简介

思科 Event Streamer （也称为 eStreamer）能让您通过流传输将 Firepower 系统事件发送到外部客户端应用。您可以从管理中心通过流传输发送主机、发现、关联、合规性允许列表、入侵、用户活动、文件、恶意软件和连接数据，并且可以从 7000 和 8000 系列设备通过流传输发送入侵数据。

请注意， NGIPSv、 Firepower 服务、 Firepower Threat Defense Virtual 和 Firepower 威胁防御不支持 eStreamer。要从这些设备通过流传输发送事件，可以在这些设备向其报告的管理中心上配置 eStreamer。

eStreamer 使用自定义应用层协议与连接的客户端应用通信。因为 eStreamer 的目的只是返回客户端请求的数据，所以本指南主要介绍请求的数据的 eStreamer 格式。

创建 eStreamer 客户端并将其与 Firepower 系统集成需要执行三个主要步骤：

1. 编写一个使用 eStreamer 应用协议与管理中心或受管设备交换消息的客户端应用。eStreamer SDK 包含一个标准客户端应用。
2. 配置一个管理中心或设备以将所需类型的事件发送到您的客户端应用。
3. 将您的客户端应用连接到管理中心或设备，并开始交换数据。

本指南为您提供需要的信息，帮助您成功创建和运行 eStreamer 版本 6.3 客户端应用。

eStreamer 版本 6.3 的重大变更

在发现和连接事件记录类型中添加了失败的用户登录、 VPN 用户登录和 VPN 用户注销事件

添加了最佳实践一节。

使用本指南

总体来看， eStreamer 服务是通过流传输将数据从 Firepower 系统发送到发出请求的客户端的一种机制。该服务可以通过流传输发送以下类别的数据：

- 入侵事件数据和事件额外数据
- 关联 （合规性）事件数据
- 发现事件数据
- 用户事件数据
- 事件的元数据

- 主机信息
- 恶意软件事件数据

本文主要介绍 eStreamer 返回的数据结构。本文的章节如下：

- 了解 eStreamer 应用协议，第 2-1 页，此章对 eStreamer 通信进行了概述，详细说明了编写 eStreamer 客户端应用的一些要求，并且介绍了用于向 eStreamer 服务发送命令和接收来自该服务的数据的四种类型的消息。
- 了解入侵和关联数据结构，第 3-1 页，此章介绍了用于返回由入侵检测和关联组件生成的事件数据的数据格式，以及用于描述入侵和关联事件的数据格式。
- 了解发现和连接数据结构，第 4-1 页，此章介绍了用于返回发现事件、用户事件和连接事件数据的数据格式。
- 了解主机数据结构，第 5-1 页，此章介绍了 eStreamer 在收到主机信息请求消息时用于返回完整主机信息数据的数据格式。
- 配置 eStreamer，第 6-1 页，此章介绍了如何在管理中心或受管设备上配置 eStreamer。此章还介绍了 eStreamer 命令行开关，并且提供了手动启动和停止 eStreamer 服务以及配置管理中心或受管设备以自动启动 eStreamer 的说明。
- 数据结构示例，第 A-1 页，此章提供了二进制格式的 eStreamer 消息数据包示例。
- 了解旧版数据结构，第 B-1 页，此章介绍了当前产品不再使用、但是旧客户端可能使用的旧数据结构的结构。

必备条件

要了解此指南中的信息，您应大体上熟悉 Firepower 系统的功能和术语以及其组件的功能，尤其应熟悉这些组件生成的不同类型的事件数据。对于不熟悉的术语或产品特定的术语，其定义通常可以从 《*Firepower eStreamer 集成指南*》获取。

Firepower 系统发行版的产品版本

本指南通篇使用版本号来描述管理中心和受管设备生成的事件的数据格式。Firepower 系统产品版本表按主要发行版列出了每个产品的版本。

表 1-1 Firepower 系统产品版本

版本	管理中心版本	受管设备版本
3D 系统 5.0	管理中心 5.0	5.0
3D 系统 5.1	管理中心 5.1	5.1
3D 系统 5.1.1	管理中心 5.1.1	5.1.1
3D 系统 5.2	管理中心 5.2	5.2
3D 系统 5.3	管理中心 5.3	5.3
Firepower 系统 5.3.1	管理中心 5.3.1	5.3.1
Firepower 系统 5.4	管理中心 5.4	5.4

