NetWitness® Platform

CrowdStrike Falcon Event Source Log Configuration Guide

NETWITNESS
Platform

CrowdStrike Falcon

Event Source Product Information:

Vendor: CrowdStrike

Event Source: CrowdStrike Falcon

Versions: N/A

NetWitness Product Information:

Supported On: NetWitness Platform12.2 and higher

Event Source Log Parser: crowdstrike

Collection Method: Syslog

Event Source Class.Subclass: Endpoint

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

Miscellaneous

February, 2024

Contents

Introduction

Today's sophisticated attackers are going "beyond malware" to breach organizations, increasingly relying on exploits, zero days, and hard-to-detect methods. CrowdStrike Falcon® responds to such challenges with a powerful yet lightweight solution that unifies next-generation antivirus (NGAV), endpoint detection and response (EDR), cyber threat intelligence, managed threat hunting capabilities and security hygiene — all contained in a tiny, single, lightweight sensor that is cloud-managed and delivered.

CrowdStrike Falcon gives you an intelligent, lightweight agent that consolidates point products and stops advanced attacks - both malware and malware-free - while capturing rich endpoint activity for industry-leading detection and response.

The CrowdStrike Falcon SIEM Connector streamlines and automates the gathering of Falcon Host data into the NetWitness Platform. Instead of writing custom connectors, customers can now deploy and configure the Falcon SIEM Connector to retrieve their Falcon Host data from the Cloud securely and add them to their SIEM.

NetWitness supports collecting LEEF (log event extended format) formatted logs from CrowdStrike Falcon. The Falcon SIEM Connector allows you to send data to NetWitness SIEM through the syslog server.

Installation and Many more options for this connector (using a proxy to reach the streaming API, syslog configurations, etc.) can be found in the "SIEM Connector" as part of the Documentation package in the Falcon UI.

Download and Install CrowdStrike Falcon SIEM Connector:

The Falcon SIEM Connector Feature Guide explains how to install and configure the Falcon SIEM Connector, a tool for gathering info from Falcon's event streams and sending them to your SIEM.The SIEM connector documentation elaborates on the System requirements and recommended system specifications for installation.

Note: We recommend installing the CrowdStrike SIEM Connector on a VM instead of LogDecoder or VLC for security concerns.

Note: The SIEM connector is managed by CrowdStrike hence for any issues with the connector you will need to reach out to CrowdStrike for assistance.

Configure the SIEM Connector to forward LEEF events to NetWitness Platform

The configuration files are located in the **/opt/crowdstrike/etc/** directory on the machine where the SIEM connector is installed.

Note: We have referred to the CrowdStrike's Streaming API dictionary to create the configuration file. Added the field names for different events referring to the link: https://developer.crowdstrike.com/crowdstrike/docs/streaming-api-events

1. Take a backup of the existing cs.falconhoseclient.cfg file.
2. On the machine where falconhoseclient is installed, Stop the cs.falconhoseclientd.service using the command:

   sudo service cs.falconhoseclientd stop
3. From the zipped file, copy the cs.falconhoseclient.cfg file to location **/opt/crowdstrike/etc/**.
4. Edit the copied cs.falconhoseclient.cfg file to add **API Client ID**, **API Client Secret**, **API Base URL**, **request_token_url** and **app_id**.
5. Update the Syslog section in the cs.falconhoseclient.cfg :
   a. host - Enter the IP address of the NetWitness Log Decoder or Remote Log Collector.
   b. port - Update the port with 514 if you are directly sending the logs to Log Decoder, else Enter the port number to which the tcp listenser is configured on Netwitness Log Collector.
   c. protocol - tcp
6. Save the cs.falconhoseclient.cfg file.
7. Start the cs.falconhoseclientd.service using the command: **sudo service cs.falconhoseclientd start**.

Configure Syslog Event Sources on the NetWitness Platform

This section provides instructions for configuring the CrowdStrike Falcon with NetWitness Log Collector. It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products to install the required components.

Perform the below steps on the NetWitness Platform to configure Syslog Event Source:

- Enable the Required Parser.
- Configure NetWitness Platform for Syslog Collection.

Enable the Required Parser

If you do not see your parser in the list while performing this procedure, you need to download it in NetWitness Platform Live.

To enable the required parser:

1. In the **NetWitness** Platform menu, select  (Admin) > **Services**.
2. In the **Services** grid, select a Log Decoder, and from the **Actions** () menu, choose **View** > **Config**.
3. In the **Service Parsers Configuration** panel, search for your event source, **crowdstrike** and ensure that the **Config Value** field for your event source is selected.

   The new device is listed under the Log Decoder(s) General Tab within the **Service Parsers Configuration**.

