Integration Guide

Integrate Trend Micro Vision One with the Netsurion Open XDR platform

Publication Date:

November 25, 2022

Abstract

This guide provides instructions to configure the Data Source Integration in the Netsurion Open XDR platform to receive the logs from Trend Micro Vision One. The Data Source Integration contains alerts, reports, dashboards, and knowledge objects.

Scope

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

Audience

This guide is for the administrators responsible for configuring the Data Source Integration 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 Prerequisite

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

> **Note**
>
> Refer to How-To guide to configure Trend Micro Vision One to forward logs to the Netsurion Open XDR platform.

3 The Netsurion Open XDR platform Data Source Integration (DSI)

After the logs are received by the Netsurion Open XDR Manager, configure the Data Source Integration into Netsurion Open XDR platform.

The following Data Source Integration are available in Netsurion Open XDR platform.

3.1 Category

Trend Micro Vision One - Workbench Alert details: This category of the saved search allows to parse the events that are specific to the workbench activities.

Trend Micro Vision One - Observed attack technique details: This category of the saved search allows to parse the events that are specific to observed attack technique activities.

3.2 Alerts

Trend Micro Vision One: Critical activity detected: This critical activity alert is triggered when the severity of the log is 7,8,9, and 10.

Trend Micro Vision One: Critical workbench activity detected: This critical workbench activity alert is triggered when the severity of the log is 7,8,9, and 10.

3.3 Reports

Trend Micro Vision One - Workbench alert details: This report provides a detailed summary of the workbench alerts activities in Trend Micro Vision One. The report includes the category, severity, requested URL, affected devices, affected accounts, MITRE IDs, and more.

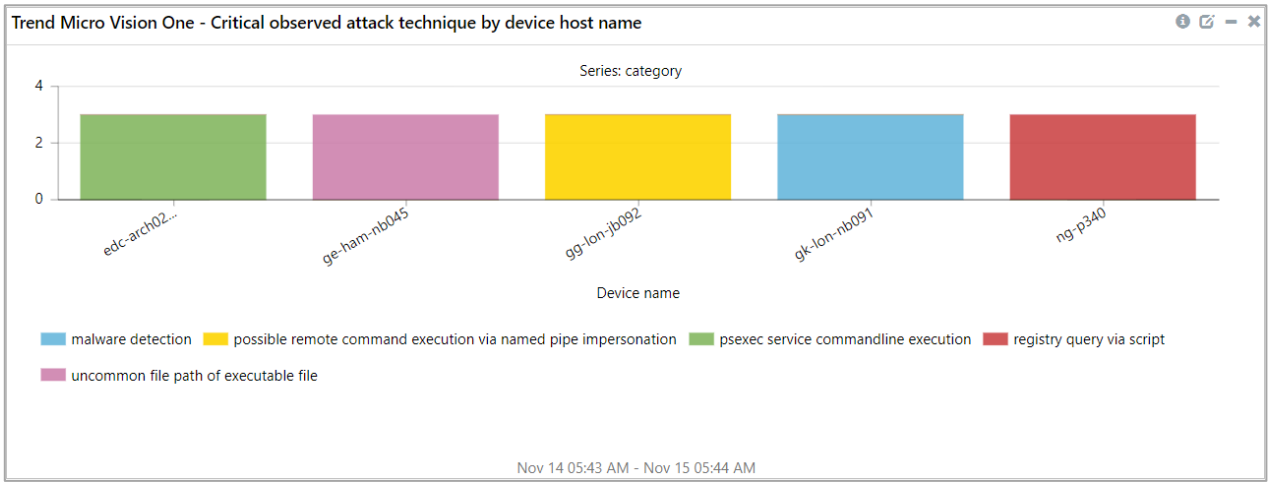
LogTime	Workbench ID	MITRE technique IDs	Severity	Threat category	Message	Devices affected count
11-13-2022 07:49:31 PM	WB-9123-20220929-00004	V9.T1021.002&V9.T1059.003	9	Possible Remote Command Execution via Named Pipe Impersonation	A command commonly exhibited remote command execution by third-party tools such as Metasploit Meterpreter or Cobalt Strike beacon	1
11-13-2022 07:49:31 PM	WB-9123-20220929-00005	V9.T1021.002&V9.T1059.003	10	Possible Cobalt Strike Beacon	Indicators of Cobalt Strike Beacon are found on an endpoint which may be used for post-exploitation.	1
11-13-2022 07:53:02 PM	WB-9123-20220929-00006	V9.T1003.004&V9.T1003.002&T1003	8	Possible Credential Dumping via Registry	A user obtained account logon information that can be used to access remote systems via Windows Registry.	1
11-13-2022 07:53:02 PM	WB-9123-20220929-00006	V9.T1012	8	Registry Query via Reg.exe	Registry Tool (reg.exe) was executed to query a registry.	1
11-14-2022 07:53:02 PM	WB-9123-20220929-00007	V9.T1036	9	Uncommon File Path of Executable File	Uncommon File Path of Executable File	2

Trend Micro Vision One - Observed attack technique details: This report provides a detailed summary of the individual activities in Trend Micro Vision One. The report includes the device hostname, device IP address, MITRE IDs, threat category, severity, and more.

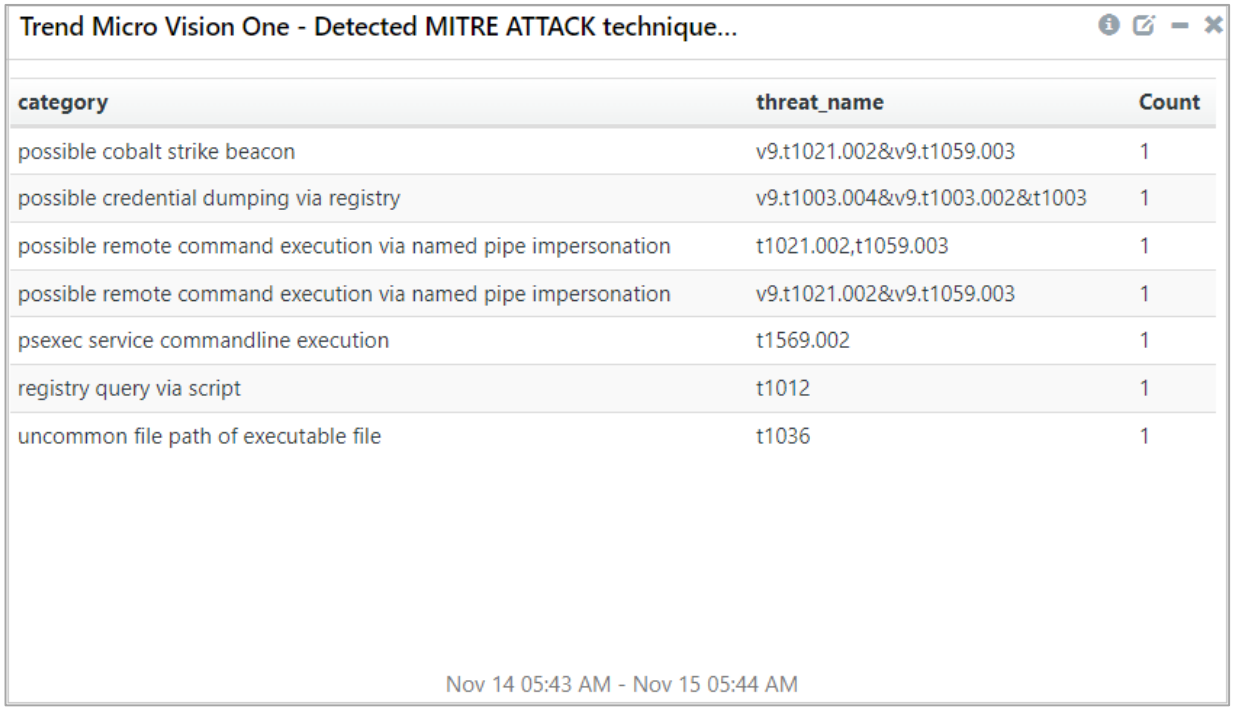
LogTime	Device host name	Device IP address	Device ID	Severity	MITRE tactic IDs	MITRE technique IDs	Threat category
11-13-2022 07:49:31 PM	ED-PS334	192.178.10.21	a275a9fa-be96-01be-3884-f8f9bb1a9a78	9	TA0002	T1569.002	PsExec Service CommandLine Execution
11-13-2022 07:49:31 PM	GE-HAM-NB045	10.10.60.30	6ca3e0df-1c1d-4970-9843-3e28300004fd	10	TA0005	T1036	Uncommon File Path of Executable File
11-13-2022 07:49:31 PM	GG-LON-JB092	198.125.23.3	7d63eb88-23c5-442b-8953-d3f5fde9328a	8	TA0002,TA0008	T1021.002,T1059.003	Possible Remote Command Execution via Named Pipe Impersonation
11-13-2022 07:49:31 PM	GK-LON-NB091	10.223.10.62	6d63eb88-23c5-442b-8953-d3f5fde9328a	9			Malware Detection
11-13-2022 07:49:31 PM	NG-P340	192.18.226.10	207c0b1a-62e3-4758-ab8b-6239612a1f4d	8	TA0007	T1012	Registry Query Via Script

