EventTracker
Secure. Comply. Succeed.

Integrate Suricata

EventTracker Enterprise

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

Publication Date: April 14, 2016

About this Guide

This guide will facilitate a **Suricata** user to send logs to **EventTracker Enterprise**.

Scope

The configuration detailed in this guide are consistent with **EventTracker Enterprise** version 7.X and later, and **Redhat, Suse, CentOS, Fedora Operating System**.

Audience

Administrators who want to monitor **Suricata** using EventTracker Enterprise.

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

This document is for informational purposes only. Prism Microsystems 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 Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems 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 Prism Microsystems, 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.

© 2016 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

About this Guide 1
Scope 1
Audience........ 1
Introduction 3
Pre-requisites........ 3
Configure Suricata to send Syslog events to EventTracker server........ 3
EventTracker Knowledge Pack 3
Alerts........ 3
Reports........ 4
Importing Suricata knowledge pack into EventTracker........ 4
Alerts........ 5
Token Templates........ 7
Flex Reports 8
Knowledge Object 10
Verifying Suricata knowledge pack in EventTracker........ 12
Suricata Alerts........ 12
Suricata Token Template 13
Suricata Reports 13
Suricata Knowledge Object........ 14
Create Flex Dashboards in EventTracker 15
Schedule Reports........ 15
Create Dashlets........ 18
Sample Dashboards........ 22

Introduction

Suricata is an open source-based Intrusion Detection System (IDS), Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine. Suricata uses the Yaml format for configuration.

Pre-requisites

- **EventTracker 7.x or later** should be installed.
- **Suricata** should be installed and configured.

Configure Suricata to send Syslog events to EventTracker server

1. Login to the Linux Redhat/CentOS machine as root.
2. Open Terminal window.
3. Open rsyslog.conf in VI Editor. vi /etc/rsyslog.conf
4. Add the below mentioned line in file rsyslog.conf at last.

```
*.* @IP address of EventTracker Enterprise machine: 514
Example *.* @10.10.10.167:514
```

5. Save the file using: wq
6. Run refresh –s syslogd

EventTracker Knowledge Pack

Once Suricata events are enabled and Suricata events are received in EventTracker: Alerts and Reports can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker to support Suricata monitoring.

Alerts

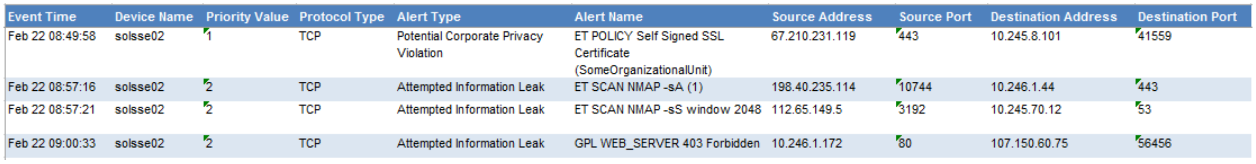
- **Suricata High priority alert generated:** This alert is generated when highest priority (1) alert has occurred in Suricata IDS.

```
Feb 22 08:49:58 suzie02 Feb 22 08:50:03 suzie02 suricata[22816]: [1:2013659:4] ET POLICY Self
Signed SSL Certificate (SomeOrganizationalUnit) [Classification: Potential Corporate Privacy
Violation] [Priority: 1] {TCP} 65.44.32.33:443 -> 10.23.44.56:41559
```

Reports

- **Suricata-Alert analysis:** This report provides information related to alerts which were detected by Suricata IDS.

Sample Report



Event Time	Device Name	Priority Value	Protocol Type	Alert Type	Alert Name	Source Address	Source Port	Destination Address	Destination Port
Feb 22 08:49:58	solsse02	1	TCP	Potential Corporate Privacy Violation	ET POLICY Self Signed SSL Certificate (SomeOrganizationalUnit)	67.210.231.119	443	10.245.8.101	41559
Feb 22 08:57:16	solsse02	2	TCP	Attempted Information Leak	ET SCAN NMAP -sA (1)	198.40.235.114	10744	10.246.1.44	443
Feb 22 08:57:21	solsse02	2	TCP	Attempted Information Leak	ET SCAN NMAP -sS window 2048	112.65.149.5	3192	10.245.70.12	53
Feb 22 09:00:33	solsse02	2	TCP	Attempted Information Leak	GPL WEB_SERVER 403 Forbidden	10.246.1.172	80	107.150.60.75	56456

Figure 1

Logs considered

```
Feb 22 08:49:58 suzie02 Feb 22 08:50:03 suzie02 suricata[22816]: [1:2013659:4] ET POLICY Self
Signed SSL Certificate (SomeOrganizationalUnit) [Classification: Potential Corporate Privacy
Violation] [Priority: 1] {TCP} 65.44.32.33:443 -> 10.23.44.56:41559
```

Importing Suricata knowledge pack into EventTracker

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

   Import **Alert/Tokens/ Flex Reports** as given below.

   Note: Importing should be in the same order as mentioned above.

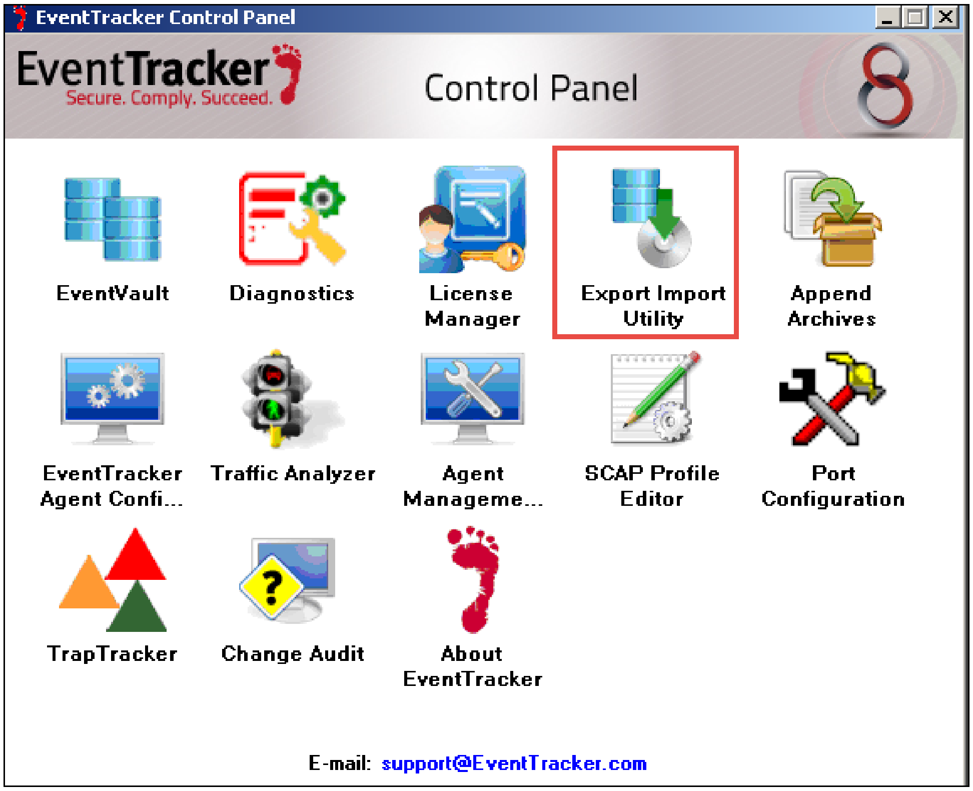
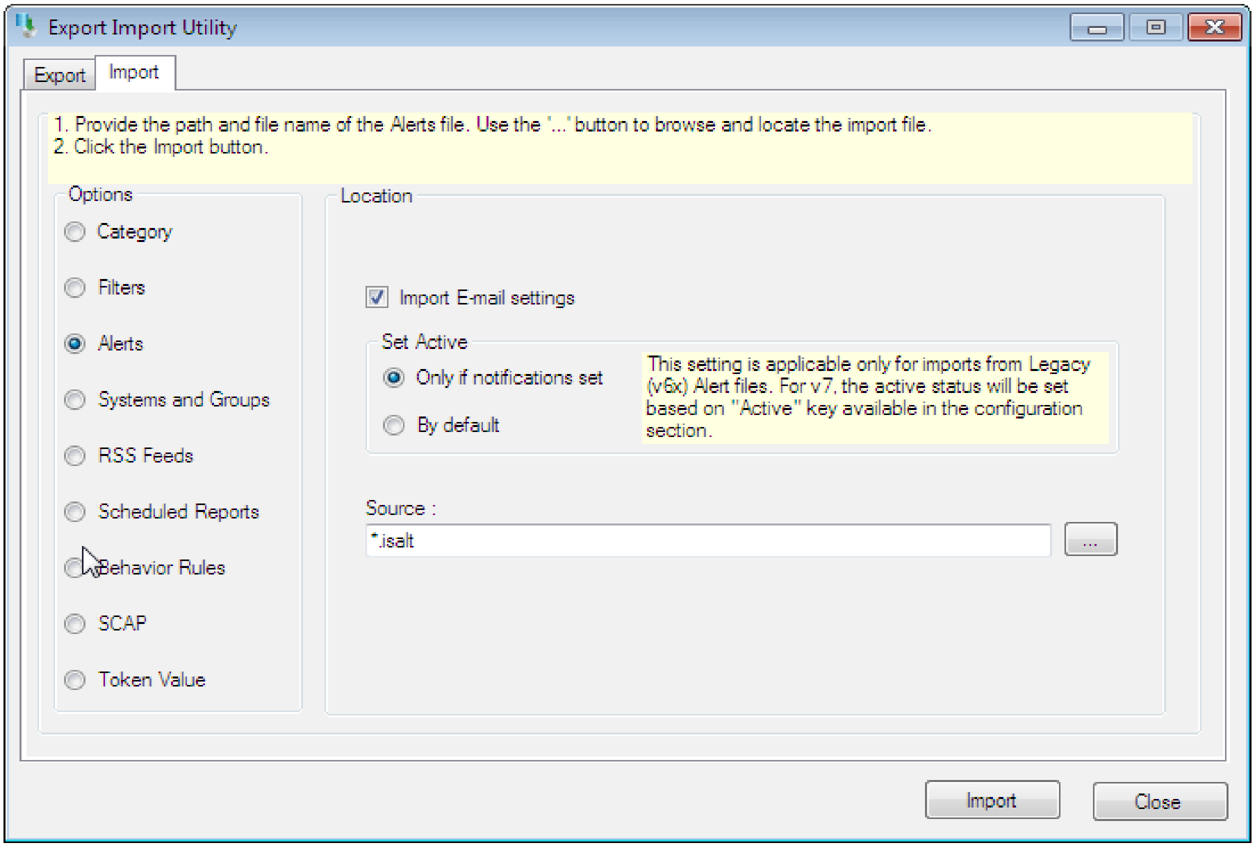


