

# Integrate Windows Defender

EventTracker v9.x and above

## Abstract

This guide provides instructions to retrieve Windows Defender event logs and integrate it with EventTracker. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor Windows Defender.

## Audience

The configurations detailed in this guide are consistent with EventTracker version v9.x or above and Windows Defender for Windows 10 and Windows Server 2016.

*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.*

*© 2019 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

## Table of Contents

Abstract .....	1
Audience .....	1
Overview .....	3
Prerequisites .....	3
Configuring Windows Defender to forward the log to EventTracker .....	3
Configuring EventTracker Event Filter .....	3
EventTracker Knowledge Pack .....	6
Alerts .....	6
Flex Reports .....	7
Dashboards .....	11
Importing Windows Defender knowledge pack into EventTracker .....	16
Alerts .....	17
Parsing Rule .....	17
Flex Reports .....	18
Dashboard .....	21
Verifying Windows Defender knowledge pack in EventTracker .....	22
Alerts .....	22
Parsing Rule .....	23
Flex Reports .....	24
Category .....	24
Dashboard .....	25

## Overview

EventTracker collects the event logs delivered from Windows Defender and filters them out to get some critical event types for creating reports, dashboard, and alerts. Among the event types, we are considering: Malware detected, Suspicious behavior detected, Windows defender configuration changes, Action taken on threats, Engine updates, Antivirus real-time protection disabled, Scan failed, etc.

## Prerequisites

- EventTracker agent must be installed in a host system/server.
- **ET91U19-031.exe** update must be installed before configuring this KP-item, in EventTracker manager.

## Configuring Windows Defender to forward the log to EventTracker

### Configuring EventTracker Event Filter

1. Follow the file path of EventTracker Agent configuration –  
**C:\Program Files (x86)\Prism Microsystems\EventTracker\Agent**
2. Double click on “**etaconfig**” application to launch “**EventTracker Agent Configuration**”.

Name	Date modified	Type	Size
Cache	5/22/2019 1:13 PM	File folder	
DLA	7/29/2019 5:18 PM	File folder	
MessageDll	1/14/2019 6:10 PM	File folder	
OtherFiles	1/14/2019 6:10 PM	File folder	
Script	1/14/2019 6:09 PM	File folder	
Symantec EP Cloud	7/8/2019 1:05 PM	File folder	
_etaconfigBase	7/29/2019 2:26 PM	Configuration sett...	78 KB
certClientLog	7/29/2019 1:04 PM	Text Document	238 KB
CertLicense.dll	3/15/2019 4:44 PM	Application extens...	1,036 KB
ClientCertificate.dll	1/4/2019 8:27 AM	Application extens...	145 KB
Data Encryption.dll	1/4/2019 8:27 AM	Application extens...	83 KB
DBPopulation	1/4/2019 8:27 AM	Application	46 KB
etaconfig	1/4/2019 8:27 AM	Application	2,372 KB
etaconfig.exe.manifest	3/16/2017 10:11 AM	MANIFEST File	3 KB
etaconfig	7/29/2019 2:29 PM	Configuration sett...	78 KB
EtaDataDispatcher	1/4/2019 8:27 AM	Application	627 KB
etagent.dll	4/8/2019 8:21 PM	Application extens...	1,745 KB
etagent	3/22/2019 6:24 PM	Application	527 KB
etalog	7/29/2019 5:24 PM	Text Document	2,934 KB
etalog.txt.bak.1	7/29/2019 12:15 PM	1 File	5,124 KB
etalog.txt.bak.2	7/26/2019 12:07 PM	2 File	5,124 KB

Figure 1

3. Navigate to **Event Filters>Filter Exception**.

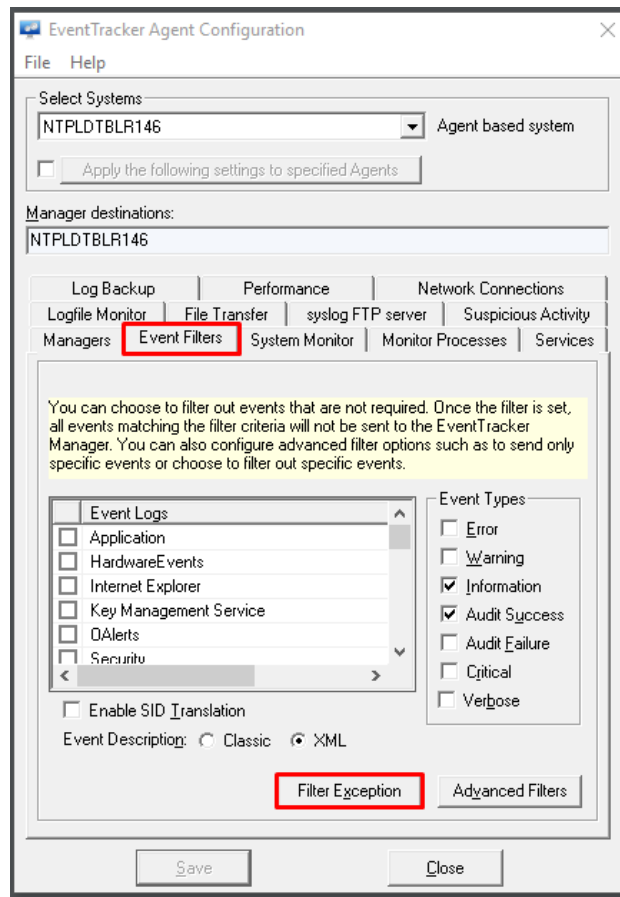


Figure 2

4. Click **New** and compose **Event Details**.

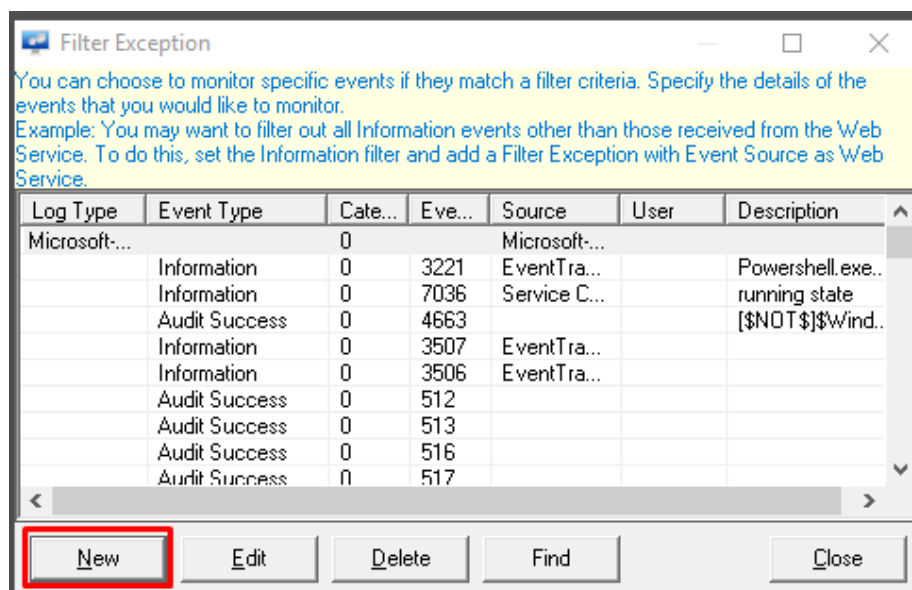


Figure 3

5. Select **Log Type Microsoft-Windows-Windows Defender/Operational**, match it in source **Microsoft-Windows-Windows Defender** and click on **OK**.

New Event Details

Event Details (empty field implies all matches)

Log Type : Microsoft-Windows-Windows Defender/Operational

Event Type : Information

Event ID :

Category :

Match in User :

Match in Source : Microsoft-Windows-Windows Defender

Match in Event Descr :

"Match in Event Descr", "Match in User" and "Match in Source" field can take multiple strings separated with && or ||. && stands for AND condition. || stands for OR condition. For negating the result of match operation, prefix the string with "[NOT\$]". If there are multiple strings, then the result of the whole expression is negated. Only one "[NOT\$]" should be used in the string.  
 Example:  
 The string "[NOT\$]Logon Type: 4||Logon Type: 5" will match all events that DO NOT contain "Logon Type: 4" or "Logon Type: 5" in the description.  
[For more information click here.](#)

OK Cancel

Figure 4

6. Click **Close** and save to apply the changes.

Filter Exception

You can choose to monitor specific events if they match a filter criteria. Specify the details of the events that you would like to monitor.  
 Example: You may want to filter out all Information events other than those received from the Web Service. To do this, set the Information filter and add a Filter Exception with Event Source as Web Service.

Log Type	Event Type	Cate...	Eve...	Source	User	Description
Microsoft...		0		Microsoft...		
	Information	0	3221	EventTra...		Powershell.exe..
	Information	0	7036	Service C...		running state
	Audit Success	0	4663			[NOT\$]\$Wind..
	Information	0	3507	EventTra...		
	Information	0	3506	EventTra...		
	Audit Success	0	512			
	Audit Success	0	513			
	Audit Success	0	516			
	Audit Success	0	517			

New Edit Delete Find Close

Figure 5

7. Click **Save** and close **EventTracker Agent configuration**.

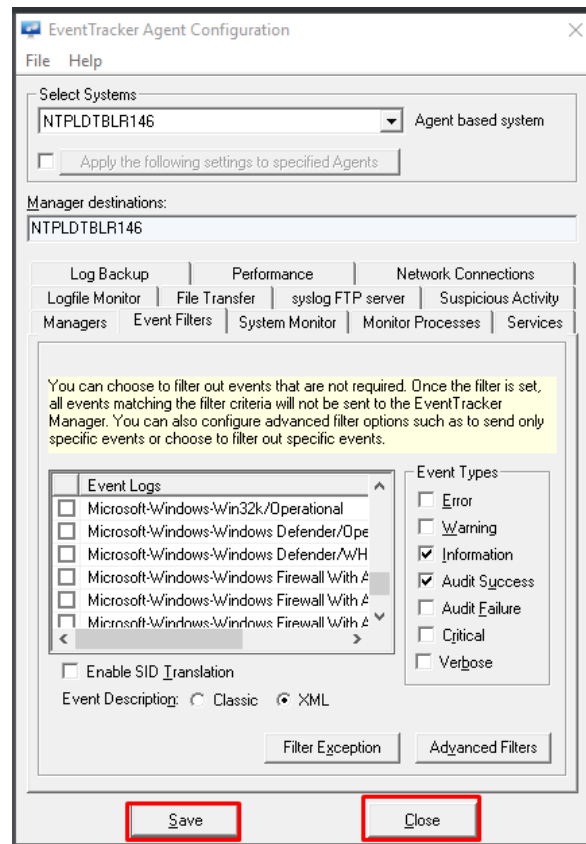


Figure 6

## EventTracker Knowledge Pack

Once logs are received by EventTracker manager, Knowledge Packs can be configured into EventTracker. The following Knowledge Packs are available in EventTracker to support Windows Defender.