3.4 Dashboard

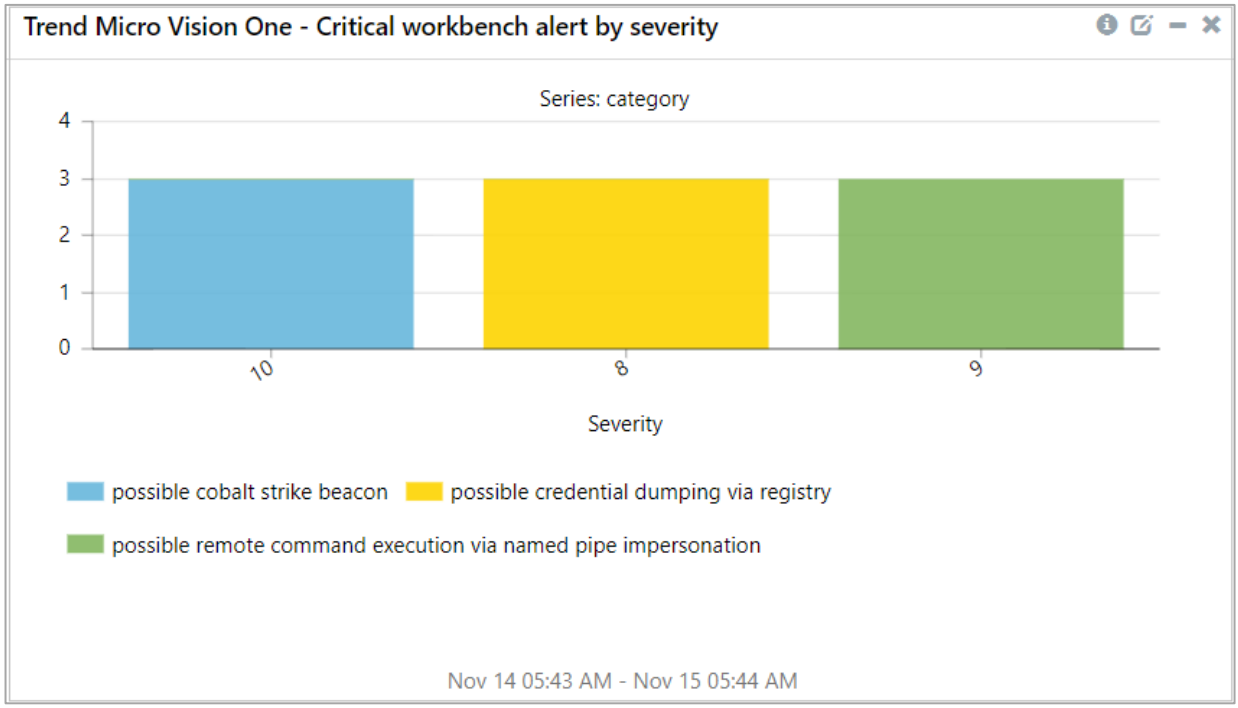
Trend Micro Vision One - Critical observed attack technique activities by Device host name: This dashlet displays the critical activities detected in the Trend Micro Vision One based on the severity.



Trend Micro Vision One - Detected MITRE ATTACK techniques by incident: This dashlet displays MITRE ATTACK technique and tactic IDs detected in the network.



Trend Micro Vision One - Critical workbench alert by severity: This dashlet displays the critical workbench alert by severity.

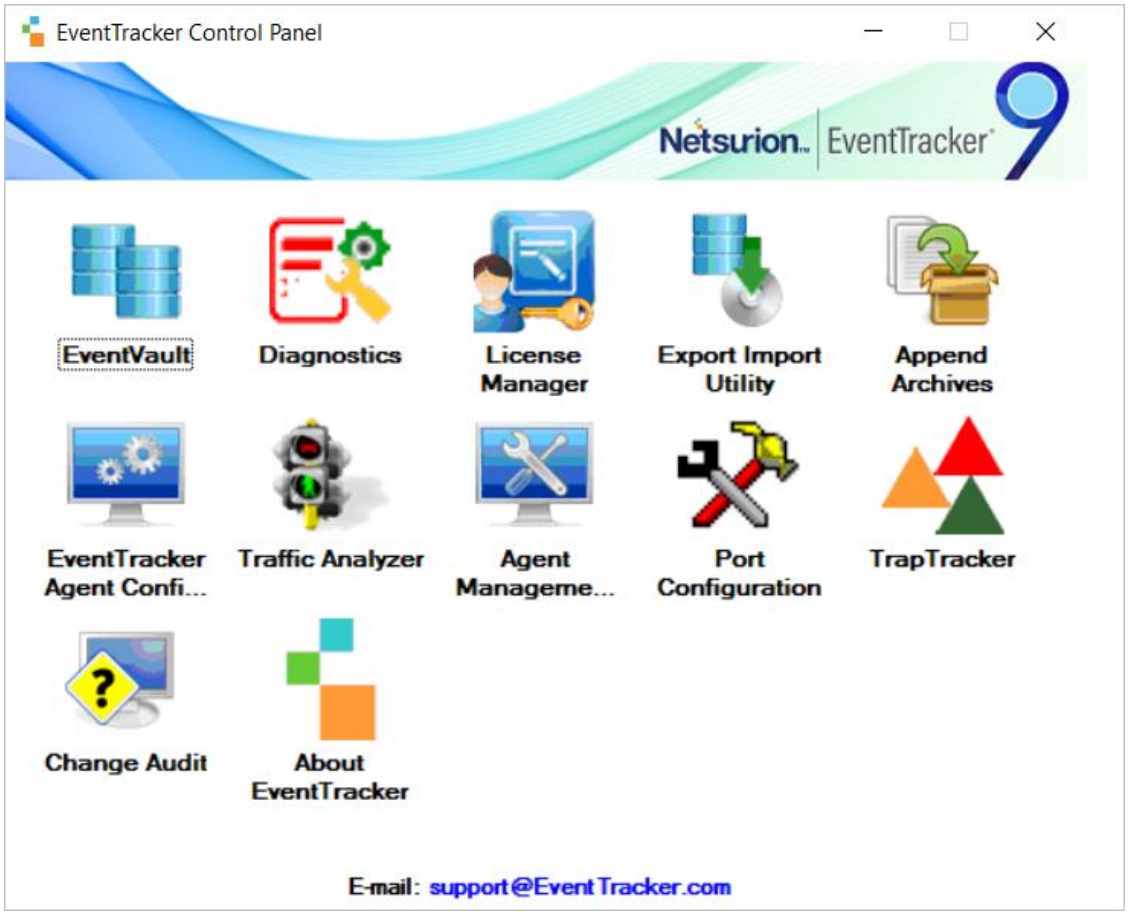


4 Importing Data Source Integration into the Netsurion Open XDR platform

Import the Data Source Integration items in the following sequence.

