Netsurion®
Powering Secure and Agile Networks

Integration Guide

Integrate Snort IDS with EventTracker

Publication Date:

June 17, 2022

Abstract

This guide provides instructions to configure the Knowledge Pack in EventTracker to receive the logs from Snort IDS. The Knowledge Pack contains the reports, dashboard, alerts, and saved searches.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.3 and Snort 2.9 or later.

Audience

This guide is for the administrators responsible to configure the Knowledge Packs to EventTracker.

Table of Contents

1 Overview

Snort IDS is an open-source intrusion detection system that analyze network traffics in real-time and provides data packet logging. It detects potentially malicious activities by employing a rule-based language that integrates anomaly, protocol, and signature inspection methods.

Netsurion monitors Snort events retrieved via syslog. Dashboard, category, alerts, and reports in Netsurion's threat protection platform, EventTracker, will benefit you in tracking possible attacks, suspicious activities, or any other threat based on rules defined in the Snort configuration file.

2 Prerequisite

- EventTracker version 9.3 or later must be installed and configured to receive logs.
- Configure Snort IDS to forward logs to EventTracker.

> **Note**:
>
> Refer to How-To Guide to configure Snort IDS to forward logs to EventTracker.

3 EventTracker Knowledge Pack

Configure categories and reports in EventTracker once the logs are available in EventTracker.

The following Knowledge Packs are available in the EventTracker.

3.1 Categories

Snort IDS - Corporate suspicious activities: This report provides information related to alerts generated by Snort IDS for Denial-of-Service attacks and Information leaks.

Snort IDS - Miscellaneous activities: This report provides information related to alerts generated by Snort IDS for miscellaneous traffic attacks.

Snort IDS - Application attacks: This report provides information related to alerts generated by Snort IDS for web application attacks.

Snort IDS - Traffic attacks: This report provides information related to alerts generated by Snort IDS for traffic issues.

Snort IDS - Potential suspicious activity: This report provides information related to alerts generated by Snort IDS for all types of possible suspicious activities.

Snort IDS - Potential privilege escalations: This report provides information related to alerts generated by Snort IDS for all types of privilege escalations activities like user log in, admin access, and failed login attempts.

Snort IDS - Potential network attacks: This report provides information related to alerts generated by Snort IDS for all types of network attacks, including port scans and Generic ICMP issues.

3.2 Alerts

Snort IDS: Critical threat detected - This alert is generated for priority one (P1) logs.

Snort IDS: Potential attacks detected - This alert is generated for priority two (P2) logs.

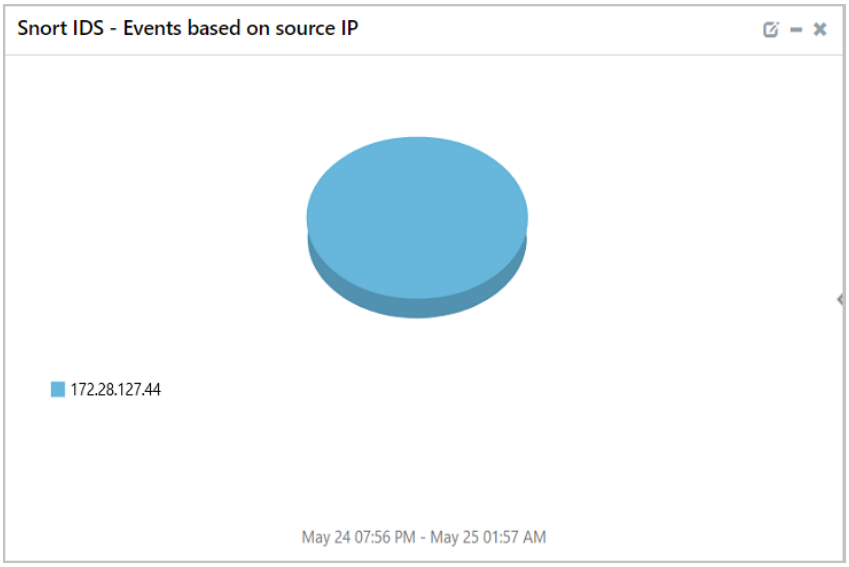
3.3 Reports

Snort IDS Activity Overview: This report provides the information about all the activities that takes place in Snort IDS.