### Alerts

- **Windows Defender: Action taken on malware failed** – This alert is generated when Windows Defender antivirus has encountered an error when acting on malware or other potentially unwanted software.
- **Windows Defender: Antivirus scanning disabled** – This alert is generated when Windows Defender antivirus scanning for virus's feature is disabled.
- **Windows Defender: Definition update failed** – This alert is generated when Windows Defender antivirus has encountered an error while trying to use dynamic signature service or update, load signatures and attempt reverting to a known-good set of signatures.
- **Windows Defender: Deletion of malware from quarantine failed** – This alert is generated when Windows Defender antivirus has encountered an error while trying to delete an item from quarantine.

- **Windows Defender: Engine update failed** – This alert is generated when Windows Defender antivirus has encountered an error while trying to update the engine, but could not load the anti-malware engine and update the platform.
- **Windows Defender: Malware and unwanted software scanning disabled** – This alert is generated when Windows Defender antivirus scanning for malware and other potentially unwanted software is disabled.
- **Windows Defender: Malware detected** – This alert is generated when the anti-malware engine finds malware or other potentially unwanted software.
- **Windows Defender: Real-time protection disabled** – This alert is generated when Windows Defender antivirus real-time protection scanning for malware and other potentially unwanted software is disabled.
- **Windows Defender: Scan failed** – This alert is generated when an anti-malware scan fails.
- **Windows Defender: Scan failed before finished** – This alert is generated when an anti-malware scan is stopped before it finishes.
- **Windows Defender: Suspicious behavior detected** - This alert is generated when Windows Defender antivirus detects suspicious behavior.

## Flex Reports

- **Windows Defender - Action taken on threats** - This report provides information related to the action taken by the Windows Defender on threats detected on the system. If the action fails, then this report provides the details for the reason.

Windows Defender- Action taken on threats

LogTime	Computer Name	Action Name	Actions String	Category Name	Error Description	Execution Name	FWLink	Origin Name	Path	Process Name	Severity Name	Signature Version	Source Name	Threat Name	User
07/26/2019 07:20:38 PM	Desktop-WKS	%%887	No additional actions required	Trojan	The operation unsuccessful	%%813	http://go.microsoft.com/fwlink/?linkid=3702	%%84	containerfile:\10.0.1.10share\Malware_Fore	C:\Windows\explorer.exe	Severe	1.295.1352.0	%%818	Trojan: Win32/Bagsult	John

Figure 7



**Sample Logs:**

```

action                +- %%887
add_info4             +- No additional actions required
add_info5             +- %%813
add_info6             +- %%846
application_name       +- C:\Windows\explorer.exe
category              +- Trojan
device_version         +- 4.18.1904.1
event_computer        +- NTP\DTBLR48@Defender
event_description      Id : 1117
                      Windows defender has taken action to protect this machine from malware or other
                      For more information please see the following:
                      %13
                      Name: SYSTEM2
                      ID: 2147694408
                      Severity: High
                      Category: Trojan
                      Path: C:\Folder\0.0.1.10\share\Malware_For_Demo\Server.exe->(VFS:svchost.exe
                      Detection Origin: Network share
                      Detection Type: Concrete
                      Detection Source: Real-Time Protection
                      User: Adam
                      Process Name: C:\Windows\explorer.exe
                      Action: Block
                      Action Status: %38
                      Error Code: 0x00000000
                      Error description: %34
                      Signature Version: AV: 1.217.2054.0
                      Engine Version: AM: 1.1.12603.0

```

Figure 8

- **Windows Defender - Configuration changes** - This report provides information related to changes happened on Windows Defender features like enabling/disabling of real-time protection, changes in the configuration of a defender.

**Windows Defender - Configuration changes**

LogTime	Computer	Product Version	Old Value	New Value
07/26/2019 12:19:07 PM	Desktop-wks1	4.18.1904.1	HKLM\SOFTWARE\Microsoft\Windows Defender\MpEngine\MpCampRing = 0x21	HKLM\SOFTWARE\Microsoft\Windows Defender\MpEngine\MpCampRing = 0x2
07/26/2019 04:35:40 PM	Dessktop-NYC	4.18.1904.1	HKLM\SOFTWARE\Microsoft\Windows Defender\MpEngine\MpCampRing = 0x21	HKLM\SOFTWARE\Microsoft\Windows Defender\MpEngine\MpCampRing = 0x2

Figure 9

**Sample Logs:**

```

device_version      +- 4.18.1904.1
event_computer      +- NTPLDTBLR48@Defender
event_description    Id : 5007
                    Windows defender Configuration has changed. If this is an unexpected event you sh
                    Old value: %3
                    New value: %4
                    <EventData> <Data Name="Product Name">%%827</Data> <Data Name="Produ
                    neMpCampRing = 0x21</Data> <Data Name="New Value">HKLMSOFTWAREMicr
event_id            +- 5007
event_log_type       +- Application
event_source         +- Microsoft-Windows-Windows Defender
event_type           +- Information
event_user_domain    +- NA
event_user_name       +- NA
log_source           +- Windows Defender
new_value            +- HKLMSOFTWAREMicrosoftWindows DefenderMpEngineMpCampRing = 0x2
object_name          +- %%827
old_value            +- HKLMSOFTWAREMicrosoftWindows DefenderMpEngineMpCampRing = 0x21
tags                 +- Windows Defender

```

Figure 10

- **Windows Defender - Suspicious behavior detected** – This report provides information when defender detects some suspicious behavior in windows machine like usage of malicious macro, changes in the registry which can compromise the system.

**Windows Defender - Suspicious behavior detected**

LogTime	Computer	User	Threat Name	Category Name	Path Found	Process Name	Target File Name
07/26/2019 12:19:07 PM	Contoso-wks01	espnet\bob.tulley	RS4_WinATP-Intro-Invoice.docm	Document Exploit	C:\Users\bob.tulley\Downloa ds\RS4_WinATP-Intro-	chrome.exe	powershell.exe
07/29/2019 04:42:39 PM	Contoso-wksSRV	espnet\bob.tulley	VBS/Agent.NSW/tr.dldr	Adware	C:\Users\bob.tulley\Downloa ds\RS4_WinATP-Intro-	chrome.exe	powershell.exe

Figure 11

**Sample Logs:**

<i>addl_info</i>	+ - Local computer
<i>addl_info2</i>	+ - S-1-5
<i>addl_info3</i>	+ - S-1-5-21-4133203243-3579683129-339516029-1001
<i>application_name</i>	+ - chrome.exe
<i>category</i>	+ - Document Exploit
<i>dest_path</i>	+ - powershell.exe
<i>device_version</i>	+ - 4.9.10586.0
<i>event_computer</i>	+ - NTPLDTBLR48@Defender
<i>event_description</i>	Id : 1015 Windows defender Antivirus has detected a suspicious behavior. Name: RS4_WinATP-Intro-Invoice.docm ID: 12376943403 Severity: Medium Category: Document Exploit Path Found: C:\Users\bob.tulley\Downloads\RS4_WinATP-Intro-Invoice.docm Detection Origin: Local computer Detection Type: Heuristics Detection Source: EDR Status: New User: espnet\bob.tulley Process Name: chrome.exe Signature ID: S-1-5-21-4133203243-3579683129-339516029-1001 Signature Version: 1.299.315.0 Engine Version: 1.1.16200.1 Fidelity Label: %32 Target File Name: powershell.exe

Figure 12

- **Windows Defender - Threat detected** - This report provides information related to threat detected in the windows machine. It provides information about the threat name, category, what actions are taken by a defender on that threat.

**Windows Defender - Threat detected**

LogTime	Computer	User	Threat Name	Category Name	File Path
07/26/2019 12:19:07 PM	Contoso-wks01	John	Trojan:Win32/Bagsulrfrn	Trojan	containerfile:_\10.0.1.10\share\Malware_For_Demo\REAL_BAD_Malz2\Server.exe;file:_\10.0.1.10\share\Malware_For_Demo\REAL_BAD_Malz2\Server.exe;file:_\10.0.1.10\share\Malware_For_Demo\REAL_BAD_Malz2\Server.exe- &gt;(VFS:svchost.exe)

Figure 13

**Sample Logs:**

event_log_type	+ Application
event_type	+ Information
event_id	+ 1006
event_source	+ Microsoft-Windows-Windows Defender
event_user_domain	+ NA
event_computer	+ NTPLDTBLR48@Defender
event_user_name	+ NA
event_description	<p>Id : 1006</p> <p>Windows defender has detected malware or other potentially unwanted software.</p> <p>For more information please see the following:</p> <p><a href="http://go.microsoft.com/fwlink/?linkid=37020&amp;name=Trojan:Win32/Bagsulrhn&amp;th">http://go.microsoft.com/fwlink/?linkid=37020&amp;name=Trojan:Win32/Bagsulrhn&amp;th</a></p> <p>Name: Trojan:Win32/Bagsulrhn</p> <p>ID: 2147694434</p> <p>Severity: Severe</p> <p>Category: Trojan</p> <p>Path Found: containerfile:\10.0.1.10\share\Malware_For_Demo\REAL_BAD_Mal2\or_Demo\REAL_BAD_Mal2\Server.exe-&gt;(VFS:svchost.exe)</p> <p>Detection Type: Concrete</p> <p>Detection Source: Real-Time Protection</p> <p>Status: %20</p> <p>User: Mike</p> <p>Process Name: C:\Windows\explorer.exe</p> <p>Signature Version: AV: 1.217.2054.0, AS: 1.217.2054.0, NIS: 115.8.0.0</p> <p>Engine Version: AM: 1.1.12603.0, NIS: 2.1.11804.0</p>