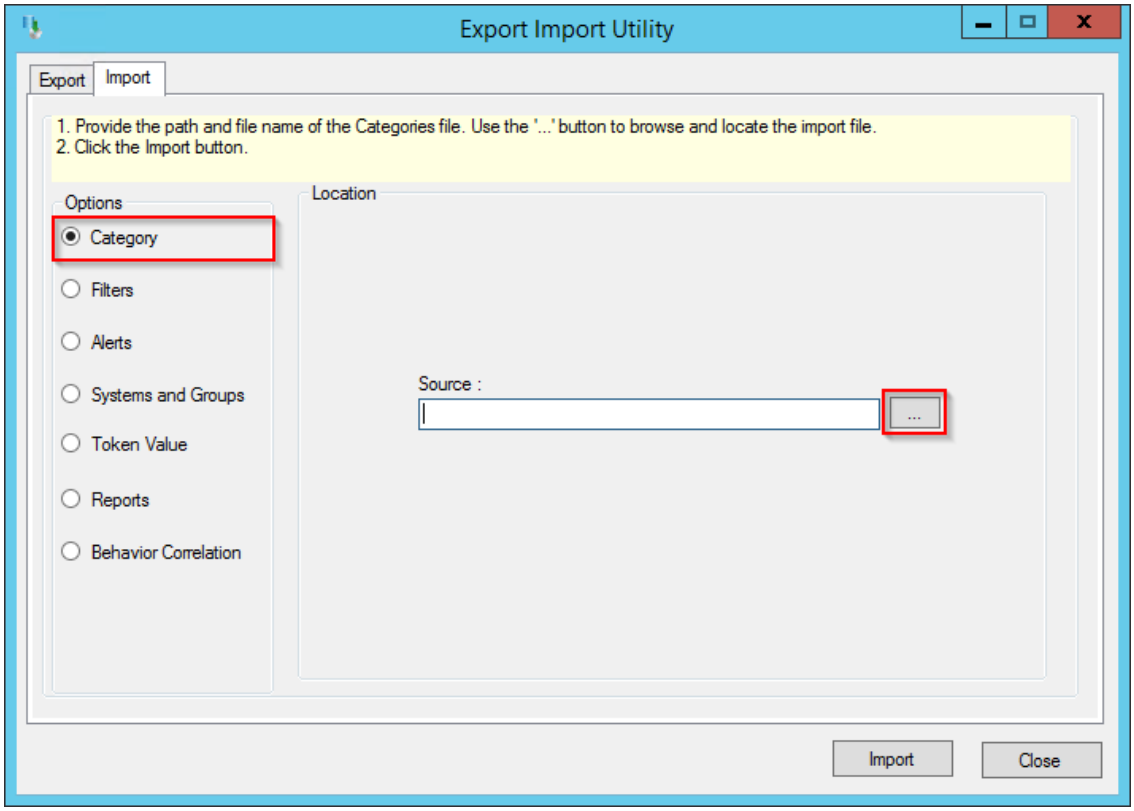
- Categories
- Alerts
- Token Template
- Reports
- Knowledge Objects
- Dashboard

1. Launch the Netsurion Open XDR platform **Control Panel**.
2. Double click **Export-Import Utility** and click the **Import** tab.

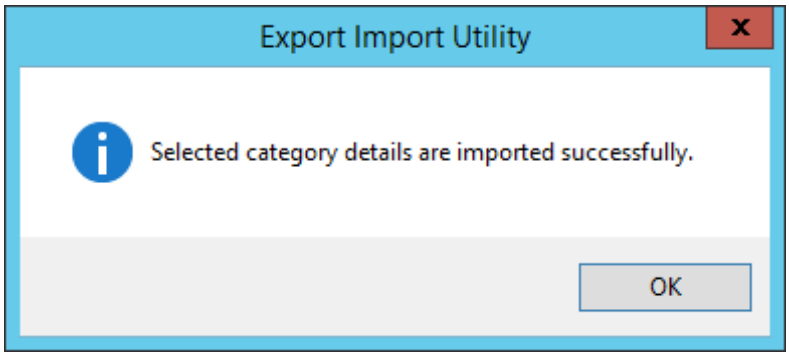


4.1 Category

1. In the **Import** tab, click **Category**, and then click the **Browse** button to locate the file.



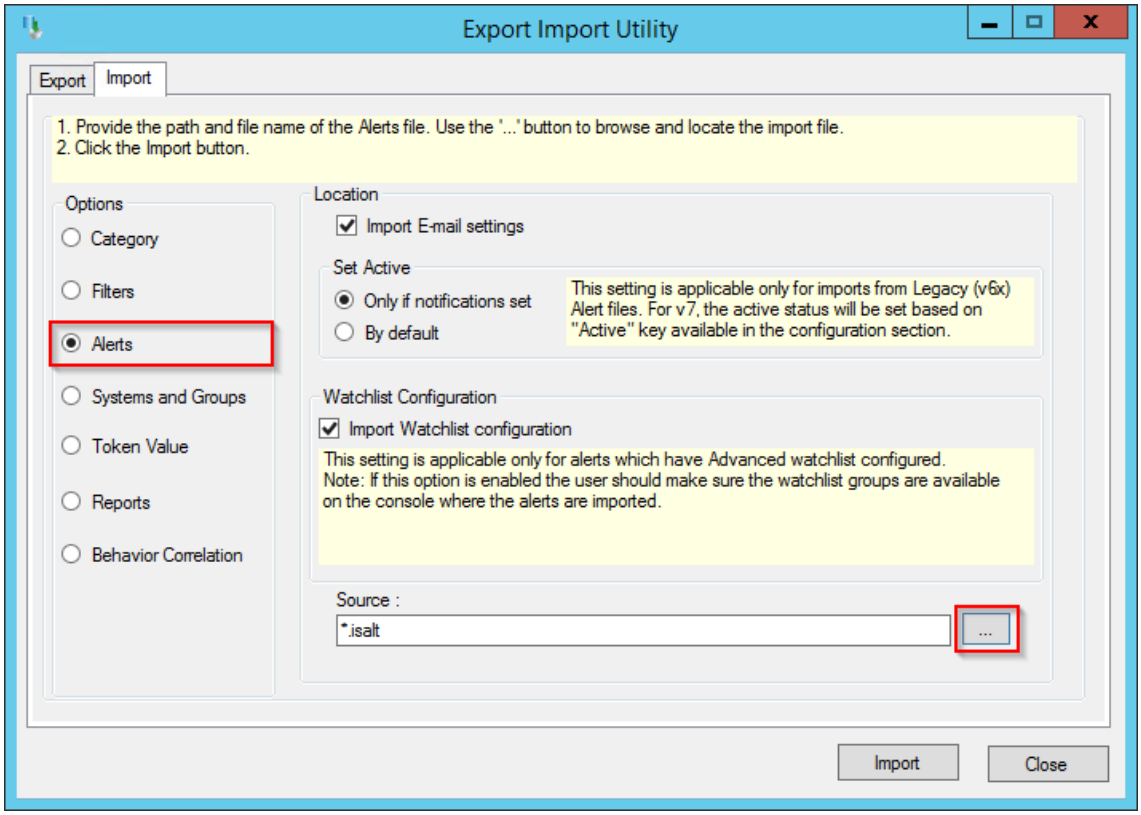
2. In the **Browse** window, locate the **Categories_Trend Micro Vision One.iscat** file and click **Open**.
3. To import the categories, click **Import**.
4. The Netsurion Open XDR platform displays a success message on successfully importing the selected file in **Category**.



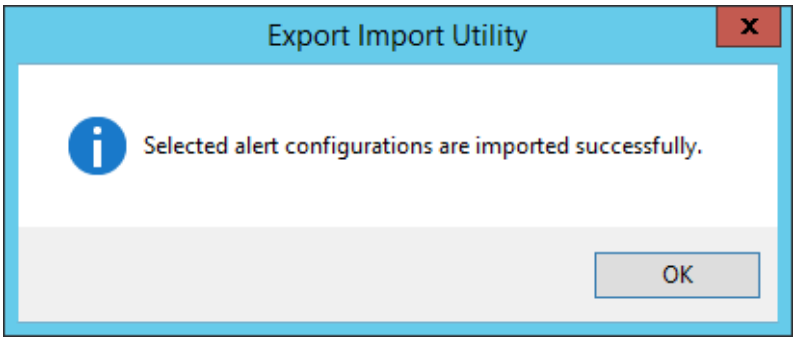
5. Click **OK** or the **Close** button to complete the process.

4.2 Alerts

1. In the **Import** tab, click **Alerts**, and then click the **Browse** ... button to locate the file.



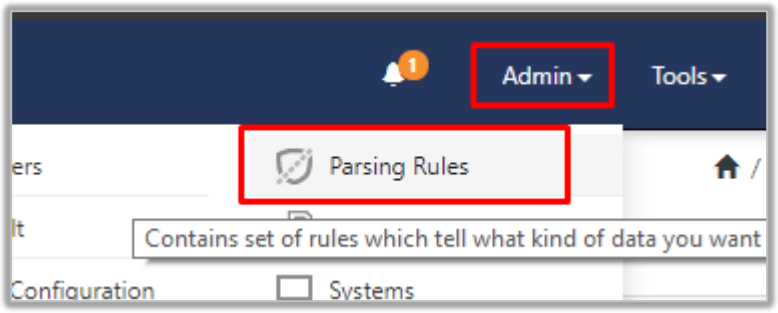
2. In the **Browse** window, locate the **Alerts_ Trend Micro Vision One.isalt** file, and then click **Open**.
3. To import the alerts, click **Import**.
4. The Netsurion Open XDR platform displays a success message on successfully importing the selected file in **Alerts**.



