Gigamon®

Application Intelligence Solution with CrowdStrike Integration Guide

Document Version: 1.0

(See *Change Notes* for document updates)

Gigamon®
Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com

Change Notes

When a document is updated, the document version number on the cover page will indicate a new version and provide a link to the Change Notes table, which describes the updates.

Document Version	Date Updated	Change Notes
1.0	20-03-2026	The original release of this document.

Contents

Application Intelligence Solution Integration with CrowdStrike

This guide provides step-by-step instructions for monitoring application metadata from Gigamon using CrowdStrike.

Note:

- *The guide is intended for customer deployments and assumes familiarity with basic GigaVUE-FM and CrowdStrike administration.*
- *The integration flow outlined in this guide is based on GigaVUE-FM version 6.12 and CrowdStrike. Menu labels and UI layouts may change slightly across releases. Always refer to the latest GigaVUE Documentation Library and CrowdStrike documentation for UI details.*

CrowdStrike Integration—Architecture and Data Flow

For details on deployment scenarios, refer to the AMX Application Deployment Options.

Prerequisites

Before you start with the integration, ensure the following are in place:

- AMI and AMX solutions are deployed. For instructions, refer to:
  - Create Application Metadata Intelligence for Physical Environment
  - Create Application Metadata Intelligence for Virtual Environment
  - Configure Application Metadata Exporter Application
- Access to the CrowdStrike Next-Gen SIEM UI.

Configure the CrowdStrike Falcon Next-Gen SIEM to accept JSON data

To create and configure CrowdStrike Next-Gen SIEM connector:

1. Log in to **CrowdStrike Next-Gen SIEM** using your CrowdStrike credentials. Multi-factor authentication is required.
2. In the **Menu** icon, click on **Next-Gen SIEM** and select **Data Onboarding**.
3. On the Data Connections page, select **Add Connection** to create a new connector.
4. Click on **Filter by connectors**, enter **Gigamon** in the filter field
5. The **Gigamon Observability App Data Connector** appears in the filter; you need to click on the title and the **Configure** button.
6. To configure the New Connection Details, provide a **Connection Name.**
7. In the **Parsing and Enrichment** section, the Gigamon AMI **Parsers is** preselected in the Parser field. Click **Enable Parser selection** checkbox and accept the Terms and Conditions.
8. Click on **Create connection** to save the configuration for the connector setup.
9. Click **Generate API key** then copy both the **HTTP endpoint** from the API **URL** and the **API key** and store them locally.

Note:

Ensure you to store the URL and API Key securely. If missed, it cannot be regenerated or viewed again.

10. After creating the connection, note that on the Data Connections page connection is in the **Pending** state, but once the data ingestion is complete it will be moved to the **Active** state.

Configure CrowdStrike Next-Gen SIEM details in GigaVUE-FM and Deploy

Before you begin, ensure AMI is deployed and running.

