

Integrate Malwarebytes Nebula (Cloud)

EventTracker v9.2 and later

Abstract

This guide provides instructions to retrieve the **Malwarebytes Nebula** events via syslog. Once the logs start coming-in into EventTracker, reports, dashboards, alerts and saved searches can be configured.

Scope

The configuration details in this guide are consistent with EventTracker version 9.2 or above and **Malwarebytes Nebula (cloud platform)**.

Audience

Administrators who are assigned the task to monitor **Malwarebytes Nebula** events using EventTracker.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2020 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

1. Overview	3
2. Prerequisites	3
3. Integrating Malwarebytes Nebula with EventTracker	3
3.1 Configuring Malwarebytes Nebula to forward logs to EventTracker	3
4. EventTracker Knowledge Packs.....	6
4.1 Saved Searches	6
4.2 Alerts	6
4.3 Flex Reports	6
4.4 Dashboards	7
5. Importing knowledge pack into EventTracker	9
5.1 Saved Searches	10
5.2 Alerts	11
5.3 Token Template	12
5.4 Flex Reports	13
5.5 Knowledge Objects	15
5.6 Dashboards	16
6. Verifying knowledge pack in EventTracker	18
6.1 Saved Searches	18
6.2 Alerts	18
6.3 Token Template	19
6.4 Flex Reports	19
6.5 Knowledge Objects	20
6.6 Dashboards	20

1. Overview

Malwarebytes Nebula is a cloud-based security platform for complete endpoint protection. It allows the user to manage products such as Malwarebytes Endpoint Protection, Malwarebytes Incident Response, Malwarebytes Endpoint Detection and Response from a single cloud-based user interface (UI).

EventTracker, when integrated with Malwarebytes Nebula, collects logs and creates detailed reports, alerts, dashboards, and saved searches. These attributes of EventTracker helps the user to view/receive critical and relevant information regarding security, operations and compliance.

Reports contain a detailed summary of security events such as malware detection, URL filtering, suspicious activity, potentially unwanted programs activities and modifications, and many more in column-value pair.

Alerts are triggered as soon as a critical event is received by EventTracker for Malwarebytes Nebula, such as malware detection, URL filtering, suspicious activity, potentially unwanted programs activities and modifications, etc.

Dashboards represent all the activities happening in Malwarebytes Nebula. These include event categories with cumulative log counts/percentage, events that are either blocked, quarantined, found, restored, or deleted, and timeline of occurrences of security related activities.

These attributes or configurations of EventTracker allows administrators to quickly take appropriate actions against any threat/adversaries trying to jeopardize an organization's normal operation.

2. Prerequisites

- EventTracker v9.2 and above should be installed.
- Administrative/root access to Malwarebytes Nebula Web UI.
- Syslog port (e.g. 514) should be allowed in firewall.
- EventTracker Manager public IP address.

3. Integrating Malwarebytes Nebula with EventTracker

3.1 Configuring Malwarebytes Nebula to forward logs to EventTracker

1. Login into your Malwarebytes Nebula Web UI using admin credentials.

2. Go to **Settings > Syslog Logging**.
3. Click **Add**. Promote one of your windows endpoints as the syslog communication endpoints.

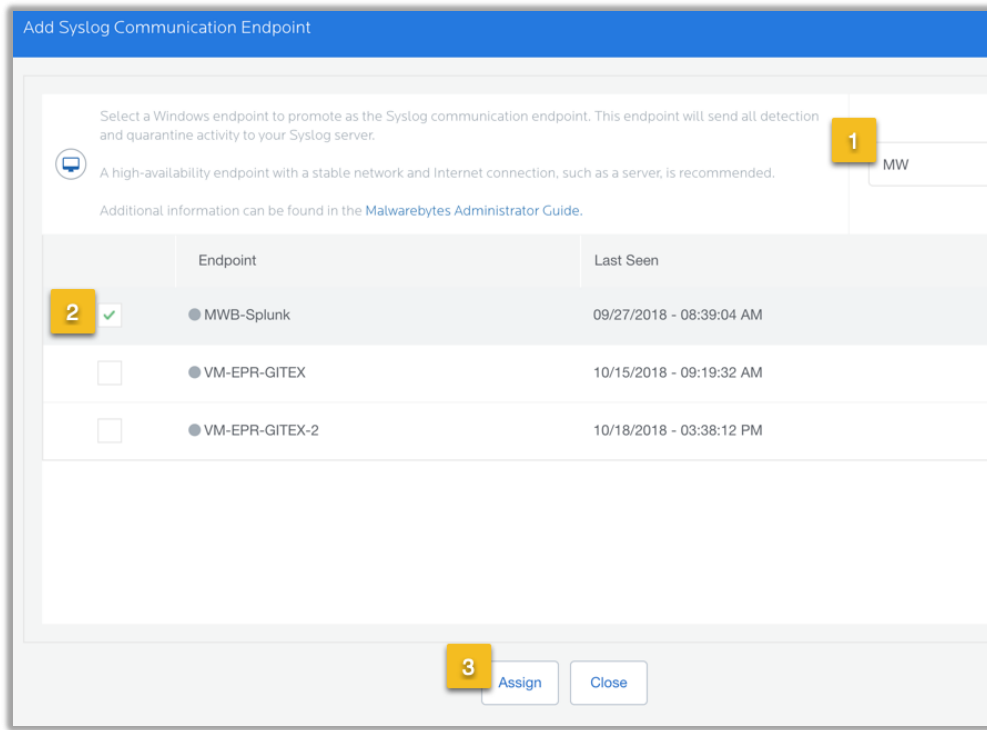


Figure 1

4. In the top-right corner, click **syslog settings**.
5. Fill in the following information, then click **Save**.
 - **IP Address/Host:** Public IP or hostname of your EventTracker manager.
 - **Port:** Port you have specified on your EventTracker manager. (e.g. 514)
 - **Protocol:** Select UDP protocol.
 - **Severity:** Choose a severity from the list. This determines the severity of all Malwarebytes events sent to syslog.
 - **Communication Interval (Minutes):** Determines how often the communication endpoint gathers syslog data from the Malwarebytes server. If the endpoint is unable to contact Malwarebytes, it buffers data from the last 24 hours. Data older than 24 hours is not sent to syslog.

Syslog Communication Settings

Specify your Syslog server settings below.

IP Address/Host:

Port (1-65535):

Protocol: TCP UDP

Severity (0-10):

Log Format: CEF

COMMUNICATION INTERVAL

Minutes (5-1440):

Figure 2

6. Navigate to **Endpoints**. Click on the syslog communication endpoint you assigned in Step 2.
7. In the **Agent Information** section, the SIEM version number displays. This confirms the SIEM plugin has activated on the endpoint.

malwarebytes Endpoints

Endpoint Properties:
Last Seen: 2019-11-01 12:05:41 PM

Overview

Agent Information

SIEM:	1.2.0.107
Operating System	

Figure 3

8. This confirms the syslog configuration of Malwarebytes Nebula.

4. EventTracker Knowledge Packs

4.1 Saved Searches

Saved searches are designed to quickly parse/filter logs and allow user to see only specific events related to.

