はじめに

Cisco Event Streamer（eStreamer とも称されます）により、外部のクライアント アプリケーションに Firepower システム イベントをストリーミングできます。Management Center からのホスト データ、検出データ、相関データ、コンプライアンスのホワイト リスト データ、侵入データ、ユーザ アクティビティ データ、ファイル データ、マルウェア データ、接続データをストリーミングでき、また、7000 および 8000 シリーズのデバイスからの侵入データをストリーミングできます。

eStreamer は、NGIPSv、Firepower Services、Firepower Threat Defense Virtual、Firepower Threat Defense には対応していない点にご注意ください。これらのデバイスからのイベントをストリーミングするには、そのデバイスが報告する Management Center 上で eStreamer を設定できます。

eStreamer では、カスタム アプリケーション層プロトコルを使用して接続されたクライアント アプリケーションとの通信を行います。eStreamer の目的は、単にクライアントが要求されたデータを戻すことであるため、このガイドは、主に、リクエストされたデータの eStreamer 形式について記述しています。

eStreamer クライアントを作成し、Firepower システム と統合するには 3 つの主要な手順があります:

1. eStreamer アプリケーション プロトコルを使用してメッセージを Management Center または管理対象デバイスと交換するクライアント アプリケーションを作成します。eStreamer SDK には、参照クライアント アプリケーションが含まれます。
2. クライアント アプリケーションに必要なイベントのタイプを送信するために Management Center またはデバイスを設定します。
3. クライアント アプリケーションを Management Center またはデバイスに接続し、データの交換を開始します。

このガイドでは、eStreamer バージョン 6.3 クライアント アプリケーションを正常に作成し、実行するのに必要な情報を提供します。

eStreamer バージョン 6.3 の主要な変更点

ディスカバリ イベントと接続イベントのレコード タイプに、失敗したユーザのログイン、VPN ユーザのログイン、および VPN ユーザのログオフの各イベントを追加しました。

「ベストプラクティス」のセクションを追加しました。

このガイドの使用方法

eStreamer サービスは、最高レベルで Firepower システム から要求元のクライアントにデータをストリーミングするメカニズムです。このサービスでは、次のデータ カテゴリをストリーミングできます:

- 侵入イベント データおよび追加のイベント データ
- 相関(コンプライアンス)イベント データ
- 検出イベント データ
- ユーザ イベント データ
- イベントのメタデータ
- ホスト情報
- マルウェア イベント データ

本書では、主に、eStreamer から戻されるデータ構造について説明します。本書の各章は、次のとおりです:

- eStreamer アプリケーション プロトコルについて(2-1 ページ)。この章では、eStreamer 通信の概要、eStreamer クライアント アプリケーションの作成に関する要件の詳細を記述し、eStreamer サービスとのコマンドの送受信に使用される 4 種類のメッセージについて説明します。
- 侵入および相関データ構造の概要(3-1 ページ)。この章では、侵入検出コンポーネントと相関コンポーネントによって作成されたイベント データを戻すのに使用されるデータ形式および侵入イベントや関連付けイベントを表すのに使用されるデータ形式について説明します。
- 検出と接続データ構造の概要(4-1 ページ)。この章では、検出データ、ユーザ データ、接続イベント データを戻すために使用されるデータ形式について説明します。
- ホスト データ構造の概要(5-1 ページ)。この章では、ホスト情報要求メッセージを受信すると完全なホスト情報データを戻すために eStreamer が使用するデータ形式について説明します。
- eStreamer の設定(6-1 ページ)。この章では、Management Center または管理対象デバイスでの eStreamer の設定方法について説明します。この章では、eStreamer コマンド ライン スイッチについても説明し、手動で eStreamer サービスを開始し、停止する方法、および eStreamer を自動的に開始させるために Management Center または管理対象デバイスを設定する方法を提示します。
- データ構造の例(A-1 ページ)。この章では、2 進数形式の eStreamer メッセージ パケットの例を示します。
- レガシー データ構造の概要(B-1 ページ)。この章では、現在出荷されている製品では使用されていませんが、旧クライアントが使用する可能性があるレガシー データ構造の構造について説明します。

前提条件

本ガイドの情報を理解するには、一般に Firepower システム の機能と名称、およびコンポーネントの機能、特に、これらのコンポーネントが生成するさまざまなタイプのイベント データに精通している必要があります。一般的ではない用語、および製品固有の用語の多くは、*Firepower eStreamer 統合ガイド*に記載されています。