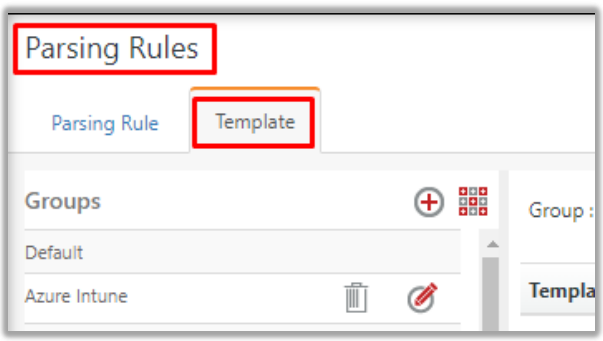
5. Click **OK** or the **Close** button to complete the process.

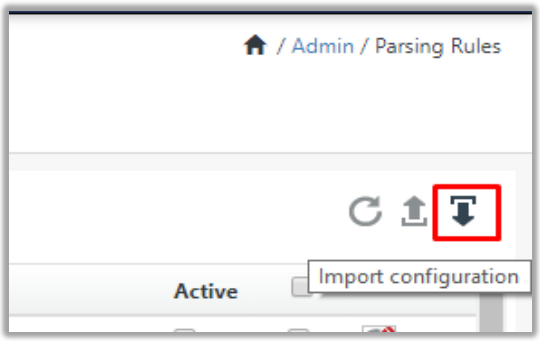
4.3 Token Template

1. In the **Netsurion Open XDR platform Manager** console, hover over the **Admin** menu and click **Parsing Rules**.

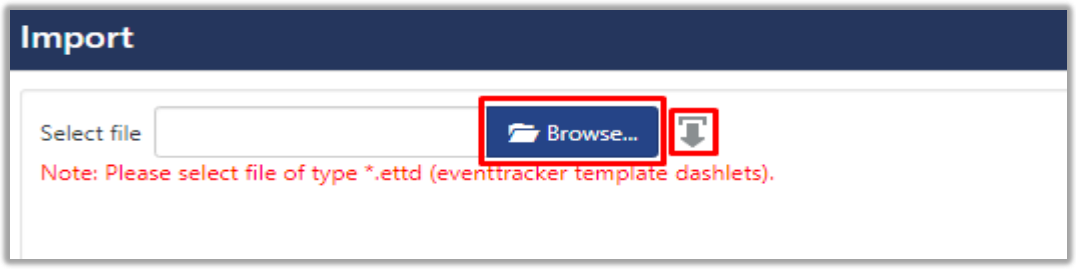


2. In the **Parsing Rules** interface, click the **Template** tab and then click **Import Configuration**.



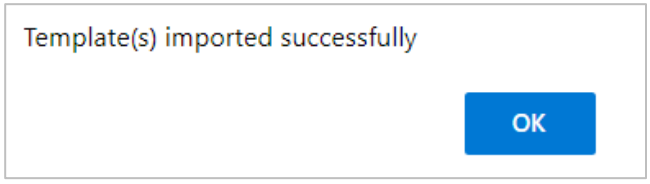


3. In the **Import** window, click **Browse** to search and locate the file name with **". ettd"** extension (example, **Templates_ Trend Micro Vision One.ettd**).



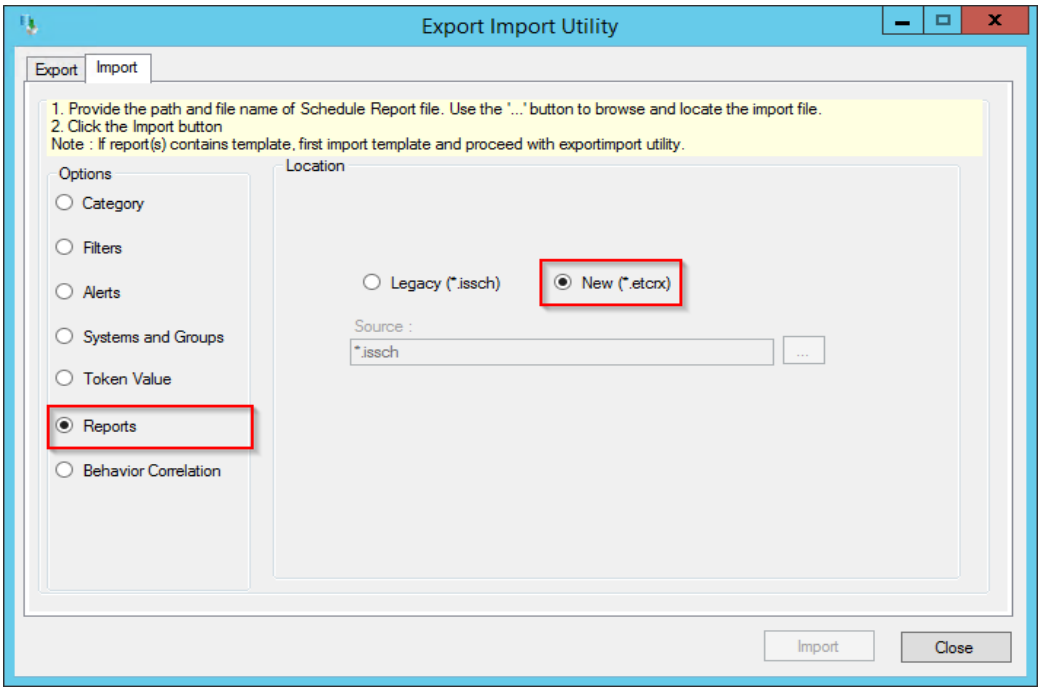
4. It takes a few seconds to load the templates and once you see the list of templates, click the appropriate template name, and click **Import**.

5. The Netsurion Open XDR platform displays a success message on successfully importing the selected file in **Template**.



