Integrate EventTracker Endpoint Security

EventTracker v9.2x and above

Publication Date: January 15, 2021

Abstract

This guide provides instructions to configure EventTracker Endpoint Security to send its logs to EventTracker.

Scope

The configuration details in this guide are consistent with EventTracker version v9.2x or above and **EventTracker Endpoint Security**

Audience

Administrators who are assigned task to monitor EventTracker Endpoint Security events using EventTracker.

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

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

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

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

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

Table of Contents

1. Overview

EventTracker Endpoint Security provides a predictive threat prevention platform by applying deep learning with its advanced artificial intelligences to cybersecurity.
Its on-device solution protects against zero-day threats and APT attacks with unmatched accuracy. It safeguards the enterprise's endpoints and mobile devices against threats on any infrastructure and provides protection against unknown and evasive cyber-attacks.

EventTracker helps to monitor events from EventTracker Endpoint Security. Its dashboard displays information for EventTracker Endpoint Security and Endpoint Security. Dashboard shows any threat detected and prevented on hosts, login activities, top high-risk users and hosts, malware family detected.

EventTracker reports will provide threat activity, administrator activity and login activity information containing username, hostname, Ip, virus/malware and other important details.

EventTracker's built-in knowledge pack enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

2. Prerequisites

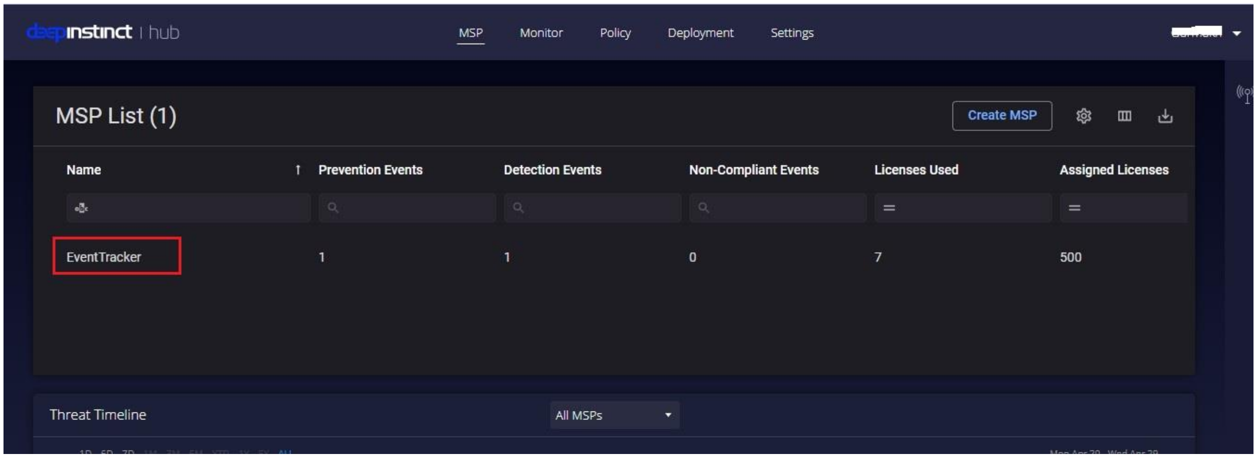
- Admin privileges for **EventTracker Endpoint Security**.
- **EventTracker agent** should be installed in the system.

3. Integration of EventTracker Endpoint Security with EventTracker

3.1 Integration can be performed via syslog configuration

Follow the below steps to configure syslog.