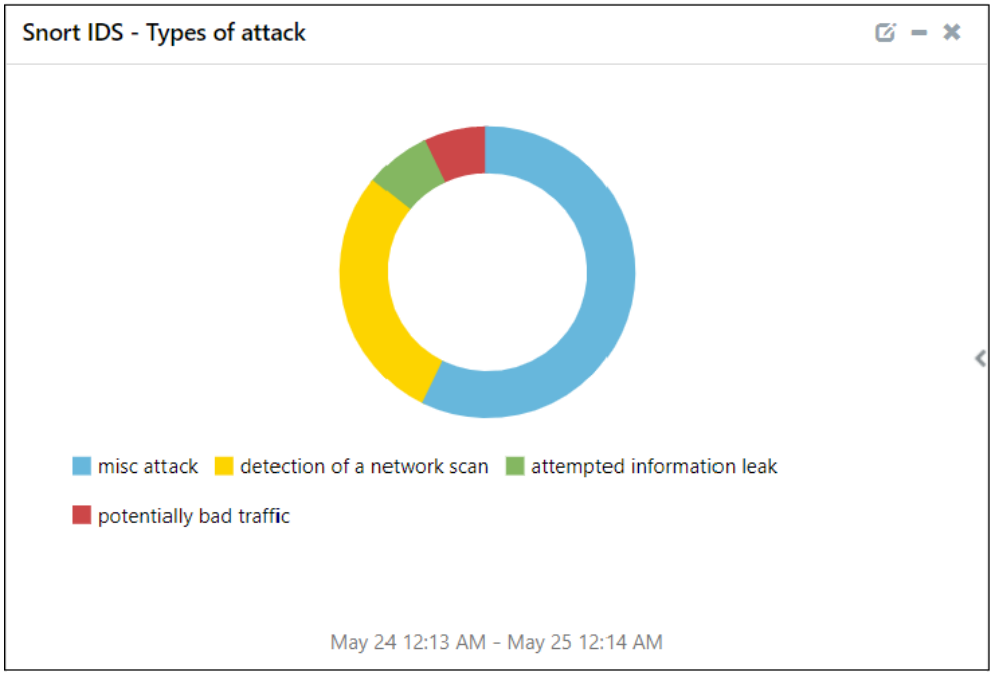
LogTime	Classification	Priority	Rule ID	Protocal	Destination IP	Source IP
05-24-2022 03:44:11 AM	Misc Attack	2	1:2403470:56634	TCP	10.12.14.233	10.12.14.253
05-24-2022 03:44:11 AM	Misc Attack	1	1:2522283:4029	TCP	10.12.14.234	10.12.14.254
05-24-2022 03:44:11 AM	Misc Attack	1	1:2402000:5511	TCP	10.12.14.235	10.12.14.255
05-24-2022 03:44:11 AM	Detection of a Network Scan	3	1:2029054:2	TCP	10.12.14.236	10.12.14.256
05-24-2022 03:44:11 AM	Potentially Bad Traffic	2	1:2010935:3	TCP	10.12.14.237	10.12.14.257
05-24-2022 03:44:11 AM	Misc Attack	2	1:2522036:4029	TCP	10.12.14.238	10.12.14.258
05-24-2022 03:44:11 AM	Misc Attack	2	1:2520036:4029	TCP	10.12.14.239	10.12.14.259
05-24-2022 03:44:11 AM	Misc Attack	2	1:2500022:5399	TCP	10.12.14.240	10.12.14.260
05-24-2022 03:44:11 AM	Detection of a Network Scan	3	1:2029054:2	TCP	10.12.14.241	10.12.14.261
05-24-2022 03:44:11 AM	Detection of a Network Scan	3	1:2029054:2	TCP	10.12.14.242	10.12.14.262
05-24-2022 03:44:11 AM	Detection of a Network Scan	3	1:2029054:2	TCP	10.12.14.243	10.12.14.263

3.4 Dashboard

Snort IDS - Events based on source IP: This dashlet displays the information of the logs generated from different source IPs.

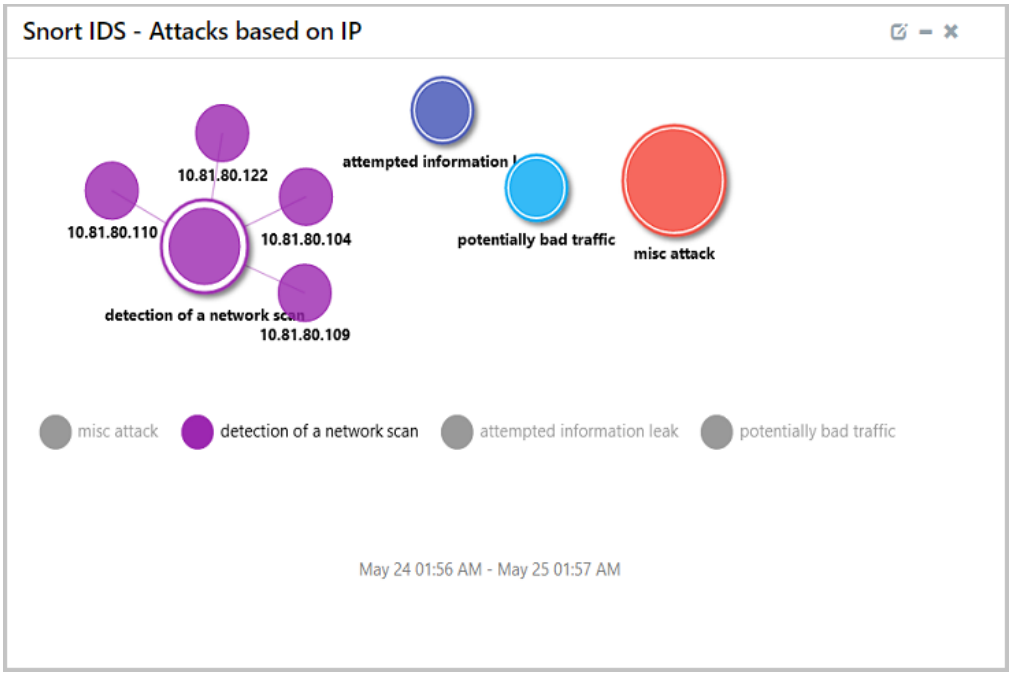


Snort IDS - Types of attack: This dashlet displays the information of all the different types of attacks in Snort IDS.