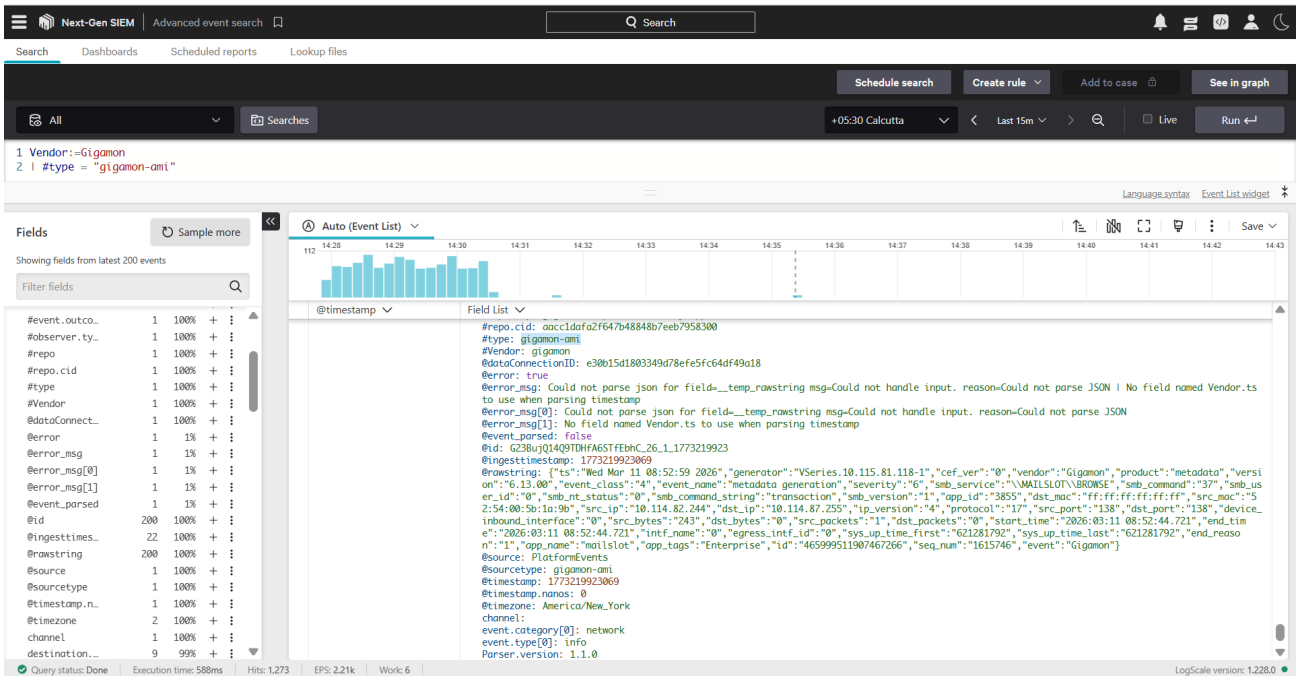
To set up CrowdStrike details in GigaVUE-FM:

1. Log into GigaVUE-FM, go to **Traffic** > **Virtual** > **Orchestrated Flows**, and select your platform.
2. Select the Monitoring Session AMX node to open the configuration panel.
3. Click the menu icon on the AMX node and select **Details**. Then navigate to **Cloud Tool Exports**.
4. In the **Cloud Tool Exports** configuration:
   - **Alias:** Provide an Alias name**.**
   - **Endpoint:** Enter the required CrowdStrike **endpoint** details. Append /raw to the end. For Example: https://<<crowdstrike-endpoint-host>>/services/collector/raw
   - **Header**: Click on to enter the Authentication Header and enter the **API key** in the placeholder. For example: Authorization: Bearer <<API key>>
   - **Cloud Tool**: select Other
   - **Type:** select AMI.
   - **Labels:** Enter **Key** as "event" and **Value** as "Gigamon".
5. In the **Advanced Settings**, enable the export option, Disable the **zip** option and click **Save**.
6. Return to the Canvas, click **Actions** > **Deploy**.

Verify the Integration

To verify if the integration is successful:

1. Log in to the **CrowdStrike UI** > **Next-Gen SIEM** > **Log Management** >**Advanced Event Search**.
2. Enter the following query in the search placeholder:
   ```
   #Vendor="gigamon"
   ```
3. The corresponding JSON logs passing through the Next-Gen SIEM will be displayed.



Visualize the Dashboards in CrowdStrike

This section covers predefined and customized dashboards for visualizing traffic.

1. From the CrowdStrike UI, go to **Next-Gen SIEM**>**Log Management**> **Dashboards.**
2. Search for **Gigamon** in the filter.
3. The relevant Dashboards will be displayed.

Note:

If the Dashboards are unavailable, contact your respective Gigamon representative for assistance.

Gigamon Inc. 3300 Olcott Street

Santa Clara, CA 95054 408.831.4000