Figure 2

Alerts

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



Export Import Utility

1. Provide the path and file name of the Alerts file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Options

○ Category
○ Filters
● Alerts
○ Systems and Groups
○ RSS Feeds
○ Scheduled Reports
○ Behavior Rules
○ SCAP
○ Token Value

Location

☑ Import E-mail settings

Set Active

● Only if notifications set
○ By default

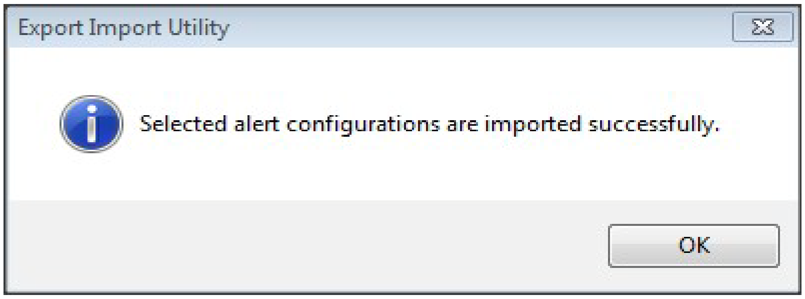
This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.

Source : *.isalt

Figure 3

2. Locate **Suricata.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

   EventTracker displays success message.



Export Import Utility

Selected alert configurations are imported successfully.

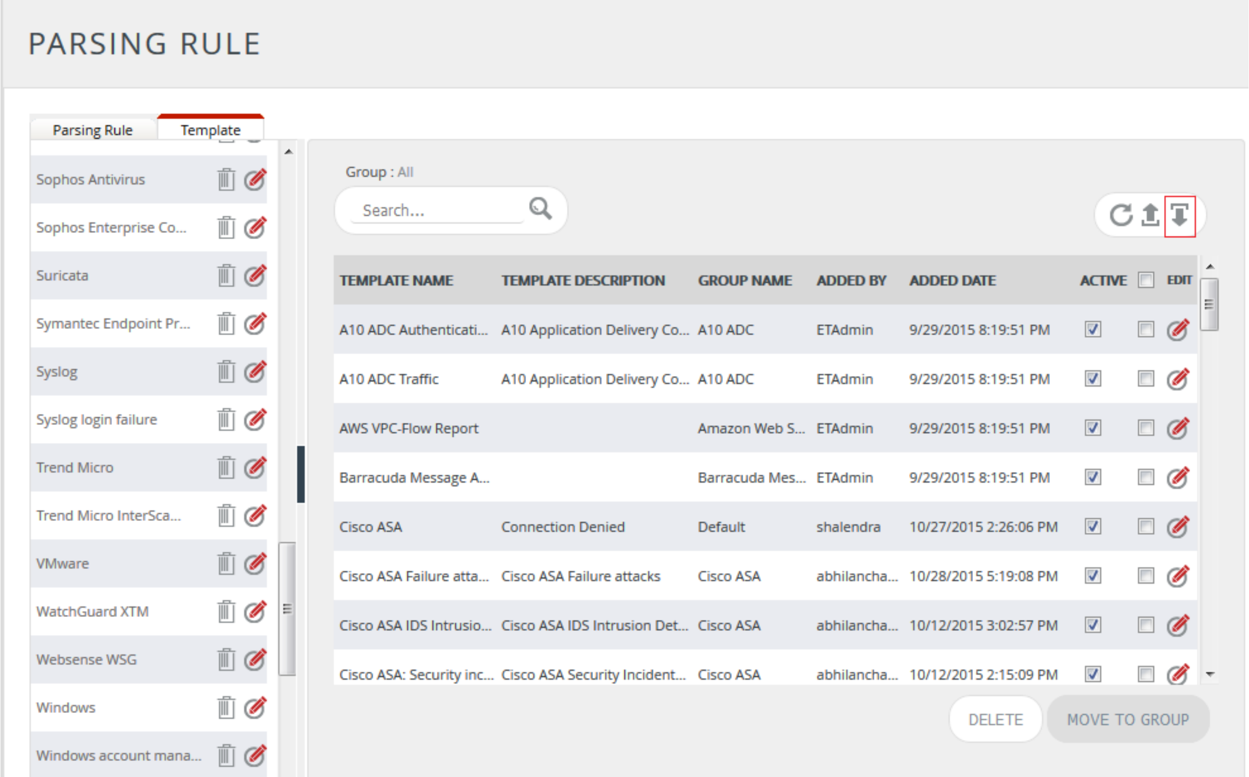
Figure 4

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

Token Templates

1. Click the **Admin** menu, and then click **Parsing rule**.

2. Select **Template** tab, and then click on ‘**Import**’ option.

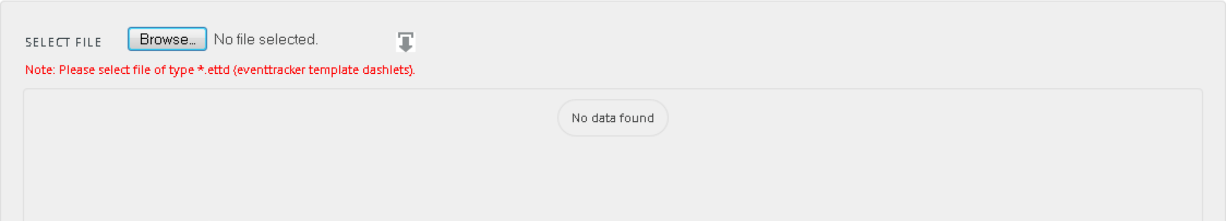


Sophos Antivirus
Sophos Enterprise Co...
Suricata
Symantec Endpoint Pr...
Syslog
Syslog login failure
Trend Micro
Trend Micro InterSca...
VMware
WatchGuard XTM
Websense WSG
Windows
Windows account mana...

TEMPLATE NAME	TEMPLATE DESCRIPTION	GROUP NAME	ADDED BY	ADDED DATE	ACTIVE	☐	EDIT
A10 ADC Authenticati...	A10 Application Delivery Co...	A10 ADC	ETAdmin	9/29/2015 8:19:51 PM	☑	☐	
A10 ADC Traffic	A10 Application Delivery Co...	A10 ADC	ETAdmin	9/29/2015 8:19:51 PM	☑	☐	
AWS VPC-Flow Report		Amazon Web S...	ETAdmin	9/29/2015 8:19:51 PM	☑	☐	
Barracuda Message A...		Barracuda Mes...	ETAdmin	9/29/2015 8:19:51 PM	☑	☐	
Cisco ASA	Connection Denied	Default	shalendra	10/27/2015 2:26:06 PM	☑	☐	
Cisco ASA Failure atta...	Cisco ASA Failure attacks	Cisco ASA	abhilancha...	10/28/2015 5:19:08 PM	☑	☐	
Cisco ASA IDS Intrusio...	Cisco ASA IDS Intrusion Det...	Cisco ASA	abhilancha...	10/12/2015 3:02:57 PM	☑	☐	
Cisco ASA: Security inc...	Cisco ASA Security Incident...	Cisco ASA	abhilancha...	10/12/2015 2:15:09 PM	☑	☐	

Figure 5

3. Click on **Browse** button.

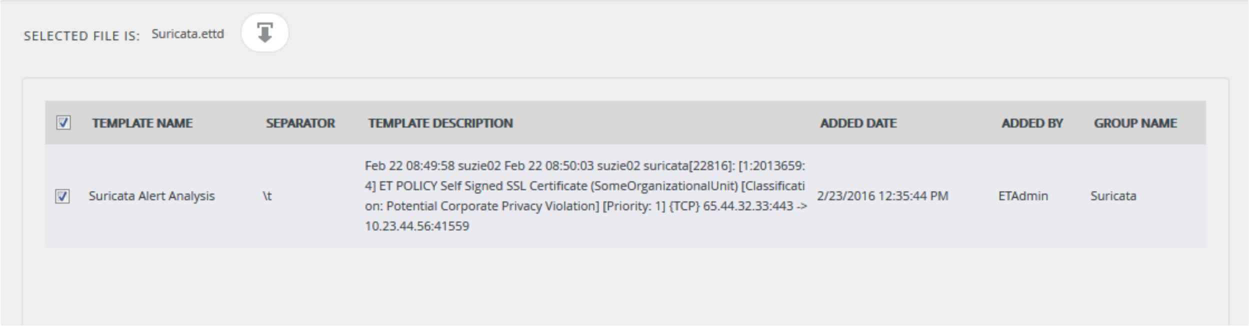


Note: Please select file of type *.ettd (eventtracker template dashlets).