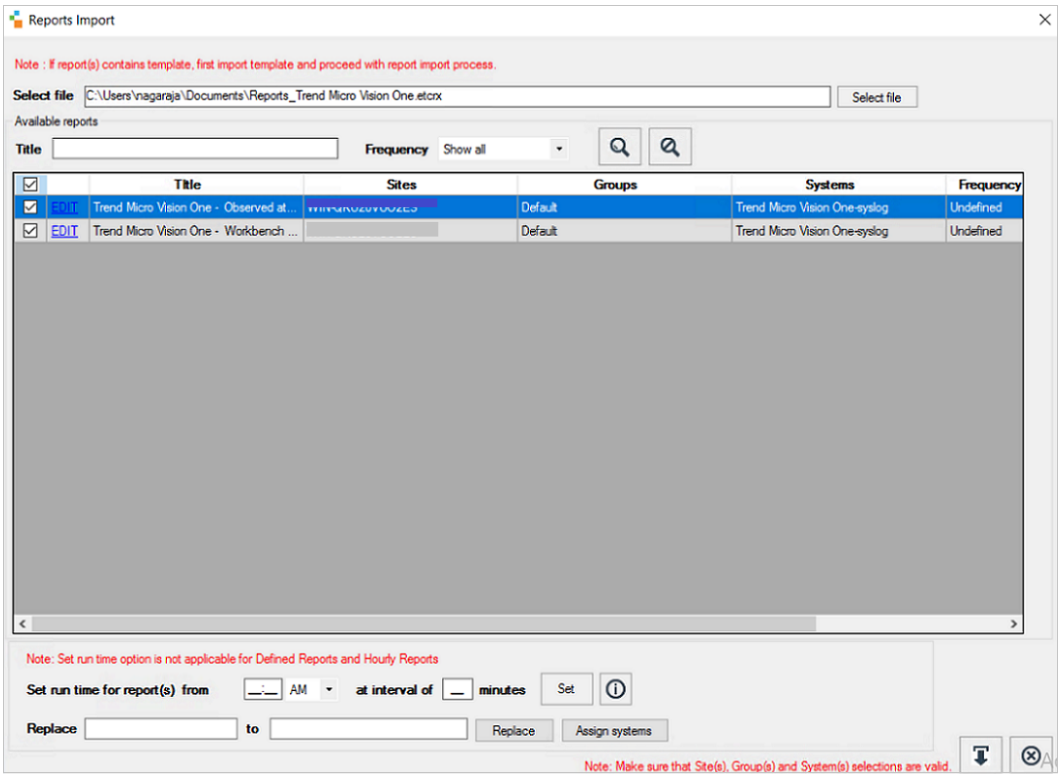
4.4 Reports

1. In the **Import** tab, click **Reports** and then click **New (*.etcrx)**.

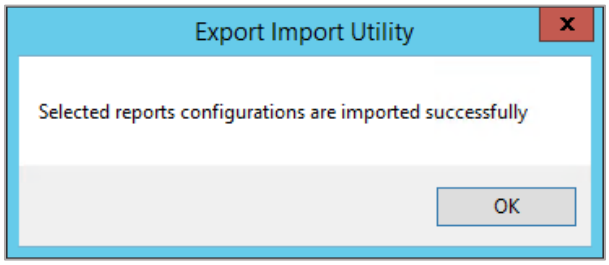


2. In the **Reports Import** window, click **Select file** to locate **Reports_ Trend Micro Vision One.etcrx** file.

3. Select the check box of all the files and click the **Import** button to import the selected files



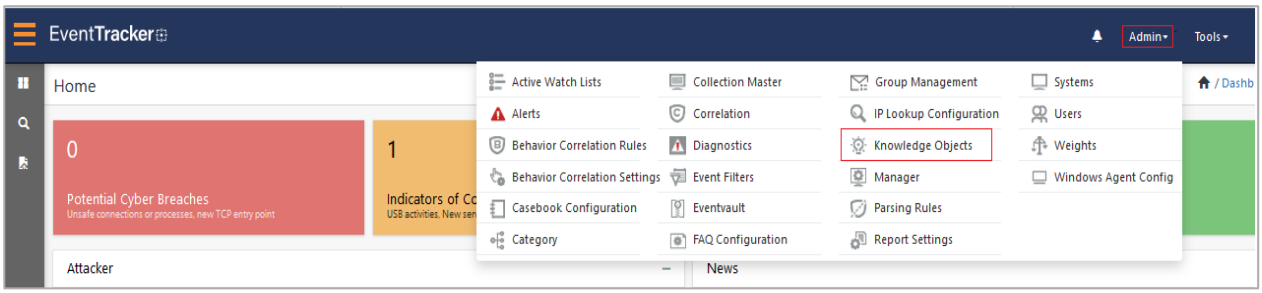
4. The Netsurion Open XDR platform displays a success message on successful importing of the selected file in **Reports**.



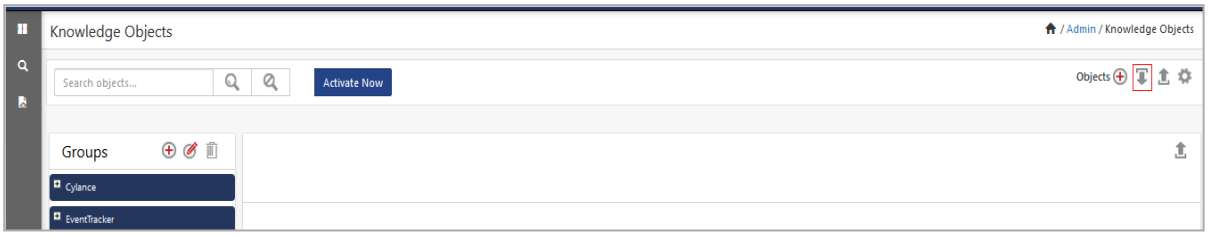
5. Click **OK** or the **Close** button to complete the process.

4.5 Knowledge Objects (KO)

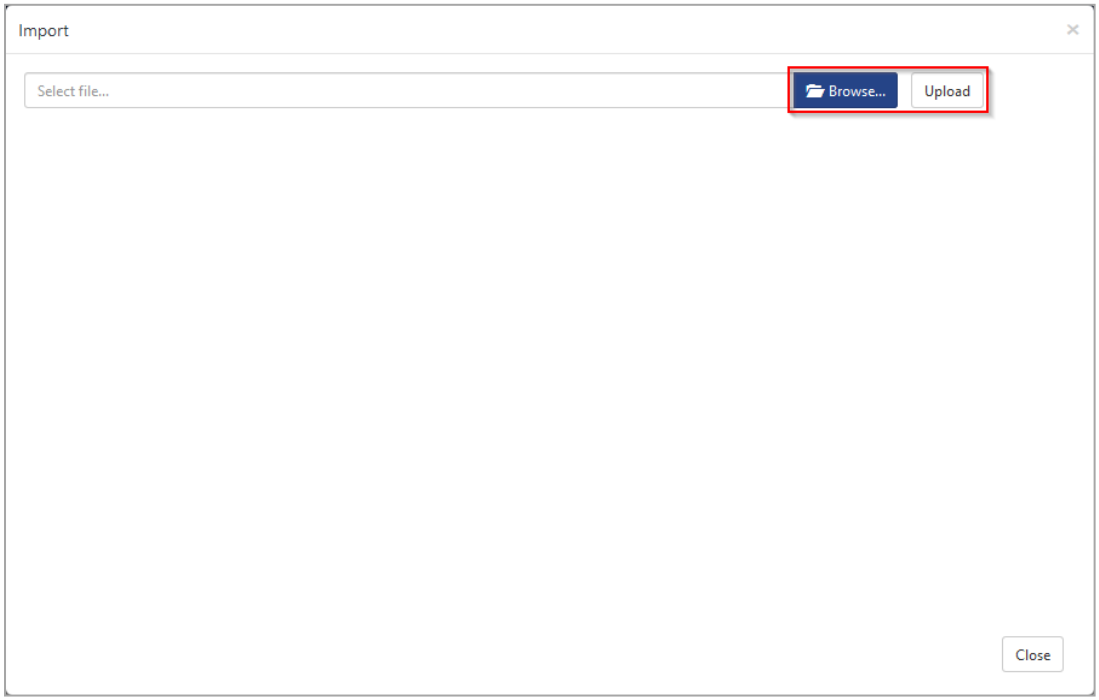
1. In the **Netsurion Open XDR platform** console, hover over the **Admin** menu and click **Knowledge Objects.**



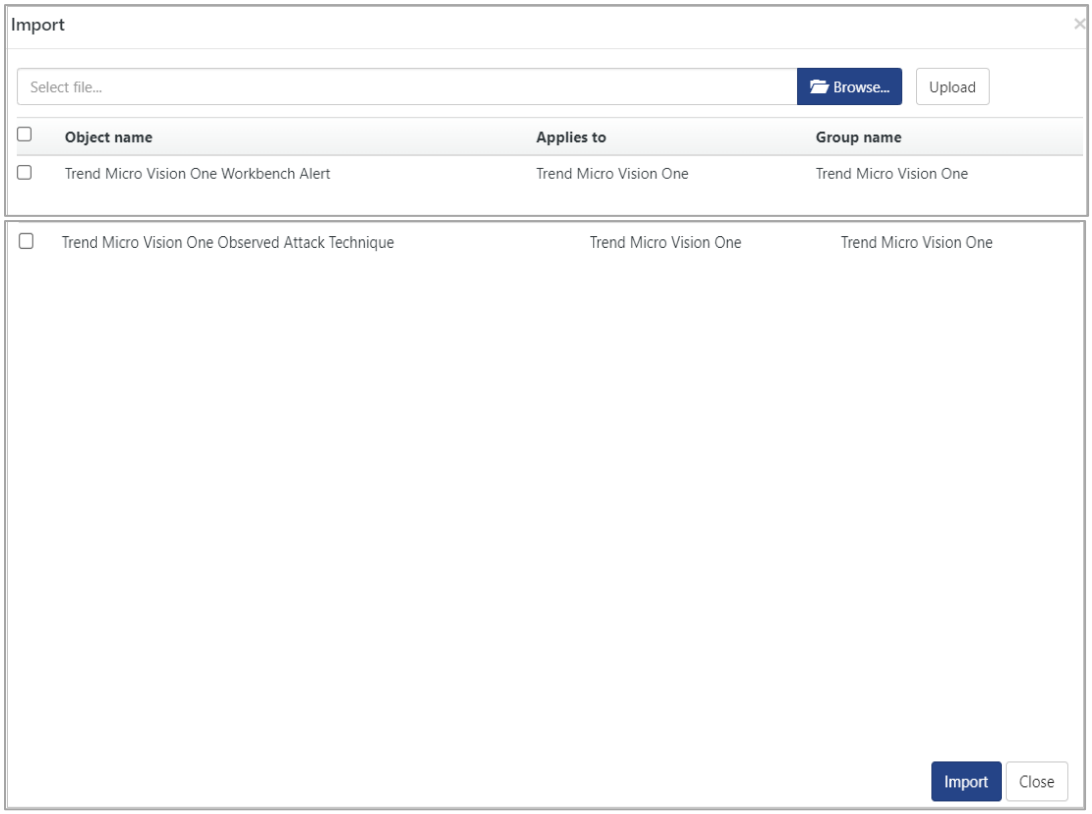
2. In the **Knowledge Objects** interface, click the **Import** button to import the KO files.



