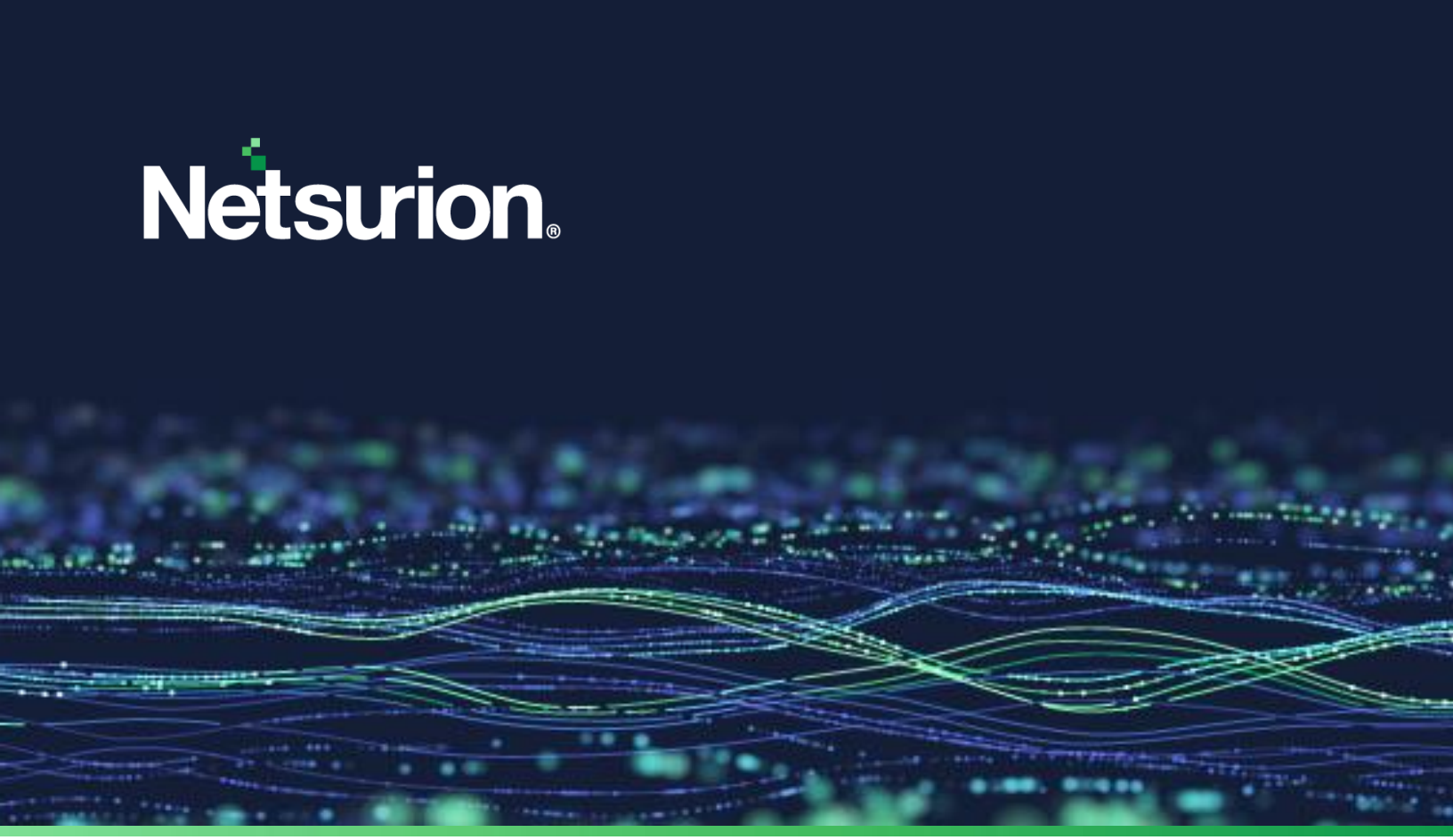

How-To Guide

Configure Trend Micro Vision One to forward logs to the Netsurion Open XDR platform

Publication Date:

November 25, 2022

Abstract

This guide provides instructions to configure and receive logs from Trend Micro Vision One via syslog and then forward the logs to the Netsurion Open XDR platform.

Scope

The configuration details in this guide are consistent with Trend Micro Vision One and the Netsurion Open XDR platform version 9.3 or later.

Audience

This guide is for the administrators responsible for configuring the Trend Micro Vision One in the Netsurion Open XDR platform.

Product Terminology

The following terms are used throughout this guide:

- The term "**Netsurion's Open XDR platform"** or "the **Netsurion Open XDR platform**" refers to EventTracker.
- The term "**Data Source Integrations**" refers to Knowledge Packs.

Table of Contents

1 Overview

Trend Micro Vision One XDR (extended detection and response) collects and automatically correlates data across multiple security layers - email, endpoint, server, cloud workload, and network. This allows for faster detection of threats and improved investigation and response times through security analysis.

Netsurion, the Managed Threat Protection platform facilitates monitoring events retrieved from Trend Micro Vision One. Its dashboard, category, alerts, and reports benefit in detecting vulnerabilities, malware attacks, phishing email attacks, lateral movements, and others.

2 Prerequisites

- Access to Trend Micro Vision One XDR console.
- Supported Trend Micro Vision One Agent System requirements.

> **Note**:
>
> Refer to Trend Micro Vision One Agent System Requirements for more details.

3 Configuring Trend Micro Vision One XDR to forward logs to the Netsurion Open XDR platform

The syslog connector is a generic SIEM connector, which allows you to send the Trend Micro Vision One XDR data to your SaaS or Cloud-based syslog server. The connector supports multiple syslog server connections.

1. Log in to **Trend Micro Vision One** console and go to **Administration** > **Third-Party Integration**.
2. Click **Syslog Connector (SaaS/Cloud)**.
3. In the **Syslog Connector (SaaS/Cloud)**, enable **Syslog Connector (SaaS/Cloud)**.
4. Select the data to send to your syslog server(s).
    i. Workbench alerts
    ii. Observed Attack Techniques

> **Note**:
>
> You must select at least one data type.

5. Click **Connect Syslog Server**.

6. In the **Syslog Server Connection** panel, configure the following settings:

Setting	Description
Server address	Specify the IP address or FQDN for your Syslog server.
Syslog format	Select the syslog format. **Note**: Currently, Syslog Connector (SaaS/Cloud) supports only the Common Event Format (CEF)
Protocol	Select the connection protocol.
Port	Specify the port. **Default port settings:** • SSL/TLS: 6514 • TCP: 601 • UDP: 514

7. Select **Use CA certificate** to upload a CA certificate to use when connecting to the server (*OPTIONAL*).

8. If your syslog server requires authenticated connections, select **Server requires client authentication** to upload the client certificate (*OPTIONAL*).

9. Click **Test Connection** to validate the connection and verify the settings.

10. Click **Connect** to test and save your connection settings.

11. After validating the successful connection, click **Save** on the Syslog Connector (SaaS/Cloud) screen.

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's managed offering includes our 24x7 SOC that 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 and Response (MDR) and a Top 25 Global MSSP. 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

Direct Enterprise	SOC@Netsurion.com	1 (877) 333-1433 Option 1, Option 1
MSP Enterprise	SOC-MSP@Netsurion.com	1 (877) 333-1433 Option 1, Option 2
Essentials	Essentials-Support@Netsurion.com	1 (877) 333-1433 Option 1, Option 3
Self-Serve	EventTracker-Support@Netsurion.com	1 (877) 333-1433 Option 1, Option 4

https://www.netsurion.com/eventtracker-support