- **Malwarebytes Nebula - Exploit events** – This category of saved search parses the events that are specific to exploit protection which guards against vulnerability exploits for installed applications.
- **Malwarebytes Nebula - Malware Events** – This category of saved search parses the events that are specific to Malware protection which protects endpoints against execution of malicious content.
- **Malwarebytes Nebula - PUM events** – This category of saved search parses events that contains potentially unwanted programs. In other word, these programs maybe dormant for a long time in an endpoint or that the program maybe identified as source of malicious behavior.
- **Malwarebytes Nebula - PUP events** – This category of saved search parses events that specifies if potentially unwanted modifications are treated as malware or ignored by Malwarebytes.
- **Malwarebytes Nebula - Ransomware events** – This category of saved search parses events that are related to ransomware activities. This includes both protection and rollback.
- **Malwarebytes Nebula - URL filtering and suspicious activity** – This category of saved search will parse web protection events which blocks access to and from known or suspicious Internet addresses. And this category also parses the events related to suspicious activity monitoring that watches process, registry, file system, and network activity on endpoints for malicious behavior.

4.2 Alerts

Alerts are triggered when an event received is identified as critical and requires immediate notification. such as,

- **Malwarebytes Nebula: Threat has been detected** – This alert is triggered as soon as EventTracker receives an event which is identified as suspicious activity, or malware activity, PUP or PUM discovery, etc.

4.3 Flex Reports

Reports are a detailed overview of any event occurring in Malwarebytes Nebula, represented in column-value format.

- Malwarebytes Nebula - Threat detection activities** – This report outlines the summary of events that are associated with malware detection, exploit detection, URL filtering, etc. It contains, device name, device IPv4 address, device MAC address, message, filePath, action taken upon the activity, etc.

LogTime	Category Name	Device hostname	Device IP address	Device MAC address	Device Product	Event Category	Event Class	Action Taken	Message	Severity
08/17/2020 04:33:14 PM	Website blocked	MININT-16Tjdoe	192.168.2.100	00:0C:29:33:C6:6A	Malwarebytes Endpoint Protection	Malware	Detection	quarantined	Website blocked\nProcess name: C:\Users\vmadmin\Desktop\test.exe	1
08/17/2020 04:33:14 PM	Website blocked	MININT-16Tjdoe	192.168.2.100	00:0C:29:33:C6:6A	Malwarebytes Endpoint Protection	PUP	Detection	blocked	Website blocked\nProcess name: C:\Users\vmadmin\Desktop\test.exe	1
08/17/2020 04:33:14 PM	Website blocked	MININT-16Tjdoe	192.168.2.100	00:0C:29:33:C6:6A	Malwarebytes Endpoint Protection	PUM	Detection	blocked	Website blocked\nProcess name: C:\Users\vmadmin\Desktop\test.exe	1
08/17/2020 04:33:14 PM	Website blocked	MININT-16Tjdoe	192.168.2.100	00:0C:29:33:C6:6A	Malwarebytes Endpoint Protection	Ransomware	Detection	blocked	Website blocked\nProcess name: C:\Users\vmadmin\Desktop\test.exe	1
08/17/2020 04:33:14 PM	Website blocked	MININT-16Tjdoe	192.168.2.100	00:0C:29:33:C6:6A	Malwarebytes Endpoint Protection	Exploit	Detection	deleted	Website blocked\nProcess name: C:\Users\vmadmin\Desktop\test.exe	1
08/17/2020 04:33:14 PM	Website blocked	MININT-16Tjdoe	192.168.2.100	00:0C:29:33:C6:6A	Malwarebytes Endpoint Protection	Suspicious Activity	Detection	restored	Website blocked\nProcess name: C:\Users\vmadmin\Desktop\test.exe	1