No data found

Figure 6

4. Locate **Suricata.ettd** file, and then click the **Open** button

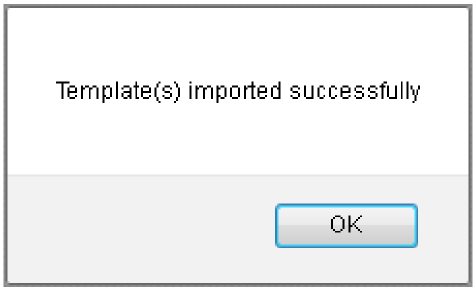


SELECTED FILE IS: Suricata.ettd

☑	TEMPLATE NAME	SEPARATOR	TEMPLATE DESCRIPTION	ADDED DATE	ADDED BY	GROUP NAME
☑	Suricata Alert Analysis	\t	Feb 22 08:49:58 suzie02 Feb 22 08:50:03 suzie02 suricata[22816]: [1:2013659:4] ET POLICY Self Signed SSL Certificate (SomeOrganizationalUnit) [Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP} 65.44.32.33:443 -> 10.23.44.56:41559	2/23/2016 12:35:44 PM	ETAdmin	Suricata

Figure 7

5. Now select the check box and then click on ‘**Import**’ option.
   EventTracker displays success message.



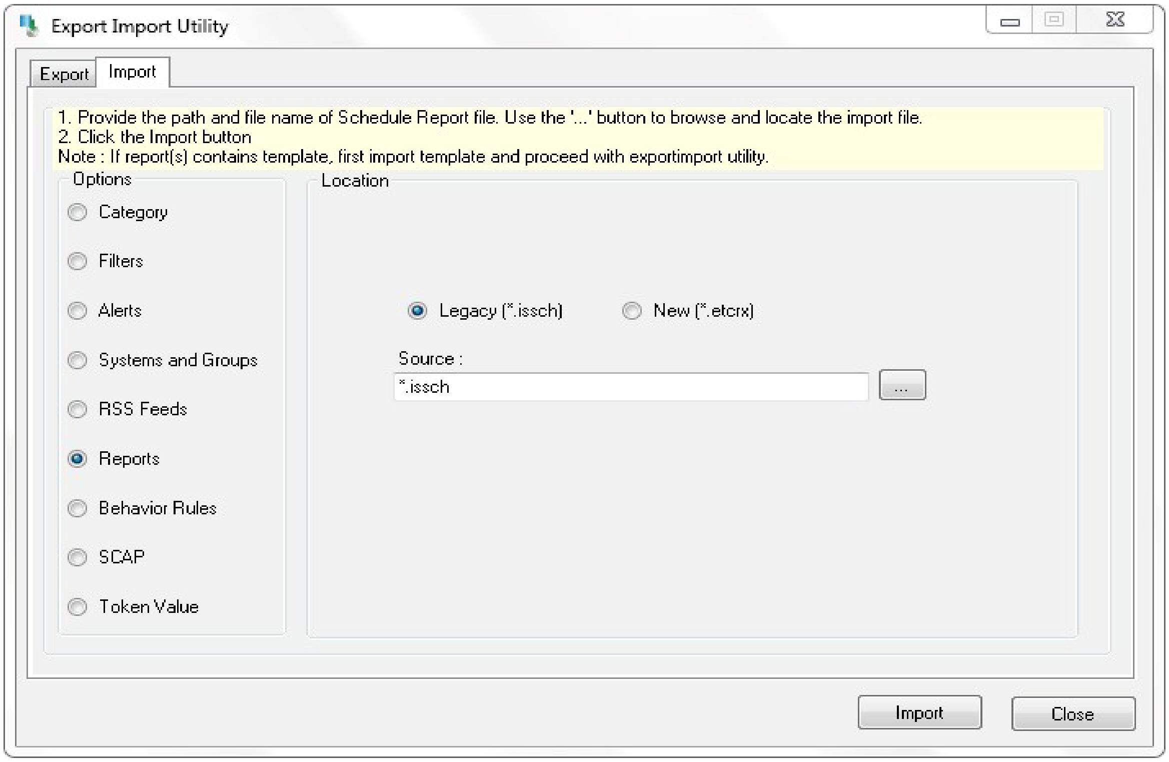
Template(s) imported successfully

Figure 8

6. Click on **OK** button.

Flex Reports

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



Export Import Utility

1. Provide the path and file name of Schedule Report file. Use the '...' button to browse and locate the import file.
2. Click the Import button
Note : If report(s) contains template, first import template and proceed with exportimport utility.

Options: ○ Category ○ Filters ○ Alerts ○ Systems and Groups ○ RSS Feeds ● Reports ○ Behavior Rules ○ SCAP ○ Token Value

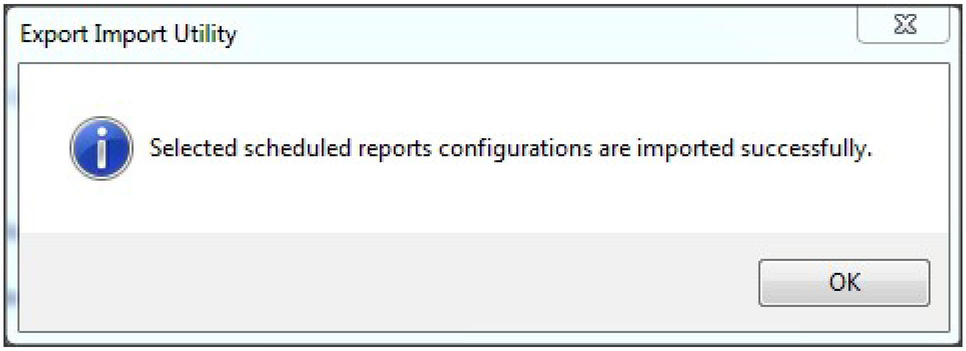
Location: ● Legacy (*.issch) ○ New (*.etcrx)

Source : *.issch

Figure 9

2. Locate **Suricata.issch** file, and then click the **Open** button.
3. To import scheduled reports, click the **Import** button.

   EventTracker displays success message.



Export Import Utility

Selected scheduled reports configurations are imported successfully.

Figure 10

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

Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects**.
2. Click on ⤓ '**Import**' option.