Figure 14

## Dashboards

- **Windows Defender - Threat detected by name.**

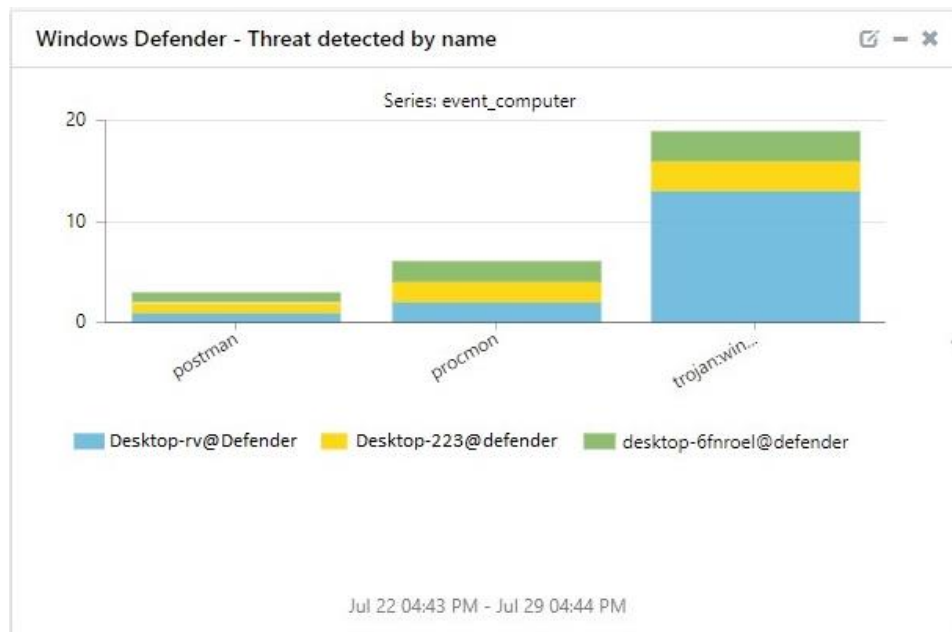


Figure 15

- **Windows Defender - Threat detected by system.**

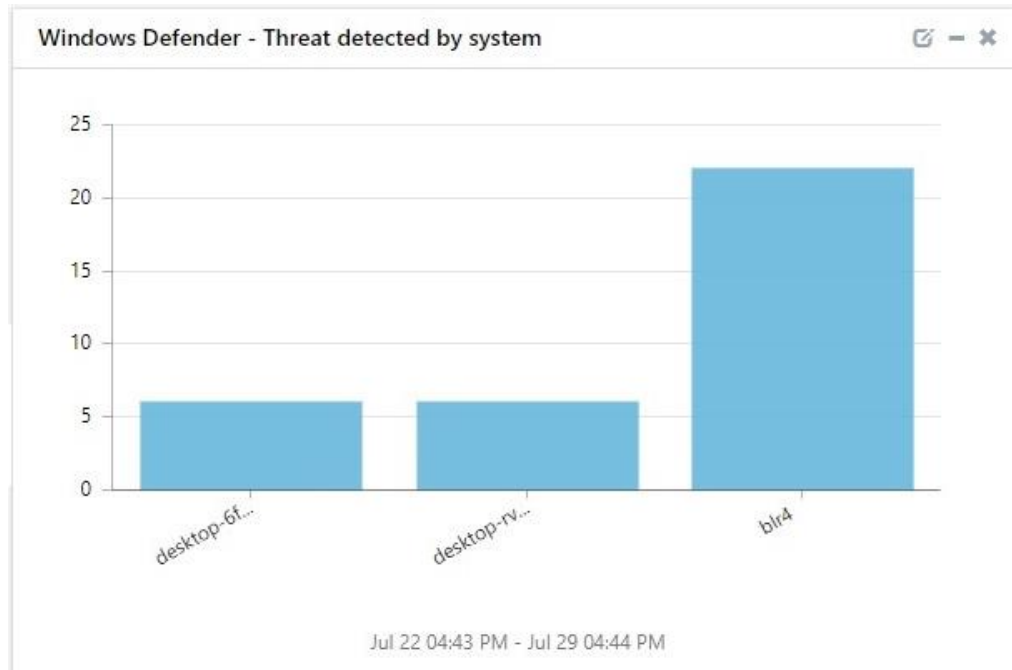


Figure 16

- **Windows Defender - Real time protection disabled by system.**

event_datetime	event_computer
Jul 29 04:42:39 PM	DESKTOP-10@dEFENDER
Jul 29 04:38:06 PM	DESKTOP-rv130@Defender
Jul 29 04:37:26 PM	DESKTOP-6FNROEL@Defender
Jul 26 07:20:38 PM	DESKTOP-633@Defender
Jul 26 07:20:30 PM	NYC-123@Defender
Jul 26 04:35:44 PM	Desktop123@Defender
Jul 26 04:35:40 PM	NYC-111@Defender

Jul 22 04:43 PM - Jul 29 04:44 PM

Figure 17

- Windows Defender - Malware and unwanted software scanning disabled by system.

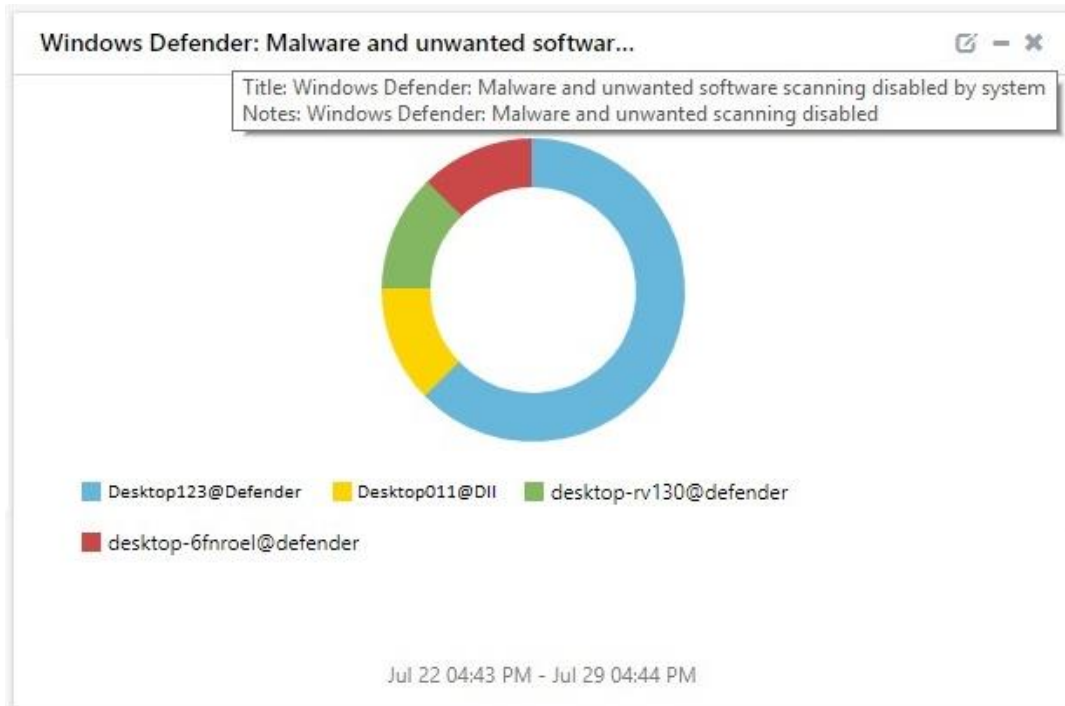


Figure 18

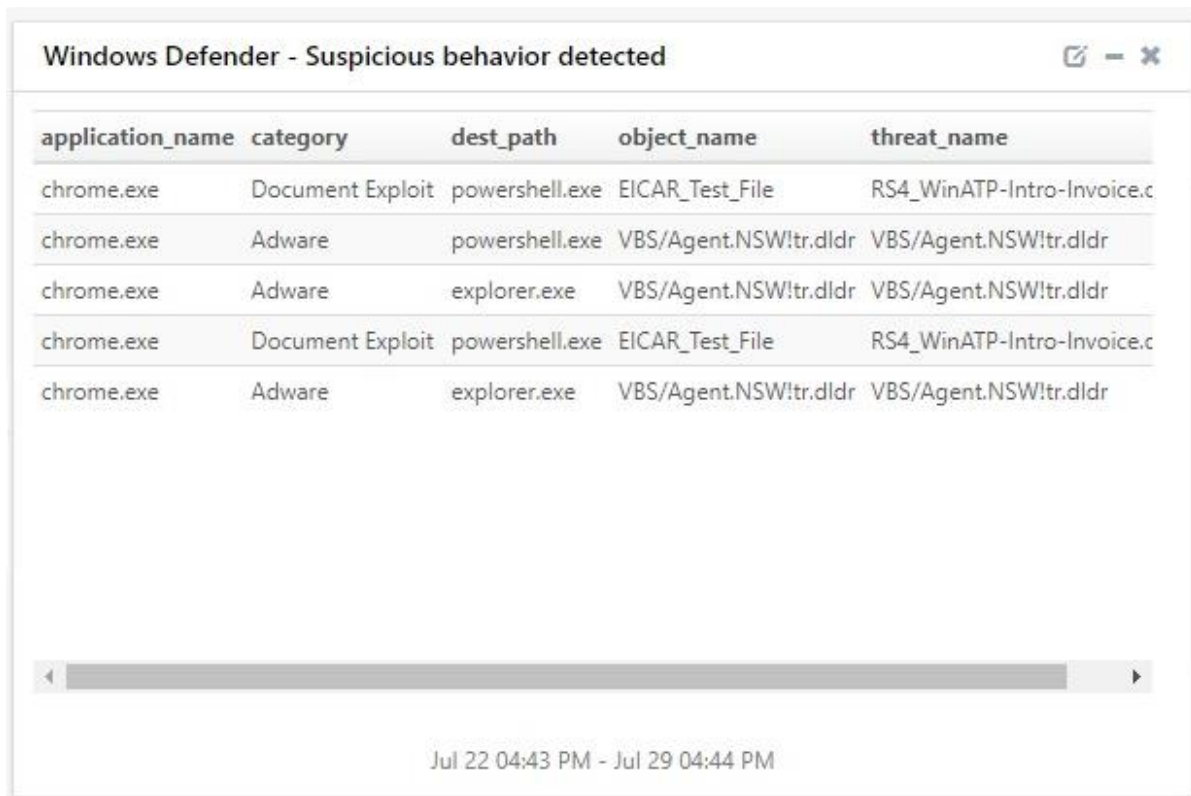
- Windows Defender - Scan stopped before finished by system.

event_datetime	event_computer	reason
Jul 29 04:42:39 PM	Desktop-rv1@Defender	An unexpected problem occurred. Install any available updates to help resolve this problem.
Jul 29 04:38:06 PM	DESKTOP-rv130@Defender	An unexpected problem occurred. Install any available updates to help resolve this problem.
Jul 29 04:37:26 PM	DESKTOP-6FNROEL@Defender	An unexpected problem occurred. Install any available updates to help resolve this problem.
Jul 26 07:20:38 PM	Desktop101@Defender	An unexpected problem occurred. Install any available updates to help resolve this problem.
Jul 26 07:20:30 PM	Desktop111@Defender	An unexpected problem occurred. Install any available updates to help resolve this problem.
Jul 26 04:35:44 PM	Desktop123	An unexpected problem occurred. Install any available updates to help resolve this problem.
Jul 26 04:35:40 PM	BTBL123@Defender	An unexpected problem occurred. Install any available updates to help resolve this problem.

