

Integration Guide

Integrate Snort IDS with EventTracker

Publication Date:

June 17, 2022

© Copyright Netsurion. All Rights Reserved.

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	Ove	erview	4
2	Pre	requisite	4
3	Eve	ntTracker Knowledge Pack	4
	3.1	Categories	4
	3.2	Alerts	5
	3.3	Reports	5
	3.4	Dashboard	5
4	Imp	oorting Snort IDS Knowledge Packs into EventTracker	B
	4.1	Category	9
	4.2	Alerts	10
	4.3	Reports	11
	4.4	Knowledge Objects	12
	4.5	Dashboard	14
5	Ver	ifying Snort IDS Knowledge Packs in EventTracker19	5
	5.1	Category	15
	5.2	Alerts	16
	5.3	Reports	17
	5.4	Knowledge Objects	18
	5.5	Dashboard	19

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 <u>How-To Guide</u> 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.



Netsurion®



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.

🔌 Export Import Utility		
Export Import		
1. Provide the path and file nam 2. Click the Import button.	e of the Categories file. Use the '' button to browse and locate the imp	port file.
Options	Location	
Category		
Filters		
Alerts		
Systems and Groups	Source :	
RSS Feeds	*iscat	
Reports		
Behavior Rules		
© SCAP		
Token Value		
		Import Close

- 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. Click the Import button.	Location	to provise and locate the import file.
 Category Filters 	✓ Import E-mail settings	
Alerts	Set Active	This setting is applicable only for imports from Legacy
Systems and Groups	 Only if notifications set Bu default 	(v6x) Alerti files. For v7, the active status will be set based on "Active" key available in the configuration
RSS Feeds	U by delauk	section.
Reports	Source :	
Behavior Rules	*.isalt	
SCAP		
🔘 Token Value		

- 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).

🐁 Export Import Utility	- 0	×
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		
⊖ Alerts	 Legacy (*.issch) New (*.etcrx) 	
O Systems and Groups	Source :	
◯ Token Value	JSGI	
Reports		
O Behavior Correlation		
	Import	ose

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.

ቶ Reports Import				
Note : If report(s) contains template, first import template and p	roceed with report import proces	SS.		
Select file *.etcrx				Select file
Available reports				
	Frequency Show al	- Q Q		
Title Site	s Groups	Systems Frequency	Runtime	Туре
Title Site	s Groups	Systems Frequency	Runtime	Туре



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

Note: Set run time option is not applicab	le for Defined Reports and Hourly Reports		
Set run time for report(s) from	AM 🔹 at interval of minutes	Set	
Replace	to Replace	Assign systems	
		Note: Make sure that Site(s), Group(s) and System(s) selections are valid.	\otimes

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

Export Import Utility	\times
Selected reports configurations are imported successfully	
ОК	

5. Click OK.

4.4 Knowledge Objects

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

		🔎 🛛 Admin 🗸	Tools 👻 📀
Active Watch Lists	Event Filters	😥 Parsing Rules	† / Da
Alerts	Sector Eventvault	Report Settings	
Behavior Correlation Rules	FAQ Tile Configuration	Systems	
🗞 Behavior Correlation Settings	Group Management	QQ Users	
Casebook Configuration	Q IP Lookup Configuration	T Weights	since the last 24 hour
Category	·☆ Knowledge Objects	Windows Agent Config	
Diagnostics	Manager		



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.
- 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.

Import		
KO_ <product name="">.etko</product>	🗁 Browse 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.

📌 / Dashboard / My Dashboard
+ 🖉 @ 🌣 1 🗐 0 🛈
Import configuration

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

S Import dashlets - Google Chrome	_	×
▲ Not secure 172.28.9.67:8080/EventTracker/Flex/ImportWidget.aspx		
Import		^
Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.		
Dashboard Snort IDS.etwd 🗁 Browse Upload		
Available widgets		
Select All		
🗹 Snort IDS - Events based 🗹 Snort IDS - Types of atta 🗹 Snort IDS - Attacks based 🗹 Snort IDS - Events by	/ geo	
Spart IDC Events by pri		
Short IDS - Events by pr		
		-



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.

Category	
Category Tree Search	
EventTracker	
Jamf Protect	
🕸 🔁 Kemp	
Microsoft Azure	
Microsoft Defender	
🖬 🔁 Mimecast	
MSSQL Audit	
🖮 🔁 NIST 800-171	
🖶 🔁 Panda Cloud Antivirus	- 64
🖶 🔁 PCI DSS	
🖶 🔁 Product Name	
🔄 🔁 Snort IDS	
🔤 Snort IDS - Application attacks	
🗐 Snort IDS - Corporate suspicious activ	ities
Snort IDS - Miscellaneous activities	
- 🗐 Snort IDS - Potential network attacks	
- 🗐 Snort IDS - Potential privilege escalati	ons
Snort IDS - Potential suspicious activit	y
Snort IDS - Traffic attacks	

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 Search button.
- 3. The Alerts interface will display all the imported Snort IDS alerts.

Alerts								📌 / Admin / Ale
Show All 🗸						Search by Alert	name 🗸	snort Q Q
443 Available Alers Istal number of alerts available	257 Active Alerts Total number of active alerts			443 System/User I Count for system a	System	219	443 Alerts by 1 Count of alert	Critical 24 High 27 Low 0.7 Service 73 Service 73 Service 74 Service 74
Click 'Activate Now	v' after making all changes							Total: 2 Page Size 25
Alert Name 🧄	Thre	at Active	Email	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
🗌 දිදි Snort IDS: Critical threat detected	•							Snort Version 2.4 and later
🗌 දි.රි Snort IDS: Potential attacks detected	•							Snort Version 2.4 and later

- **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.

	\$
Successfully saved configure	ation.

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**.

Report Configuration			
O Scheduled O Queued O Defined			
Report Groups		ŧ	
ΜΙΟΓΟΣΟΠ ΑΙΡ		۷	
Microsoft Azure	Ē	Ø	
Microsoft Defender	Ŵ	Ø	
🔁 Mimecast	1	0	
MSSQL Audit	1	Ø	
OpenDNS		0	
Panda Cloud Antiviru		0	
Product		0	
Snort IDS		0	
SonicWall UTM	Ē	0	
SQL Server		0	

- **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.**

Repo	rts configuration: Sno	t IDS					
Ð	Ū Q,					Tot	tal: 1
	Title		Created on	Modified on			
	Snort Snort	DS - Activity overview	Jun 08 01:48:29 AM	Dec 31 04:00:00 PM	(i)	6	+

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.

Knowledge Objects			
Search objects		Q	Q
Groups 🕂) 🧭 🗵]	
• OpenDNS			
Palo Alto Firewall			
Panda Cloud Antivirus			
E SEP Cloud			
 Snort IDS 			

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 <u>Managed</u> <u>Threat Protection</u> 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 <u>Secure Edge Networking</u> 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 <u>netsurion.com</u> or follow us on <u>Twitter</u> or <u>LinkedIn</u>.

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