

# **Integrate Windows Defender**

# EventTracker v9.x and above

Publication Date: August 21, 2019

### 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
Dverview	3
Prerequisites	3
Configuring Windows Defender to forward the log to EventTracker Configuring EventTracker Event Filter	3 3
ventTracker Knowledge Pack	6
Alerts	6
Flex Reports	7
Dashboards	11
mporting Windows Defender knowledge pack into EventTracker	16
Alerts	17
Parsing Rule	17
Flex Reports	18
Dashboard	21
/erifying 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	Туре	Size
- Cache	5/22/2019 1:13 PM	File folder	
📙 DLA	7/29/2019 5:18 PM	File folder	
MessageDII	1/14/2019 6:10 PM	File folder	
	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	M Application extens	
ClientCertificate.dll	1/4/2019 8:27 AM	Application extens	
🚳 Data Encryption.dll	1/4/2019 8:27 AM	Application extens	
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	A Text Document 2,9	
📄 etalog.txt.bak.1	7/29/2019 12:15 PM	1 File	5,124 KB
atalan tatkak 2	7/20/2010 12 07 014	2.51	C 104 KD



3. Navigate to Event Filters>Filter Exception.

🚅 EventTracker Agent Configuration	×
File Help	
C Select Systems	
NTPLDTBLR146	Agent based system
Apply the following settings to specified Agents	
Apply the following settings to specified Agents	
Manager destinations:	
NTPLDTBLR146	
Log Backup Performance N Logfile Monitor File Transfer systog FTP serve Managers Event Filters System Monitor Monitor	Vetwork Connections   r   Suspicious Activity   pr Processes   Services
all events matching the filter criteria will not be sent to the Manager. You can also configure advanced filter option specific events or choose to filter out specific events.	e EventTracker s such as to send only Event Types
HardwareEvents	□ <u>W</u> arning
Internet Explorer	☑ Information
Key Management Service	Audit Success
UAlerts V	Audit <u>F</u> ailure
< >	Critical
Enable SID <u>Translation</u>	□ Ver <u>b</u> ose
Event Descriptio <u>n</u> : C Classic C XML	
Filter Exception	Advanced Filters
Save	Close

Figure 2

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

록 Filter Exc	eption						<
You can choo: events that you Example: You Service, To do Service,	se to monitor specific u would like to monit may want to filter out this, set the Informa	e events i or. t all Inform ation filter	f they maination even and add	tch a filter criter ents other than a Filter Excepti	ria. Specify I those recei on with Eve	the details of the ved from the Web nt Source as Web	
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	Π	517				×
<						>	
<u>N</u> ew	<u>E</u> dit	<u>D</u> ek	ete	Find		<u>C</u> lose	

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/Opera	tional
<u>E</u> vent Type :	Event <u>I</u> D :
Information	
Category :	Match in <u>U</u> ser :
Match in <u>S</u> ource :	
Microsoft-Windows-Windows Defender	
Match in Event <u>D</u> escr :	
I	
"Match in Event Descr", "Match in User" and strings separated with && or IL- && stands for AN For negating the result of match operation, prefi multiple strings, then the result of the whole exp should be used in the string. Example:	"Match in Source" field can take multiple ID condition II stands for OR condition. κ the string with "[\$NOT\$]". If there are ression is negated. Only one "[\$NOT\$]"
The string "[\$NOT\$]Logon Type: 4  Logon Type contain "Logon Type: 4" or "Logon Type: 5" in	e: 5" will match all events that DO NOT the description.
For more information click here.	
ОК	Cancel

Figure 4

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

록 Filter Exception — 🗆 🗙						<	
You can choo events that you Example: You Service, To do Service,	se to monitor specific u would like to monit may want to filter out this, set the Informa	c events if or. t all Inform ation filter	they maination even and add	tch a filter crite ents other than a Filter Excepti	ria. Specify t those receir on with Evel	he details of the ved from the Web ht Source as Web	
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	Π	517				~
<						>	
New	Edit	<u>D</u> ele	ete	Find		<u>C</u> lose	

Figure 5

Integrate Windows Defender

7. Click Save and close EventTracker Agent configuration.

醒 EventTracker Agent Configuration	×
File Help	
Select Systems	Agent based system
Apply the following settings to specified Agents  Manager destinations:  NTPLDTBLR146	
Log Backup Performance II Logfile Monitor File Transfer syslog FTP serve Managers Event Filters System Monitor Monit You can choose to filter out events that are not required all events matching the filter criteria will not be sent to th Manager. You can also configure advanced filter optior specific events or choose to filter out specific events.	Network Connections r Suspicious Activity or Processes Services d. Once the filter is set, the EventTracker is such as to send only
Event Logs  Event Logs  Microsoft-Windows-Win32k/Operational Microsoft-Windows-Windows Defender/Ope Microsoft-Windows-Windows Defender/WH Microsoft-Windows-Windows Firewall With A Microsoft-Windows-Windows-Windows Firewall With A Microsoft-Windows-Windows-Windows Firewall With A Microsoft-Windows-Windows-Windows Firewall With A Microsoft-Windows-Wi	Event Types Error Warning I Information Audit Success Audit Eailure Critical Verbose
Filter Exception	Ad <u>v</u> anced Filters
<u>S</u> ave	<u>C</u> lose

