How-To Guide

Integrate Trend Micro Apex One with Netsurion Open XDR

Publication Date

August 21, 2023

Abstract

This guide provides instructions to configure and integrate Trend Micro Apex One with Netsurion Open XDR to retrieve its logs via Syslog Integration and forward them to Netsurion Open XDR.

Note:

Trend Micro OfficeScan and Trend Micro Control Manager are now labelled as Trend Micro Apex One and Trend Micro Apex Central respectively.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Scope

The configuration details in this guide are consistent with Trend Micro Apex One, Trend Micro Apex Central and Netsurion Open XDR 9.3 or later.

Audience

This guide is for the administrators responsible for configuring and monitoring Trend Micro Apex One in Netsurion Open XDR.

Table of Contents

1 Overview

Trend Micro Apex One is an integrated solution that protects enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks. Trend Micro Apex Central is a centralized management console that manages Trend Micro products and services which allows administrators to monitor and report on activities such as infections, security violations, or virus/malware entry points.

Netsurion Open XDR manages logs retrieved from Trend Micro Apex One. The alerts, reports, dashboards, and saved searches in Netsurion Open XDR are enhanced by capturing important and critical activities in Trend Micro Apex One.

2 Prerequisites

- Administrative/root access to Trend Micro Apex Central or Management UI.
- Port 514 should be allowed in the firewall.
- The Data Source Integration package.

> **Note:**
>
> To get the Data Source Integration package, contact your Netsurion Account Manager.

3 Integrating Trend Micro Apex One with Netsurion Open XDR

3.1 Enable Syslog Forwarding

1. Log in to Apex Central console via Administrator account and goo to **Administration** > **Settings** > **Syslog Settings**. The screen appears.
2. In the **Syslog Settings** section, configure the following settings for the server to forward the logs.
   - Select the **Enable syslog forwarding** check box to enable the syslog forwarding.
   - **Server address**: Provide the Server address, that is the FQDN or IP address of the Netsurion Open XDR machine.

   > **Note**:
   >
   > Recommended providing the FQDN details.

   - **Port**: Provide the Syslog server port number. For UDP, the IANA standard port number is 514.
   - **Protocol**: Choose the TCP option as the method of communication with the syslog server.

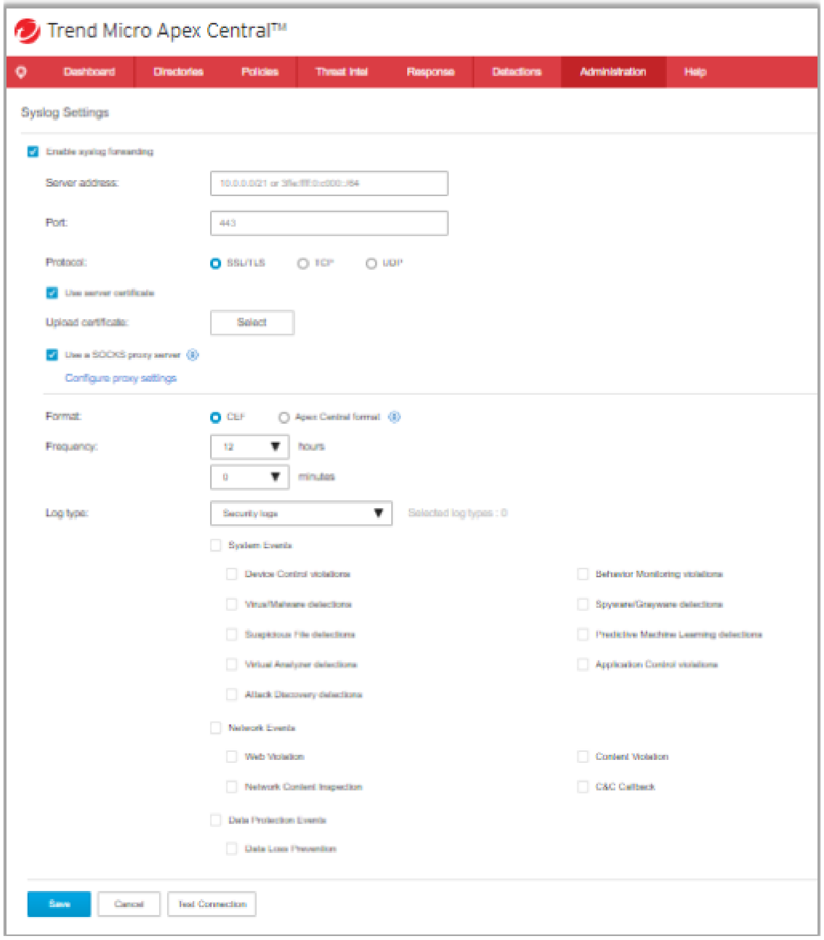
   > **Note**:
   >
   > For other configuration options like SSL/TLS and for optional proxy server configurations, refer to the Trend Micro documentation and the Configure Syslog Over TLS in Netsurion Open XDR guide for more details.