Firepower システム リリース向け製品バージョン

本ガイドでは、バージョン番号を使用して Management Center および管理対象デバイスによって生成されるイベントのデータ形式を説明します。Firepower システム 製品バージョン表には、主要なリリースごとの各製品バージョンを示します。

表 1-1　Firepower システム 製品バージョン

リリース	Management Center バージョン	マスター Management Center バージョン	侵入センサー バージョン	センサー バージョン	管理対象 Device のバージョン
IMS 3.0	管理コンソール 3.0	該当なし	ネットワーク センサー 3.0	該当なし	該当なし
IMS 3.1	管理コンソール 3.1	該当なし	ネットワーク センサー 3.1	無応答（RNA）センサー 1.0	該当なし
IMS 3.2	管理コンソール 3.2	該当なし	ネットワーク センサー 3.2	無応答（RNA）センサー 2.0	該当なし
3D システム 4.0	Management Center 4.0	該当なし	侵入センサー 4.0	無応答（RNA）センサー 3.0	該当なし
3D システム 4.5	Management Center 4.5	該当なし	侵入センサー 4.5	無応答（RNA）センサー 3.5	該当なし
3D システム 4.6.1	Management Center 4.6.1	マスター Management Center 4.6.1	該当なし	該当なし	4.6.1
3D システム 4.7	Management Center 4.7	マスター Management Center 4.7	該当なし	該当なし	4.7
3D システム 4.8	Management Center 4.8	マスター Management Center 4.8	該当なし	該当なし	4.8
3D システム 4.8.0.2	Management Center 4.8.0.2	マスター Management Center 4.8.0.2	該当なし	該当なし	4.8.0.2
3D システム 4.9	Management Center 4.9	マスター Management Center 4.9	該当なし	該当なし	4.9
3D システム 4.9.1	Management Center 4.9.1	マスター Management Center 4.9.1	該当なし	該当なし	4.9.1
3D システム 4.10	Management Center 4.10	マスター Management Center 4.10	該当なし	該当なし	4.10
3D システム 4.10.1	Management Center 4.10.1	マスター Management Center 4.10.1	該当なし	該当なし	4.10.1

表 1-1　Firepower システム 製品バージョン(続き)

リリース	Management Center バージョン	マスター Management Center バージョン	侵入センサー バージョン	センサー バージョン	管理対象 Device のバージョン
3D システム 4.10.2	Management Center 4.10.2	マスター Management Center 4.10.2	該当なし	該当なし	4.10.2
3D システム 4.10.3	Management Center 4.10.3	マスター Management Center 4.10.3	該当なし	該当なし	4.10.3
3D システム 5.0	Management Center 5.0	該当なし	該当なし	該当なし	5.0
3D システム 5.1	Management Center 5.1	該当なし	該当なし	該当なし	5.1
3D システム 5.1.1	Management Center 5.1.1	該当なし	該当なし	該当なし	5.1.1
3D システム 5.2	Management Center 5.2	該当なし	該当なし	該当なし	5.2
3D システム 5.3	Management Center 5.3	該当なし	該当なし	該当なし	5.3
Firepower システム 5.3.1	Management Center 5.3.1	該当なし	該当なし	該当なし	5.3.1
Firepower システム 5.4	Management Center 5.4	該当なし	該当なし	該当なし	5.4
Firepower システム 6.0	Management Center 6.0	該当なし	該当なし	該当なし	6.0
Firepower システム 6.1	Management Center 6.1	該当なし	該当なし	該当なし	6.1
Firepower システム 6.2	Management Center 6.2	該当なし	該当なし	該当なし	6.2
Firepower システム 6.2.1	Management Center 6.2.1	該当なし	該当なし	該当なし	6.2.1
Firepower システム 6.2.2	Management Center 6.2.2	該当なし	該当なし	該当なし	6.2.2
Firepower システム 6.2.2	Management Center 6.2.3	該当なし	該当なし	該当なし	6.2.3
Firepower システム 6.3.0	Management Center 6.3.0	該当なし	該当なし	該当なし	6.3.0

表記法

eStreamer メッセージ データ タイプの表記法表には、eStreamer メッセージで使用されるさまざまなデータ フィールド形式を説明するために、本書で使用する名前を示します。eStreamer サービスで使用する数値定数は通常、符号なし整数値です。別途注記のない限り、ビット フィールドには下位ビットを使用します。たとえば、フラグ データの 5 ビットを含む 1 バイト フィールドでは、下位 5 ビットにデータが含まれています。