Figure 4

4.4 Dashboards

- Malwarebytes Nebula - Event Categories**

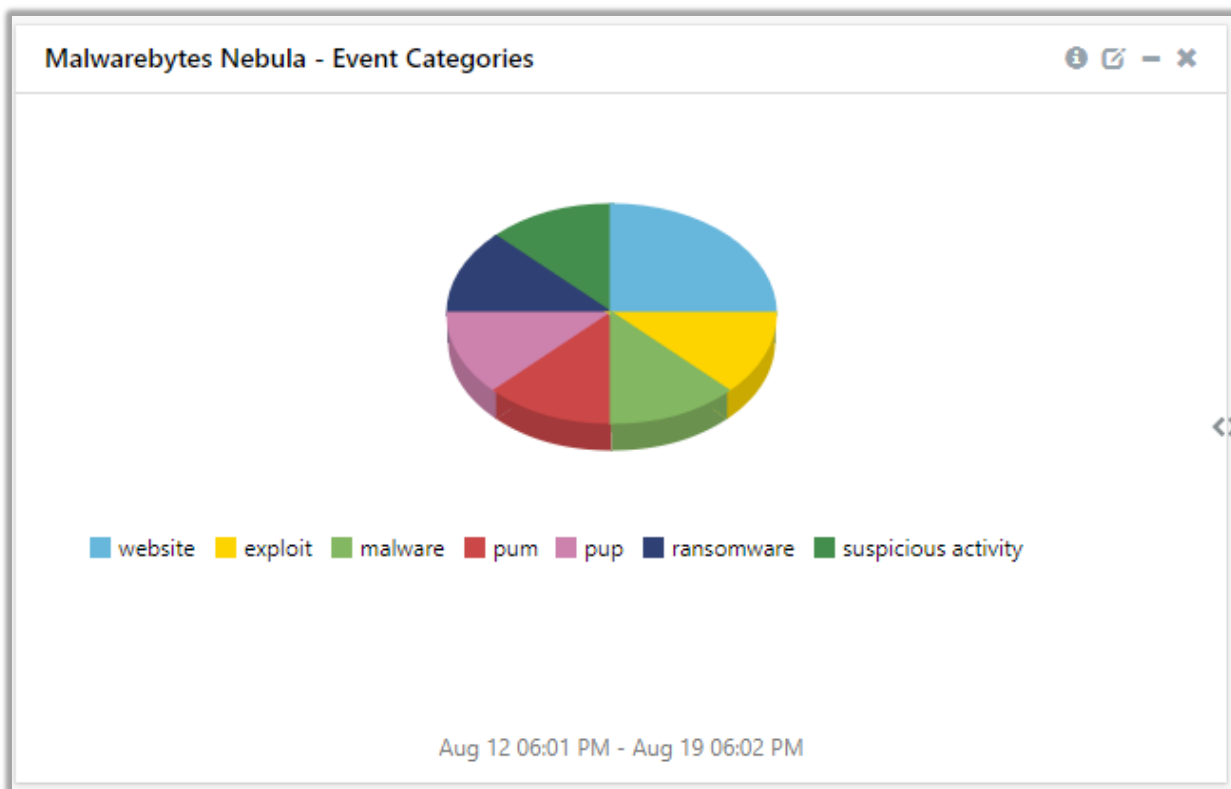


Figure 5

- **Malwarebytes Nebula - Threat timeline**

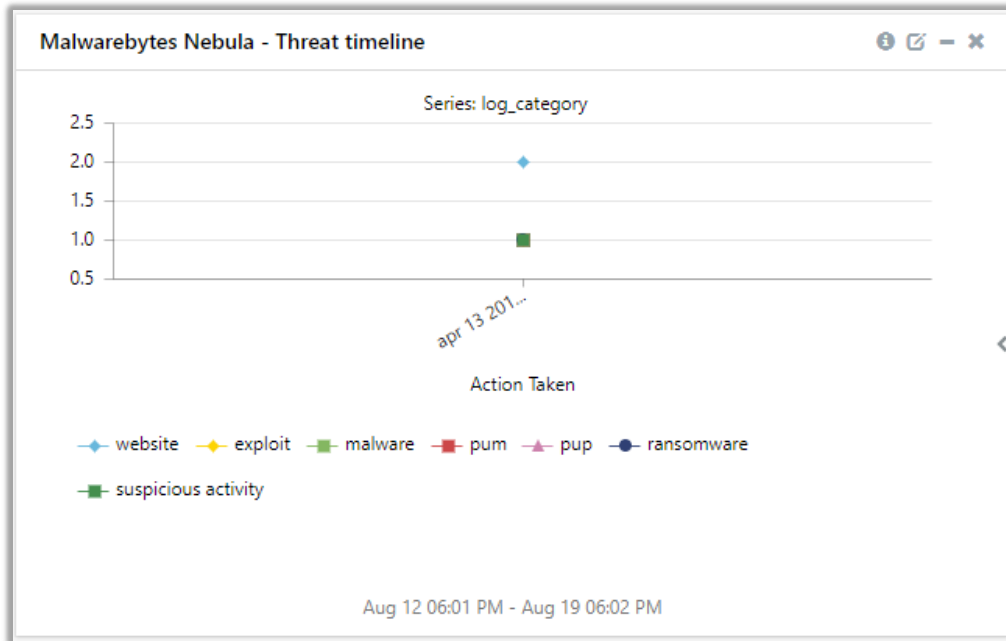


Figure 6

- **Malwarebytes Nebula - Action taken by event category**

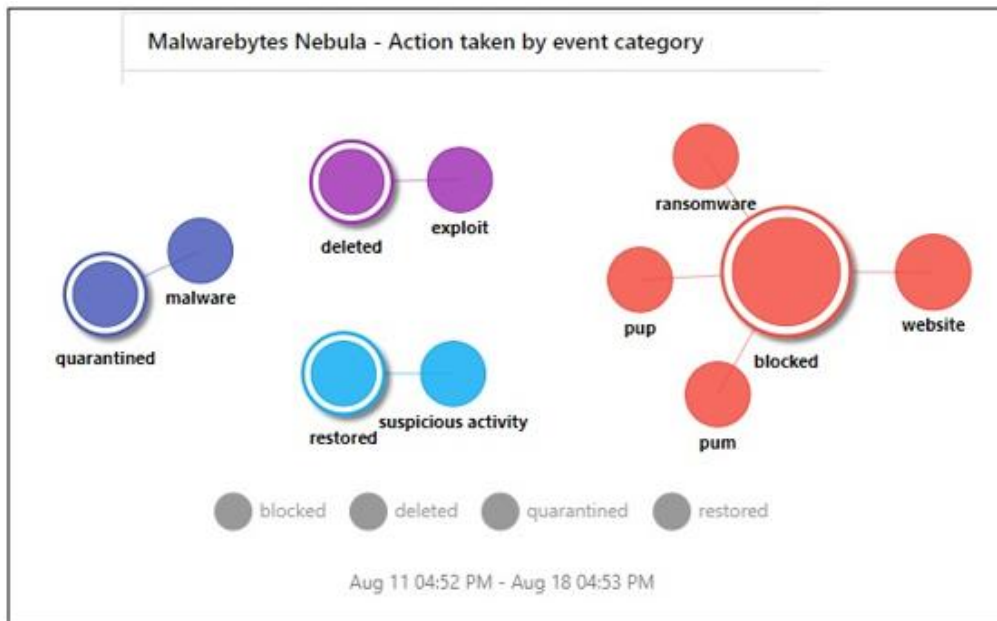


Figure 7

5. Importing knowledge pack into EventTracker

Getting Knowledge Packs

To get the knowledge packs, locate the knowledge pack folder. Follow the below steps.

1. Press “**Windows** + R”.
2. Now, type “%et_install_path%\Knowledge Packs” and press “**Enter**”.
(**Note** – If, not able to locate the file path as mentioned above, please contact [EventTracker support](#) to get the assistance).

NOTE: Import knowledge pack items in the following sequence:

- Categories
 - Alerts
 - Token Template
 - Flex Reports
 - Knowledge Objects
 - Dashboards
1. Launch the **EventTracker Control Panel**.
 2. Double click **Export-Import Utility**.

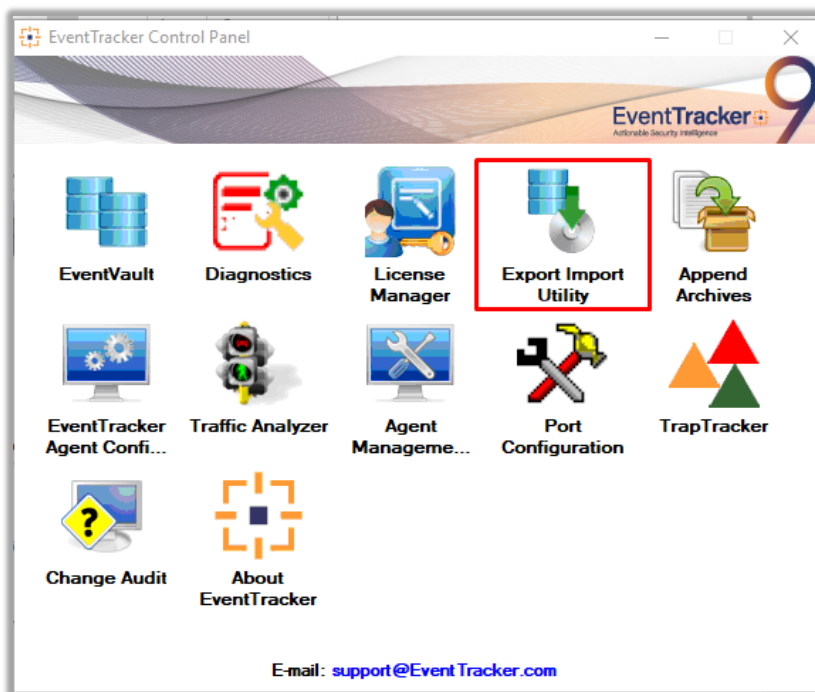


Figure 8

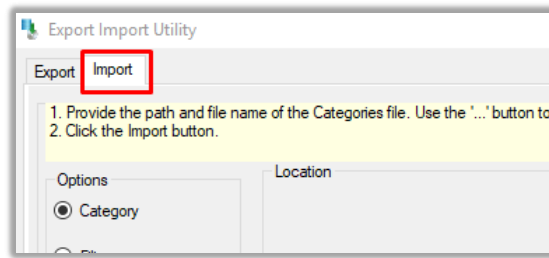


Figure 9

3. Click the **Import** tab.

5.1 Saved Searches

1. Once you have opened “**Export Import Utility**” via “**EventTracker Control Panel**”, click the **Category** option, and then click the browse button.
2. Navigate to the knowledge pack folder and select the file with extension “.iscat”, e.g. “**Categories_Malwarebytes Nebula.iscat**” and then click on the “**Import**” button:

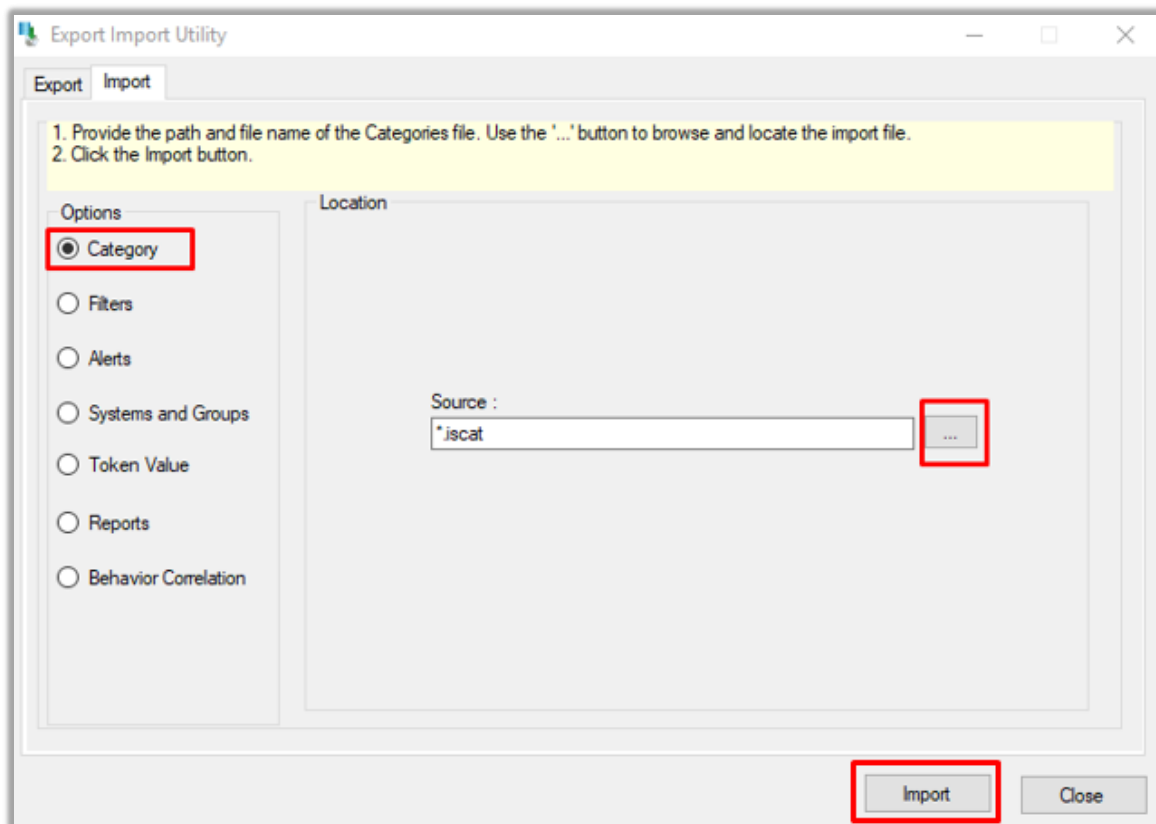


Figure 10

EventTracker displays a success message.

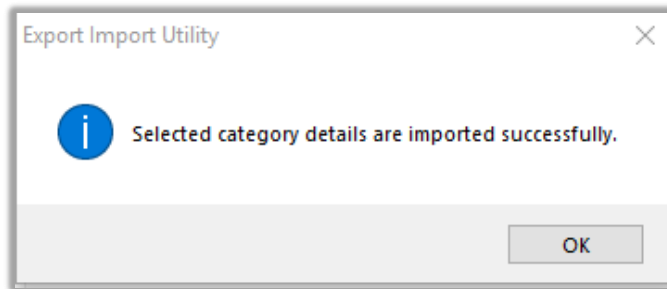



Figure 11

5.2 Alerts

1. Once you have opened "Export Import Utility" via "EventTracker Control Panel", click **Alert** option, and then click the browse button. 
2. Navigate to the knowledge pack folder and select the file with extension ".isalt", e.g. "Alerts_Malwarebytes Nebula.isalt" and then click on the "Import" button.

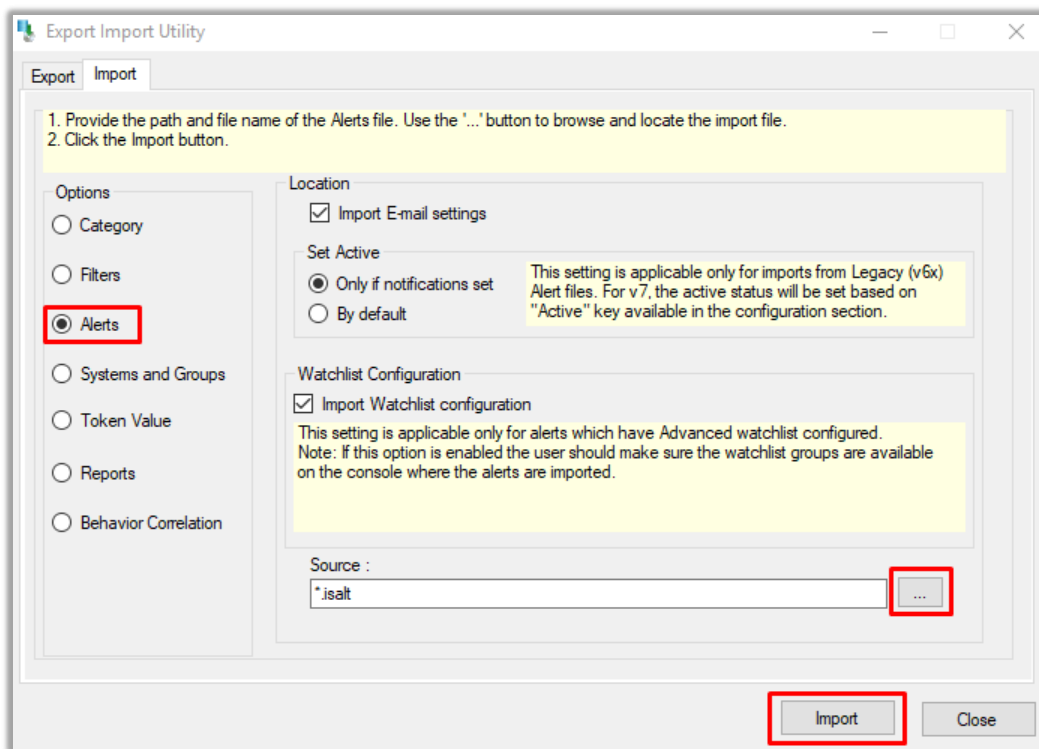


Figure 12

EventTracker displays a success message.

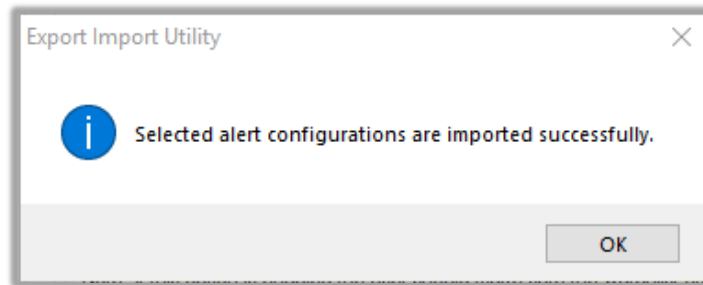


Figure 13

5.3 Token Template

For importing “**Token Template**”, navigate to **EventTracker manager** web interface.