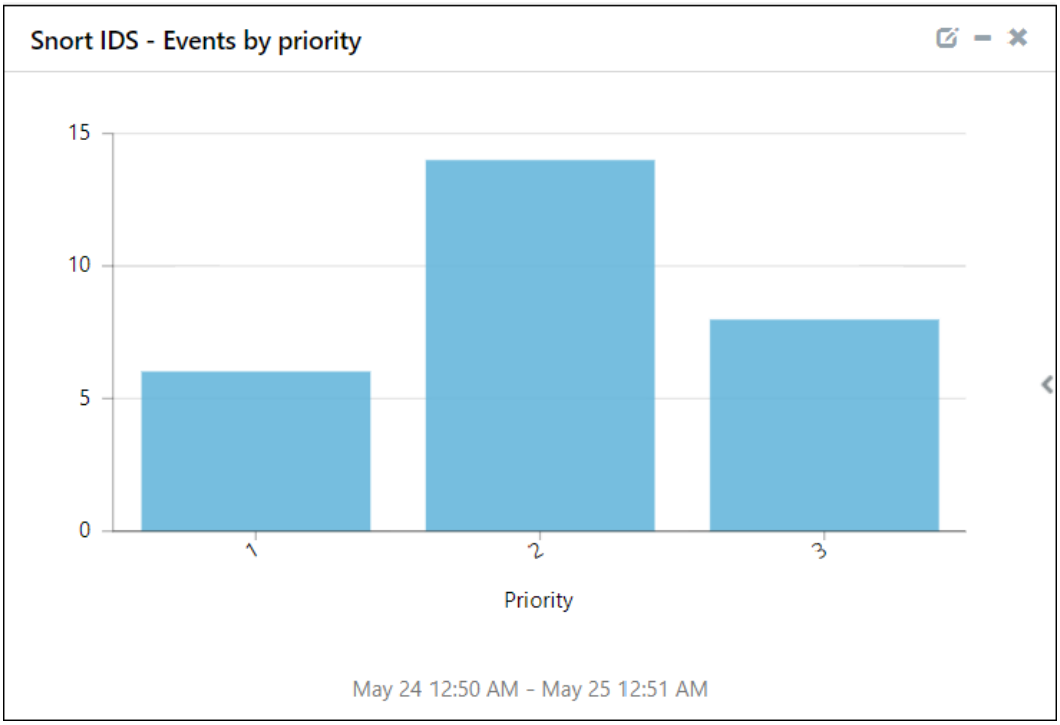


Snort IDS - Attacks based on IP: This dashlet displays the information of various attacks on a particular IP.

Note:
There could be multiple attacks on the same IP address.



Snort IDS - Events by priority: This dashlet displays the information of Priority based events.



Snort IDS - Events by geolocation: This dashlet displays the event details based on the geolocation.

4 Importing Snort IDS Knowledge Packs into EventTracker

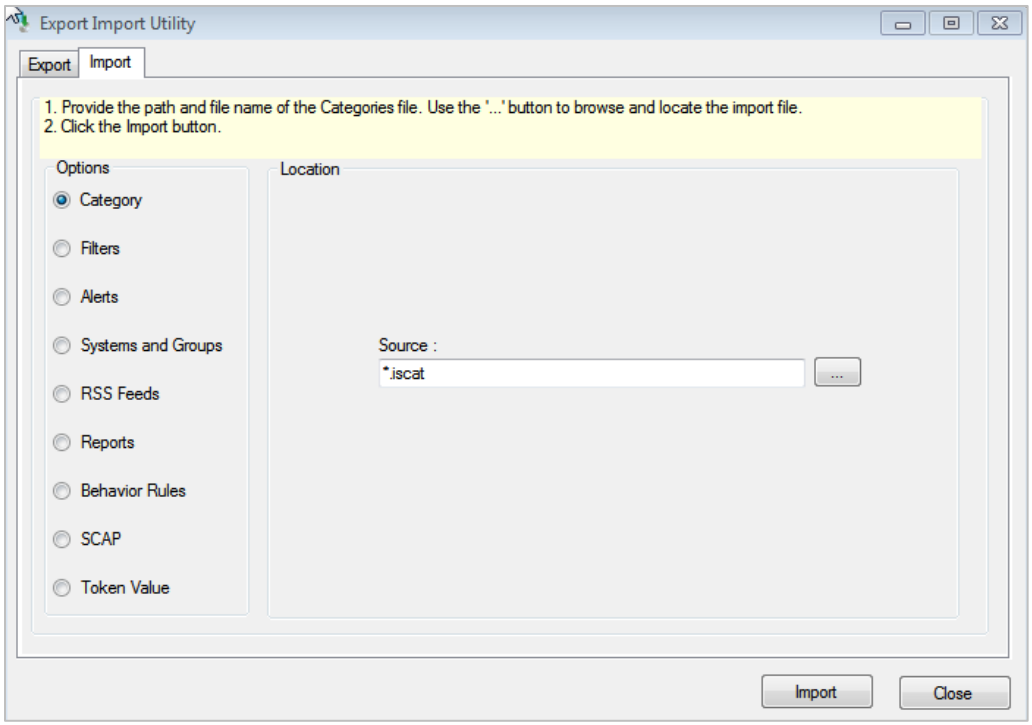
Import the Snort IDS knowledge pack items in the following sequence.

- Categories
- Alerts
- Flex Reports
- Knowledge Objects
- Dashboards

1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility** and click the **Import** tab.

4.1 Category

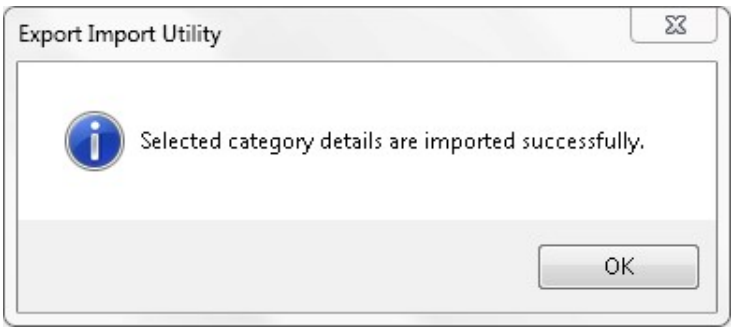
1. In the **Import** tab, click **Category**, and then click the **Browse** button to locate the file.



