NetWitness® Platform

Proofpoint Targeted Attack Protection Events Event Source Log Configuration Guide

NETWITNESS
Platform

Proofpoint Targeted Attack Protection Events

Last Modified: Thursday, July 18, 2024

Event Source Product Information:

Vendor: Proofpoint

Event Source: Proofpoint Targeted Attack Protection Events

Versions: API v1.0

RSA Product Information:

Supported On: NetWitness Platform 12.2 and later

Event Source Log Parser: proofpoint

> **Note:** proofpoint parser is required for log parsing
> **device.type**=proofpoint

Collection Method: Plugin Framework

Event Source Class.Subclass: Host.Cloud

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

This document describes the integration of Proofpoint Targeted Attack Protection Events with the NetWitness Platform . For details on the Proofpoint SIEM API, see the following URL:

https://help.proofpoint.com/Threat_Insight_Dashboard/API_Documentation/SIEM_API

The current integration with NetWitness exposes the following event types:

- Blocked or permitted clicks to threats recognized by URL Defense
- Blocked or delivered messages that contain threats recognized by URL Defense or Attachment Defense

To integrate Proofpoint Targeted Attack Protection Events with NetWitness, complete the following tasks:

I. Configure the Proofpoint TAP Event Source

II. Setup the Proofpoint TAP Event Source in NetWitness

Configure the Proofpoint TAP Event Source

You need to ensure that credentials (username and password) with access to Proofpoint SIEM API are available.

Note: SIEM API username and password are needed to configure the proofpoint plugin in RSA NetWitness Platform.

Setup the Proofpoint TAP Event Source in NetWitness

In NetWitness Platform , perform the following tasks:

I. Deploy Proofpoint TAP Files from Live

II. Configure the event source.

Deploy Proofpoint TAP Files from Live

Proofpoint TAP plugin requires resources available in Live in order to collect logs.

To deploy the Proofpoint TAP content from Live:

1. In the RSA NetWitness Platform menu, select **CONFIGURE**.

   The **Live Content** tab is displayed.

2. Browse Live Content for the Proofpoint TAP plugin by typing **proofpoint** into the Keywords text box and clicking **Search**.
3. Select the items returned from the search and click **Deploy** to do the following:
   - Deploy the **proofpoint_tap** log collection file it to the appropriate Log Collectors
   - Deploy the proofpoint log parser to the appropriate Log Decoders

For more details, see the Add or Update Supported Event Source Log Parsers topic, or the *Live Services Management Guide*.

Ensure the Required Parser is Enabled

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

Ensure that the parser for your event source is available:

1. In the **NetWitness** 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, and ensure that the **Config Value** field for your event source is selected.

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

Configure the Event Source

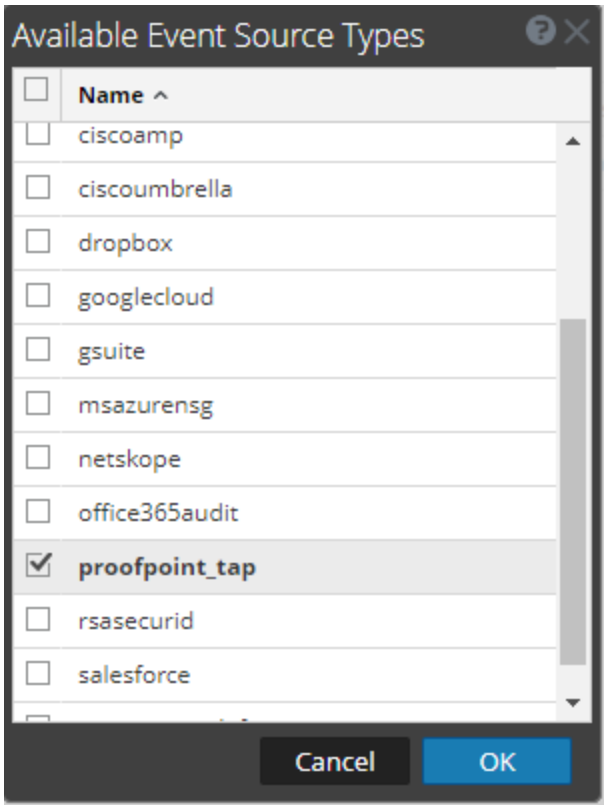
This section contains details on setting up the event source in NetWitness Platform.

To configure the Proofpoint Targeted Attack Protection Event Source:

1. In the RSA NetWitness Platform menu, select **ADMIN > Services**.
2. In the Services grid, select a Log Collector service, and from the Actions menu, choose **View** > **Config**.
3. In the **Event Sources** tab, select **Plugins/Config** from the drop-down menu.

   The Event Categories panel displays the File event sources that are configured, if any.
4. In the Event Categories panel toolbar, click +.

   The Available Event Source Types dialog is displayed.



5. Select **proofpoint_tap** from the list, and click **OK**.

   The newly added event source type is displayed in the Event Categories panel.
6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The Add Source dialog is displayed.
7. Define parameter values, as described in Proofpoint TAP Collection Configuration Parameters.

8. Click **Test Connection**.

   The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the device or service information and retry.

   Note: The Log Collector takes approximately 60 seconds to return the test results. If it exceeds the time limit, the test times out and RSA NetWitness Platform displays an error message.

9. If the test is successful, click **OK**.

   The new event source is displayed in the Sources panel.

Proofpoint TAP Collection Configuration Parameters

The following tables describe the configuration parameters for the Proofpoint TAP integration with NetWitness Platform . Fields marked with an asterisk (*) are required.

Basic Parameters

Name	Description
Name *	Enter an alpha-numeric, descriptive name for the source. This value is only used for displaying the name on this screen.
Enabled	Select the box to enable the event source configuration to start collection. The box is selected by default.
Username*	Provide the username and password for an account that has access to the Proofpoint TAP SIEM API.
Password*	
Start Date*	Choose the hours from which to start collecting. This parameter defaults to the current date.
Use Proxy	Check to enable proxy.
Proxy Server	If you are using a proxy, enter the proxy server address.
Proxy Port	Enter the proxy port.
Proxy User	Username for the proxy (leave empty if using anonymous proxy).
Proxy Password	Password for the proxy (leave empty if using anonymous proxy).
Source Address*	An arbitrary IP address that is passed to the Proofpoint plugin instance. This IP is used only to label all the logs collected via this instance using **device.ip** meta.
Base URL (optional)	The base URL for the Proofpoint SIEM API. The value is optional, and defaults to: `https://tap-api-v2.proofpoint.com/v2/siem/”`
Test Connection	Checks the configuration parameters specified in this dialog to make sure they are correct.

Advanced Parameters

Parameter	Description
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is **180**. For example, if you specify **180**, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, it will wait for it to finish that cycle. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy.
Max Duration Poll	Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit. The default is set to 600.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).
Max Idle Time Poll	Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit.
Command Args	Optional arguments to be added to the script invocation.
Debug	**Caution:** Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables or disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). The debug logging is verbose, so limit the number of event sources to minimize performance impact.
SSL Enabled	The check box is selected by default. Uncheck this box to disable SSL certificate verification.

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.