3. In the **Configure Proxy Settings** section, configure the following proxy settings to receive the forwarded logs.

   - **Format**: Choose the log Format as **CEF.** The **CEF** format uses the standard Common Event Format (CEF) for log messages.
   - **Log Type**: From the Log Type drop-down list, either select **Security Logs** and select all the log types or select **Product information** and select **Managed Product Logon/Logoff Events**.

4. After providing the appropriate details, click **Test Connection** to test the server connection.

5. The syslog server connection status appears at the top of the screen. Click **Save** to update the Syslog configurations.



Syslog Settings

☑ Enable syslog forwarding

Server address: 10.0.0.0/21 or 3ffe:ffff:0:c000::/64

Port: 443

Protocol: ● SSL/TLS ○ TCP ○ UDP

☑ Use server certificate

Upload certificate: Select

☑ Use a SOCKS proxy server

Configure proxy settings

Format: ● CEF ○ Apex Central format

Frequency: 12 hours
0 minutes

Log type: Security logs — Selected log types : 0

□ System Events
- □ Device Control violations
- □ Virus/Malware detections
- □ Suspicious File detections
- □ Virtual Analyzer detections
- □ Attack Discovery detections
- □ Behavior Monitoring violations
- □ Spyware/Grayware detections
- □ Predictive Machine Learning detections
- □ Application Control violations

□ Network Events
- □ Web Violation
- □ Network Content Inspection
- □ Content Violation
- □ C&C Callback

□ Data Protection Events
- □ Data Loss Prevention

4 Data Source Integration (DSI) in Netsurion Open XDR

After the logs are received by Netsurion Open XDR, configure the Data Source Integrations in Netsurion Open XDR.

The Data Source Integrations package contains the following files for Trend Micro Apex One.

- Categories_Trend Micro Apex.iscat
- Alerts_Trend Micro Apex.isalt
- Reports_Trend Micro Apex.etcrx
- KO_Trend Micro Apex.etko
- Dashboards_Trend Micro Apex.etwd
- Templates_Trend Micro Apex.ettd

Note

Refer the How To Configure DSI guide for the procedures to configure the above DSIs in Netsurion Open XDR.

4.1 Alerts

Name	Description
Trend Micro Apex: A potential threat could not be quarantined	Generated whenever a Trend Micro Apex One fails to quarantine a potential threat.
Trend Micro Apex: A potential threat has been quarantined	Generated whenever a Trend Micro Apex One quarantines a potential threat.

4.2 Reports

Name	Description
Trend Micro Apex - Web security activities	Provides information on events such as threat protection on web threats, URL filtering, and application control.
Trend Micro Apex - Virus detected	Provides information about viruses that can cause damage by exploiting vulnerabilities in corporate networks, email systems, and websites. For example, Trojan Horse, Ransomware, and more.
Trend Micro Apex - Suspicious files	Provides information about the suspicious files detected on your network.
Trend Micro Apex - Spyware detected	Provides information about spyware or grayware detections on a network, such as applications that have annoying, undesirable, or undisclosed behavior but do not fall into any of the major threat categories such as Virus, Trojan, and Worm. These applications monitor, gather personal information, and