2. Locate the **All Snort group of Categories_Snort IDS.iscat** file and click **Open**.

3. To import categories, click **Import**.

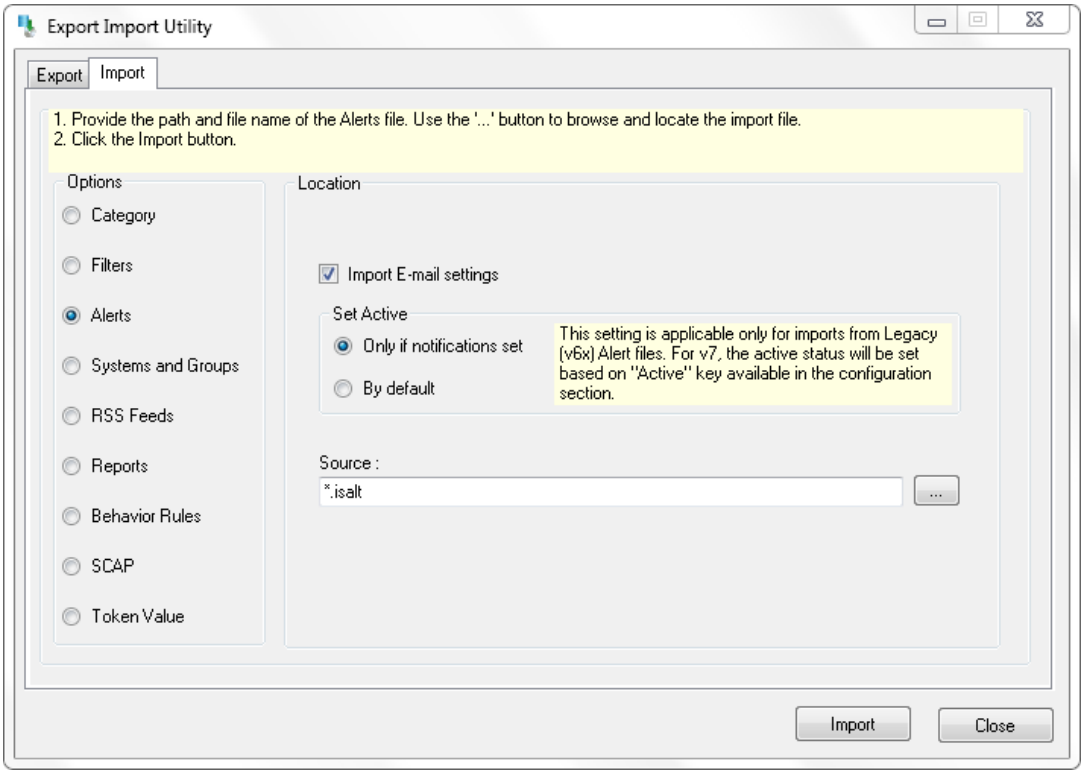
4. EventTracker displays success message on successfully importing the selected file in **Category**.



5. Click **OK**.

4.2 Alerts

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

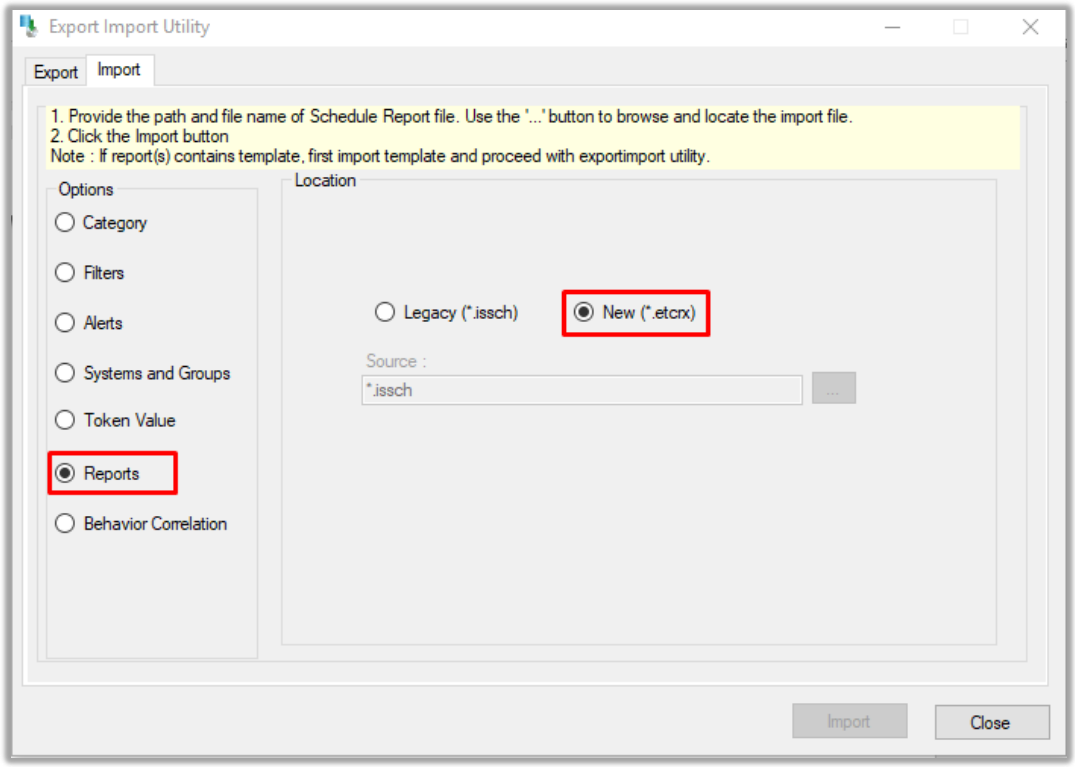


2. Locate the **Alerts_Snort IDS.isalt** file, and then click **Open**.
3. To import alerts, click **Import**.
4. EventTracker displays success message on successfully importing the selected file in **Alerts**.