1. Login to the EventTracker Endpoint Security console.
2. Click on the MSP Name.

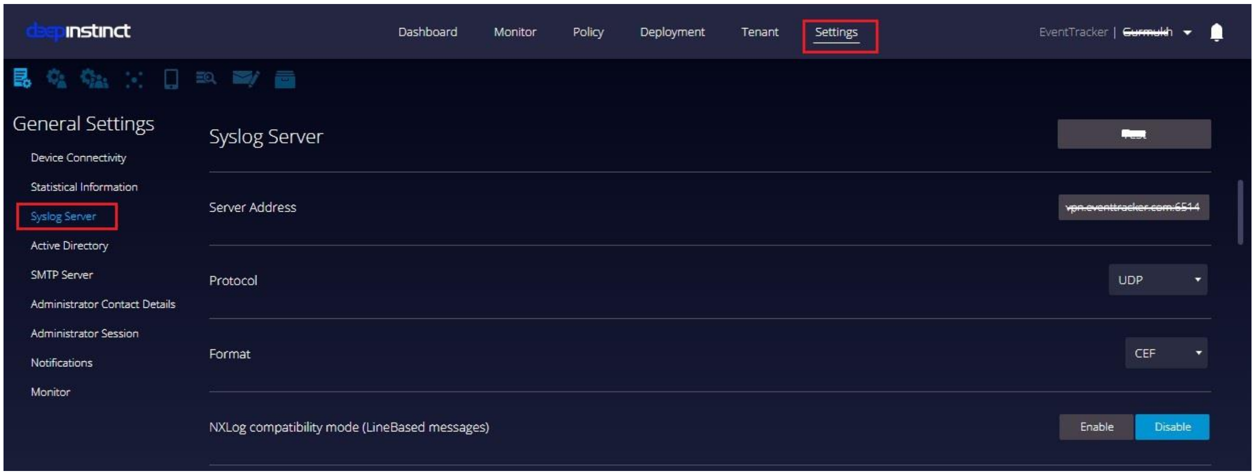


MSP List (1)

Name	Prevention Events	Detection Events	Non-Compliant Events	Licenses Used	Assigned Licenses
EventTracker	1	1	0	7	500

Figure 1

3. A new page opens, go to **setting > syslog server.**
4. Fill in the required details:



Syslog Server [redacted]

Server Address ~~vpn.eventtracker.com:6514~~

Protocol UDP

Format CEF

NXLog compatibility mode (LineBased messages) Enable Disable

Figure 2

- Syslog Server as **Manager Name**
- Server Address as **EventTracker Manager IP**
- Protocol as **UDP**.
- Format as **CEF**.

Integration is complete, EventTracker will receive EventTracker Endpoint Security logs.

4. EventTracker Knowledge Pack

After receiving the logs from EventTracker manager, knowledge packs can be configured into EventTracker.

The following knowledge packs are available in EventTracker to support EventTracker Endpoint Security.

4.1 Category

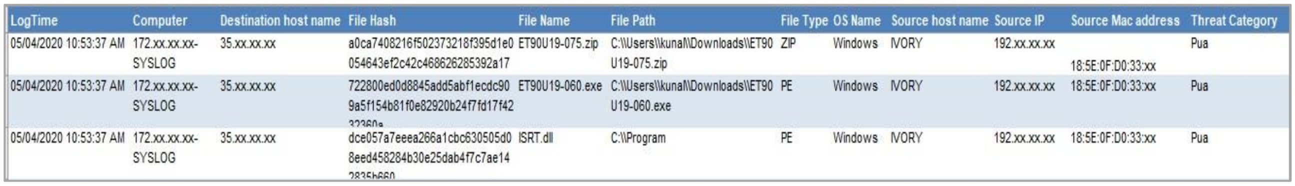
- **EventTracker Endpoint Security: login failed -** This category provides information related to login failure detected in EventTracker Endpoint Security.
- **EventTracker Endpoint Security: Login/Logout activity –** This category provides information related to all login and logout activity performed in EventTracker Endpoint Security.
- **EventTracker Endpoint Security: Non-Compliant Events –** This category provides information related to all the Non-Compliant related activity.
- **EventTracker Endpoint Security: Threat Detected –** This category provides information related to all the security events detected by EventTracker Endpoint Security.
- **EventTracker Endpoint Security: Security Event Prevented –** This category provides information related to all the security events prevented by EventTracker Endpoint Security.
- **EventTracker Endpoint Security: Policy Management -** This category provides information related to all policy management activity.
- **EventTracker Endpoint Security: Whitelist/Blacklist Activity -** This category provides information related to all whitelist/blacklist activities.

4.2 Alert

- **EventTracker Endpoint Security: Login failed -** This alert is generated when any login failure is detected in EventTracker Endpoint Security.
- **EventTracker Endpoint Security: Threat Detected –** This alert is generated when any security event/attack is detected.
- **EventTracker Endpoint Security: Non-Compliant event –** This alert is generated when any non-compliant event is detected.
- **EventTracker Endpoint Security: Threat Prevented –** This alert is generated when any threat is prevented.