	sends to a third party without the user's knowledge or consent.
Trend Micro Apex - User login and logout activities	Provides details about the Trend Micro Apex One Central user log in or log out activities.
Trend Micro Apex - Command and control activities	Provides details about C&C servers which cybercriminals use to communicate with systems compromised by malware and receive stolen data from the target network. This report contains information such as, action type, risk level, detection source, requested URL, etc.
Trend Micro Apex - Endpoint application control activities	Provides information about the Endpoint Application Control activities that allows users to enhance their defense against malware and targeted attacks by preventing unknown and unwanted applications from executing on a corporate endpoint.
Trend Micro Apex - Network content inspection activities	Provides information about Network Content Inspection that depends on two components, Global C&C IP list and relevance rule pattern to detect any network content violations on a network.
Trend Micro Apex - Behavior monitoring activities	Provides information about Behavior Monitoring that detects malicious scripts executed by legitimate windows programs and the true payload path of script files executed by legitimate DLLs to protect endpoints against malware hidden in file-less attack vectors.

4.3 Dashboards

Name	Description
Trend Micro Apex - Threat detected	Displays all the Threat detected by Trend Micro Apex.
Trend Micro Apex - Log types	Displays all the log types captured by Trend Micro Apex.
Trend Micro Apex - Successful login activities by source IP	Displays all the successful login activities by source IP captured by Trend Micro Apex.

4.4 Saved Searches

Name	Description
Trend Micro Apex - Data loss prevention events	Provides information about data loss prevention safeguards of an organization's sensitive data against accidental or deliberate leakage or accessed by unauthorized users.
Trend Micro Apex - Device access control events	Provides information about device control that regulates access to external storage devices and network resources connected to computers. Device Control helps prevent data loss or leakage and combined

	with file scanning helps guard against security risks.
Trend Micro Apex - Predictive machine learning events	Provides information about Predictive Machine Learning (PML) that is used to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks through digital DNA fingerprinting, API mapping, and other file features.
Trend Micro Apex - Spyware/grayware detection events	Provides information about the spyware/grayware detections on a network, such as applications that have annoying, undesirable, or undisclosed behavior but do not fall into any of the major threat categories such as Virus, Trojan, and Worm. These applications monitor, gather personal information, and send to a third party without the user's knowledge or consent.
Trend Micro Apex - Suspicious file detection events	Provides information about specific suspicious files detected on your network.
Trend Micro Apex - Virus/Malware detection events	Provides information about viruses that can cause damage by exploiting vulnerabilities in corporate networks, email systems and websites. For example, Trojan Horse, Ransomware, and more.
Trend Micro Apex - Web security events	Provides information about events such as threat protection on web threats, URL filtering and application control.
Trend Micro Apex - Product logon/logoff events	Provides details about the Trend Micro Apex One Central user log in or log out activities.
Trend Micro Apex - Attack discovery detection Events	Provides information about attack discovery using Trend Micro threat intelligence based on Indicators of Attack (IoA) behaviors. After detecting a known IoA, Attack Discovery logs the detection.
Trend Micro Apex - C&C callback events	Provides information about C&C servers that are used by cybercriminals to send commands to systems compromised by malware and receive stolen information from the target network. This report contains information such as, action type, risk level, detection source, requested URL, etc.
Trend Micro Apex - Endpoint application control events	Provides information about Endpoint Application Control allows user to enhance their defences against malware and targeted attacks by preventing unknown and unwanted applications from executing on a corporate endpoint.
Trend Micro Apex - Content security Events	Provides information about content security can be described as content injection vulnerabilities such as cross-site scripting (XSS attacks), clickjacking and other code injection attacks resulting from execution of malicious content in the trusted web page context.
Trend Micro Apex - Network content inspection events	Provides information about network Content Inspection depends on two components: Global C&C IP List and Relevance Rule Pattern to detect any network content violations on a network.
Trend Micro Apex - Behavior monitoring events	Provides information about Behavior Monitoring detects malicious scripts executed by legitimate windows programs and the true payload path of script files executed by legitimate DLLs to protect endpoints against malware hidden in file-less attack vectors.

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection & Response (MXDR). Learn more at www.netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

Use the form to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers	SOC@Netsurion.com
Managed XDR Enterprise MSPs	SOC-MSP@Netsurion.com
Managed XDR Essentials	Essentials@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

https://www.netsurion.com/support