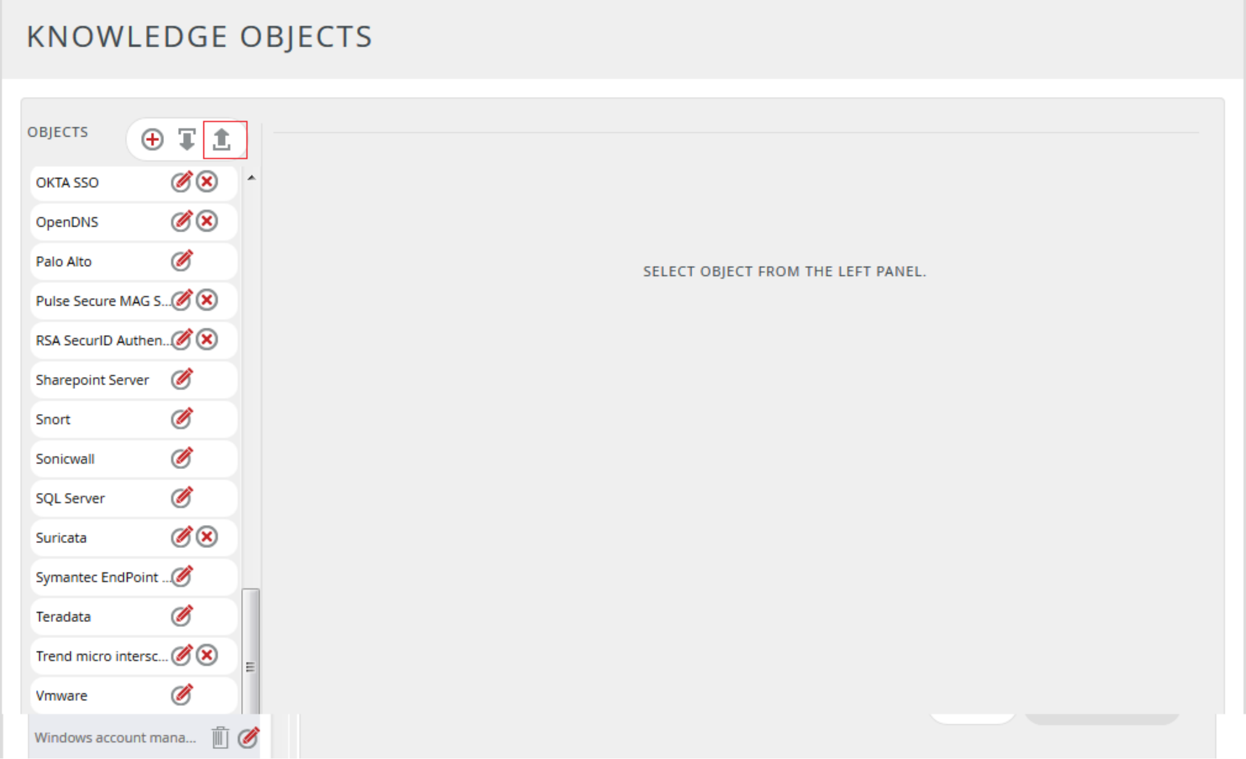


Figure 11

3. In **IMPORT** pane click on **Browse** button.

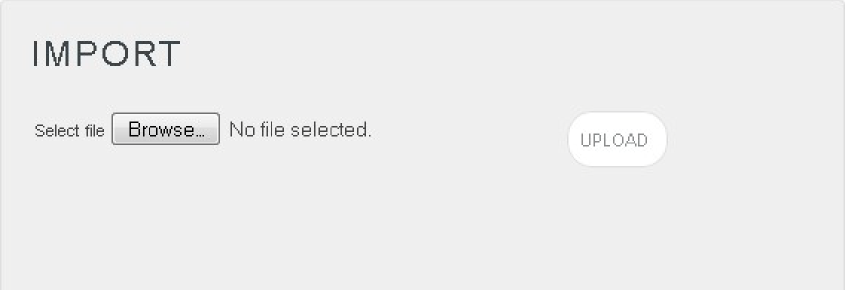
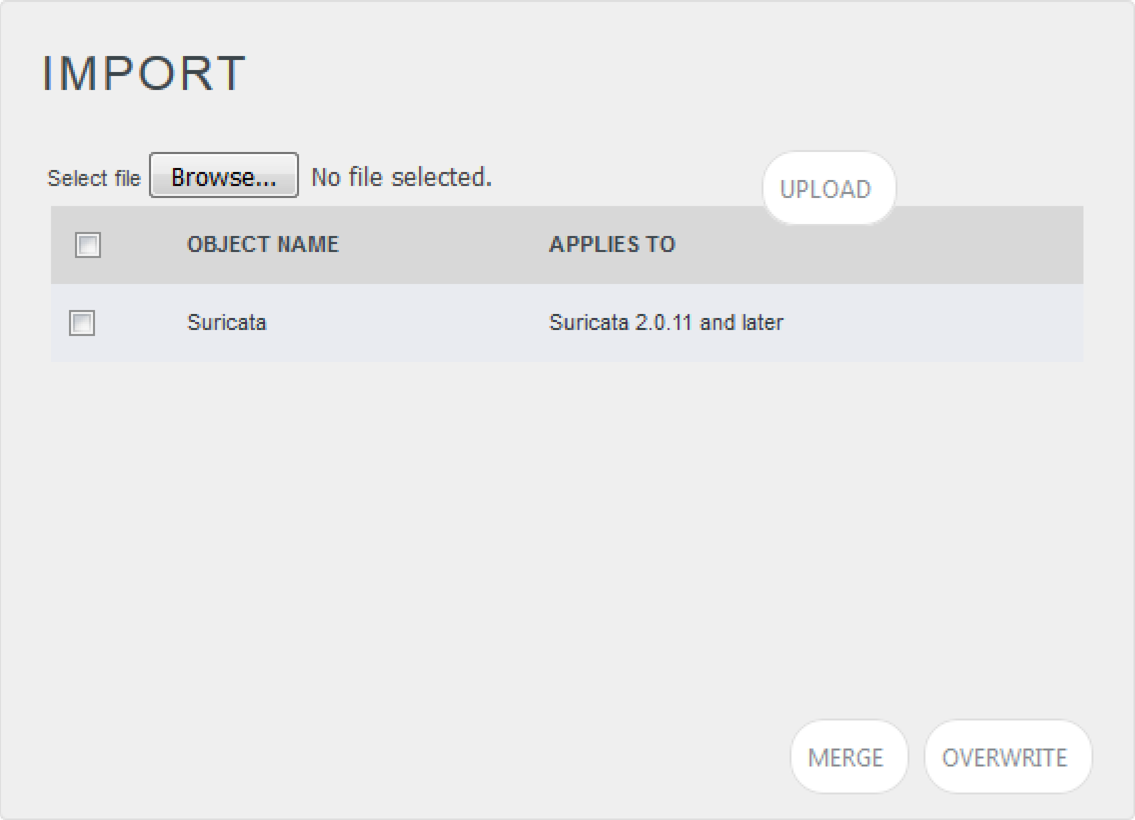


Figure 12

4. Locate **Suricata.etko** file, and then click the **UPLOAD** button.



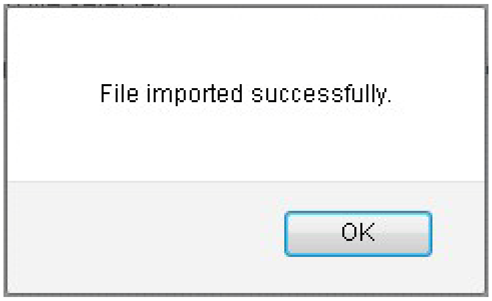
IMPORT

Select file Browse... No file selected.

□	OBJECT NAME	APPLIES TO
□	Suricata	Suricata 2.0.11 and later

Figure 13

5. Now select the check box and then click on '**OVERWRITE**' option.
   EventTracker displays success message.



File imported successfully.

Figure 14

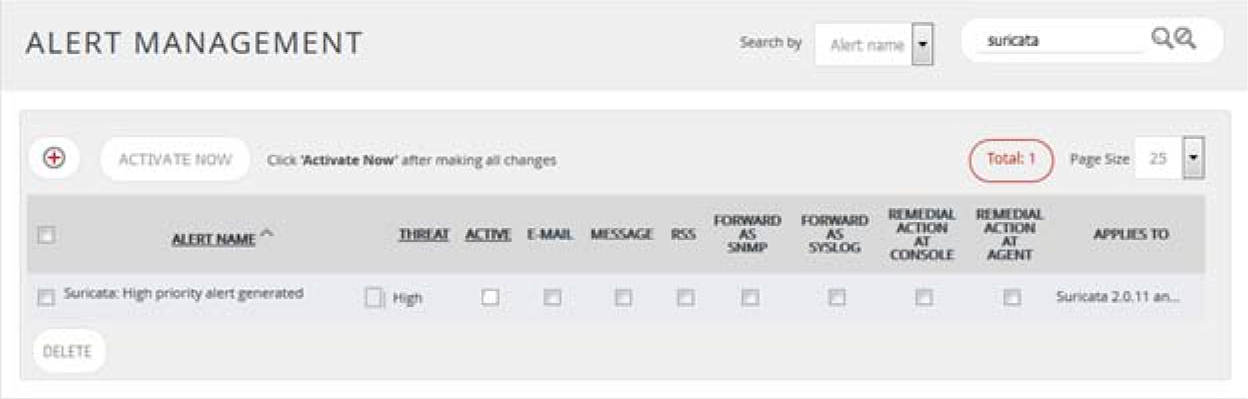
6. Click on **OK** button.

Verifying Suricata knowledge pack in EventTracker

Suricata Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Alerts**.
3. In **Search** field, type '**Suricata**', and then click the **Go** button.

Alert Management page will display all the imported Suricata alerts.



ALERT MANAGEMENT

Search by: Alert name | suricata

Click **'Activate Now'** after making all changes

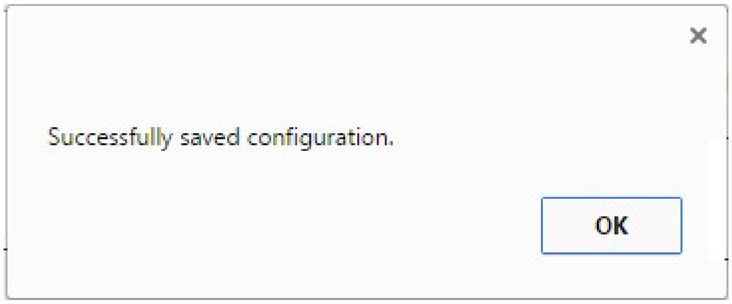
Total: 1 | Page Size 25

□	ALERT NAME	THREAT	ACTIVE	E-MAIL	MESSAGE	RSS	FORWARD AS SNMP	FORWARD AS SYSLOG	REMEDIAL ACTION AT CONSOLE	REMEDIAL ACTION AT AGENT	APPLIES TO
□	Suricata: High priority alert generated	□ High	□	□	□	□	□	□	□	□	Suricata 2.0.11 an...

Figure 15

4. To activate the imported alerts, select the respective checkbox in the **Active** column.

EventTracker displays message box.



Successfully saved configuration.