4.3 Report

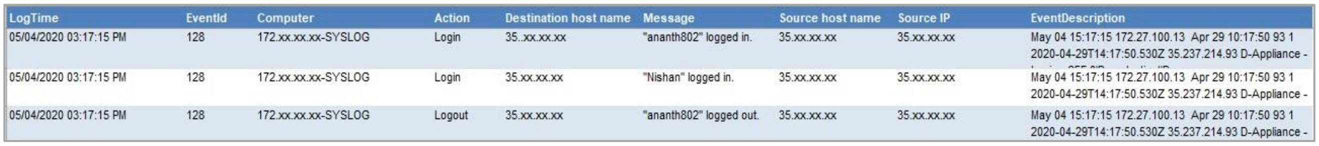
- **EventTracker Endpoint Security Threat Activity Report-** This report provides information about all the security events such as malware/virus or any attack is detected. Report contains username, source IP, hostname, mac address, file path , filetype, attack type and various details which can be useful for further analysis.



LogTime	Computer	Destination host name	File Hash	File Name	File Path	File Type	OS Name	Source host name	Source IP	Source Mac address	Threat Category
05/04/2020 10:53:37 AM	172.xx.xx.xx-SYSLOG	35.xx.xx.xx	a0ca7408216f502373218f395d1e0054643ef2c42c468626285392a17	ET90U19-075.zip	C:\\Users\\kunal\\Downloads\\ET90U19-075.zip	ZIP	Windows	IVORY	192.xx.xx.xx	18:5E:0F:D0:33:xx	Pua
05/04/2020 10:53:37 AM	172.xx.xx.xx-SYSLOG	35.xx.xx.xx	722800ed0d8845add5abf1ecdc909a5f154b81f0e82920b24f7fd17f4232360a	ET90U19-060.exe	C:\\Users\\kunal\\Downloads\\ET90U19-060.exe	PE	Windows	IVORY	192.xx.xx.xx	18:5E:0F:D0:33:xx	Pua
05/04/2020 10:53:37 AM	172.xx.xx.xx-SYSLOG	35.xx.xx.xx	dce057a7eeea266a1cbc630505d08eed458284b30e25dab4f7c7ae142835b660	ISRT.dll	C:\\Program	PE	Windows	IVORY	192.xx.xx.xx	18:5E:0F:D0:33:xx	Pua

Figure 3

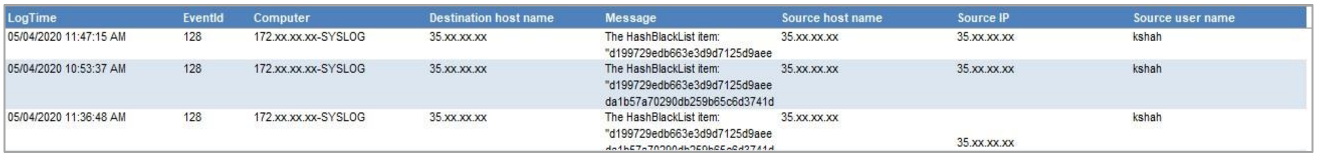
- **EventTracker Endpoint Security Login Activity Report –** This report provides information related to all the login and logout activity detected in EventTracker Endpoint Security. Report contains username, source IP and activity details along with other information.



LogTime	EventId	Computer	Action	Destination host name	Message	Source host name	Source IP	EventDescription
05/04/2020 03:17:15 PM	128	172.xx.xx.xx-SYSLOG	Login	35..xx.xx.xx	"ananth802" logged in.	35.xx.xx.xx	35.xx.xx.xx	May 04 15:17:15 172.27.100.13 Apr 29 10:17:50 93 1 2020-04-29T14:17:50.530Z 35.237.214.93 D-Appliance -
05/04/2020 03:17:15 PM	128	172.xx.xx.xx-SYSLOG	Login	35.xx.xx.xx	"Nishan" logged in.	35.xx.xx.xx	35.xx.xx.xx	May 04 15:17:15 172.27.100.13 Apr 29 10:17:50 93 1 2020-04-29T14:17:50.530Z 35.237.214.93 D-Appliance -
05/04/2020 03:17:15 PM	128	172.xx.xx.xx-SYSLOG	Logout	35.xx.xx.xx	"ananth802" logged out.	35.xx.xx.xx	35.xx.xx.xx	May 04 15:17:15 172.27.100.13 Apr 29 10:17:50 93 1 2020-04-29T14:17:50.530Z 35.237.214.93 D-Appliance -

