャン検出機能は、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、FireSIGHT 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

ライセンス：Protection

通常、各組織では、セキュリティ インシデントを処理するための独自のプロセスを定義しています。ほとんどの手法には、次のフェーズの一部またはすべてが含まれます。

- 準備（42-2 ページ）
- 検出と通知（42-3 ページ）
- 調査と認定（42-3 ページ）
- 通信（42-3 ページ）
- 封じ込めとリカバリ（42-4 ページ）
- 学んだ教訓（42-4 ページ）

これらの各フェーズについては、続くセクションで説明します。各フェーズで FireSIGHT システムがどのように役立つかについても説明します。

準備

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 FireSIGHT システム コンポーネントを展開することで、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は、検出できるセキュリティ関連イベントの種類と、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、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適用するアクセス 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、および優先順位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。ある組織では、チームの新人メンバーが、すべてのインシデントのトリアージを行い、重大度や優先度の低いケースは自分で処理します。重大度や優先度の高いインシデントは、チームの上級メンバーが対応します。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。

FireSIGHT 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がイベントを発生させると、自動的にそのイベントの優先順位付けと見極めが行われ、脆弱であることが分かっているホストに対して行われたのがどの攻撃かを示す特別なインジケータが付されます。

FireSIGHT システムのインシデント トラッキング機能には、エスカレーション済みのインシデントを示すための、ユーザが変更できるステータス インジケータも含まれます。

通信

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。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サービス拒否（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。

FireSIGHT 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、以下のような FireSIGHT システムから簡単に抽出できる情報を探しています。

- 影響を受けるマシンに関する情報。これには、以下が含まれます。
- 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
- インシデントを扱う概算コスト
- 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
- 侵入者のツールの出力（存在する場合）
- 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、脆弱な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削除まで、さまざまなオプションがあります。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。

FireSIGHT 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。パッチ管理への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。

FireSIGHT システムのインシデント タイプ

ライセンス：Protection

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。FireSIGHT 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
- 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

カスタム インシデント タイプの作成（42-8 ページ）で説明されているように、独自のインシデント タイプを作成することもできます。

インシデントの作成

ライセンス：Protection

このセクションでは、インシデントを作成する方法について説明します。

インシデントの作成方法：

アクセス：Admin/Intrusion Admin

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

[インシデント（Incidents）] ページが表示されます。

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

[インシデントの作成（Create Incident）] ページが表示されます。

クリップボードに侵入イベントをコピーした場合は、ページの下部に表示されます。クリップボードの使用についてはクリップボードの使用（41-54 ページ）を参照してください。

手順 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。

手順 4　[費やした時間（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。

手順 5　[サマリ（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、および記号）を入力します。

手順 6　[コメントの追加（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、および記号）を入力します。

手順 7　インシデントにイベントを追加しますか。

- **追加する**場合、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。

  [インシデントにすべて追加（Add All to Incident）] をクリックして、クリップボードからすべてのイベントを追加することもできます。

- **追加しない**場合、[保存（Save）] をクリックします。

いずれの場合も、インシデントは入力した情報とともに保存されます。

（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）。

インシデントの編集

ライセンス：Protection

追加の情報を収集しながらインシデントを更新できます。調査の進展に伴って、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もできます。

インシデントの編集方法：

アクセス：Admin/Intrusion Admin

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

[インシデント（Incidents）] ページが表示されます。

手順 2　編集するインシデントの横にある [編集（Edit）] アイコン（）をクリックします。

手順 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

手順 4　[費やした時間（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。

手順 5　[コメントの追加（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。

手順 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。

インシデントへの変更内容が保存されます。

インシデント レポートの生成

ライセンス：Protection

FireSIGHT 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。インシデント 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。

インシデント レポートの生成方法：

アクセス：Admin/Intrusion Admin

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

[インシデント（Incidents）] ページが表示されます。

手順 2　レポートに含めるインシデントの横にある [編集（Edit）] アイコン（  ）をクリックします。

手順 3　以下の 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には、[レポートを生成すべて生成（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には、含めるイベントの横にあるチェック ボックスを選択してから、[レポートの生成（Generate Report）] をクリックします。

いずれの場合も、インシデント レポートのオプションを含む [レポートの生成（Generate Report）] ページが表示されます。

手順 4　レポートの名前を入力します。英数字、ピリオド、およびスペースを使用できます。

手順 5　[インシデント レポート 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**、**概要**、および**コメント**）のチェック ボックスを選択します。

手順 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 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。

手順 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 ボックスを選択します。

手順 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 ボックスを選択します。

（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。また、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**。

手順 9　[レポートの生成（Generate Report）] をクリックして、レポート プロファイルを更新することを確認します。

レポートが生成されます。

カスタム インシデント タイプの作成

ライセンス: Protection

FireSIGHT システムには、インシデントの分類に使用できる以下のインシデント タイプが用意されています。

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

これらのインシデント タイプがニーズを満たしていない場合、独自のタイプを追加できます。カスタム インシデント タイプは削除できないことに注意してください。

新しいインシデント タイプの作成方法:

アクセス: Admin/Intrusion Admin

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

[インシデント（Incident）] ページが表示されます。

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

[インシデントの作成（Create Incident）] ページが表示されます。

手順 3　[タイプ（Type）] 領域で、[タイプ（Types）] をクリックします。

インシデント管理の [タイプ（Types）] ページが表示されます。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。

手順 4　[インシデント タイプの名前（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。

英数字とスペースを使用します。

手順 5　[追加（Add）] をクリックします。

新しいインシデント タイプが追加されます。

手順 6　[完了（Done）] をクリックしてポップアップ ウィンドウを閉じ、[インシデント（Incidents）] ページに戻ります。

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。