Figure 16

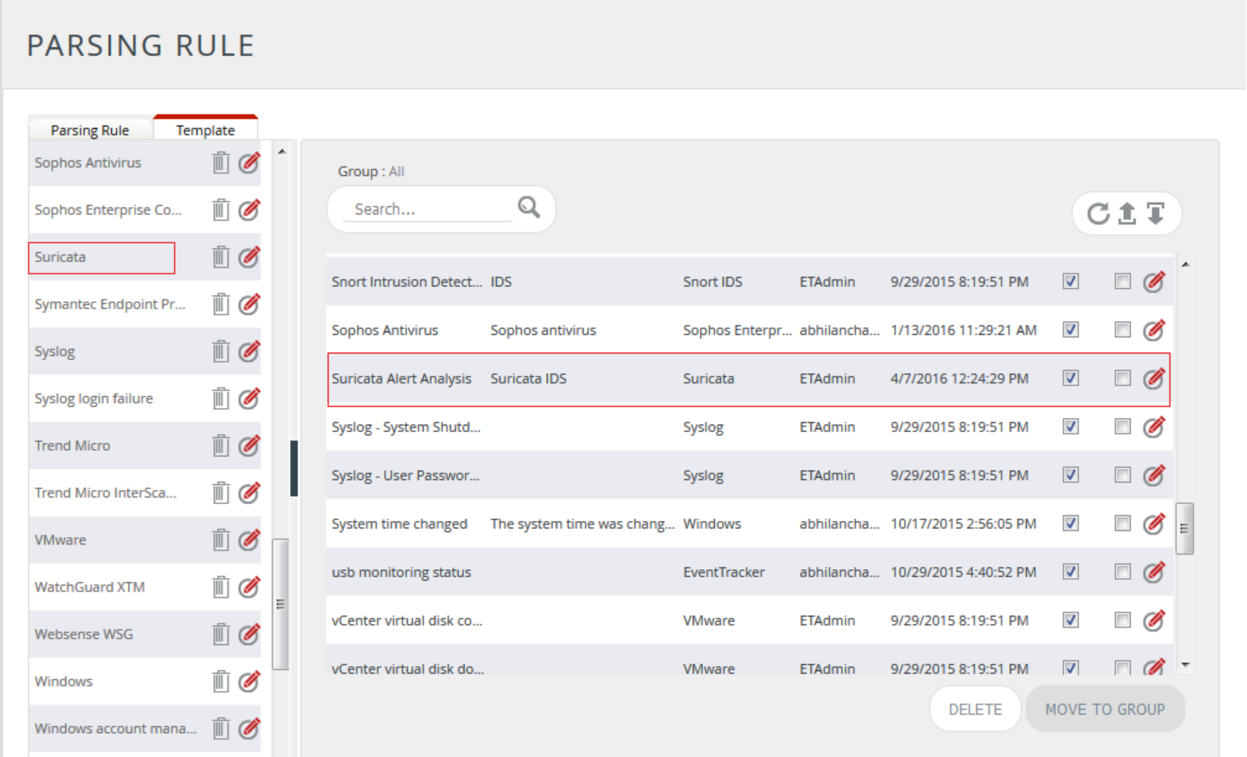
5. Click **OK**, and then click the **Activate Now** button.

NOTE:

You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.

Suricata Token Template

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Parsing Rules**.



- Sophos Antivirus
- Sophos Enterprise Co...
- Suricata
- Symantec Endpoint Pr...
- Syslog
- Syslog login failure
- Trend Micro
- Trend Micro InterSca...
- VMware
- WatchGuard XTM
- Websense WSG
- Windows
- Windows account mana...

Snort Intrusion Detect...	IDS	Snort IDS	ETAdmin	9/29/2015 8:19:51 PM	☑	☐
Sophos Antivirus	Sophos antivirus	Sophos Enterpr...	abhilancha...	1/13/2016 11:29:21 AM	☑	☐
Suricata Alert Analysis	Suricata IDS	Suricata	ETAdmin	4/7/2016 12:24:29 PM	☑	☐
Syslog - System Shutd...		Syslog	ETAdmin	9/29/2015 8:19:51 PM	☑	☐
Syslog - User Passwor...		Syslog	ETAdmin	9/29/2015 8:19:51 PM	☑	☐
System time changed	The system time was chang...	Windows	abhilancha...	10/17/2015 2:56:05 PM	☑	☐
usb monitoring status		EventTracker	abhilancha...	10/29/2015 4:40:52 PM	☑	☐
vCenter virtual disk co...		VMware	ETAdmin	9/29/2015 8:19:51 PM	☑	☐
vCenter virtual disk do...		VMware	ETAdmin	9/29/2015 8:19:51 PM	☑	☐

Figure 17

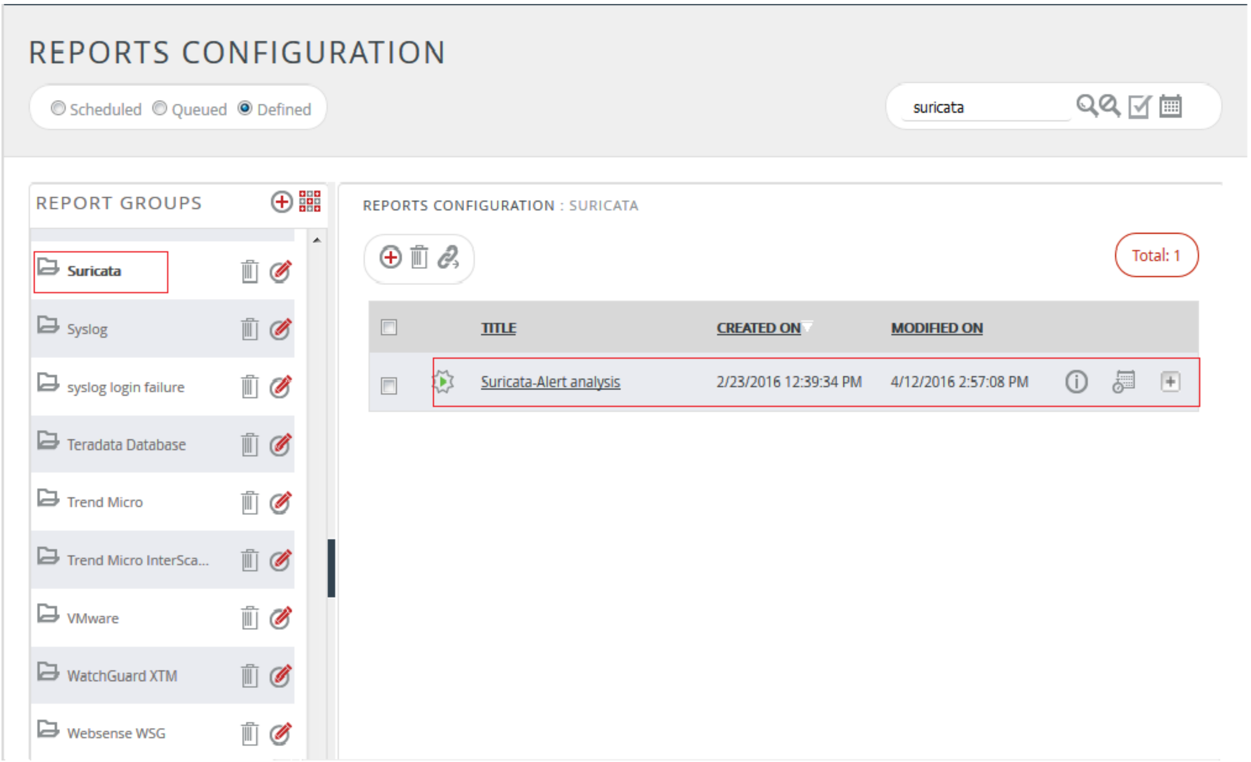
Suricata Reports

1. Logon to **EventTracker Enterprise**.
2. Click the **Reports** menu, and then select **Configuration**.
3. In **Reports Configuration** pane, select **Defined** option.

EventTracker displays **Defined** page.

4. In search box enter '**Suricata**', and then click the **Search** button.

   EventTracker displays Flex reports of Suricata.

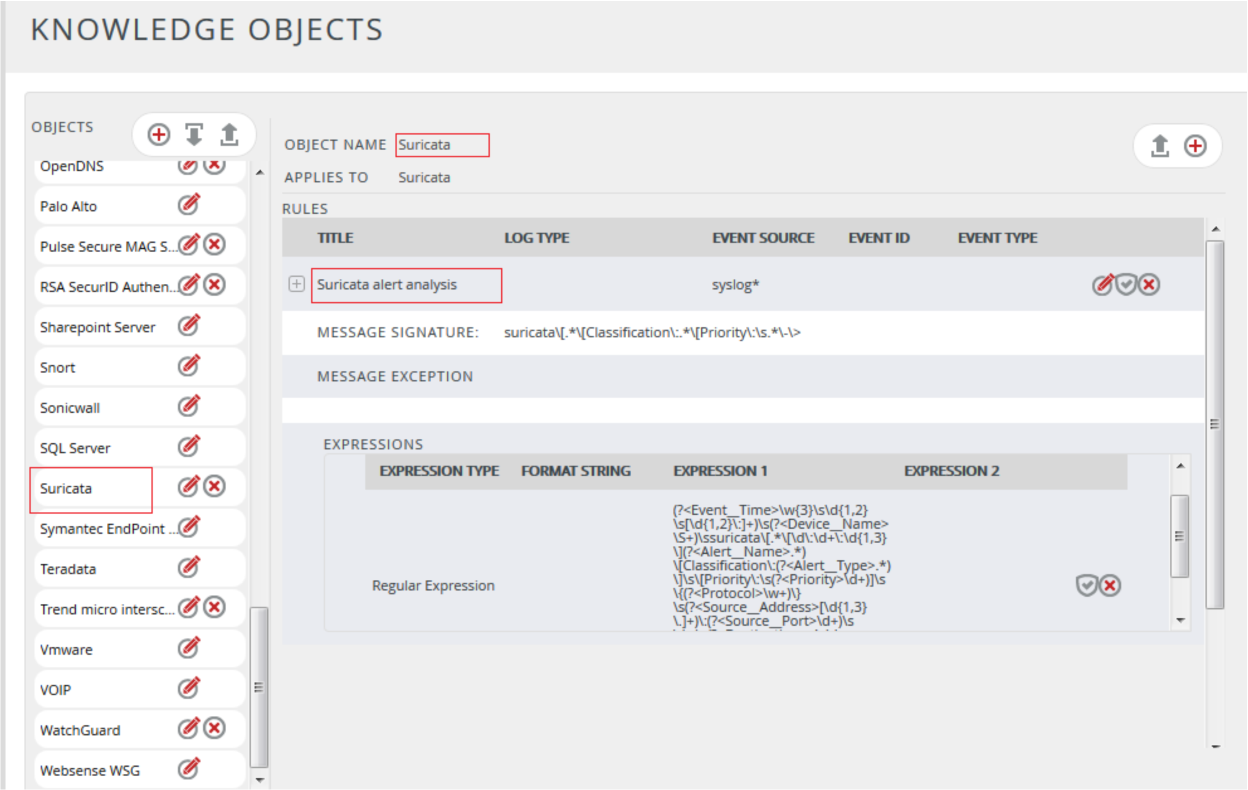


□	TITLE	CREATED ON	MODIFIED ON
□	Suricata-Alert analysis	2/23/2016 12:39:34 PM	4/12/2016 2:57:08 PM

Figure 18

Suricata Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects**
2. Scroll down and select **Suricata** in **Objects** pane. Imported **Suricata** object details are shown.