Figure 4

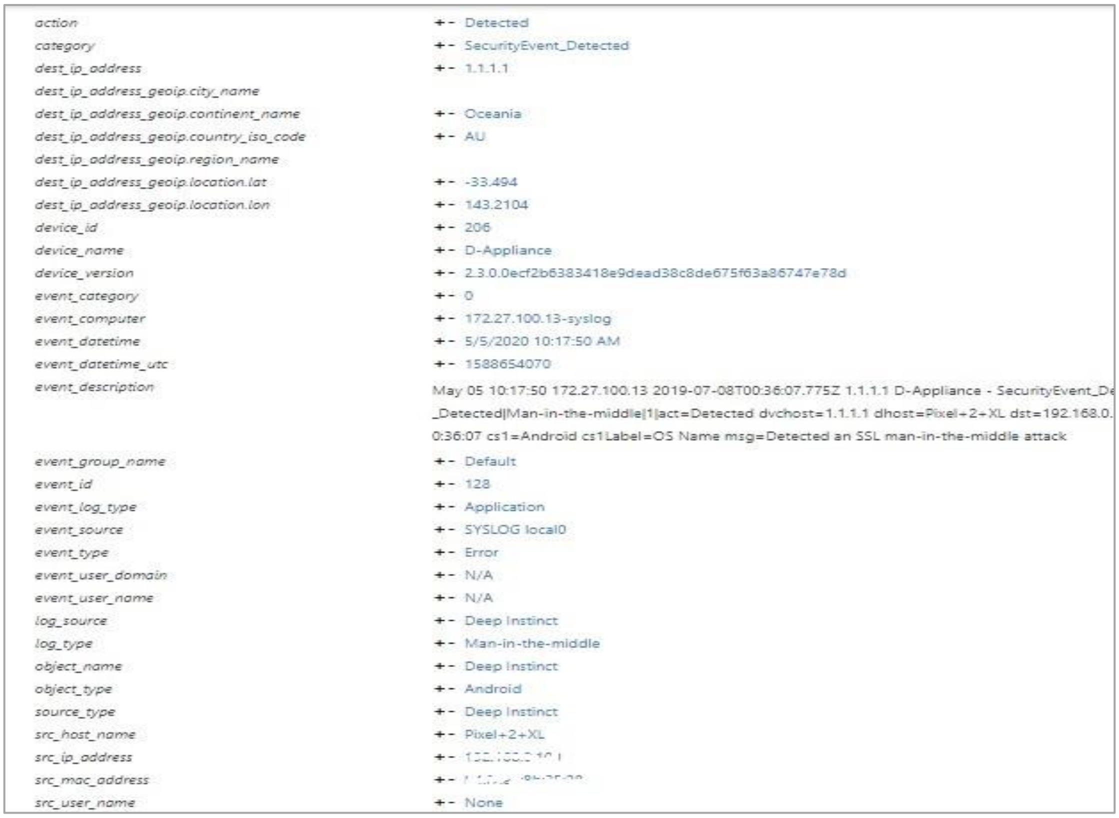
- **EventTracker Endpoint Security Administrator Activity Report-** This report provides information about all the administrator activity performed. Report contains admin username, source IP, hostname, activity details along with other useful information.



LogTime	EventId	Computer	Destination host name	Message	Source host name	Source IP	Source user name
05/04/2020 11:47:15 AM	128	172.xx.xx.xx-SYSLOG	35.xx.xx.xx	The HashBlackList item: "d199729edb663e3d9d7125d9aee	35.xx.xx.xx	35.xx.xx.xx	kshah
05/04/2020 10:53:37 AM	128	172.xx.xx.xx-SYSLOG	35.xx.xx.xx	The HashBlackList item: "d199729edb663e3d9d7125d9aeeda1b57a70290db259b65c6d3741d	35.xx.xx.xx	35.xx.xx.xx	kshah
05/04/2020 11:36:48 AM	128	172.xx.xx.xx-SYSLOG	35.xx.xx.xx	The HashBlackList item: "d199729edb663e3d9d7125d9aeeda1b57a70290db259b65c6d3741d	35.xx.xx.xx	35.xx.xx.xx	kshah