Jul 22 04:43 PM - Jul 29 04:44 PM

Figure 19

- Windows Defender - Suspicious behavior detected.



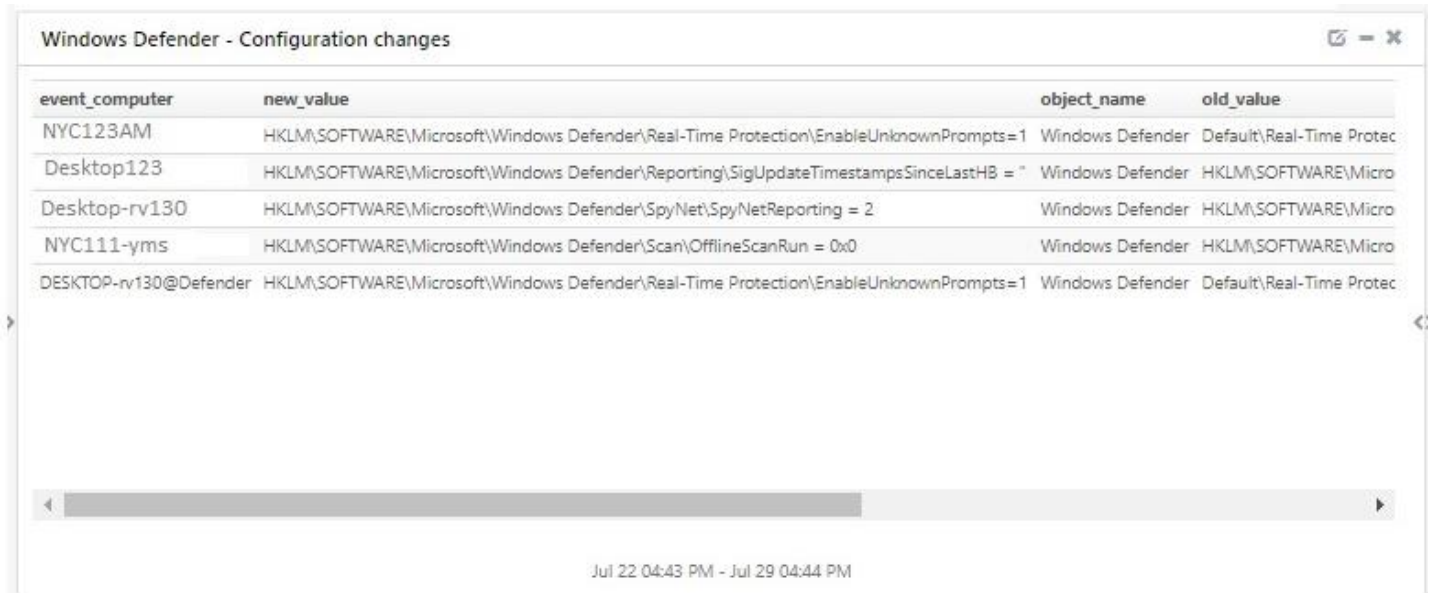
Windows Defender - Suspicious behavior detected

application_name	category	dest_path	object_name	threat_name
chrome.exe	Document Exploit	powershell.exe	EICAR_Test_File	RS4_WinATP-Intro-Invoice.c
chrome.exe	Adware	powershell.exe	VBS/Agent.NSW!tr.dldr	VBS/Agent.NSW!tr.dldr
chrome.exe	Adware	explorer.exe	VBS/Agent.NSW!tr.dldr	VBS/Agent.NSW!tr.dldr
chrome.exe	Document Exploit	powershell.exe	EICAR_Test_File	RS4_WinATP-Intro-Invoice.c
chrome.exe	Adware	explorer.exe	VBS/Agent.NSW!tr.dldr	VBS/Agent.NSW!tr.dldr

Jul 22 04:43 PM - Jul 29 04:44 PM

Figure 20

- Windows Defender - Configuration changes.



Windows Defender - Configuration changes

event_computer	new_value	object_name	old_value
NYC123AM	HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection\EnableUnknownPrompts=1	Windows Defender	Default\Real-Time Protec
Desktop123	HKLM\SOFTWARE\Microsoft\Windows Defender\Reporting\SigUpdateTimestampsSinceLastHB = "	Windows Defender	HKLM\SOFTWARE\Micro
Desktop-rv130	HKLM\SOFTWARE\Microsoft\Windows Defender\SpyNet\SpyNetReporting = 2	Windows Defender	HKLM\SOFTWARE\Micro
NYC111-yms	HKLM\SOFTWARE\Microsoft\Windows Defender\Scan\OfflineScanRun = 0x0	Windows Defender	HKLM\SOFTWARE\Micro
DESKTOP-rv130@Defender	HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection\EnableUnknownPrompts=1	Windows Defender	Default\Real-Time Protec

Jul 22 04:43 PM - Jul 29 04:44 PM

Figure 21



- Windows Defender - Action taken on threats.

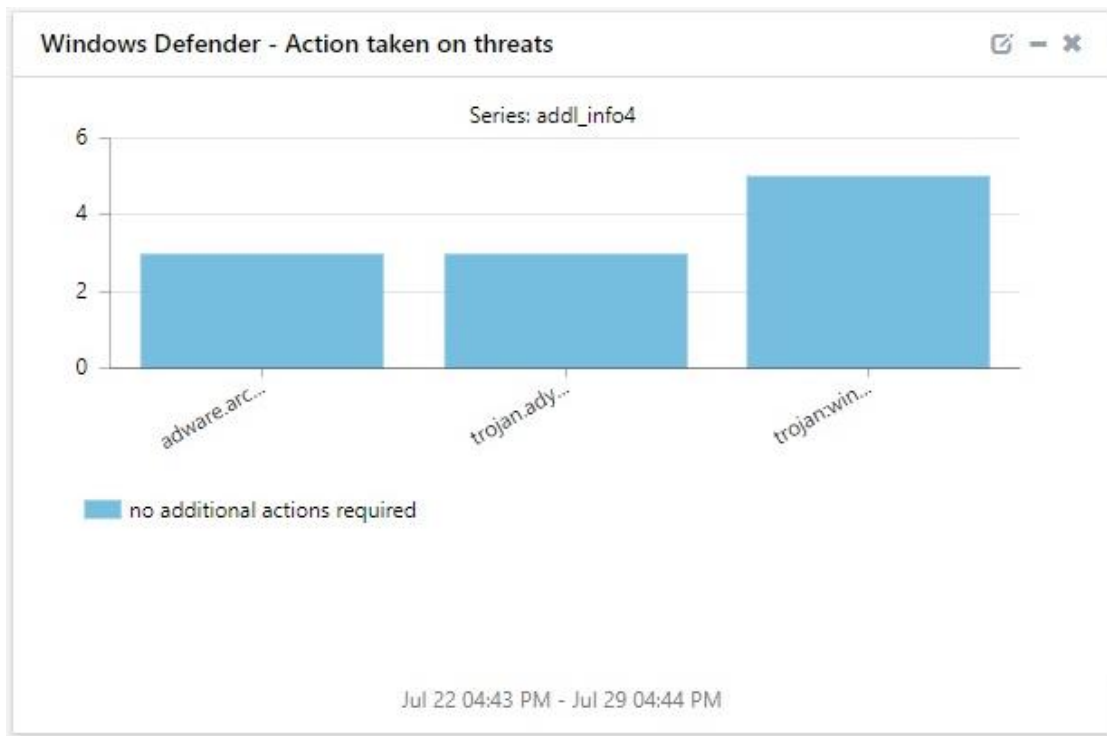


Figure 22

- Windows Defender - Antivirus scanning disabled by system.

Windows Defender - Antivirus scanning disabled by system	
event_datetime	event_computer
Jul 29 04:42:39 PM	Desktop-mn@Defender
Jul 29 04:38:06 PM	DESKTOP-rv130@Defender
Jul 29 04:37:26 PM	DESKTOP-6FNROEL@Defender
Jul 26 07:20:38 PM	NYC123@Defender
Jul 26 07:20:30 PM	NYC10A@Defender
Jul 26 04:35:44 PM	NYC01@Defender
Jul 26 04:35:40 PM	Desktop123
Jul 23 10:16:06 AM	NYC111@Defender

Jul 22 04:43 PM - Jul 29 04:44 PM

Figure 23



# Importing Windows Defender knowledge pack into EventTracker

**NOTE:** Import knowledge pack items in the following sequence:

- Alerts.
  - Parsing Rules.
  - Flex Reports.
  - Categories.
  - Dashboard.
1. Launch the **EventTracker Control Panel**.
  2. Double click **Export-Import Utility**.