OBJECT NAME Suricata

APPLIES TO Suricata

RULES

TITLE	LOG TYPE	EVENT SOURCE	EVENT ID	EVENT TYPE
Suricata alert analysis		syslog*		

MESSAGE SIGNATURE: suricata\[.*\[Classification\:.*\[Priority\:\s.*\-\>

MESSAGE EXCEPTION

EXPRESSIONS

EXPRESSION TYPE	FORMAT STRING	EXPRESSION 1	EXPRESSION 2
Regular Expression		(?<Event__Time>\w{3}\s\d{1,2} \s[\d{1,2}\:]+)\s(?<Device__Name> \S+)\ssuricata\[.*\[\d\:\d+\:\d{1,3} \](?<Alert__Name>.*) \[Classification\:(?<Alert__Type>.*) \]\s\[Priority\:\s(?<Priority>\d+)]\s \{(?<Protocol>\w+)\} \s(?<Source__Address>[\d{1,3} \.]+)\:(?<Source__Port>\d+)\s	

Figure 19

Create Flex Dashboards in EventTracker

Schedule Reports

1. Open **EventTracker** in browser and logon.

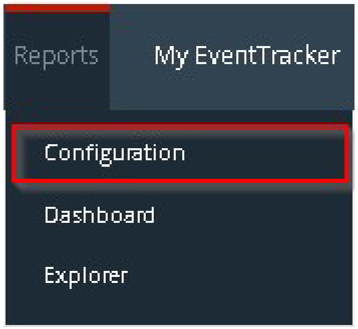
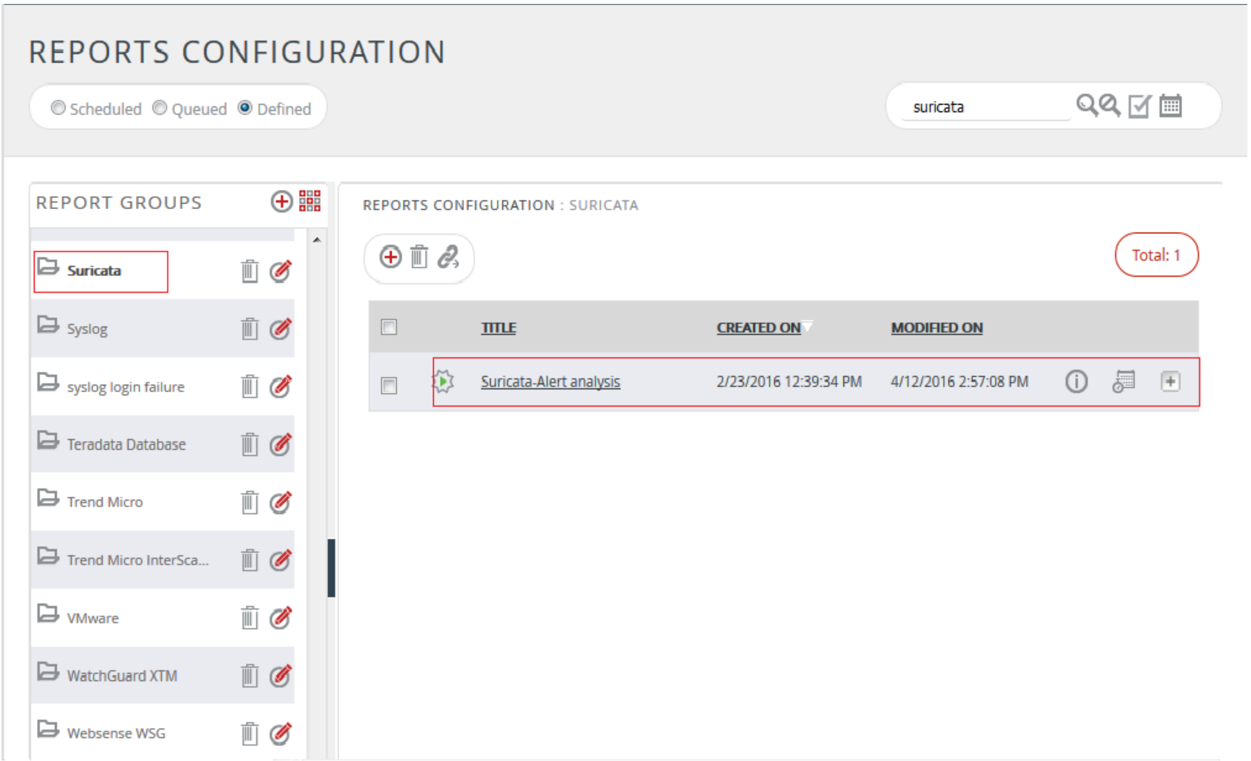


Figure 20

2. Navigate to **Reports>Configuration**.



REPORTS CONFIGURATION

○ Scheduled ○ Queued ● Defined

suricata

REPORT GROUPS

- Suricata
- Syslog
- syslog login failure
- Teradata Database
- Trend Micro
- Trend Micro InterSca...
- VMware
- WatchGuard XTM
- Websense WSG

REPORTS CONFIGURATION : SURICATA

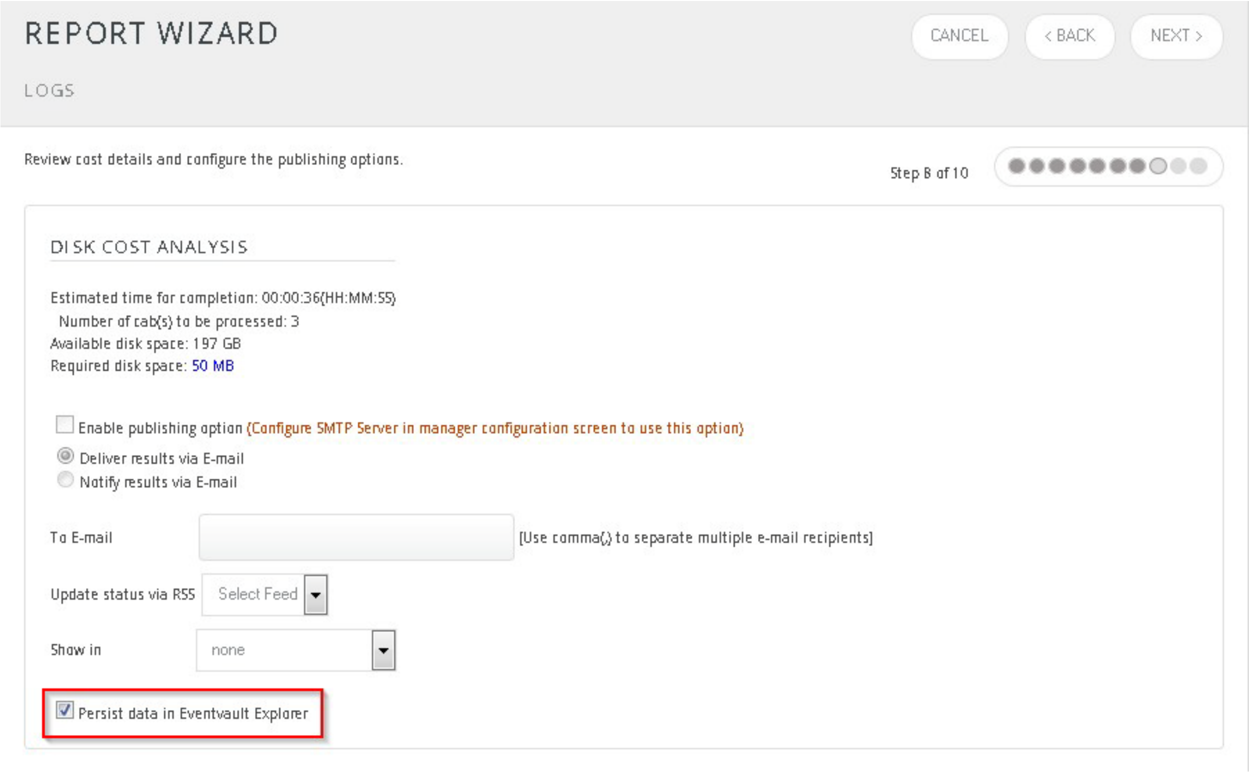
Total: 1

□	TITLE	CREATED ON	MODIFIED ON
□	Suricata-Alert analysis	2/23/2016 12:39:34 PM	4/12/2016 2:57:08 PM

Figure 21

3. Select **Suricata** in report groups. Check **defined** dialog box.

4. Click on '**schedule**' to plan a report for later execution.



Review cost details and configure the publishing options.