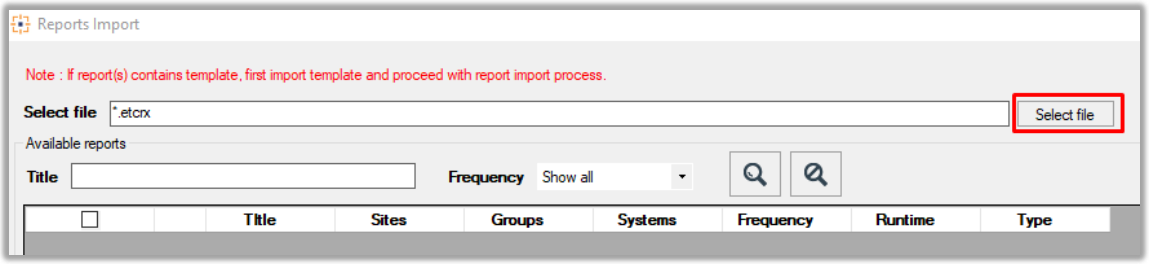
5. Click **OK**.

4.3 Reports

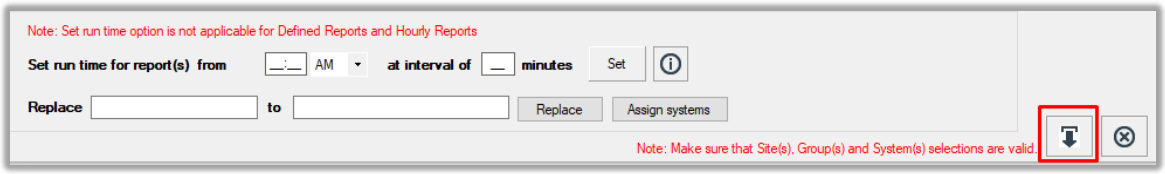
1. In the **Import** tab, click **Reports**, and then click **New (*.etcrx)**.



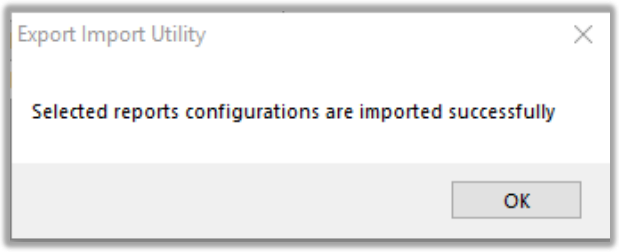
2. In the **Reports Import** window, click **Select file** to go to the appropriate Knowledge Pack path file and select the file with the **.etcrx** (**Reports_ Snort IDS.etcrx)** extension.



3. Then, select all the relevant reports and click the **Import** button.



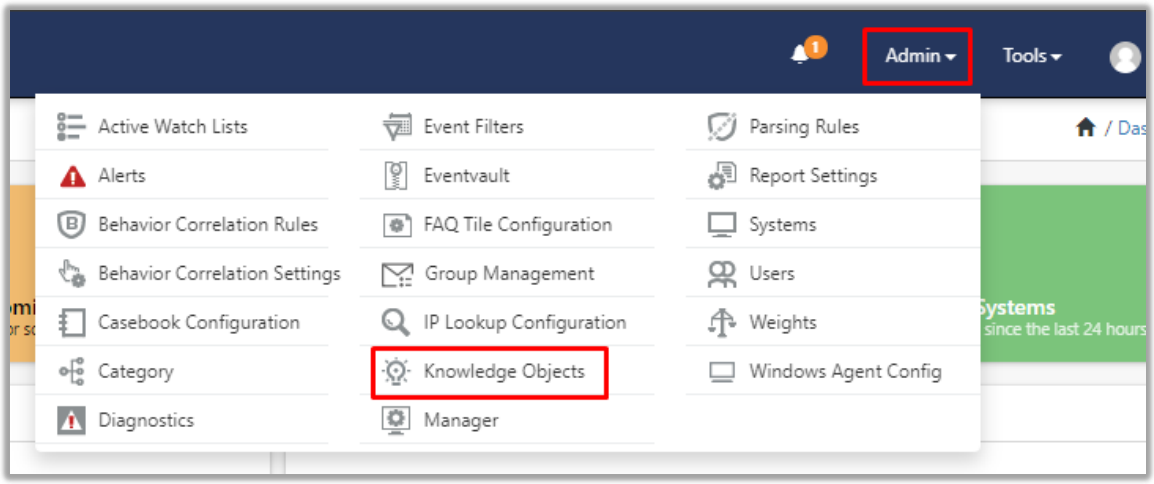
4. EventTracker displays a success message on successfully importing the selected file in **Reports**.



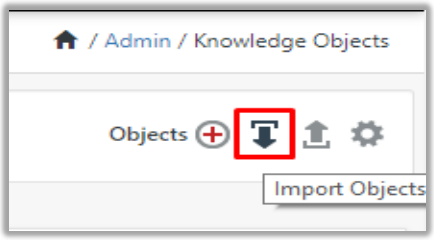
5. Click **OK**.

4.4 Knowledge Objects

1. In the **EventTracker Manager** console, hover over the **Admin** menu and click **Knowledge Objects**.



2. In the **Knowledge Objects** interface, click **Import** as shown in the below image.



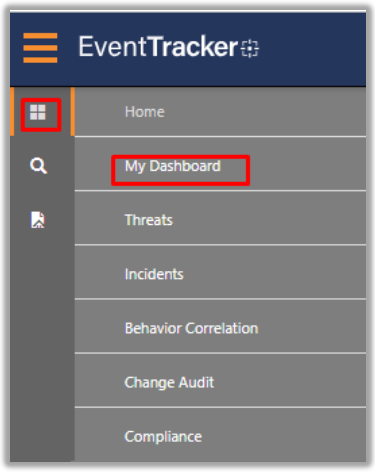
3. In the **Import** window, click **Browse** to locate the appropriate file name.