1. Click **Parsing Rules** under the **Admin** option in the EventTracker manager web interface.

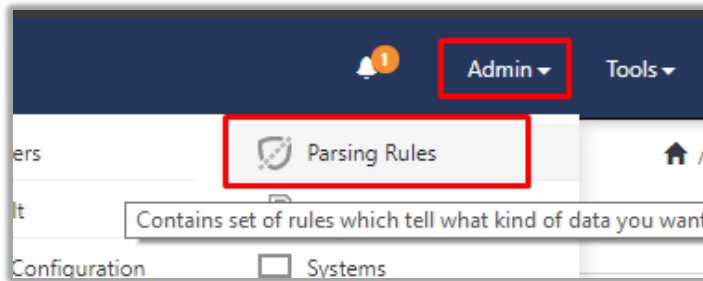


Figure 14

2. Next, click the “**Template**” tab and then click the “**Import Configuration**” button.

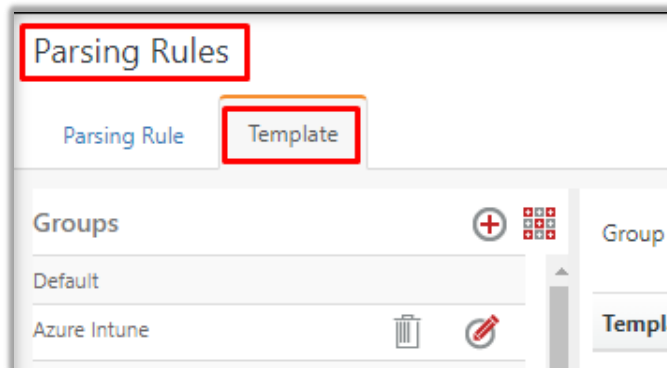


Figure 15

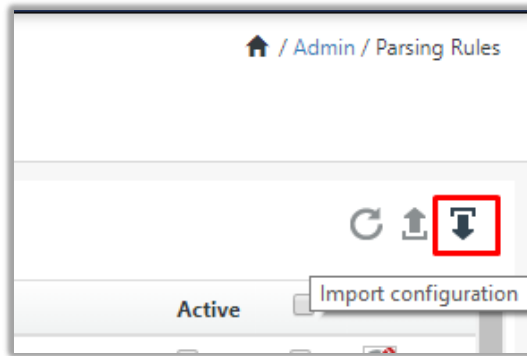


Figure 16

3. Click **“Browse”** and navigate to the knowledge packs folder (type **“%et_install_path%\Knowledge Packs”** in navigation bar) where **“.ettd”**, e.g. **“Templates_Malwarebytes Nebula.ettd”** file is located. Wait for few seconds, as templates will be loaded. Once you see the templates, click desired templates and click **“Import”** button:

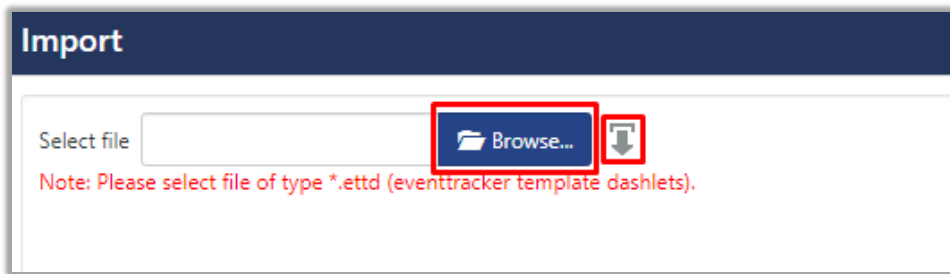


Figure 17

5.4 Flex Reports

1. In EventTracker control panel, select **“Export/ Import utility”** and select the **“Import tab”**. Then, click **Reports** option, and choose **“New (*.etcrx)”**:

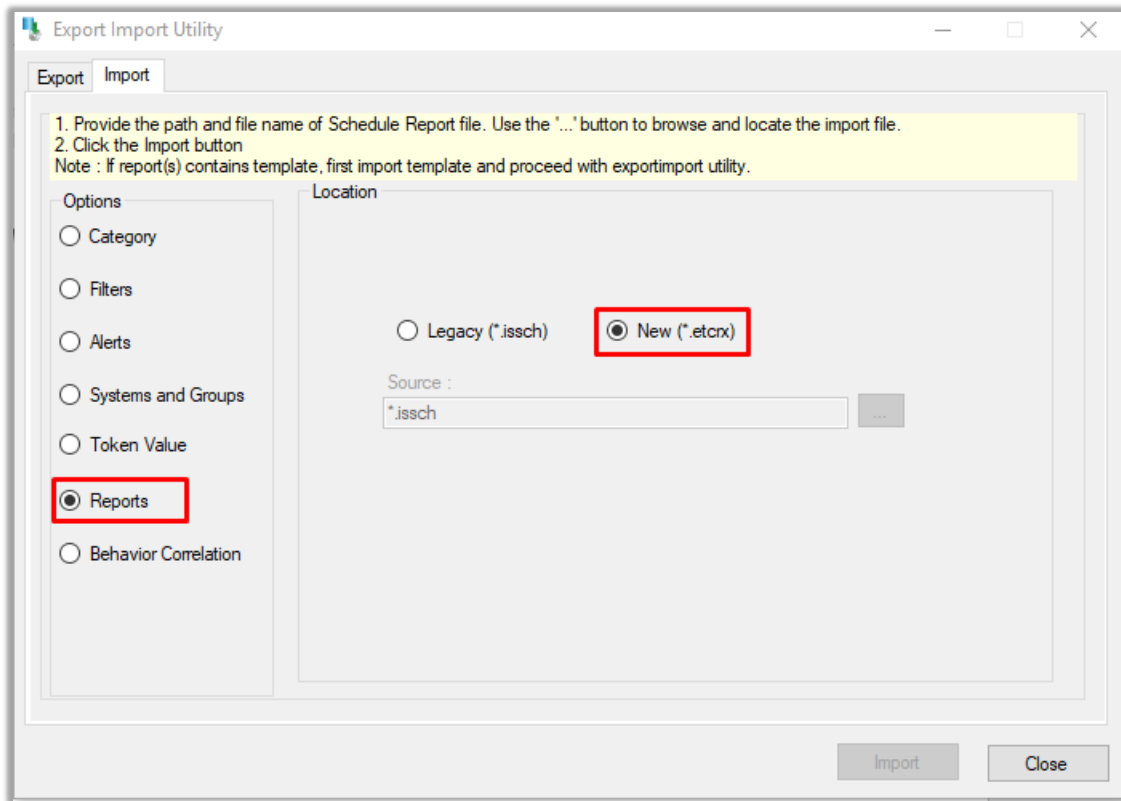


Figure 18

- Once you have selected **“New (*.etcrx)”**, a new pop-up window will appear. Click **“Select File”** button and navigate to knowledge pack folder and select file with extension **“.etcrx”**, e.g. **“Reports_Malwarebytes Nebula.etcrx”**.