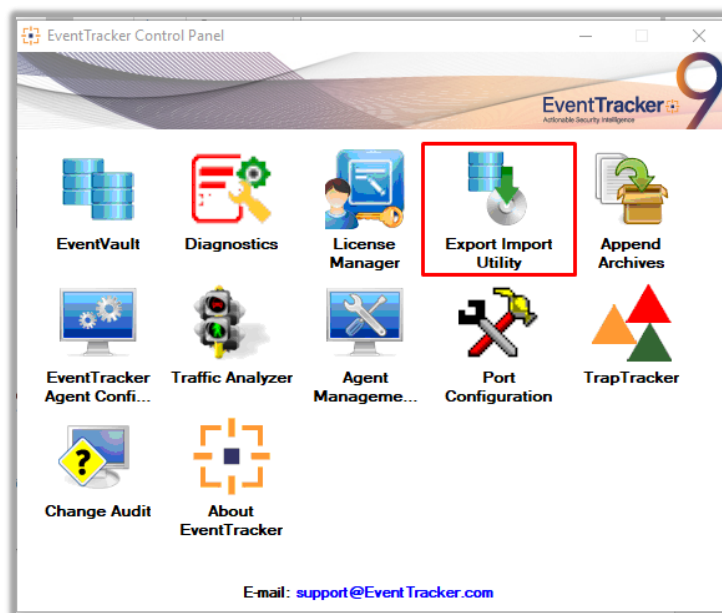


Figure 24

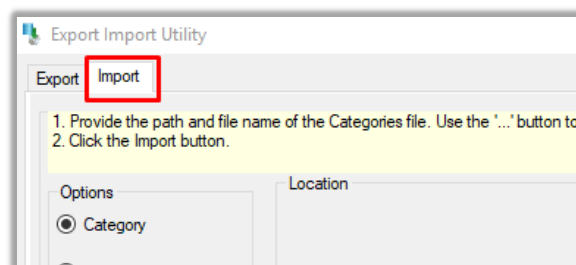



Figure 25

3. Click the **Import** tab.

## Alerts

1. Click the **Alert** option, and then click the browse  button.
2. Navigate to the location having a file with the extension **“.isalt”** and then click on the **“Import”** button:

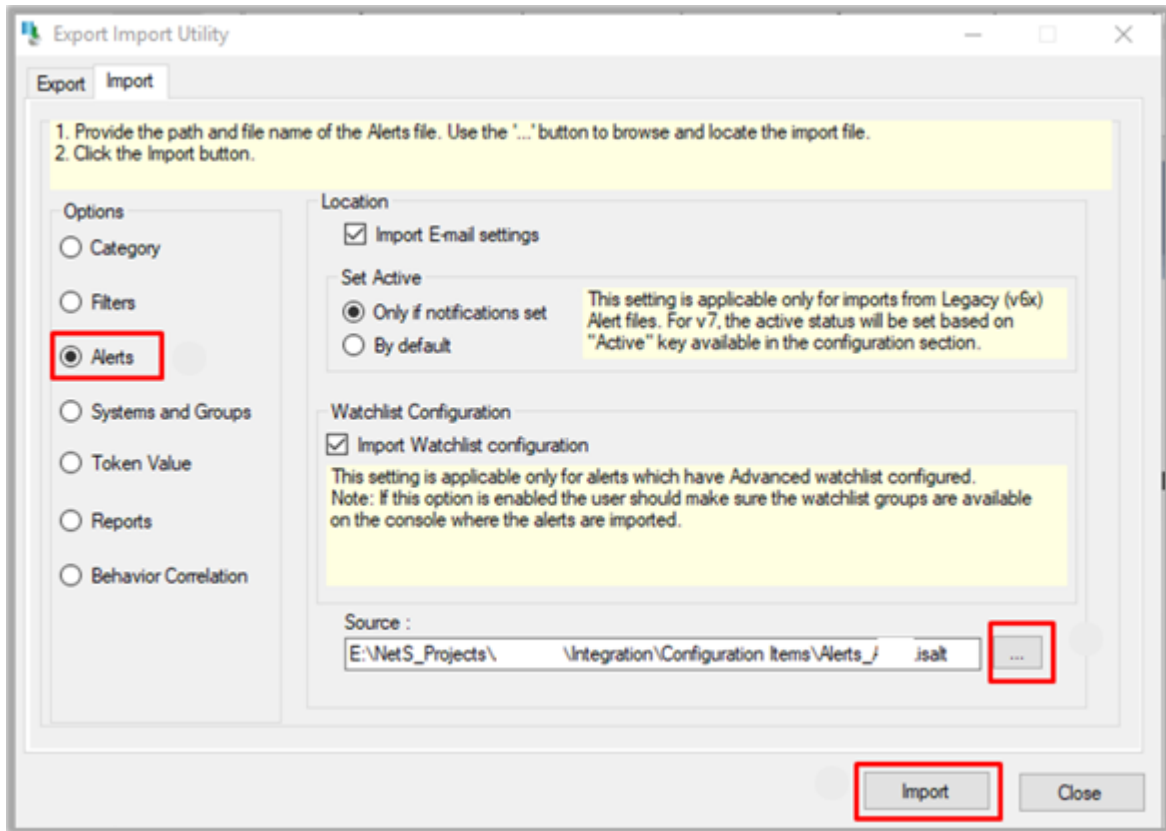


Figure 26

3. EventTracker displays a success message:

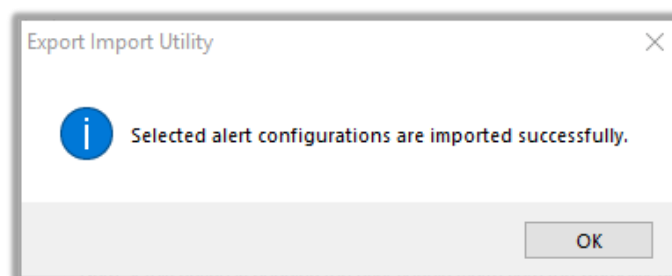



Figure 27

## Parsing Rule

1. Click the **Token Value** option, and then click the  browse button.

2. Navigate to the location having a file with the extension “.istoken” and then click on the “Import” button:

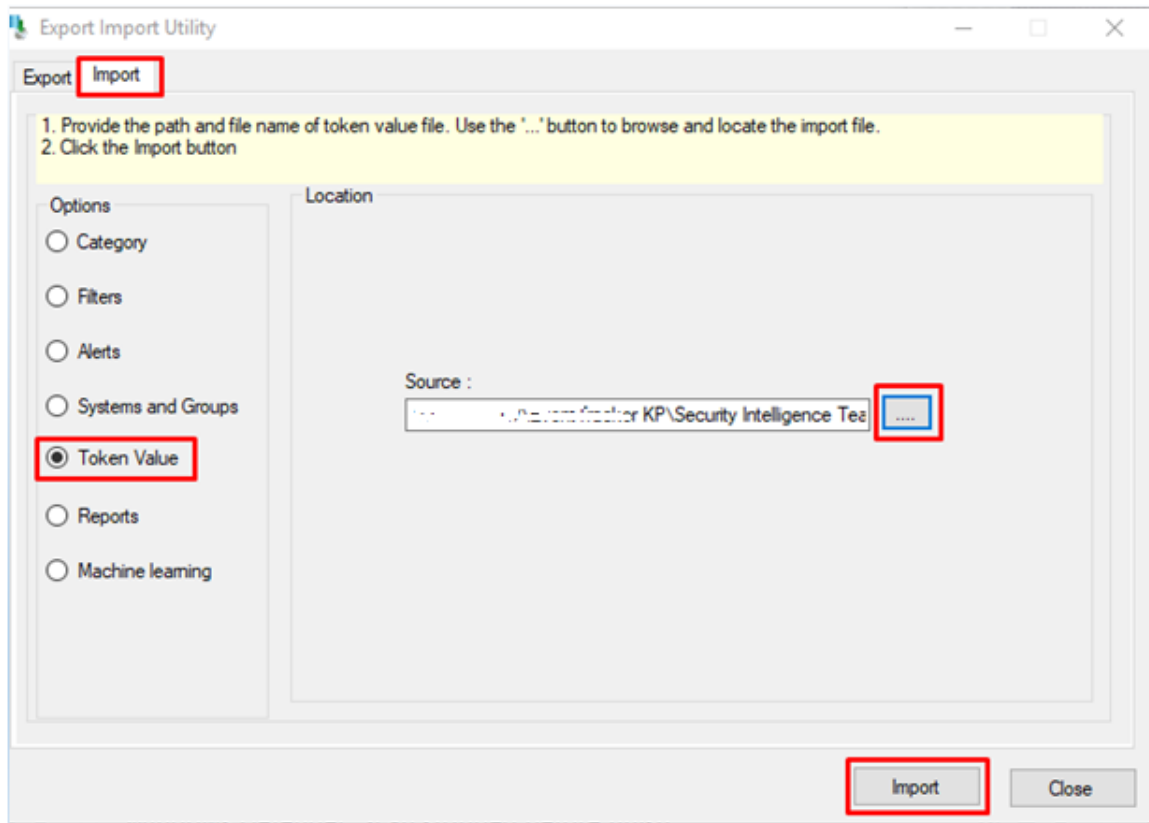


Figure 28

3. EventTracker displays a success message:

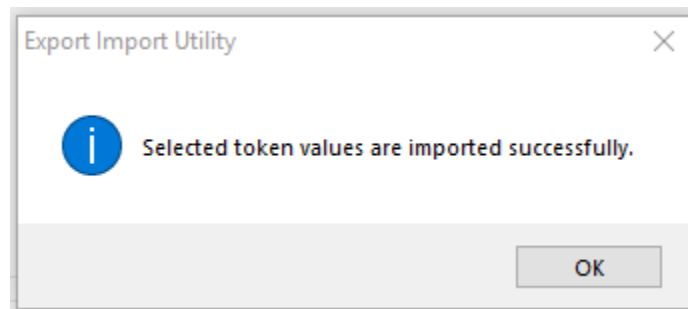


Figure 29

## Flex Reports

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

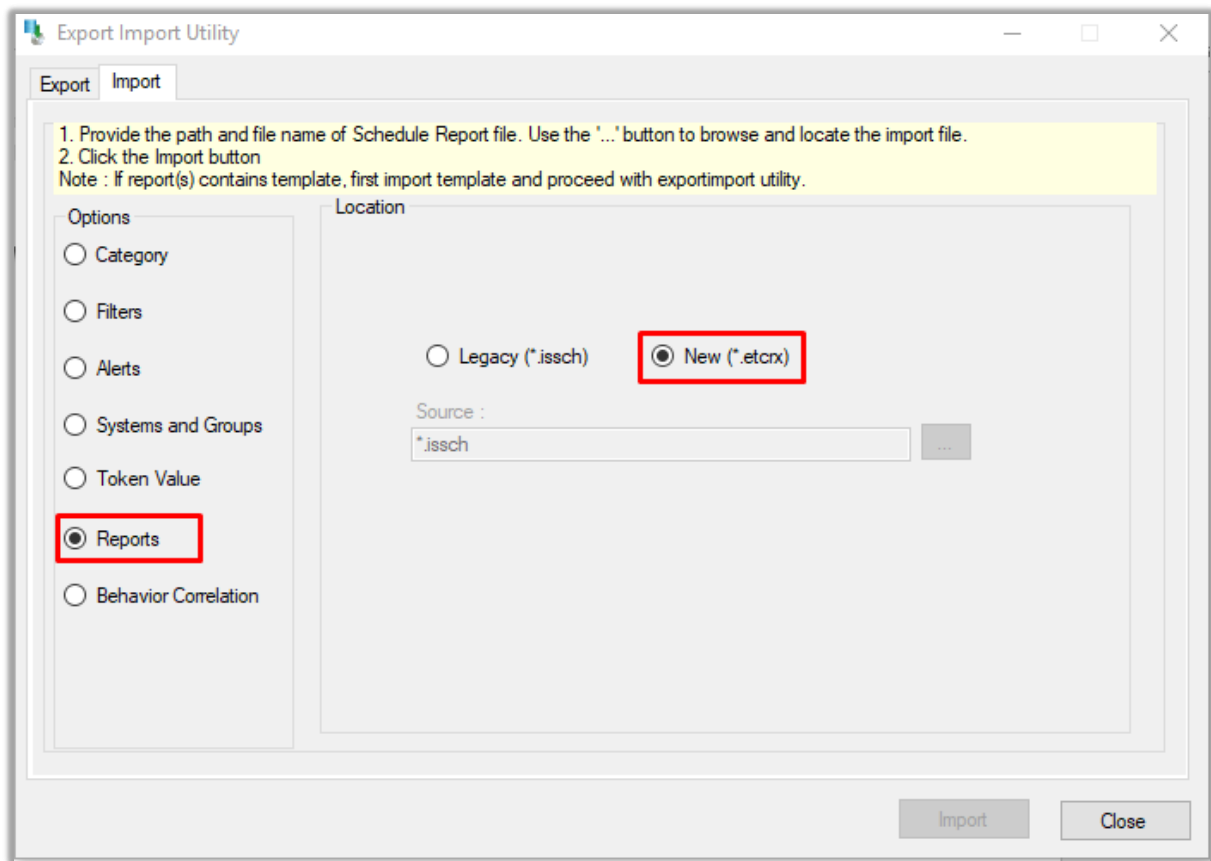


Figure 30

2. Once you have selected “**New (\*.etcrx)**”, a new pop-up window appears. Click the “**Select File**” button and navigate to the file path with a file having the extension “**.etcrx**”.
3. Select all the relevant files and then click **Import**  button.
4. EventTracker displays a success message:

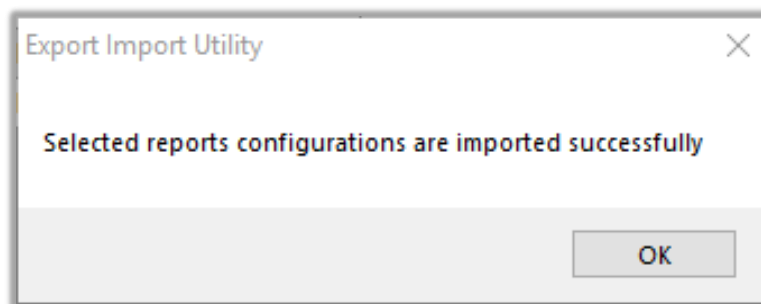



Figure 31

## Category

1. Click the **Category** option, and then click the  browse button.

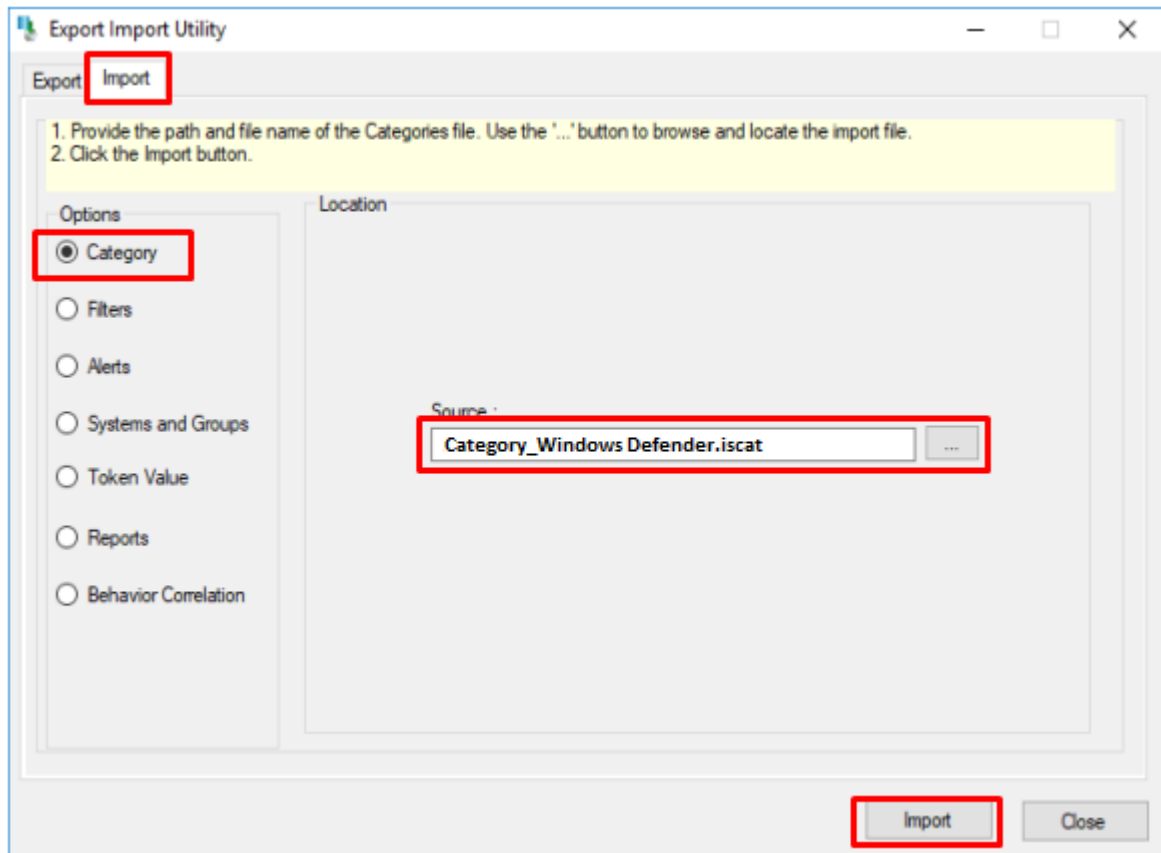


Figure 32

2. Locate the **Category\_Windows Defender.iscat** file, and then click the open button.
3. To import category, click the Import button.
4. EventTracker displays a success message.

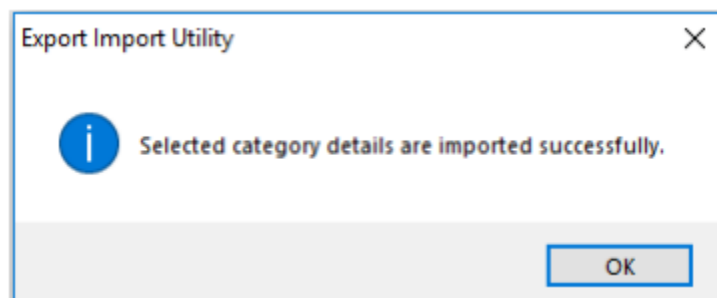


Figure 33

4. Click the OK button, and then click the Close button.

## Dashboard

1. Login to **EventTracker**.
2. Navigate to **Dashboard** → **My Dashboard**.
3. In “My Dashboard”, click **Import Button**:

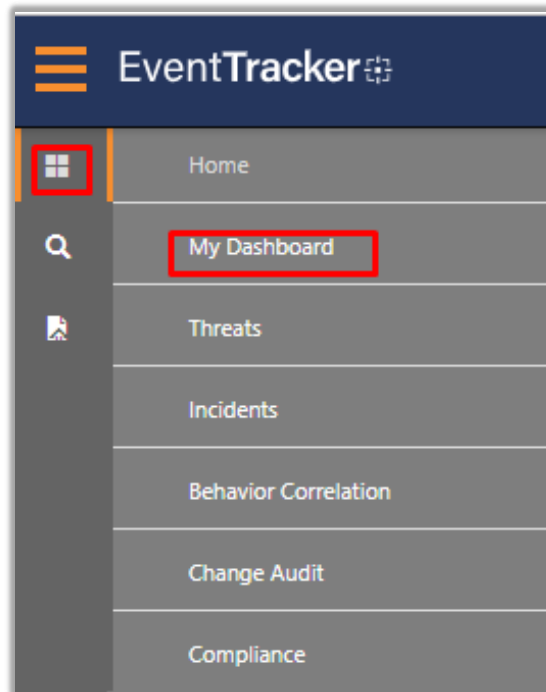


Figure 34

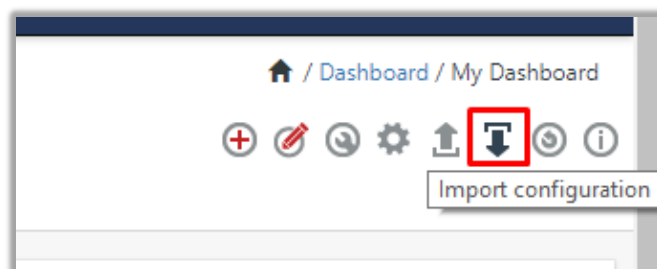


Figure 35

4. Select the **Browse** button and navigate to the file path where the dashboard file is saved and click on the **Upload** button.
5. Once completed, choose **Select All** and click on **Import** Button.
6. Next, click **Customize dashlet** button as shown below:

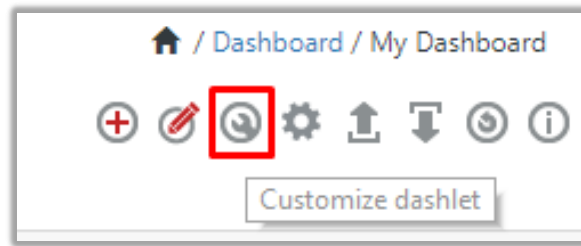


Figure 36

- Now, put a text on the **Search bar**: **"Windows Defender"** and then select the Windows Defender dashlets and then click **"Add"** button.