4. In the **Browse** window, enter the file path (**C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs\Snort IDS**) and search for the **.etko (KO_Snort IDS.etko)** extension, and then click **Upload**.

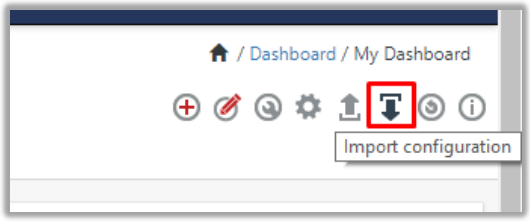
5. The EventTracker populates all the relevant knowledge objects and once displayed, select the required file, and click **Import**.

4.5 Dashboard

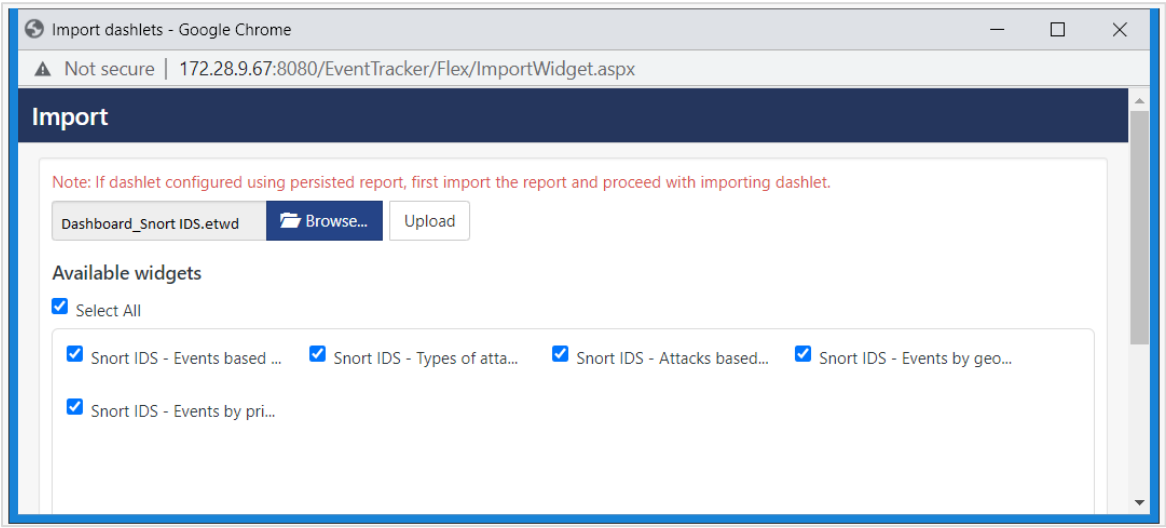
1. Log in to the **EventTracker** web interface and go to **Dashboard** > **My Dashboard**.



2. In the **My Dashboard** interface, click **Import** to import the Snort IDS files.



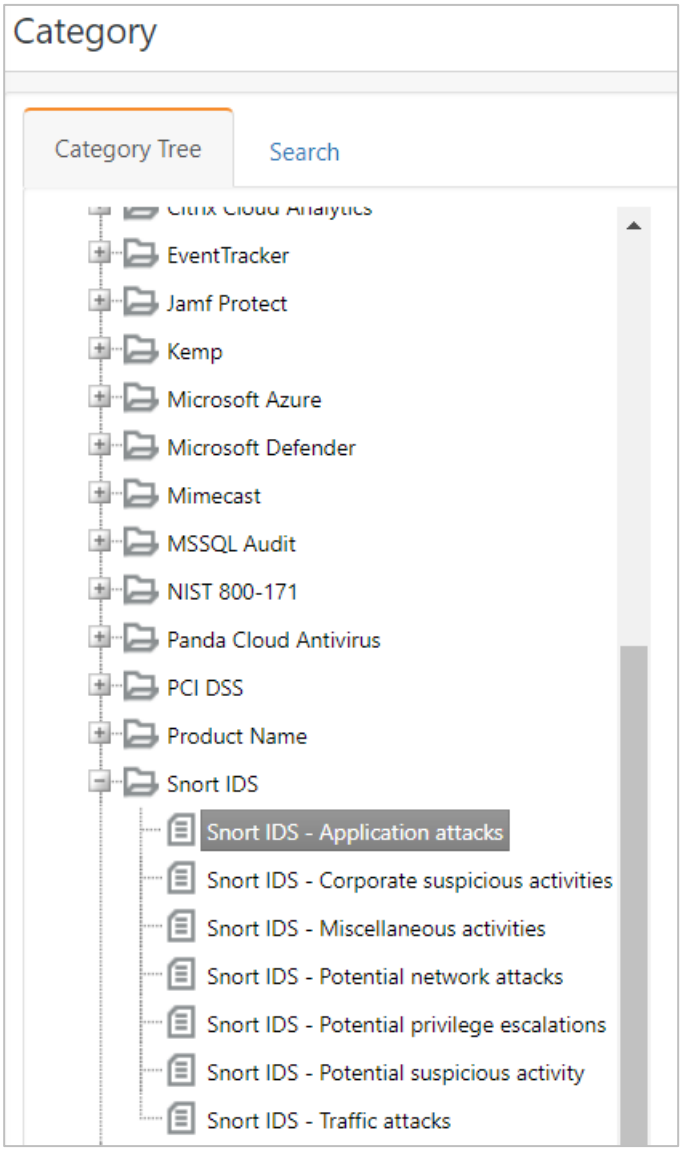
3. In the **Import** window, click **Browse** to locate the appropriate file name.
4. In the **Browse** window, enter the file path (**C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs\Snort IDS**) and search for the **.etwd (Dashboard_ Snort IDS.etwd**) extension.
5. Select the **Select All** checkbox and click **Upload** to include all the Snort IDS dashlets.