表 1-2　eStreamer メッセージ データ タイプの表記法

データ タイプ	説明
nn-ビット フィールド	nn ビットのビット フィールド
バイト	任意の形式のデータを含む 8 ビット バイト
int8	符号付き 8 ビット バイト
uint8	符号なし 8 ビット バイト
int16	符号付き 16 ビット整数
uint16	符号なし 16 ビット整数
int32	符号付き 32 ビット整数
uint32	符号なし 32 ビット整数
uint64	符号なし 64 ビット整数
string	文字データを格納する可変長フィールド。
[n]	指定されたデータ タイプの n インスタンスを示す上記のデータ タイプに続く配列添字（たとえば、uint8 [4]）
変数	さまざまなデータ タイプの収集
BLOB	パケットからキャプチャされるとき、指定されていないタイプ、通常、生データの 2 進数オブジェクト

IP アドレス

Cisco データベースは、2 進数形式の同じフィールドに IPv4 アドレスと IPv6 アドレスを保存します。IPv6 アドレスを取得するには、16 進表記に変換します。例: `20010db8000000000000000000004321` データベースでは、RFC に準拠して 80 ～ 95 ビットに 1 を取り込むことによって IPv4 アドレスを保存し、これによって無効な IPv6 アドレスが生成されます。たとえば IPv4 アドレス 10.5.15.1 は `00000000000000000000FFFF0A050F01` として保存されます。

ベストプラクティス

eStreamer を使用する際は、次に示す API の最善の使用方法を推奨します。

設計

- クライアントには、Python で記述されたシスコの着脱可能な eStreamer クライアントを基盤として使用することを検討してください。これにより、SIEM のスキーマでデータをフォーマットする際にプラグインを構築するだけで済みます。

- スキーマのあらゆる部分がカスタマー ベースのどこかしらで重要となるため、eStreamer クライアントは API で提供できるすべての内容をサポートするように構築してください。
  - メッセージの構造を理解する：『eStreamer Integration Guide』で理解を深めます。
  - メタデータ構造およびコード構造で定義されたレコードを取得する：ほとんどのレコードでメッセージを解析できます。
  - メタデータの一般的な仕組みについて理解する（メタデータ レコードの事前送信など）。
  - オブジェクト モデルについて理解する：レコードを相互に関連付ける方法と、レコードに関連付けられるメタデータの内容について理解を深めます。

- 強力なエラー処理とロギングを実装します。これにより、問題が生じたときに、原因となったメッセージや状況を必ずしもエラーを再現することなく確認できるようになります。
- 言語を慎重に選択します。解析にかかるコストは計算的には高くありませんが、1 秒あたりのイベント数が何千もある場合に、すべてがカウントされてしまいます。C や C++ などの言語をコンパイルします。Python や JavaScript より高速になります。このような方法の欠点は、移植性が低いことです。
- マルチスレッディングやプロセスを実装する場合は、メタデータを扱う際に必ずメッセージを順番に処理していく必要があることを理解しておいてください。つまり、配信順序が正しくない場合は修正する必要があります。
- 既存の eStreamer 実装で、他のユーザがこれまでどのようにして目標を達成したかを確認してください。リソースの一部を以下に示します。
  - https://splunkbase.splunk.com で eStreamer を検索します。
  - https://software.cisco.com/download/home/ で、[製品の選択（Select a Product）] の横にある [すべてを参照（Browse All）] を選択してから、[ファイアウォール（Firewalls）]、[ファイアウォール管理（Firewall Management）]、[Firepower Management Center 仮想アプライアンス（Firepower Management Center Virtual Appliance）]、[Firepowerシステムのツールと API（Firepower System Tools and APIs）] の順に選択します。
  - https:/community.cisco.com で「eNcoreCLI」と検索します。
- Cisco Security Technical Alliance チームと連携し、eStreamer および Cisco FirePOWER との統合に関するその他の側面に対する変更に常に迅速に対応します。不明な点は、ask-csta-pm@cisco.com までお問い合わせください。

テスト

- シスコで Firepower の新しいバージョンが導入されたら、速やかにクライアントのテストを実行し、クライアントが収集したデータに変更がないことを確認します。
- 便利なテスト ベッドをご用意していますので、簡単かつ頻繁にテストできます。
- テスト ベッドを構築しない場合は、dcloud サンドボックスのテスト ベッドを使用します。Cisco Security Technical Alliance では、このテスト ベッドの設定および使用をサポートするリソースを提供しています。dcloud は包括的なテストを無料で実現します。ただし、お客様の用途に完全に対応しているわけではなく、イベントを 100% カバーできるとも限りません。また、インスタンスの使用可能期間も短くなります。dcloud の詳細については、https://dcloud2-rtp.cisco.com にアクセスの上、ご確認ください。