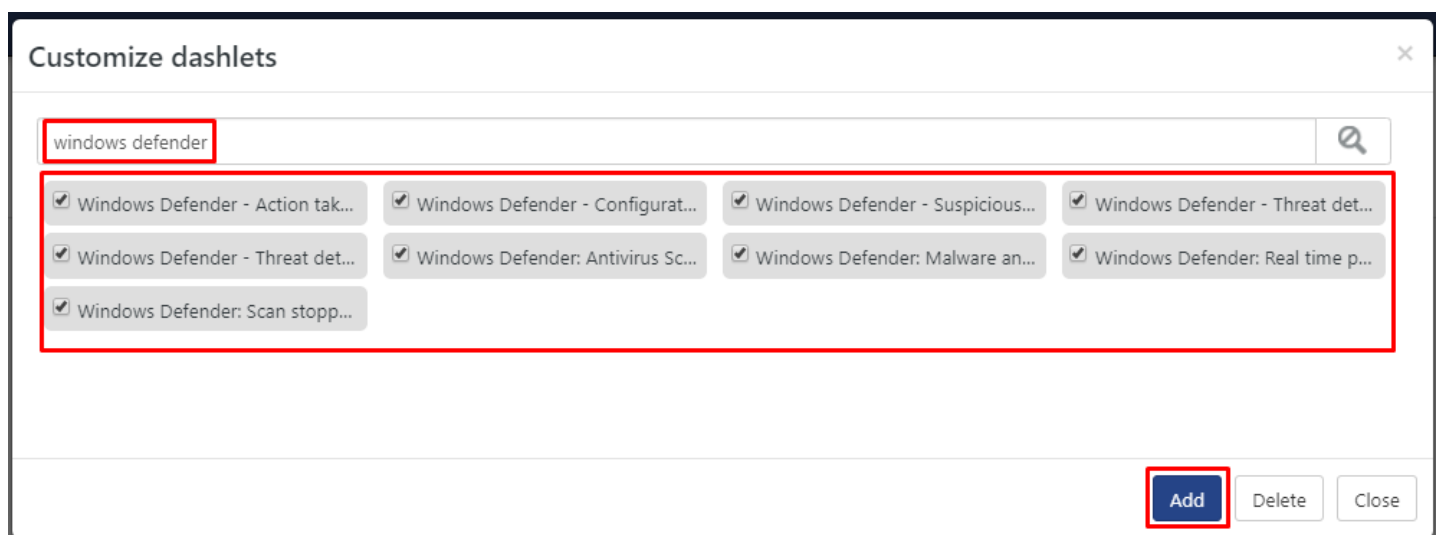


Figure 37

## Verifying Windows Defender knowledge pack in EventTracker

### Alerts

- In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Alerts**.
- In search box enter **"Windows Defender"** and then click the **Search** button.
- EventTracker displays an alert related to **"Windows Defender"**

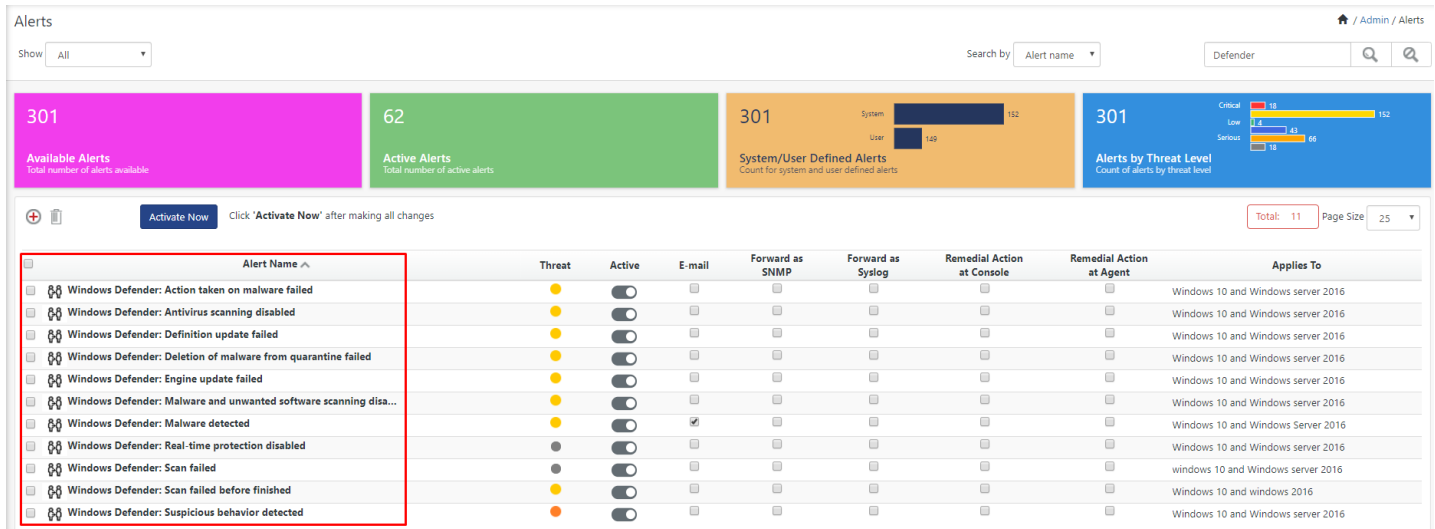


Figure 38

## Parsing Rule

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Parsing Rules**.
2. In the **Parsing Rule** tab, click on the **"Windows Defender"** group folder to view the imported templates.

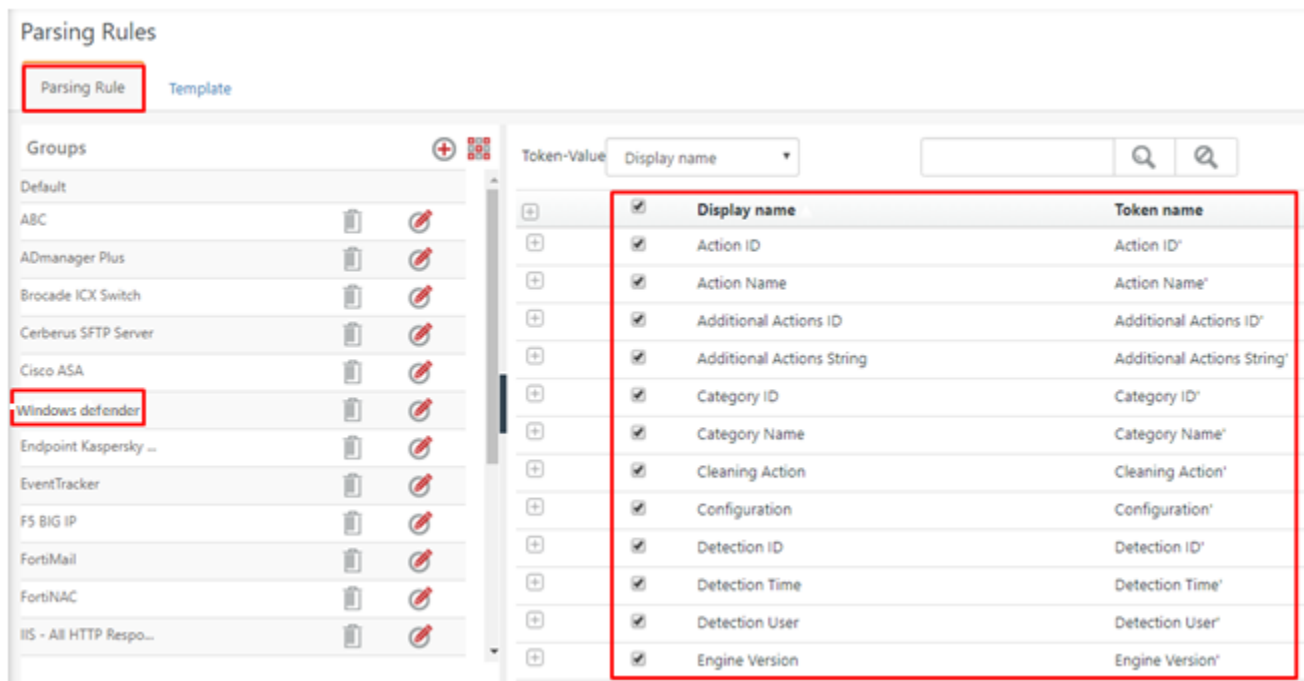


Figure 39



## Flex Reports

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

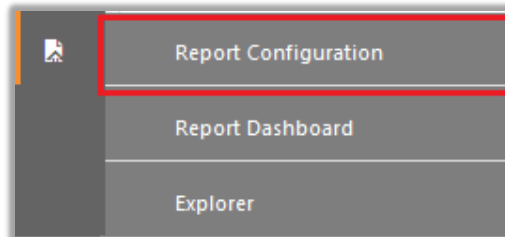


Figure 40

2. In **Reports Configuration** pane, select the **Defined** option.
3. Click on the **Windows Defender** group folder to view the imported reports.