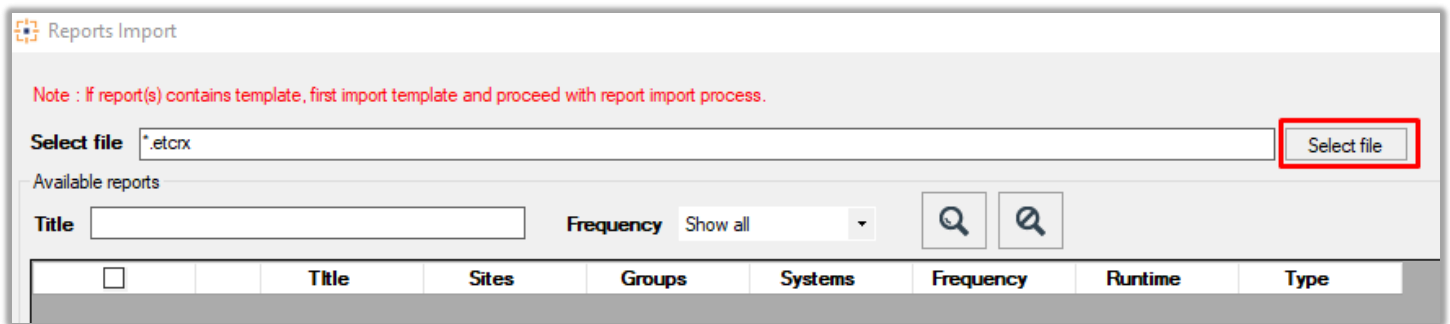



Figure 19

- Wait while reports are being populated in below tables. Now, select all the relevant reports and then click **Import**  button.

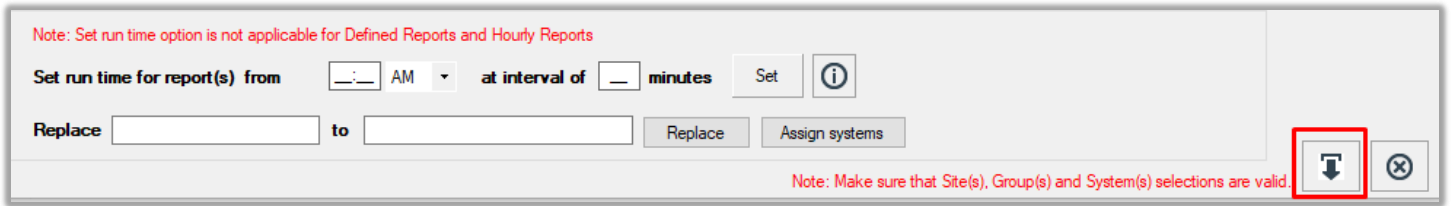


Figure 20

EventTracker displays a success message:

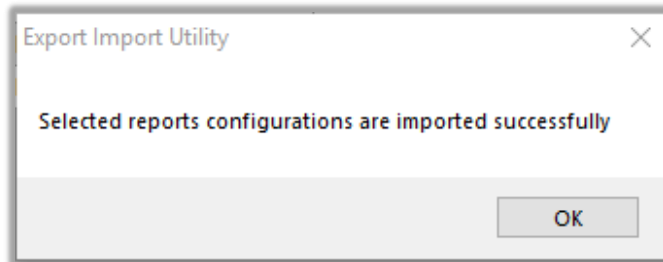


Figure 21

5.5 Knowledge Objects

1. Click **Knowledge objects** under the **Admin** option in the EventTracker manager web interface.

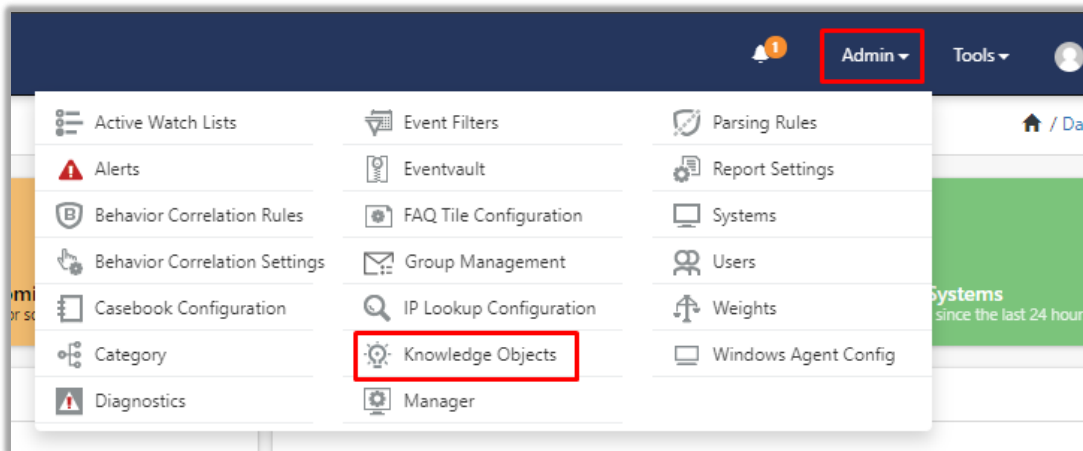


Figure 22

2. Next, click the **"import object"** icon.

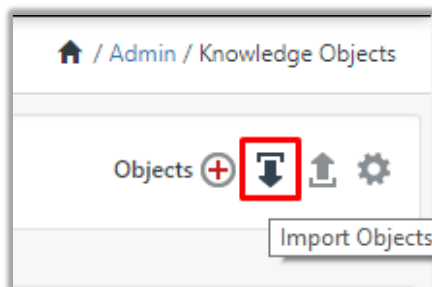


Figure 23

3. A pop-up box will appear, click “**Browse**” in that and navigate to knowledge packs folder (type “%et_install_path%\Knowledge Packs” in navigation bar) with the extension “.etko”, e.g. “KO_Malwarebytes Nebula.etko” and then click “**Upload**”.



Figure 24

4. Wait while EventTracker populates all the relevant knowledge objects. Once the objects are displayed, select the required ones and click “**Import**” button.

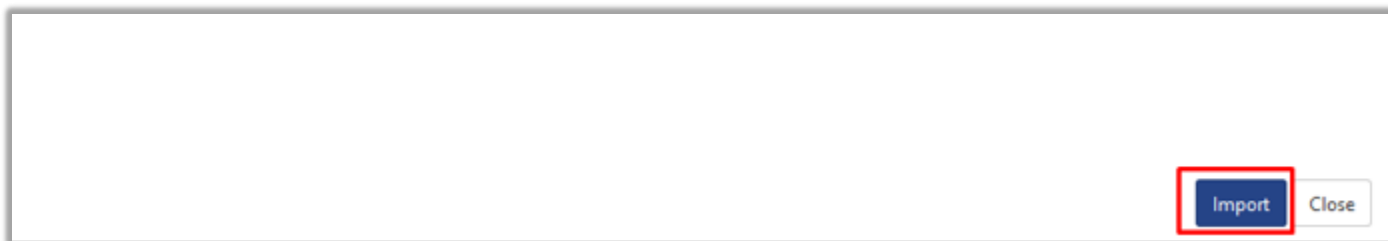


Figure 25

5.6 Dashboards

1. Login to **EventTracker manager web interface**.
2. Navigate to **Dashboard → My Dashboard**.
3. In “My Dashboard”, Click **Import**.