表 1-1　　Firepower 系统产品版本 （续）

版本	管理中心版本	受管设备版本
Firepower 系统 6.0	管理中心 6.0	6.0
Firepower 系统 6.1	管理中心 6.1	6.1
Firepower 系统 6.2	管理中心 6.2	6.2
Firepower 系统 6.2.1	管理中心 6.2.1	6.2.1
Firepower 系统 6.2.2	管理中心 6.2.2	6.2.2
Firepower 系统 6.2.2	管理中心 6.2.3	6.2.3
Firepower 系统 6.3.0	管理中心 6.3.0	6.3.0

文档约定

eStreamer 消息数据类型约定表列出了本文中用于介绍 eStreamer 消息中采用的各种数据字段格式的名称。 eStreamer 服务使用的数字常数通常为无符号整数值。除非另有说明，位字段使用低顺序位。例如，在包含五位标志数据的单字节字段中，低顺序五位将包含数据。

表 1-2　　eStreamer 消息数据类型约定

数据类型	说明
nn- 位字段	nn 位的位字段
字节	包含任意格式数据的 8 位字节
int8	带符号 8 位字节
uint8	无符号 8 位字节
int16	带符号 16 位整数
uint16	无符号 16 位整数
int32	带符号 32 位整数
uint32	无符号 32 位整数
uint64	无符号 64 位整数
字符串	包含字符数据的变长字段
[n]	跟在以上任何数据类型后面的数组下标，表示该数据类型的 n 个实例，例如 uint8[4]
变量	各种数据类型的集合
BLOB	未指定类型的二进制对象，通常为从数据包捕获的原始数据

IP 地址

思科数据库以二进制格式将 IPv4 和 IPv6 地址存储在同一字段中。要获取 IPv6 地址，请转换为十六进制表示法，例如：`20010db80000000000000000000004321`。此数据库存储 IPv4 地址时遵循 RFC，用 1 填充位 80-95，生成无效的 IPv6 地址。例如 IPv4 地址 10.5.15.1 会存储为 `00000000000000000000FFFF0A050F01`。

最佳实践

使用 eStreamer 时，思科给出了以下建议以最佳利用 API。

设计

- 考虑使用以 Python 编写的 Cisco 可插拔 eStreamer 客户端作为客户端基础，这样您只需构建一个插件即可设置 SIEM 方案的数据格式。
- 构建您的 eStreamer 客户端，以支持 API 可以提供的所有内容，因为方案的每一部分都至少对一小部分客户群很重要。
  - 了解消息结构 - 逐渐了解 eStreamer 集成指南。
  - 花时间获取在元数据和代码结构中定义的记录 - 其中很大一部分能够解析消息。
  - 从一般意义上了解元数据的工作方式，例如，元数据记录被提前发送。
  - 了解对象模型 - 记录如何相互关联以及哪些元数据与哪些记录相关。
- 实施强大的错误处理和日志记录，以便在出现问题时，您可以查看消息和导致问题的情况，而不必重现错误。
- 仔细挑选您的语言。解析似乎不需要进行大量计算，但当每秒钟有数千个事件时，一切都非常重要。诸如 C、 C++、 Go 等编译语言将比 Python/JavaScript 更快。这种方法的缺点是缺乏可移植性。
- 如果您实施多线程处理 或常规处理，请明白处理元数据的任何方法都必须按顺序处理消息 - 这必须包括无序传送更正。
- 查看现有的 eStreamer 实施，了解其他人过去如何实现您的目标。访问以下某些资源：
  - https://splunkbase.splunk.com，并搜索 eStreamer
  - https://software.cisco.com/download/home/，在 “ 选择产品 ” 旁边，选择 “ 浏览全部 ”，再选择 “ 安全性 ”，然后依次选择 “ 防火墙 ”、 “ 防火墙管理 ”、 “Firepower 管理中心虚拟设备 ”、 “Firepower 系统工具和 API”。
  - https:/community.cisco.com，并搜索 “eNcoreCLI”。
- 确保与思科安全技术联盟团队合作，及时了解对 eStreamer 所做的更改以及与思科 Firepower 集成的其他方面。您可以通过 ask-csta-pm@cisco.com 与他们联系。

测试

- 当思科推出新版本的 Firepower 时，请立即针对它测试您的客户端，以确保您的客户端收集的数据不会更改。
- 拥有良好的测试平台，以便您可以轻松、频繁地进行测试。
- 如果您不希望构建自己的测试平台，请使用 dcloud 沙盒测试平台。思科安全技术联盟将提供资源来帮助设置和使用此平台。 Dcloud 是免费的，并且支持全面测试。但是，它不一定是供您使用的完整平台，并且没有 100% 覆盖事件。此外，实例仅供短期使用。有关 dcloud 的详细信息，请访问 https://dcloud2-rtp.cisco.com