5 Verifying Snort IDS Knowledge Packs in EventTracker

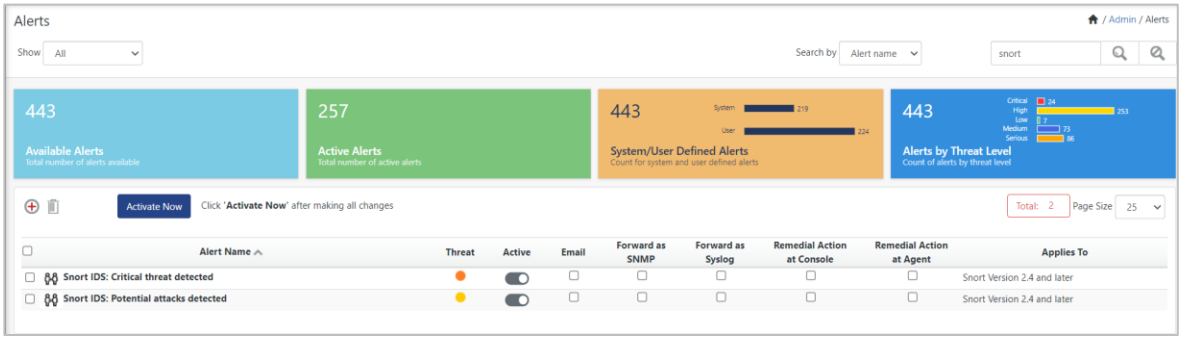
5.1 Category

1. In the **EventTracker** web interface, hover over the **Admin** menu and click **Category**.
2. In the **Category** interface, under the **Category Tree** tab, expand **Snort IDS** group folder to see the imported categories.



5.2 Alerts

1. In the **EventTracker** web interface, hover over the **Admin** menu and click **Alerts**.
2. In the **Alerts** interface, type **Snort** in the search field, and click the **Search** button.
3. The **Alerts** interface will display all the imported **Snort IDS** alerts.



4. To activate the imported alerts, click **Active**, which is available next to the respective alert name.
5. EventTracker displays success message on successfully configuring the alert.

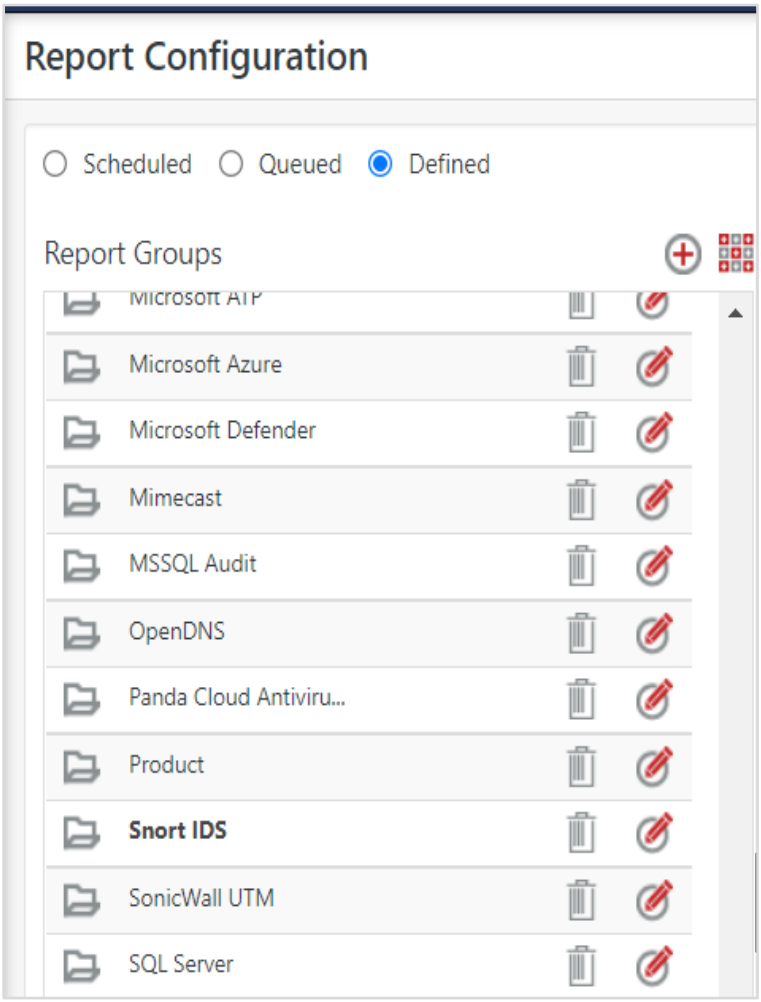
6. Click **OK** and click **Activate now** to activate the alerts after making the required changes.

Note:

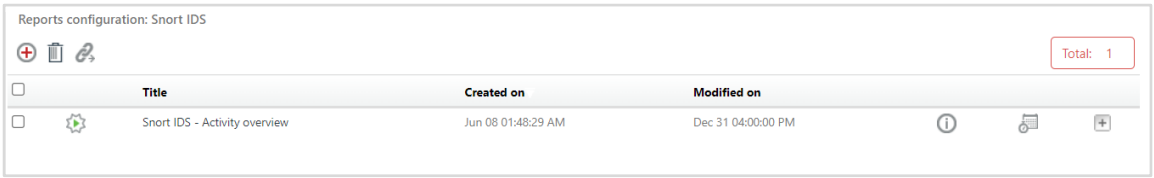
You can modify the required alert separately, and select the respective alert name check box, and then click **Activate Now** to save the alert modifications.

5.3 Reports

1. In the **EventTracker** web interface, click the **Reports** menu, and then click **Report Configuration**.
2. In the **Report Configuration** interface, click **Defined**.