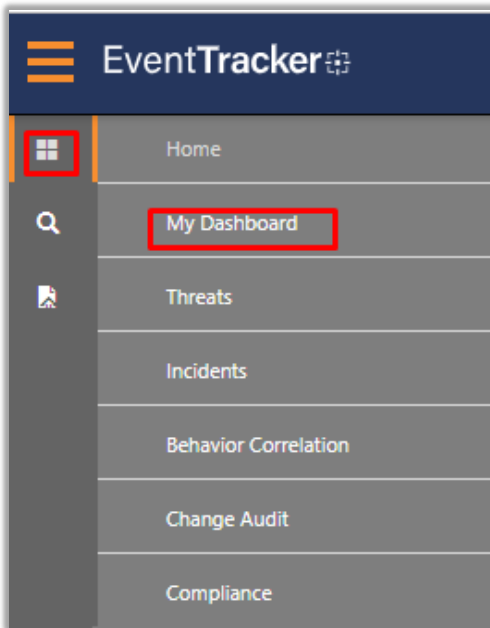


Figure 26

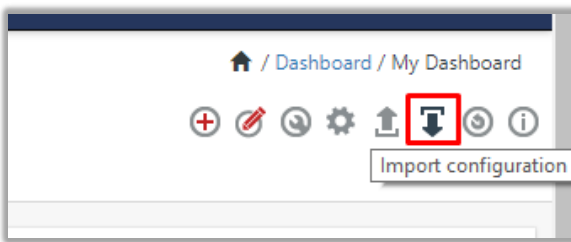


Figure 27

4. Select the **browse** button and navigate to knowledge pack folder (type “%et_install_path%\Knowledge Packs” in navigation bar) where “.etwd”, e.g. “Dashboards_Malwarebytes Nebula.etwd” is saved and click on “**Upload**” button.
5. Wait while EventTracker populates all the available dashboards. Now, choose “**Select All**” and click on “**Import**” Button.

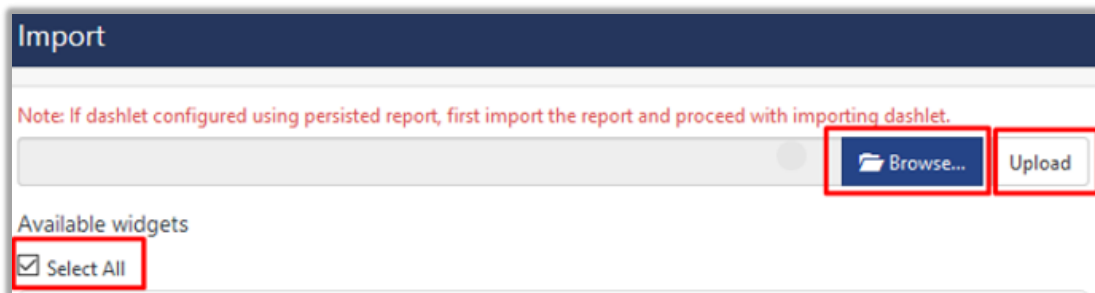


Figure 28



Figure 29

6. Verifying knowledge pack in EventTracker

6.1 Saved Searches

1. Login to **EventTracker manager web interface**.
2. Click **Admin** dropdown, and then click **Categories**.
3. In **Category Tree** to view imported categories, scroll down and expand “**Malwarebytes Nebula**” group folder to view the imported categories.

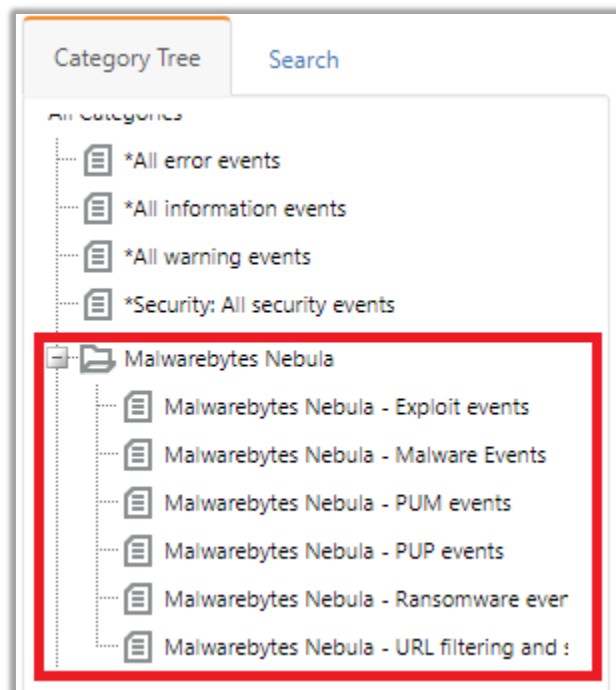


Figure 30

6.2 Alerts

1. In the **EventTracker manager** web interface, click the **Admin** dropdown, and then click **Alerts**.

- In search box enter “<search criteria> e.g. “**Malwarebytes Nebula**” and then click the **Search** button. EventTracker displays an alert related to “**Malwarebytes Nebula**”:

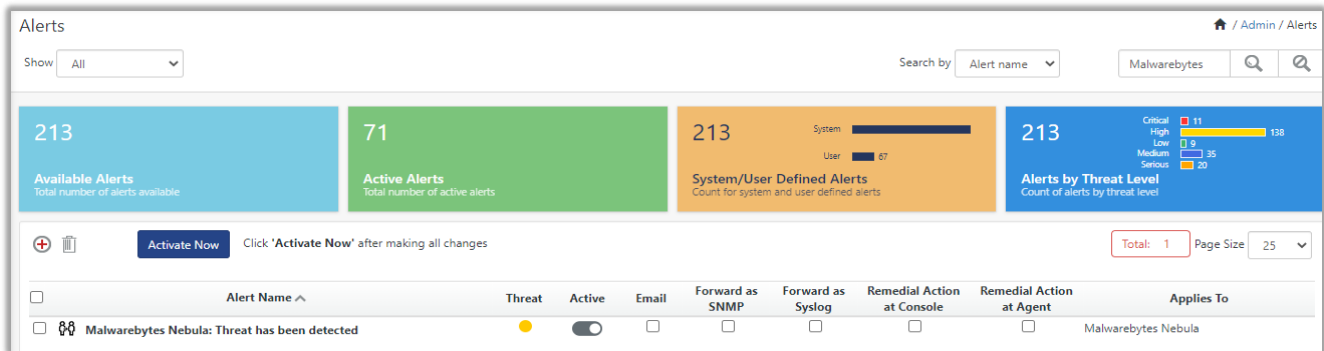


Figure 31

6.3 Token Template

- In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Parsing Rules**.
- In the **Template** tab, click on the “<product name/ report group name>” e.g. “**Malwarebytes Nebula**” group folder to view the imported templates.

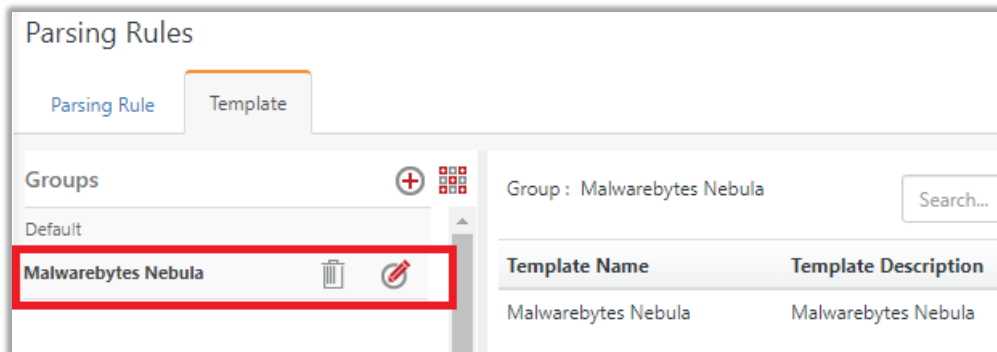


Figure 32

6.4 Flex Reports

- In the **EventTracker** web interface, click the **Reports** menu, and then select the **Report Configuration**.