Step 8 of 10

DISK COST ANALYSIS

Estimated time for completion: 00:00:36(HH:MM:SS)
Number of cab(s) to be processed: 3
Available disk space: 197 GB
Required disk space: 50 MB

□ Enable publishing option (Configure SMTP Server in manager configuration screen to use this option)
● Deliver results via E-mail
○ Notify results via E-mail

To E-mail [Use comma(,) to separate multiple e-mail recipients]

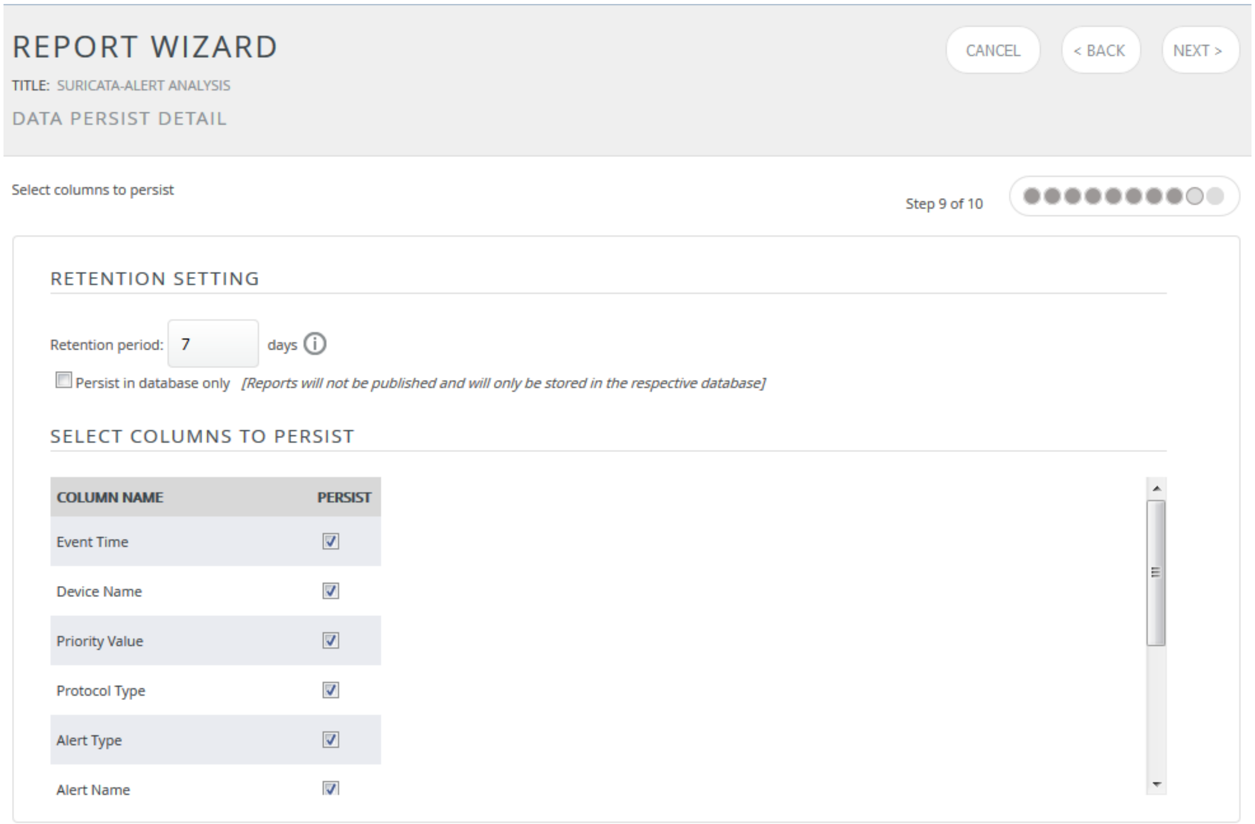
Update status via RSS Select Feed

Show in none

☑ Persist data in Eventvault Explorer

Figure 22

5. Choose appropriate time for report execution and in **Step 8** check **Persist data in Eventvault explorer** box.



REPORT WIZARD

TITLE: SURICATA-ALERT ANALYSIS

DATA PERSIST DETAIL

Select columns to persist

Step 9 of 10

RETENTION SETTING

Retention period: 7 days

□ Persist in database only *[Reports will not be published and will only be stored in the respective database]*

SELECT COLUMNS TO PERSIST

COLUMN NAME	PERSIST
Event Time	☑
Device Name	☑
Priority Value	☑
Protocol Type	☑
Alert Type	☑
Alert Name	☑

Figure 23

6. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.

7. Proceed to next step and click **Schedule** button.

8. Wait for scheduled time or generate report manually.

Create Dashlets

1. **EventTracker 8** is required to configure flex dashboard.
2. Open **EventTracker** in browser and logon.

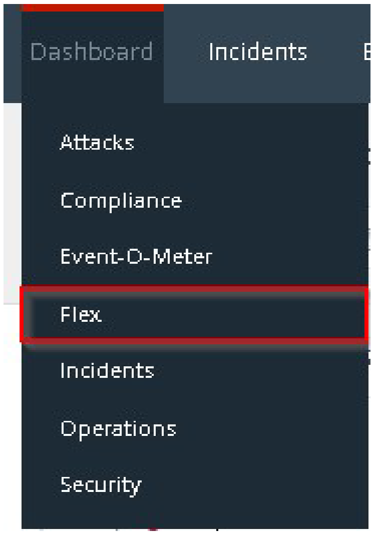
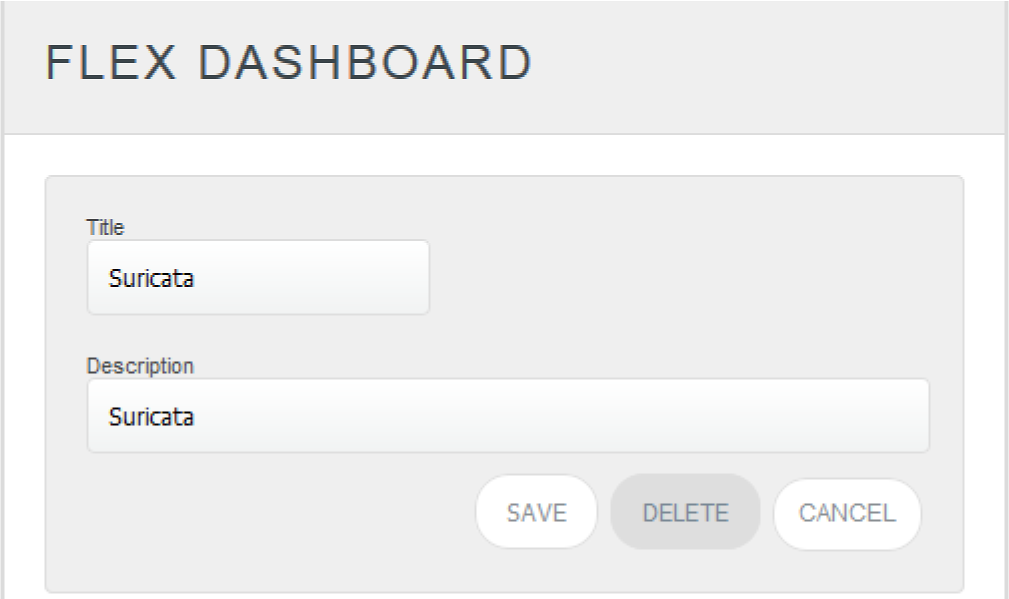


Figure 24

3. Navigate to **Dashboard>Flex**.
   Flex Dashboard pane is shown.

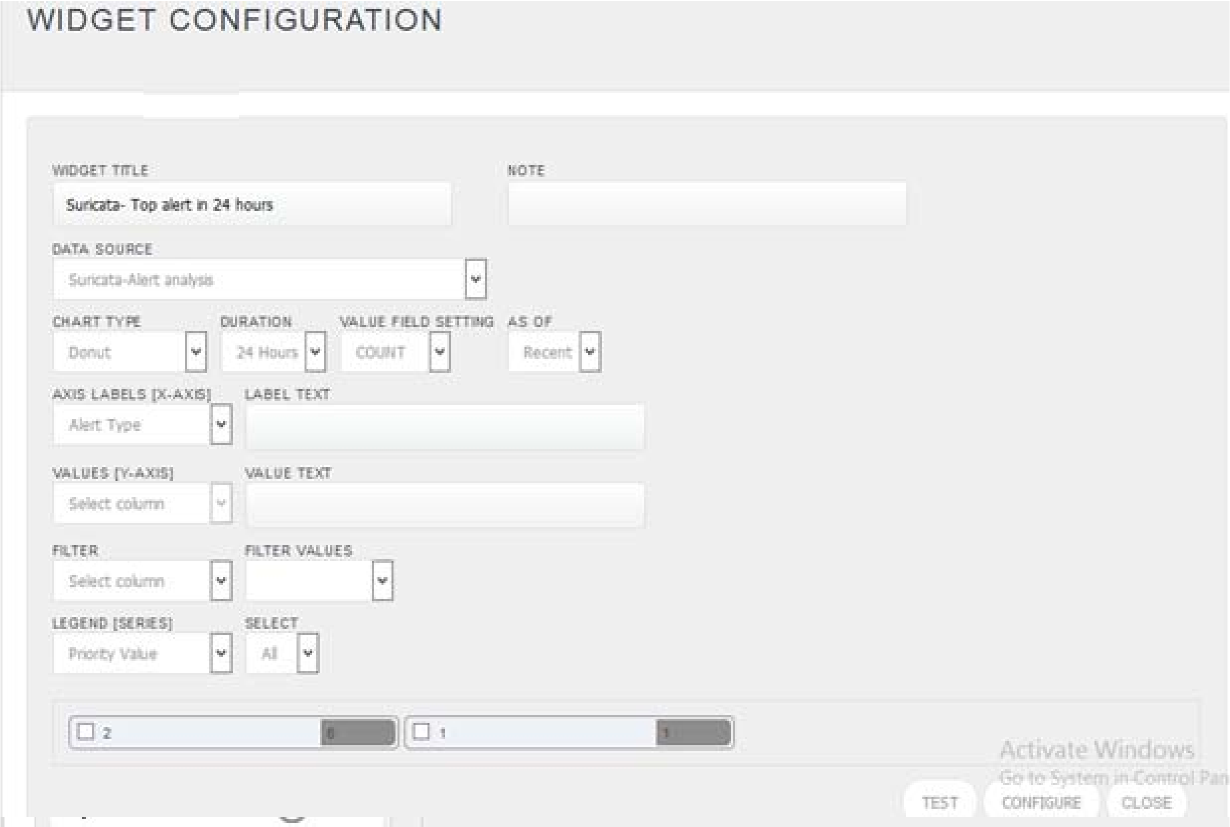

FLEX DASHBOARD

Title: Suricata

Description: Suricata

Figure 25

4. Fill suitable title and description and click **Save** button.
5. Click ⚙ to configure a new flex dashlet. Widget configuration pane is shown.