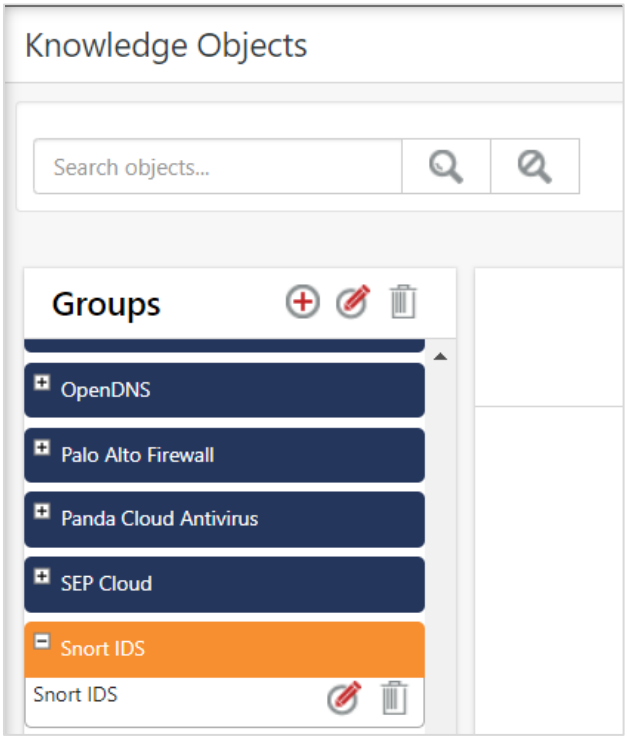


3. In the search field, type **Snort IDS** and click **Search** to search for the Snort files.
4. EventTracker displays the reports for **Snort IDS.**



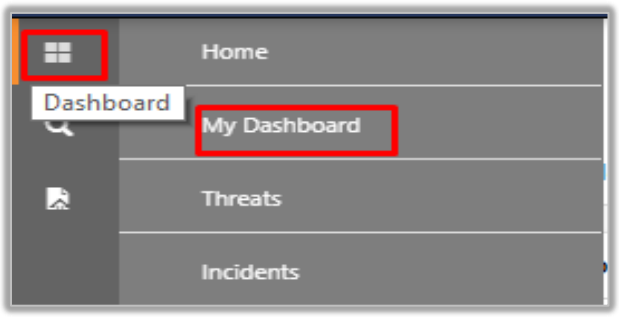
5.4 Knowledge Objects

1. In the **EventTracker** web interface, hover over the **Admin** menu and click **Knowledge Objects.**
2. In the **Knowledge Object** interface, under **Groups** tree, expand the **Snort IDS** group to view the imported Knowledge objects.

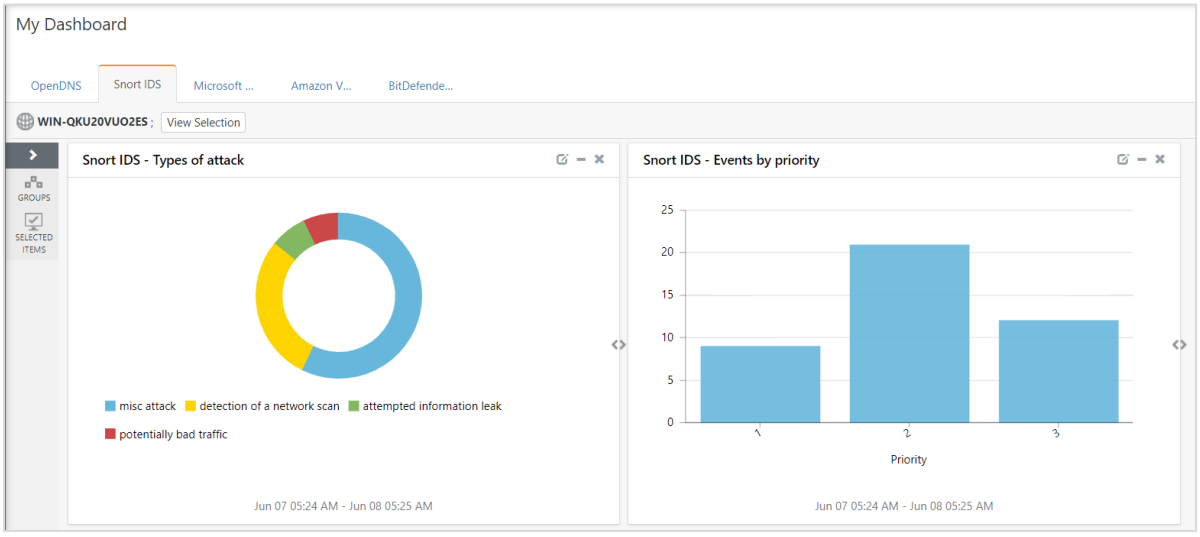


5.5 Dashboard

1. In the EventTracker web interface, go to **Home** > **My Dashboard**.



2. The **My Dashboard** interface displays the all the dashlets related to **Snort IDS.**



About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's managed cybersecurity platforms enable companies to deliver on both. Netsurion Managed Threat Protection combines our ISO-certified security operations center (SOC) with our own award-winning cybersecurity platform to better predict, prevent, detect, and respond to threats against your business. Netsurion Secure Edge Networking delivers our purpose-built edge networking platform with flexible managed services to multi-location businesses that need optimized network security, agility, resilience, and compliance for all branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn.

Contact Us

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

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)
EventTracker Enterprise for MSPs SOC: 877-333-1433 (Option 3)
EventTracker Essentials SOC: 877-333-1433 (Option 4)
EventTracker Software Support: 877-333-1433 (Option 5)
https://www.netsurion.com/eventtracker-support