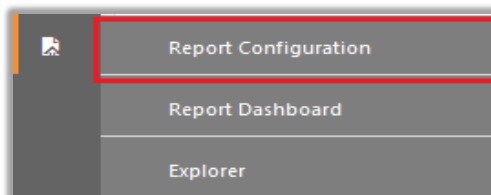


Figure 33

2. In **Reports Configuration** pane, select the **Defined** option.
3. Click on the **“Malwarebytes Nebula”** group folder to view the imported reports.

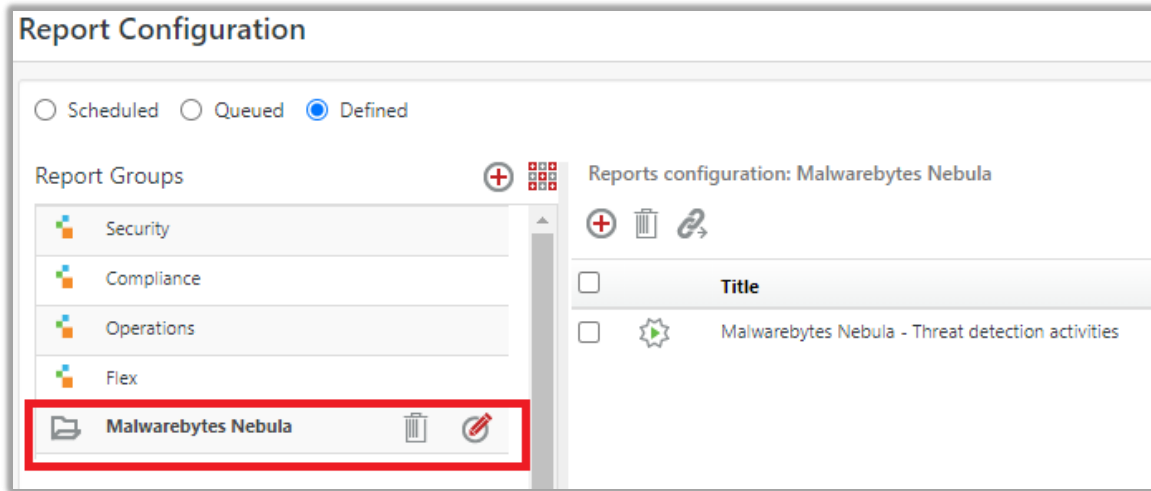


Figure 34

6.5 Knowledge Objects

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Knowledge Objects**.
2. In the **Knowledge Object** tree, expand the **“Malwarebytes Nebula”** group folder to view the imported Knowledge objects.

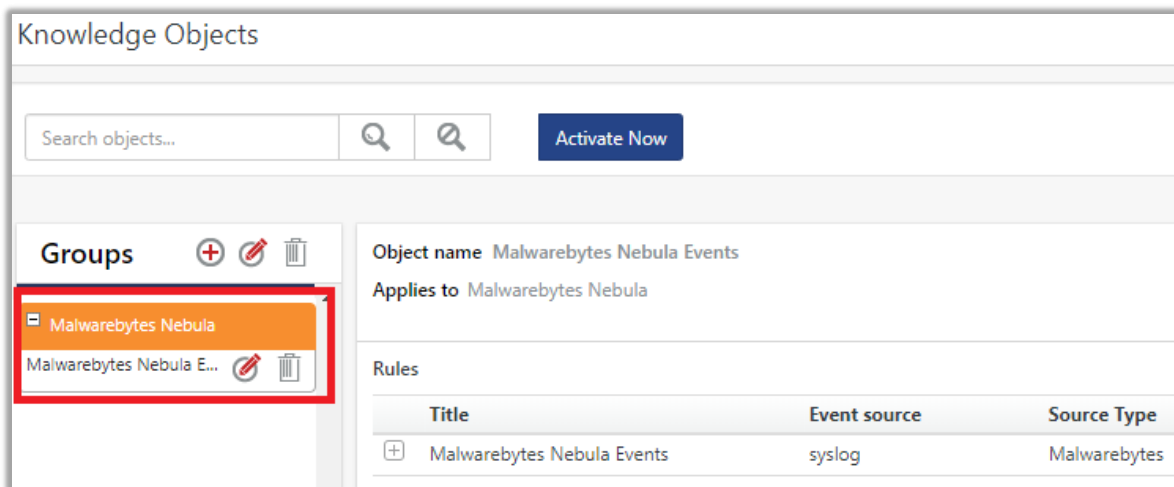


Figure 35

6.6 Dashboards

1. In the EventTracker web interface, Click on Home Button  and select **“My Dashboard”**.

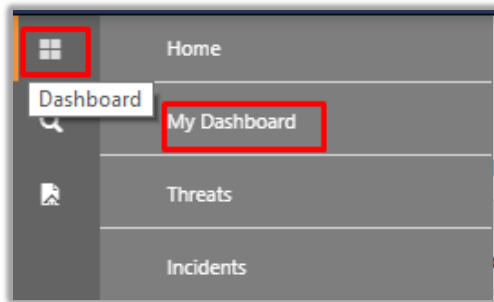


Figure 36

- 2. Select “Customize daslets” button and type “Malwarebytes Nebula” in the search bar.

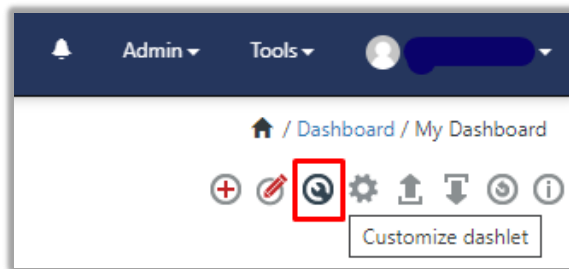


Figure 37

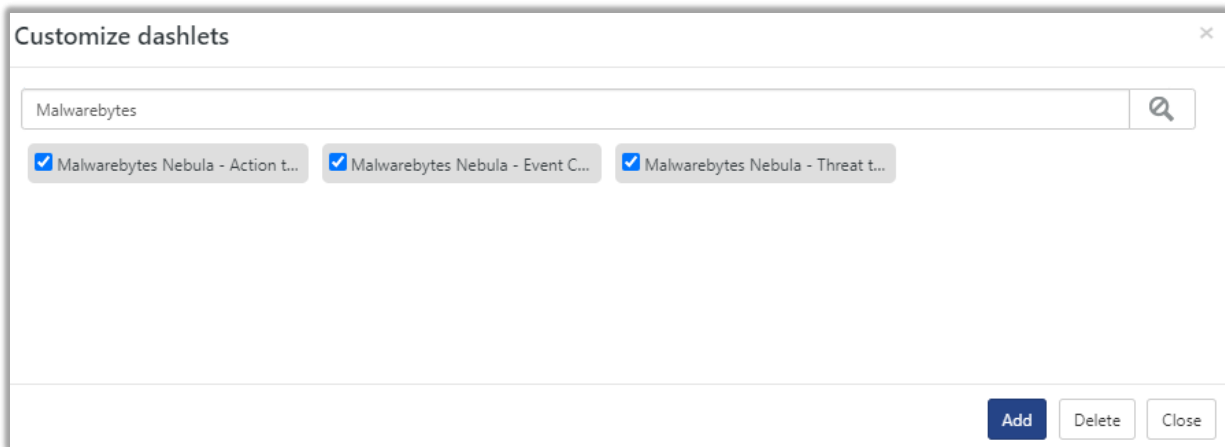


Figure 38