Figure 5

- **Logs Considered**



action	+- Detected
category	+- SecurityEvent_Detected
dest_ip_address	+- 1.1.1.1
dest_ip_address_geoip.city_name	
dest_ip_address_geoip.continent_name	+- Oceania
dest_ip_address_geoip.country_iso_code	+- AU
dest_ip_address_geoip.region_name	
dest_ip_address_geoip.location.lat	+- -33.494
dest_ip_address_geoip.location.lon	+- 143.2104
device_id	+- 206
device_name	+- D-Appliance
device_version	+- 2.3.0.0ecf2b6383418e9dead38c8de675f63a86747e78d
event_category	+- 0
event_computer	+- 172.27.100.13-syslog
event_datetime	+- 5/5/2020 10:17:50 AM
event_datetime_utc	+- 1588654070
event_description	May 05 10:17:50 172.27.100.13 2019-07-08T00:36:07.775Z 1.1.1.1 D-Appliance - SecurityEvent_De _Detected|Man-in-the-middle|1|act=Detected dvchost=1.1.1.1 dhost=Pixel+2+XL dst=192.168.0. 0:36:07 cs1=Android cs1Label=OS Name msg=Detected an SSL man-in-the-middle attack
event_group_name	+- Default
event_id	+- 128
event_log_type	+- Application
event_source	+- SYSLOG local0
event_type	+- Error
event_user_domain	+- N/A
event_user_name	+- N/A
log_source	+- Deep Instinct
log_type	+- Man-in-the-middle
object_name	+- Deep Instinct
object_type	+- Android
source_type	+- Deep Instinct
src_host_name	+- Pixel+2+XL
src_ip_address	+- [illegible]
src_mac_address	+- [illegible]
src_user_name	+- None

Figure 6

4.4 Dashboards

EventTracker Endpoint Security Dashboard

- **EventTracker Endpoint Security: Login Failed**

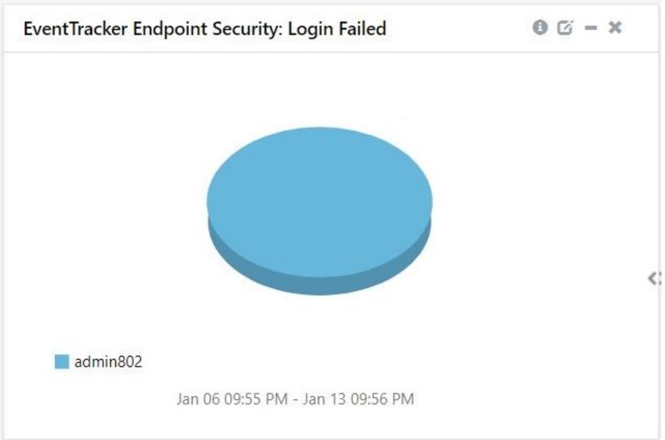
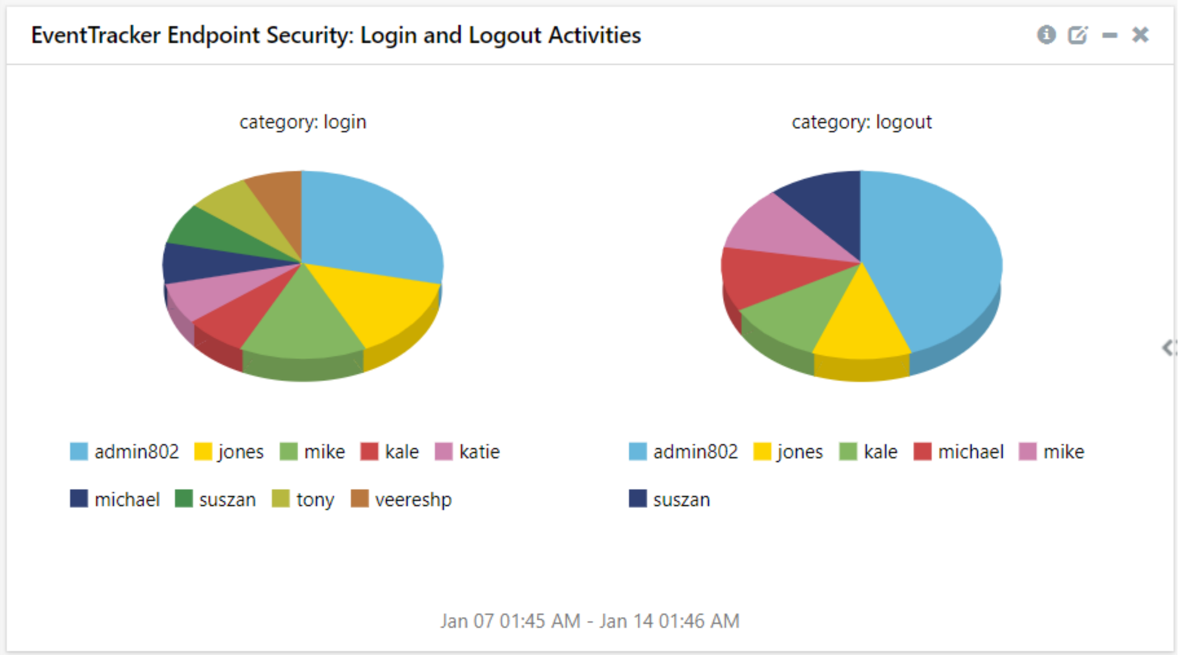