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	Defe	ender-	Action	taken	on	threats
		onuor	rectori	- and a second	•	cilli Carco

f La serie de la s	Compu	Action	Actions	Category	Error	Execution		Origin		Process	Severit	Signature	Source	Threat	Q
LogTime	ter	Name	String	Name	Description	Name	FWLink	Name	Path	Name	y Name	Version	Name	Name	User
07/26/2019 07:20:38 PM	Desktop- WKS	- %%887	No additional actions required	Trojan	The operation unsuccessfu	%%813	http://go.micro soft.com/fwlin k/?linkid=3702	%%84 6	containerfile:_ \10.0.1.10shar eMalware_For	C:Windo wslxplo rer.exe	Severe	1.295.1352. 0	%%818	Trojan: Win32/ Bagsu!r	John



#### Sample Logs:

action	+- %%887
addLinfo4	+- No additional actions required
addL_info5	+- %%813
addL_info6	<b>+-</b> %%846
application_name	+- C:Windows Ixplorer.exe
category	+- Trojan
device_version	<b>+-</b> 4.18.1904.1
event_computer	+- NTPLDTBLR48@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 ٠ 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	HKLMSOFTWAREMicrosoftWindo ws DefenderMpEngineMpCampRing = 0x21	HKLMSOFTWAREMicrosoftWindo ws DefenderMpEngineMpCampRing = 0x2
07/26/2019 04:35:40 PM	Dessktop-NYC	4.18.1904.1	HKLMSOFTWAREMicrosoftWindo ws DefenderMpEngineMpCampRing = 0x21	HKLMSOFTWAREMicrosoftWindo ws DefenderMpEngineMpCampRing = 0x2

Figure 9

# Netsurion... EventTracker

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-&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;&lt;/th&gt;&lt;th&gt;neMpCampRing = 0x21&lt;/Data&gt;&lt;Data Name=" new="" value"="">HKLMSOFTWAREMicrc</data></eventdata>
event_id	<b>+-</b> 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 Defend	er - 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.NSWItr.dldr	Adware	C:\Users\bob.tulley\Downloa ds\RS4_WinATP-Intro-	chrome.exe	powershell.exe



#### Sample Logs:

addL_info	+- Local computer
addL_info2	+- S-1-5
addL_info3	+- S-1-5-21-4133203243-3579683129-339516029-1001
application_name	+- chrome.exe
category	+- Document Exploit
dest_path	+- powershell.exe
device_version	+- 4.9.10586.0
event_computer	+- NTPLDTBLR48@Defender
event_description	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	<b>Category Name</b>	File Path
07/26/2019 12:19:07 PM	Contoso-wks01	John	Trojan:Win32/Bagsu!rfn	Trojan	containerfile:_\\10.0.1.10\share\Mal ware_For_Demo\REAL_BAD_Malz 2\Server.exe;file:_\\10.0.1.10\shar e\Malware_For_Demo\REAL_BAD_ Malz2\Server.exe;file:_\\10.0.1.10\ share\Malware_For_Demo\REAL_ BAD_Malz2\Server.exe- >(VFS:svchost.exe)



#### 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	Id : 1006
	Windows defender has detected malware or other potentially unwanted software.
	For more information please see the following:
	http://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win32/Bagsu!rfn&thi
	Name: Trojan:Win32/Bagsu!rfn
	ID: 2147694434
	Severity: Severe
	Category: Trojan
	Path Found: containerfile:_\\10.0.1.10\share\Malware_For_Demo\REAL_BAD_Malz2'
	or_Demo\REAL_BAD_Malz2\Server.exe->(VFS:svchost.exe)
	Detection Type: Concrete
	Detection Source: Real-Time Protection
	Status: %20
	User: Mike
	Process Name: C:\Windows\explorer.exe
	Signature Version: AV: 1.217.2054.0, AS: 1.217.2054.0, NIS: 115.8.0.0
	Engine Version: AM: 1.1.12603.0, NIS: 2.1.11804.0

Figure 14

### Dashboards

#### Windows Defender - Threat detected by name. •



Figure 15





#### • Windows Defender - Threat detected by system.



#### Windows Defender - Real time protection disabled by system 6 - X event\_datetime event\_computer DESKTOP-10@dEFENDER Jul 29 04:42:39 PM Jul 29 04:38:06 PM DESKTOP-rv130@Defender Jul 29 04:37:26 PM DESKTOP-6FNROEL@Defender DESKTOP-633@Defender Jul 26 07:20:38 PM Jul 26 07:20:30 PM NYC-123@Defender Jul 26 04:35:44 PM Desktop123@Defender NYC-111@Defender Jul 26 04:35:40 PM

• Windows Defender - Real time protection disabled by system.