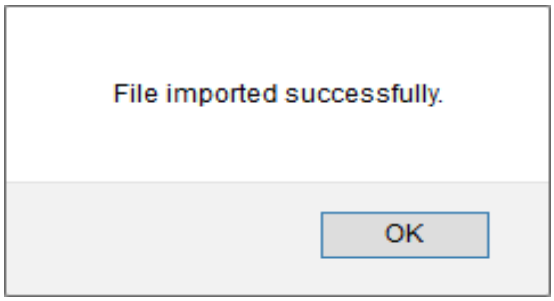
3. In the **Import** window, click **Browse** and locate the **KO_ Trend Micro Vision One.etko** file.



4. Select the check box next to the browsed KO file and then click the **Import** button.



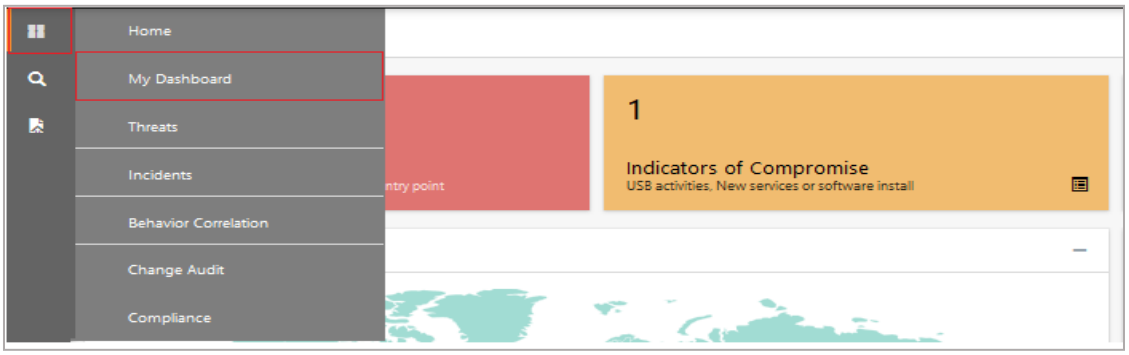
5. The Netsurion Open XDR platform displays a successful message on successfully importing the selected file in **Knowledge Objects**.



6. Click **OK** or the **Close** button to complete the process.

4.6 Dashboard

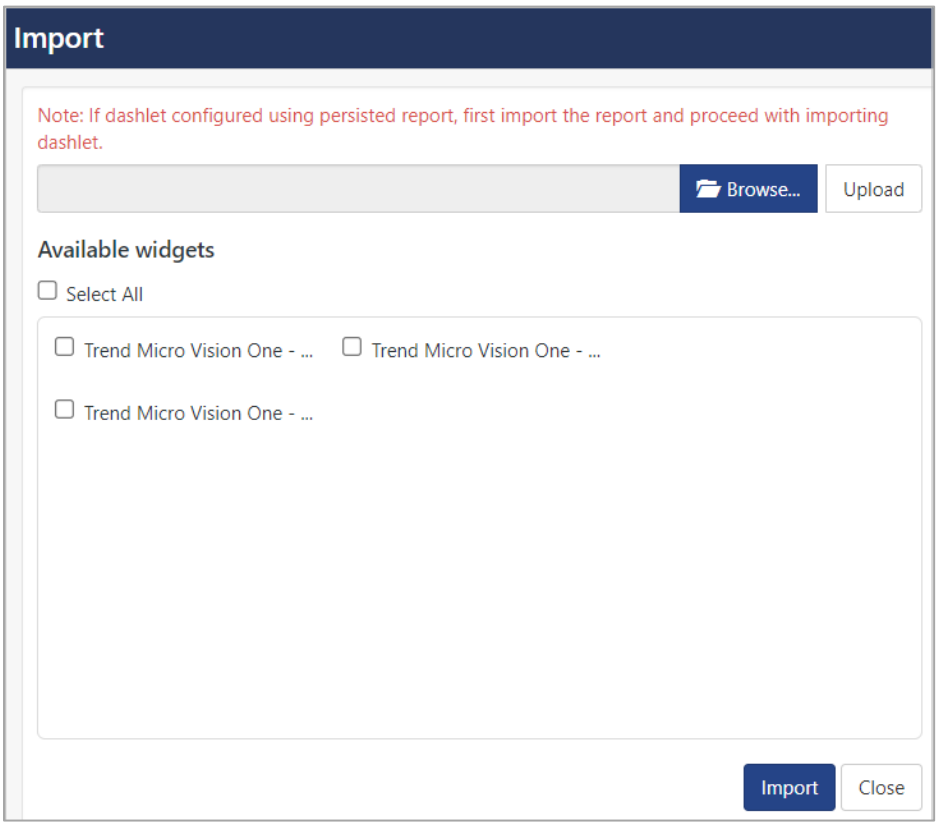
1. Log in to The **Netsurion Open XDR platform** web interface and go to **Dashboard** > **My Dashboard**.



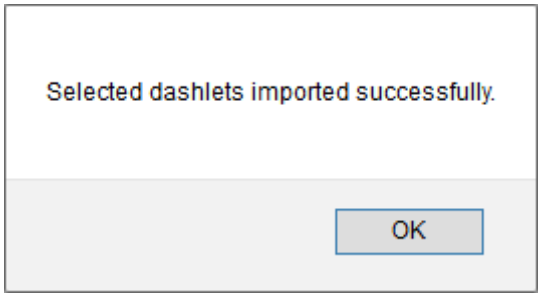
2. In the **My Dashboard** interface, click the **Import** button to import the dashlet files.

3. In the **Import** window, click **Browse** to locate the **Dashboards_Trend Micro Vision One.etwd** file and then click **Upload.**

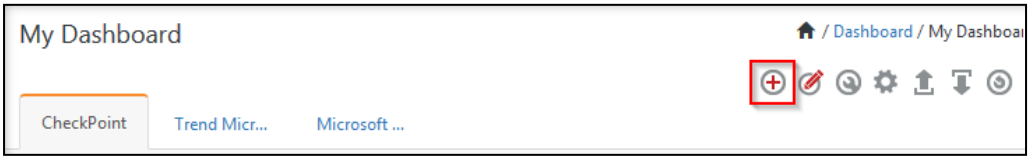
4. Select the **Select All** checkbox to select all the dashlet files and click **Import** to import the selected dashlet files.



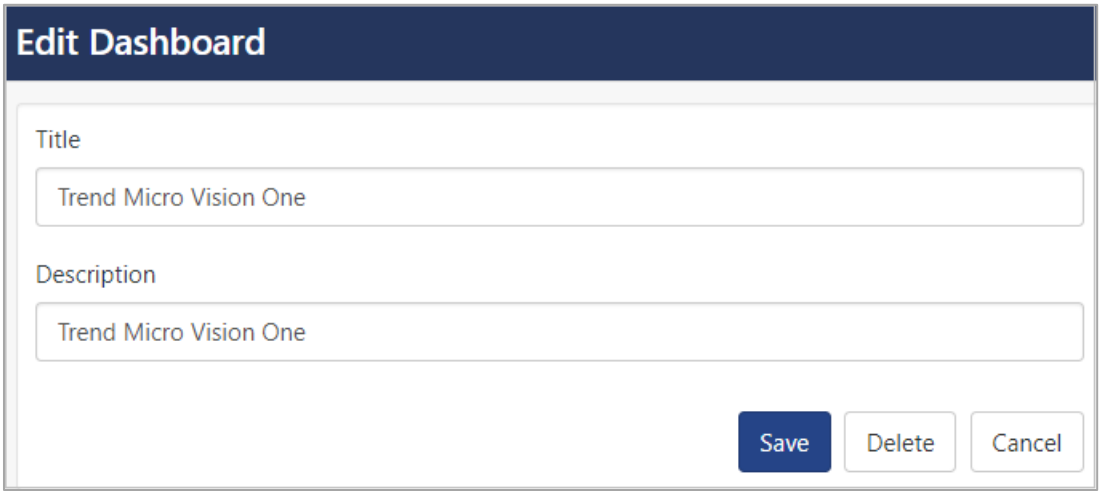
5. The Netsurion Open XDR platform displays the success message on successful import of the dashlet files.