Figure 7

- **EventTracker Endpoint Security: Login and Logout Activities**

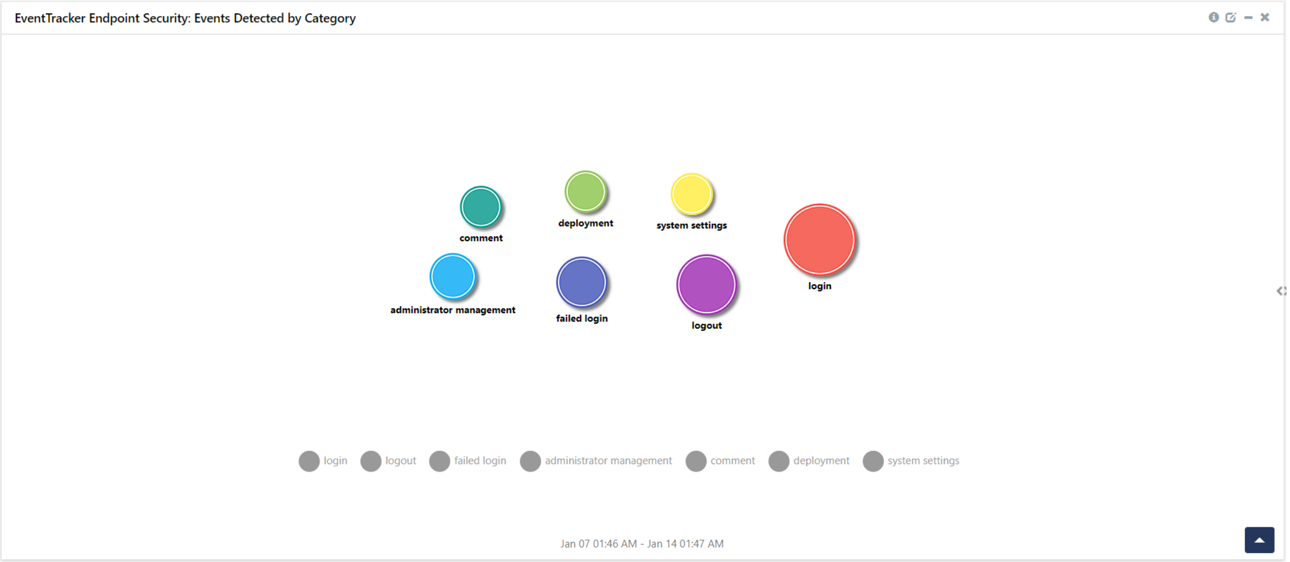


EventTracker Endpoint Security: Login and Logout Activities

Jan 07 01:45 AM - Jan 14 01:46 AM

Figure 8

- **EventTracker Endpoint Security: Events Detected by Category**