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





• 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
lul 29 04:42:39 PM	Desktop-rv1@Defender	An unexpected problem occurred. Install any available of
lul 29 04:38:06 PM	DESKTOP-rv130@Defender	An unexpected problem occurred. Install any available u
lul 29 04:37:26 PM	DESKTOP-6FNROEL@Defender	An unexpected problem occurred. Install any available u
lul 26 07:20:38 PM	Desktop101@Defender	An unexpected problem occurred. Install any available u
lul 26 07:20:30 PM	Desktop111@Defender	An unexpected problem occurred. Install any available of
lul 26 04:35:44 PM	Desktop123	An unexpected problem occurred. Install any available u
lul 26 04:35:40 PM	BTBL123@Defender	An unexpected problem occurred. Install any available of



• Windows Defender - Suspicious behavior detected.

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

Figure 20

#### • 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 Prote
Desktop123	${\sf HKLM}\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	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 Prote
4			•

Figure 21





• Windows Defender - Action taken on threats.



• 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



# 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

💺 Export Import Utility					
Export Import					
1. Provide the path and file name of the Categories file. Use the '' button to 2. Click the Import button.					
Options	Location				
Category					
0.0					

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:

Export Import Utility		- 🗆 🗙			
Export Import					
1. Provide the path and file nar 2. Click the Import button.	ne of the Alerts file. Use the '' butt	on to browse and locate the import file.			
Options	Location				
Category	Import E-mail settings				
Filters     Alerts	Set Active Only if notifications set By default	This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.			
<ul> <li>Systems and Groups</li> </ul>	Watchlist Configuration				
O Token Value	Import Watchlist configuration				
	This setting is applicable only for Note: If this option is enabled to	or alerts which have Advanced watchlist configured.			
O Reports	on the console where the alert	s are imported.			
O Behavior Correlation					
	Source :				
	E:\NetS_Projects\	Integration\Configuration Items\Alerts_/ isalt			
		Import			

Figure 26

3. EventTracker displays a success message:





### 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:

ł	Export Import Utility			_		$\times$
E	Export Import					
	1. Provide the path and file na 2. Click the Import button	ame of token va	lue file. Use the '' button to browse and locate the import file.			
	Options	Location				
	Category					
	O Filters					
	⊖ Alerts					
	O Systems and Groups		Source :	ה		
	Token Value			٥		
	O Reports					
	O Machine learning					
					<b>C</b>	
			impo	π	Close	•

Figure 28

3. EventTracker displays a success message:





### Flex Reports

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

Export Import Utility		_		$\times$
Export Import				
1. Provide the path and file nam 2. Click the Import button Note : If report(s) contains templ	e of Schedule Report file. Use the '' button to browse and locate the import file ate, first import template and proceed with exportimport utility.	-		
Options	Location			
Category				
) Filters				
<ul> <li>Alerts</li> </ul>	Legacy (*.issch)     New (*.etcrx)			
O Systems and Groups	Source : *issch			
○ Token Value				
Reports				
O Behavior Correlation				
	Imp	port	Clo	se

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 T** button.
- 4. EventTracker displays a success message:

Export Import Utility	×
Selected reports configurations are imported successfully	
ОК	

Figure 31



### Category

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

ŋ,	Export Import Utility	-		$\times$
E	kport Import			
	<ol> <li>Provide the path and file nar</li> <li>Click the Import button.</li> </ol>	me of the Categories file. Use the '' button to browse and locate the import file.		
[	Options Category	Location		
	⊖ Filters			
	⊖ Alerts			
	O Systems and Groups	Source :		
	O Token Value	Category_windows belender.iscat		
	○ Reports			
	O Behavior Correlation			
		Import	Clos	e



- 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**  $\rightarrow$  **My Dashboard**.
- 3. In "My Dashboard", click Import Button:

	≡	Event <b>Tracker</b> #	
		Home	
	۹	My Dashboard	
	2	Threats	
		Incidents	
		Behavior Correlation	
		Change Audit	
		Compliance	
_		Figure 34	
		1 Dashboard / My Dashboard	
		+ 🖉 9 🌣 1 🚺 6 (	)
		Import configura	tioi