   Note: The required parser is **crowdstrike**.

Configure NetWitness Platform for Syslog Collection

Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness. You only need to configure either the Log Decoder or the Remote Log Collector for Syslog, not both.

To configure Log Decoder for Syslog Collection

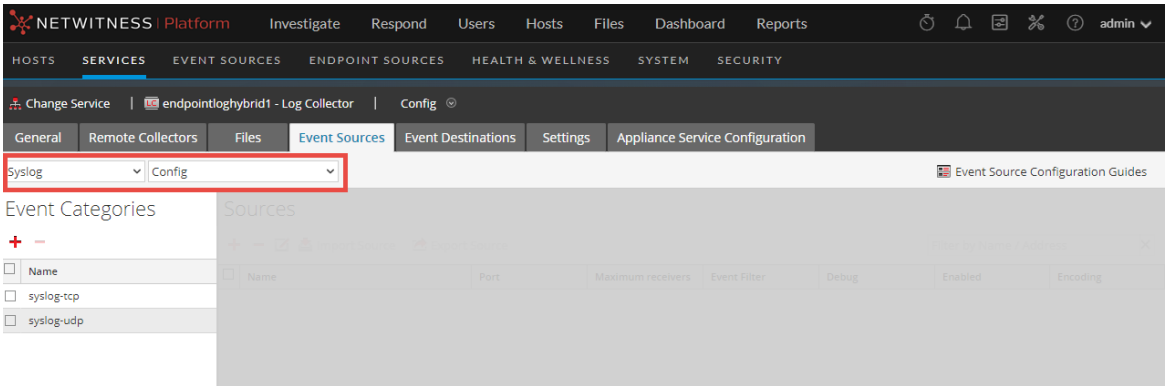
1. In the NetWitness Platform menu, select  (Admin) > **Services**.
2. In the **Services** grid, choose a Log Decoder and from the **Actions (**  **)** menu, choose **View** > **System**.

3. Depending on the icon you see, do one of the following:
   - If you see Start Capture , click the icon to start capturing Syslog.
   - If you see Stop Capture , you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure Remote Log Collector for Syslog Collection

1. In the NetWitness Platform menu, go to (Admin) > **Services**.
2. In the **Services** grid, select a Remote Log Collector and from the **Actions** ( ) menu, choose **View** > **Config** > **Event Sources**.
3. Select **Syslog / Config** from the drop-down menu.

   The **Event Categories** panel displays the Syslog event sources that are configured, if any.



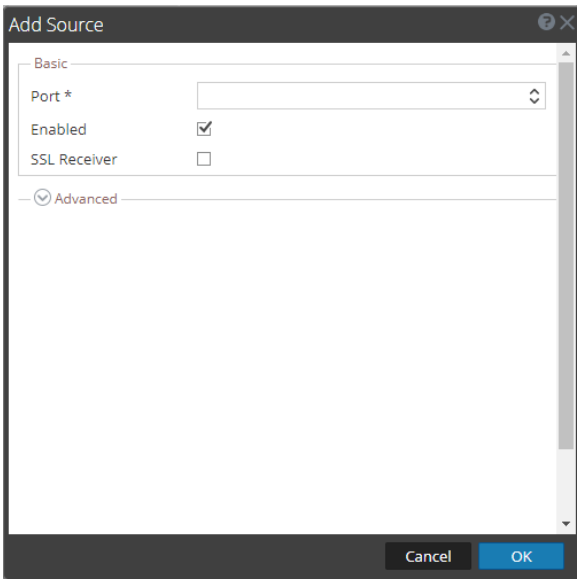
4. In the **Event Categories** panel toolbar, click +.

   The **Available Event Source Types** dialog will appear.

5. Choose either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.

6. Choose the **New Type** in the **Event Categories** panel and click + in the **Sources** panel toolbar.

   The **Add Source** dialog will appear.



7. Enter **514** for the port and choose **Enabled**. Optionally, configure any of the Advanced parameters as necessary.

   Click **OK** to accept your changes and close the dialog box.

After you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. You can continue to add Syslog event sources to your system without a need to do any further configuration in NetWitness Platform.

Getting Help with NetWitness Platform

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions.
- See the NetWitness Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base.
- See the documentation for Logstash JDBC input plugin here: https://www.elastic.co/guide/en/logstash/current/plugins-inputs-jdbc.html.
- See Troubleshooting section in the guides.
- See also NetWitness® Platform Blog Posts.
- If you need further assistance, Contact NetWitness Support.

Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click **Support > Case Portal > View My Cases**.
International Contacts (How to Contact NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

Feedback on Product Documentation

You can send an email to feedbacknwdocs@netwitness.com to provide feedback on NetWitness Platform documentation.