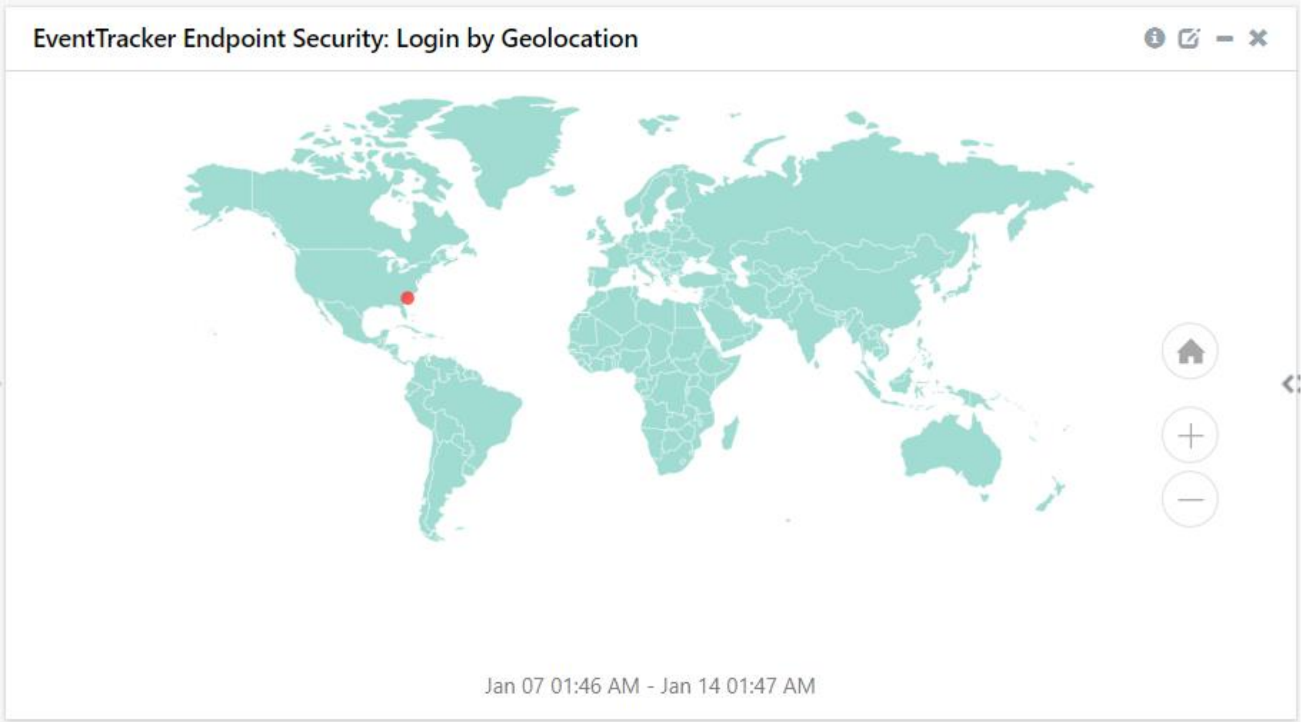


EventTracker Endpoint Security: Events Detected by Category

Jan 07 01:46 AM - Jan 14 01:47 AM

Figure 9

- **EventTracker Endpoint Security: Login by Geolocation**



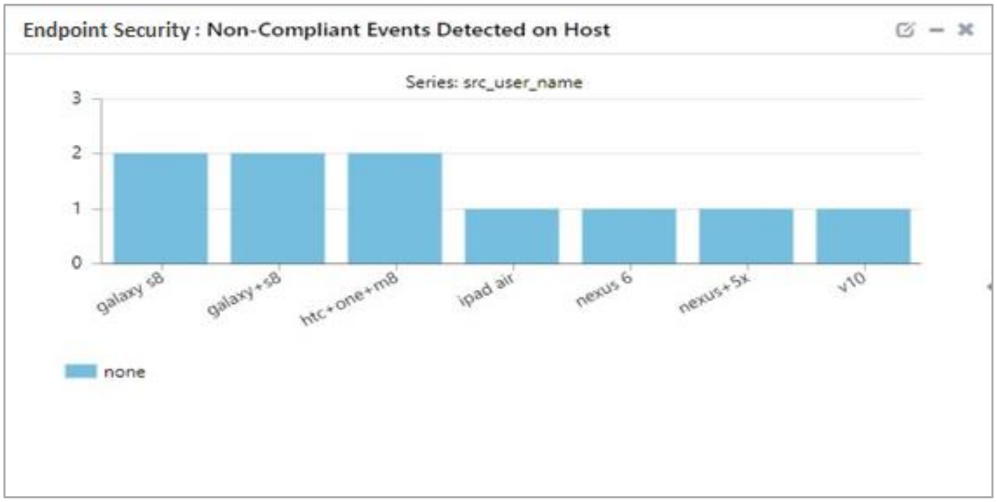
EventTracker Endpoint Security: Login by Geolocation