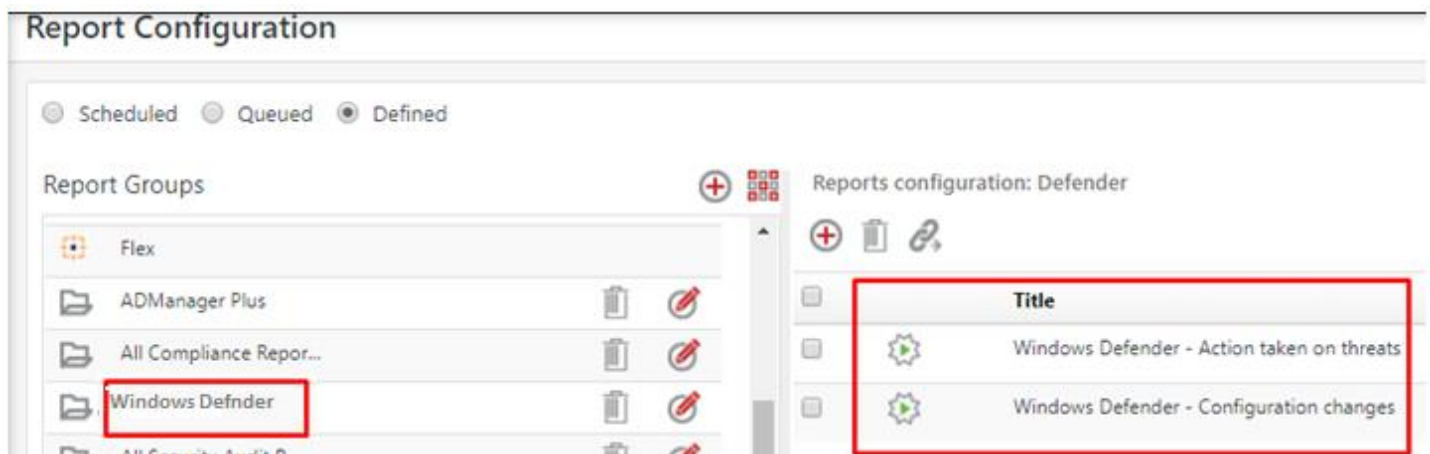


Figure 41

## Category

1. Login to EventTracker.
2. Click the **Admin** menu, and then click **Category**.

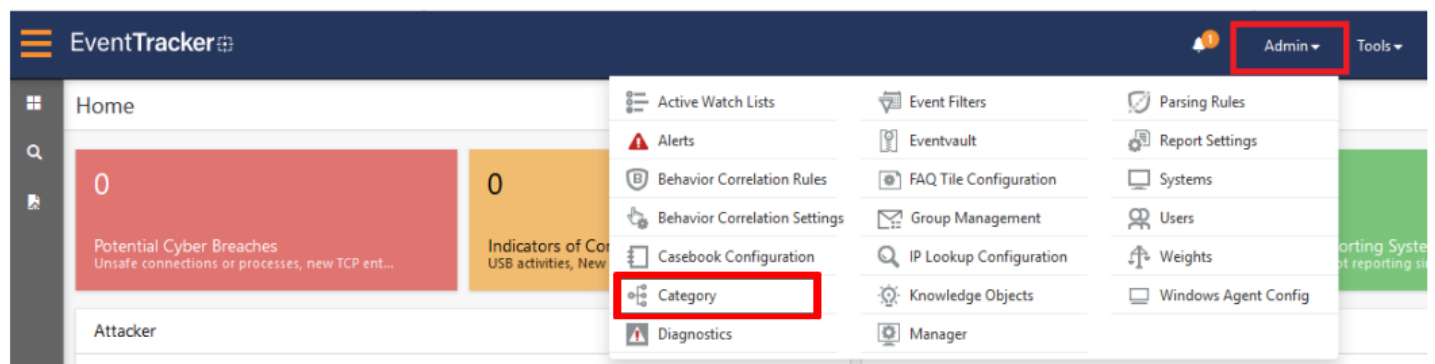


Figure 42

3. Click the search, and then search with Windows Defender.

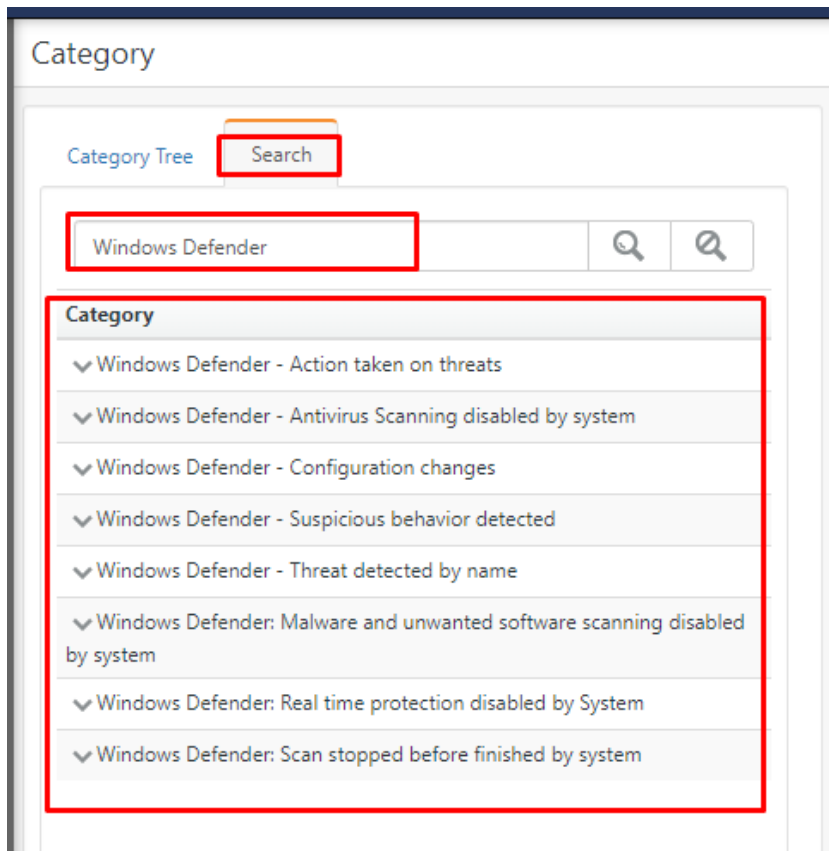


Figure 43

## Dashboard

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

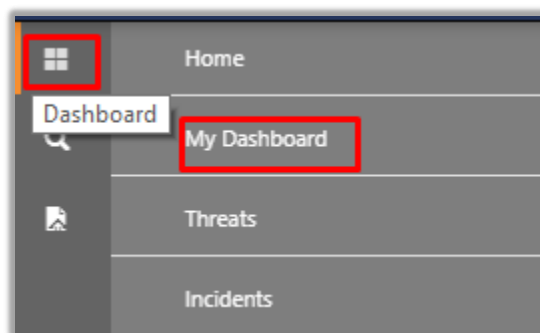
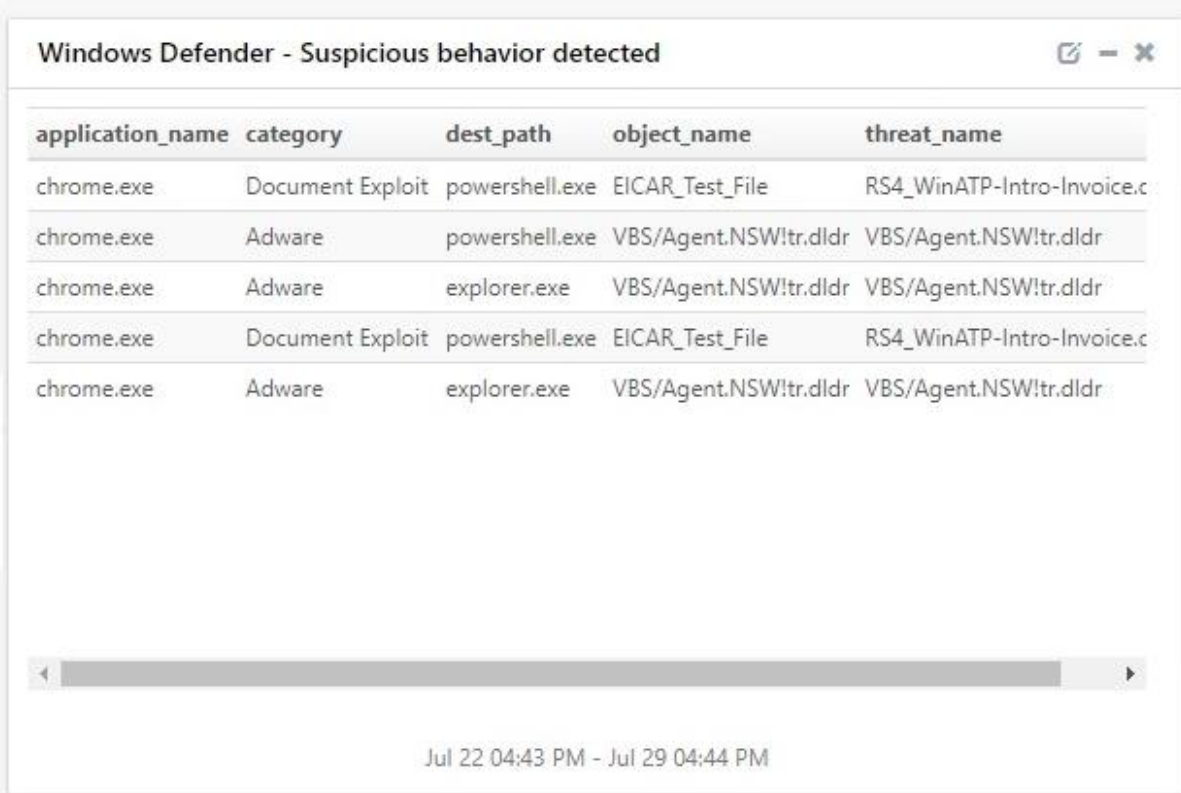


Figure 44

2. In “**Windows Defender**” dashboard you should be now able to see something like this



The screenshot shows a Windows Defender window titled "Windows Defender - Suspicious behavior detected". It contains a table with five columns: application\_name, category, dest\_path, object\_name, and threat\_name. The table lists five detected threats, all originating from chrome.exe. The threats include Document Exploits, Adware, and a specific threat named RS4\_WinATP-Intro-Invoice.c. The window also features a scrollbar and a date range at the bottom: Jul 22 04:43 PM - Jul 29 04:44 PM.

application_name	category	dest_path	object_name	threat_name
chrome.exe	Document Exploit	powershell.exe	EICAR_Test_File	RS4_WinATP-Intro-Invoice.c
chrome.exe	Adware	powershell.exe	VBS/Agent.NSW!tr.dldr	VBS/Agent.NSW!tr.dldr
chrome.exe	Adware	explorer.exe	VBS/Agent.NSW!tr.dldr	VBS/Agent.NSW!tr.dldr
chrome.exe	Document Exploit	powershell.exe	EICAR_Test_File	RS4_WinATP-Intro-Invoice.c
chrome.exe	Adware	explorer.exe	VBS/Agent.NSW!tr.dldr	VBS/Agent.NSW!tr.dldr

Jul 22 04:43 PM - Jul 29 04:44 PM

Figure 45