6. Then, in the **My Dashboard** interface click the **Add** ⊕ button to add dashboard.

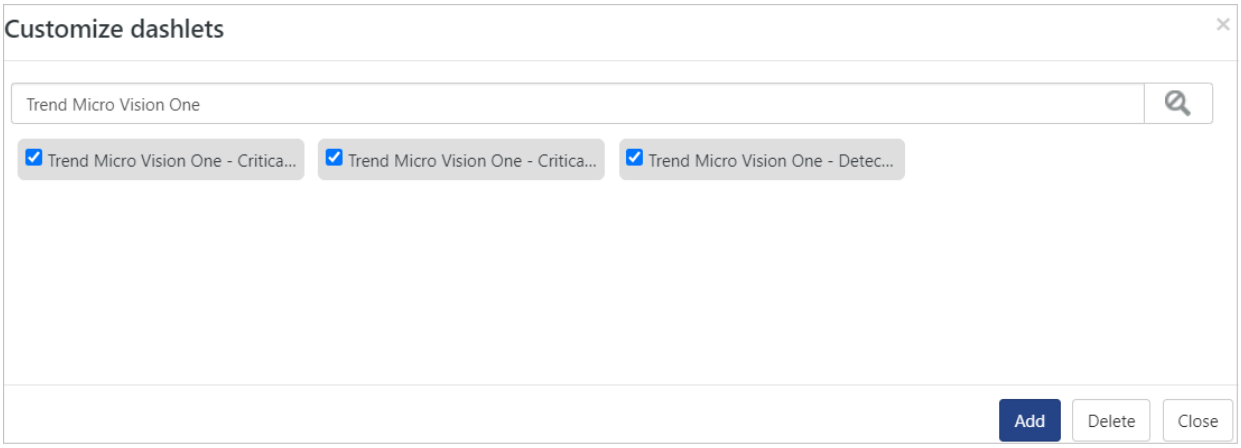


7. In the **Add Dashboard** interface, specify the **Title** and **Description** and click **Save**.



8. From the newly created dashboard interface (for example, **Trend Micro Vision One**), click the **Configuration** button to add the Trend Micro Vision One dashlets.

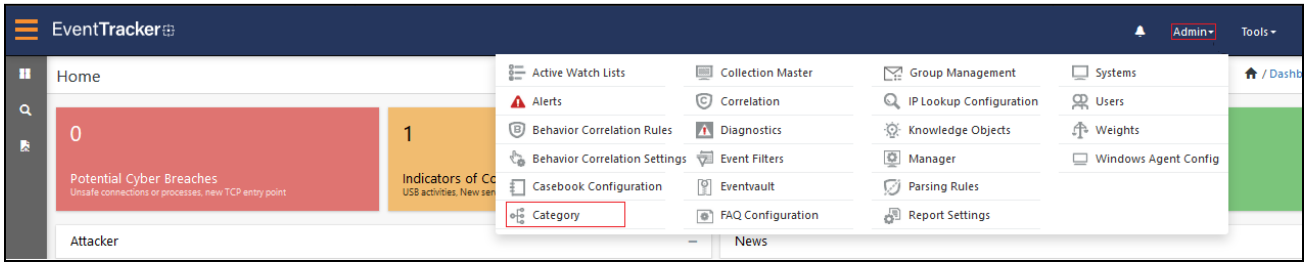
9. Search and select the newly imported dashlets and click **Add**.



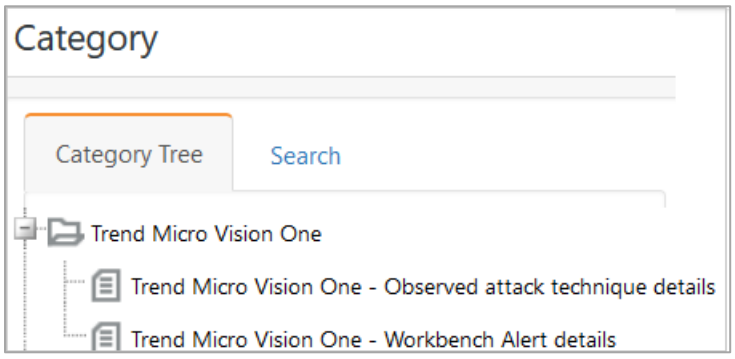
5 Verifying Data Source Integration in the Netsurion Open XDR platform

5.1 Category

1. In the **Netsurion Open XDR platform** web interface, hover over the **Admin** menu and click **Category**.

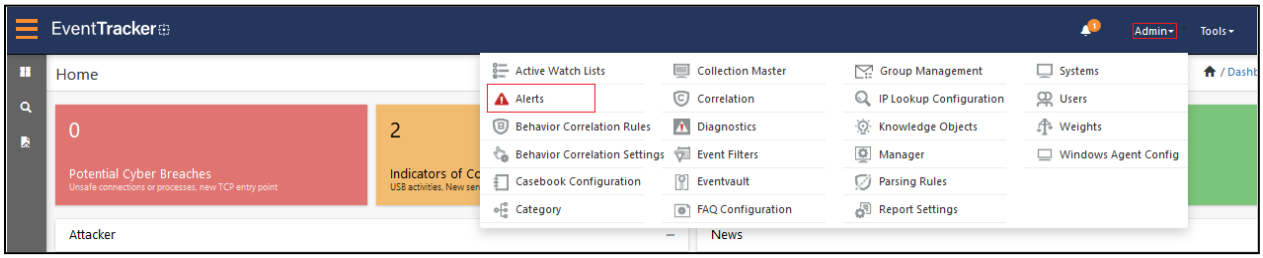


2. In the **Category** interface, under the **Category Tree** tab, click the **Trend Micro Vision One** group folder to expand and see the imported categories.



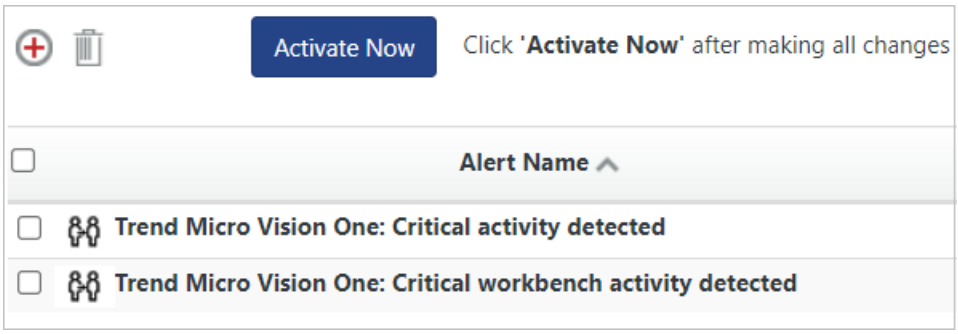
5.2 Alerts

1. In the **Netsurion Open XDR platform** web interface, hover over the **Admin** menu and click **Alerts**.

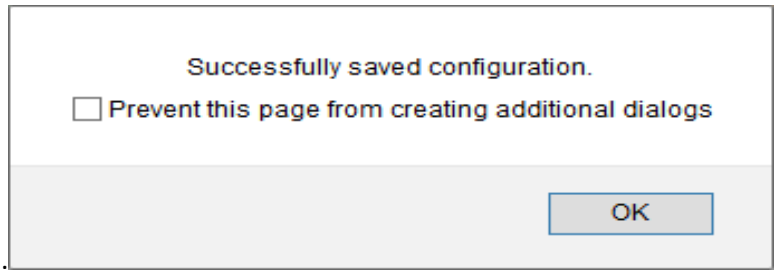


2. In the **Alerts** interface, type **Trend Micro Vision One** in the **Search** field and click the **Search** button.

3. The **Alerts** interface will display all the imported **Trend Micro Vision One** alerts.



4. To activate the imported alert, toggle the **Active** button, which is available next to the respective alert name.
5. The Netsurion Open XDR platform displays a success message on successfully configuring the alerts.