- 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

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

Customize dashlets			×
windows defender			Q
✓ Windows Defender - Action tak	☑ Windows Defender - Configurat	☑ Windows Defender - Suspicious	☑ Windows Defender - Threat det
✓ Windows Defender - Threat det	☑ Windows Defender: Antivirus Sc	Vindows Defender: Malware an	✓ Windows Defender: Real time p
✓ Windows Defender: Scan stopp			
			Add Delete Close

Figure 37

# Verifying Windows Defender knowledge pack in EventTracker

### Alerts

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

# Netsurion... EventTracker

Alerts								🔶 / Admin / Alerts
Show All 🔻						Search by Alert na	ame 🔻	Defender Q Q
301 Available Alerts Fodd number of alerts available	62 Active Alerts Total number of active alerts			301 System/User De Count for system and	System User fined Alerts user defined alerts	152	301 Alerts by Th Count of alerts b	Crical 19 12 (res 14 6 reat Level threat level
Activate Now     Click 'Activate Now' after mak	ng all changes							Total: 11 Page Size 25 V
Alert Name 🔨	Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
📄 និ្នភ្លិ Windows Defender: Action taken on malware failed	•							Windows 10 and Windows server 2016
📄 ជុំស្ថិ Windows Defender: Antivirus scanning disabled	•							Windows 10 and Windows server 2016
ββ Windows Defender: Definition update failed	•							Windows 10 and Windows server 2016
βδ Windows Defender: Deletion of malware from quarantine failed	•							Windows 10 and Windows server 2016
📃 ត្តិស្តិ Windows Defender: Engine update failed	•							Windows 10 and Windows server 2016
📄 និ្តស្ថិ Windows Defender: Malware and unwanted software scanning	disa 😑							Windows 10 and Windows server 2016
🗌 දිදි Windows Defender: Malware detected	•		•					Windows 10 and Windows Server 2016
βδ Windows Defender: Real-time protection disabled	•							Windows 10 and Windows server 2016
🔲 දිදි Windows Defender: Scan failed	•							windows 10 and Windows server 2016
🔲 දිරි Windows Defender: Scan failed before finished	•							Windows 10 and windows 2016
📄     ស្តីភ្លំ Windows Defender: Suspicious behavior detected	•							Windows 10 and Windows server 2016

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.

Groups	<b>(</b>	Token-Value	Displa	y name	QQ
Default				Diselau anna	Takan anna
ABC	10 🧭	+		Action ID	Action (D)
ADmanager Plus	11 🧭	0	۲	Action ID	Action ID
Brocade ICX Switch	ii 🧭	+	8	Action Name	Action Name'
Cerberus SFTP Server	ii 🧭	+	2	Additional Actions ID	Additional Actions ID'
Cisco ASA	10 0	+		Additional Actions String	Additional Actions String
Mindows detender	1 0	+		Category ID	Category ID'
Endopint Kaspersky	11 0	+		Category Name	Category Name'
EventTracker	E Ø	+		Cleaning Action	Cleaning Action'
		+		Configuration	Configuration'
PD BIG IP		+		Detection ID	Detection ID'
FortiMail		+	2	Detection Time	Detection Time'
FortiNAC	11 🧭	-			



### **Flex Reports**

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





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

Scheduled Queued I Defined						
Report Groups		Ð	000	Repo	orts configu	iration: Defender
Elex Flex			^	Ð	Î 0,	
ADManager Plus	Û	1		8		Title
All Compliance Repor	Û	0		8	$\langle \tilde{\omega} \rangle$	Windows Defender - Action taken on threat
Windows Definder	Ē	1		8	-	Windows Defender - Configuration changes
The same share as a	101	CA.		- L	11.551	

### Category

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



Figure 42

# Netsurion... EventTracker

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

tegory	
Category Tree Search	
Windows Defender	Q Q
Category	
✓ Windows Defender - Action	taken on threats
✓ Windows Defender - Antivir	us Scanning disabled by system
✓ Windows Defender - Config	uration changes
✓ Windows Defender - Suspic	ious behavior detected
✓ Windows Defender - Threat	detected by name
✓ Windows Defender: Malwar by system	e and unwanted software scanning disabled
✓ Windows Defender: Real tim	ne protection disabled by System
✓ Windows Defender: Scan sto	opped before finished by system

Figure 43

### Dashboard

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







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

application_name	category	dest_path	object_name	threat_name
chrome.exe	Document Exploit	powershell.exe	EICAR_Test_File	RS4_WinATP-Intro-Invoice.c
:hrome.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
(				•