WIDGET CONFIGURATION

WIDGET TITLE: Suricata- Top alert in 24 hours

NOTE:

DATA SOURCE: Suricata-Alert analysis

CHART TYPE: Donut

DURATION: 24 Hours

VALUE FIELD SETTING: COUNT

AS OF: Recent

AXIS LABELS [X-AXIS]: Alert Type

LABEL TEXT:

VALUES [Y-AXIS]: Select column

VALUE TEXT:

FILTER: Select column

FILTER VALUES:

LEGEND [SERIES]: Priority Value

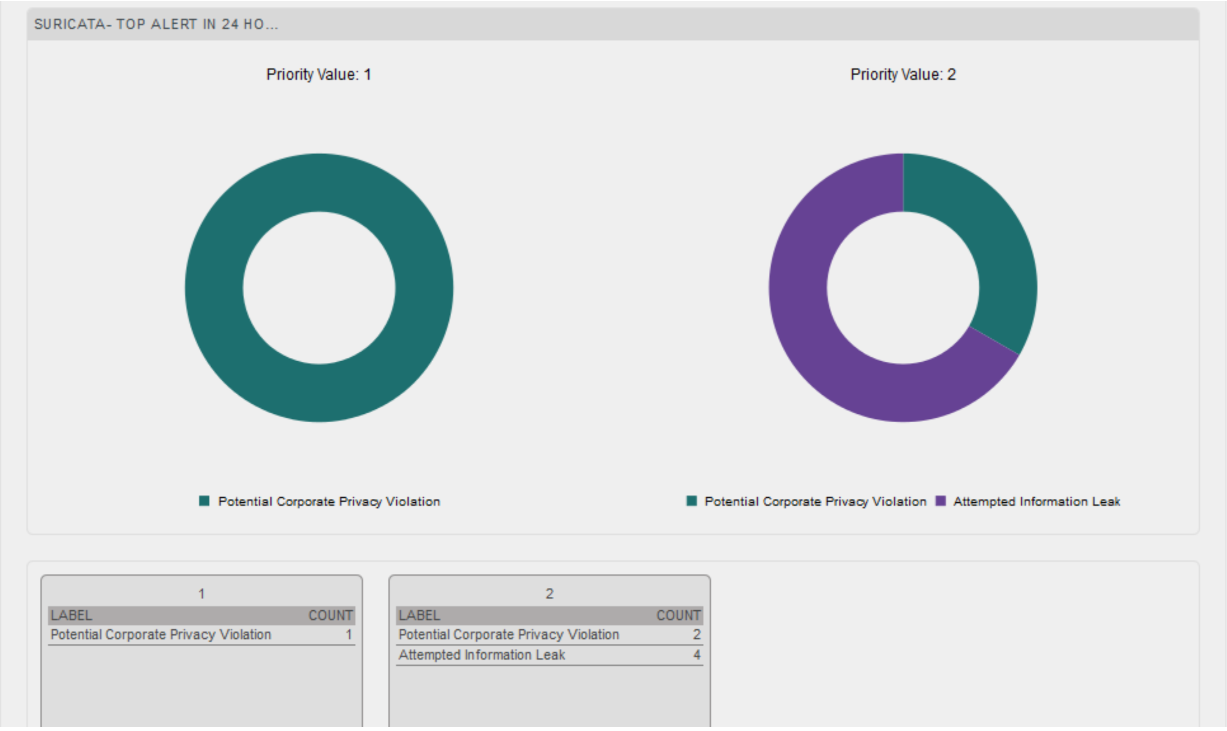
SELECT: All

□ 2 6

□ 1 1

Figure 26

4. Locate earlier scheduled report in **Data Source** dropdown.
5. Select **Chart Type** from dropdown.
6. Select extent of data to be displayed in **Duration** dropdown.
7. Select computation type in **Value Field Setting** dropdown.
8. Select evaluation duration in **as Of** dropdown.
9. Select comparable values in **X Axis** with suitable label.
10. Select numeric values in **Y Axis** with suitable label.
11. Select comparable sequence in **Legend**.
12. Click **Test** button to evaluate. Evaluated chart is shown.



1

LABEL	COUNT
Potential Corporate Privacy Violation	1

2

LABEL	COUNT
Potential Corporate Privacy Violation	2
Attempted Information Leak	4

Figure 27

13. If satisfied, click **Configure** button

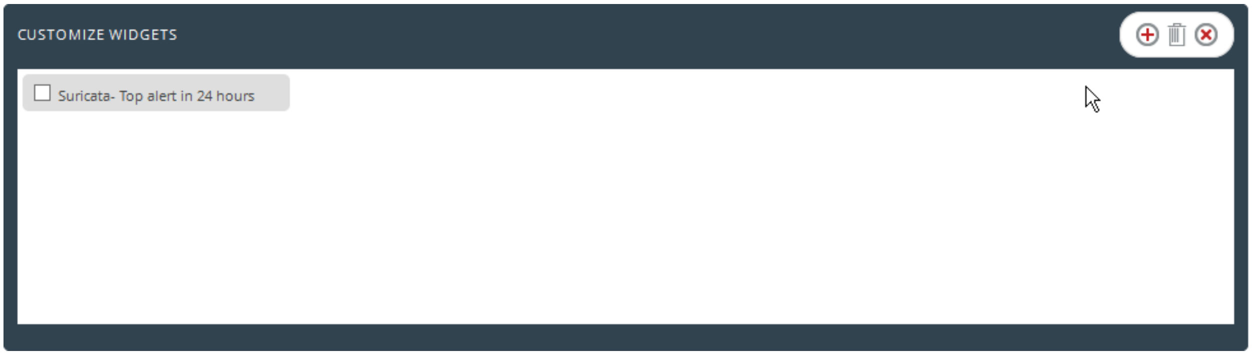


Figure 28

14. Click 'customize' ⚙ to locate and choose created dashlet.
15. Click ⊕ to add dashlet to earlier created dashboard.

Sample Dashboards

1. Suricata- Top alerts in 24 hours

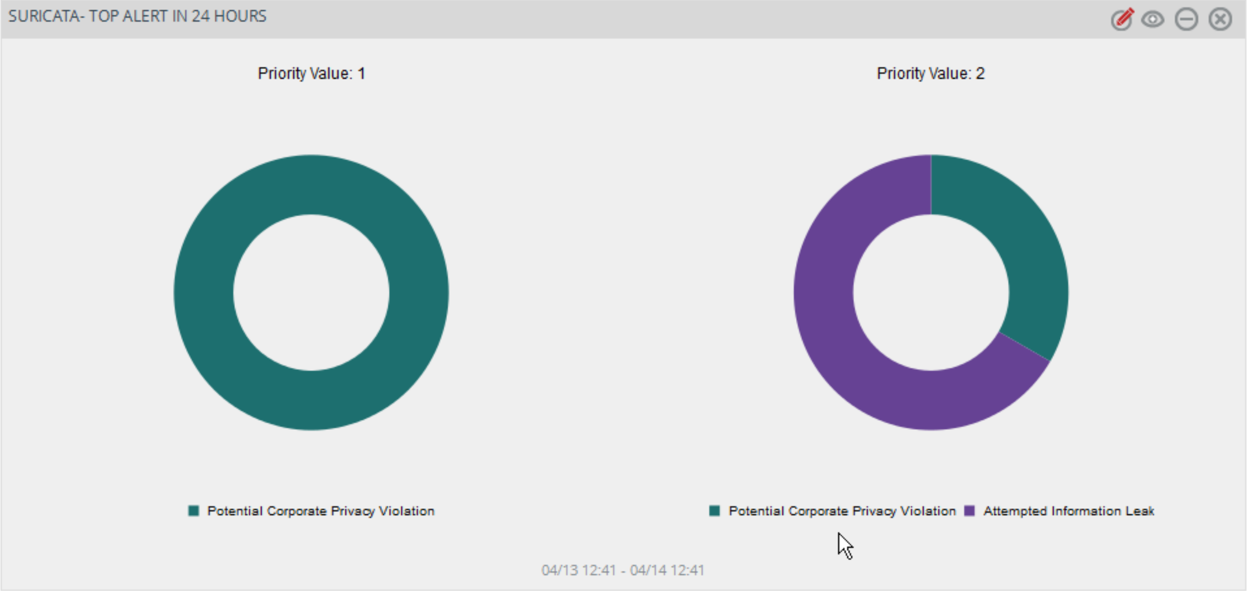

SURICATA- TOP ALERT IN 24 HOURS
Priority Value: 1
Priority Value: 2
🟩 Potential Corporate Privacy Violation
🟩 Potential Corporate Privacy Violation
🟪 Attempted Information Leak
04/13 12:41 - 04/14 12:41

Figure 29