6. Click **OK** and click **Activate now** to activate the alerts after making the required changes.

Note

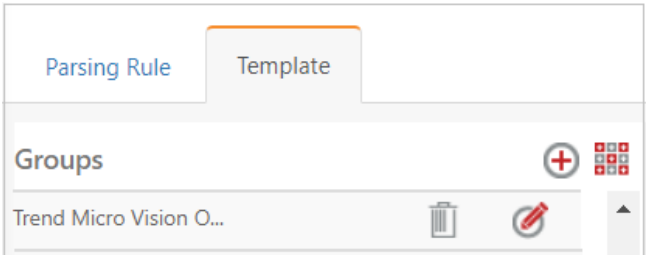
You can modify the required alert separately, and select the respective alert name check box, and then click **Activate Now** to save the alert modifications.

Note

In the **Alert Configuration** interface, specify the appropriate **System** for better performance.

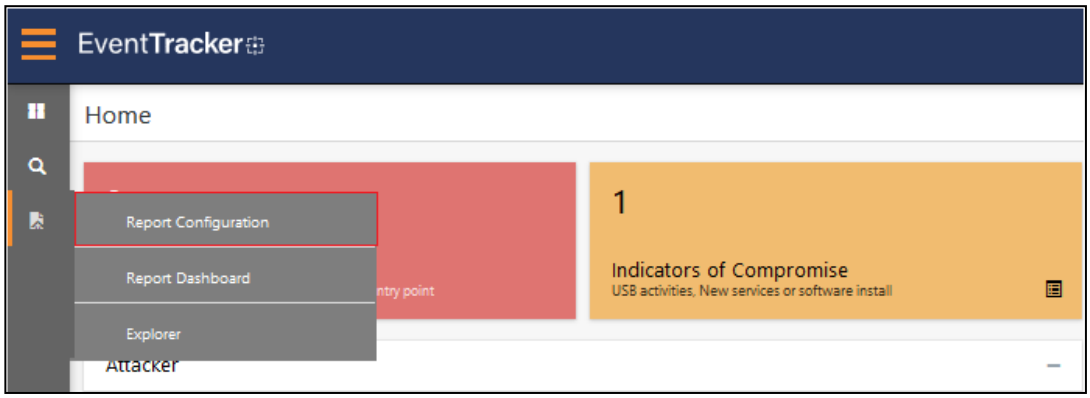
5.3 Token Template

1. In the **Netsurion Open XDR platform** web interface, hover over the **Admin** menu and click **Parsing Rules.**
2. Go to the **Template** tab and click the **Trend Micro Vision One** group folder to view the imported Token template.

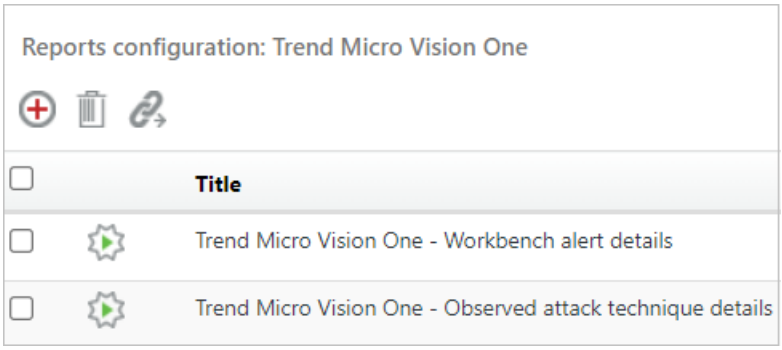


5.4 Reports

1. In the **Netsurion Open XDR platform** web interface, click the **Reports** menu, and then click **Report Configuration**.

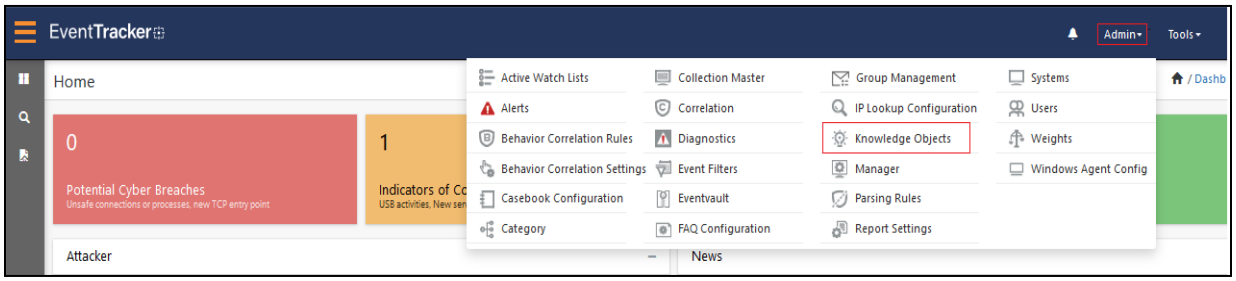


2. In the **Reports Configuration** interface, select the **Defined** option.
3. In the search field, type **Trend Micro Vision One** and click **Search** to search for the Trend Micro Vision One files.
4. The Netsurion Open XDR platform displays the reports for Trend Micro Vision One.

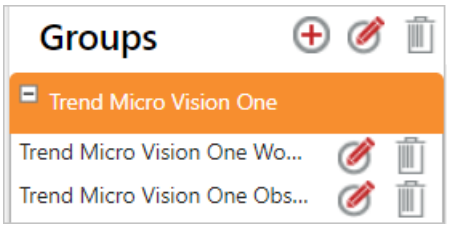


5.5 Knowledge Objects (KO)

1. In the **Netsurion Open XDR platform** web interface, hover over the **Admin** menu and click **Knowledge Objects.**



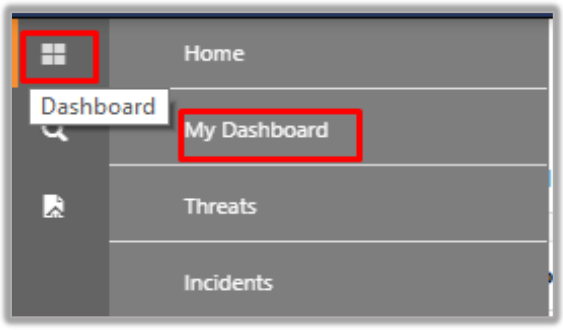
2. In the **Knowledge Object** interface, under **Groups** tree, click the **Trend Micro Vision One** group to expand and view the imported Knowledge objects.



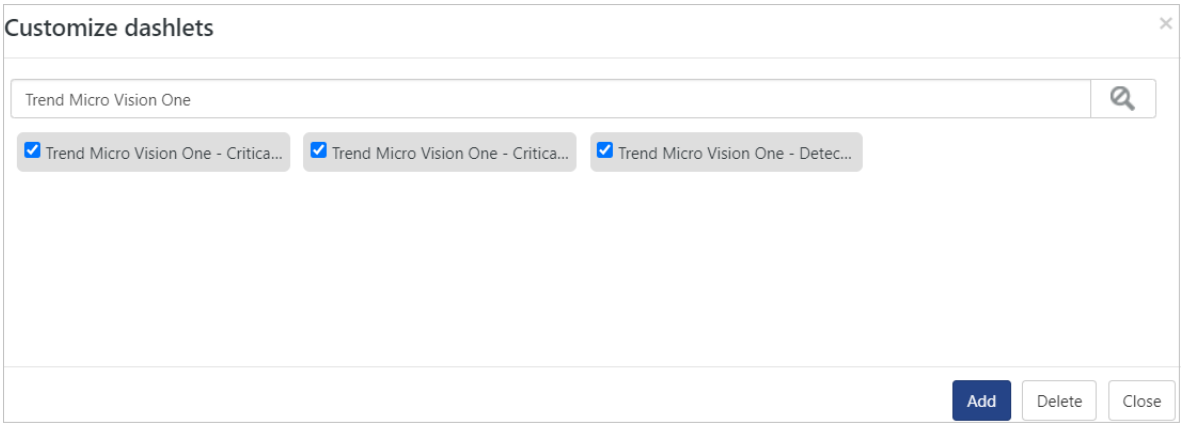
3. Click **Activate Now** to apply the imported Knowledge Objects.

5.6 Dashboard

1. In the **Netsurion Open XDR platform** web interface, go to **Home** > **My Dashboard**, and click the **Customize dashlets** button.



2. In the **Customize dashlets** interface, search for **Trend Micro Vision One** in the search field.
3. The following Trend Micro Vision One dashlet files will get displayed.



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 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