Jan 07 01:46 AM - Jan 14 01:47 AM

Figure 10

Endpoint Security Dashboard

- **EventTracker Endpoint Security: Non-Compliant Events Detected on Host**



Endpoint Security : Non-Compliant Events Detected on Host

Figure 11

- **EventTracker Endpoint Security: File Detected Info**

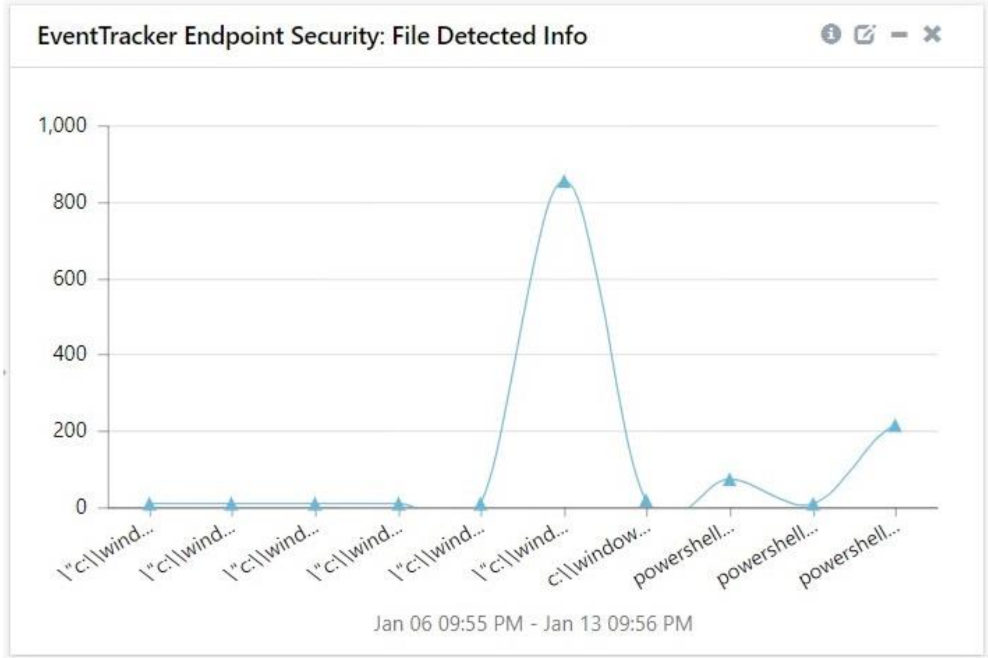


Figure 12

- **EventTracker Endpoint Security: Filename Detected**

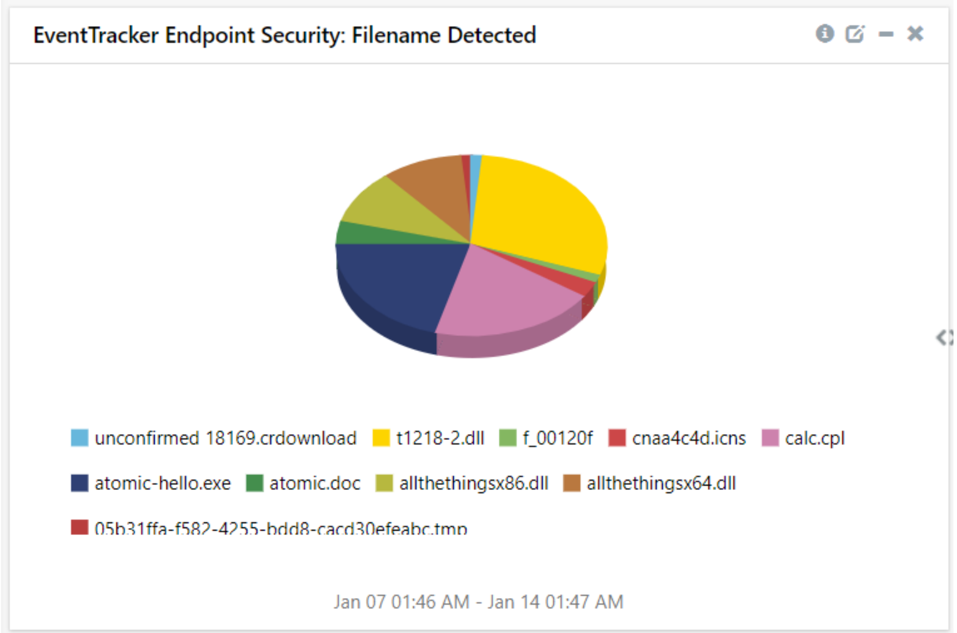

EventTracker Endpoint Security: Filename Detected
unconfirmed 18169.crdownload
t1218-2.dll
f_00120f
cnaa4c4d.icns
calc.cpl
atomic-hello.exe
atomic.doc
allthethingsx86.dll
allthethingsx64.dll
05b31ffa-f582-4255-bdd8-cacd30efeabc.tmp
Jan 07 01:46 AM - Jan 14 01:47 AM

Figure 13

- **EventTracker Endpoint Security: Top High-Risk Users**

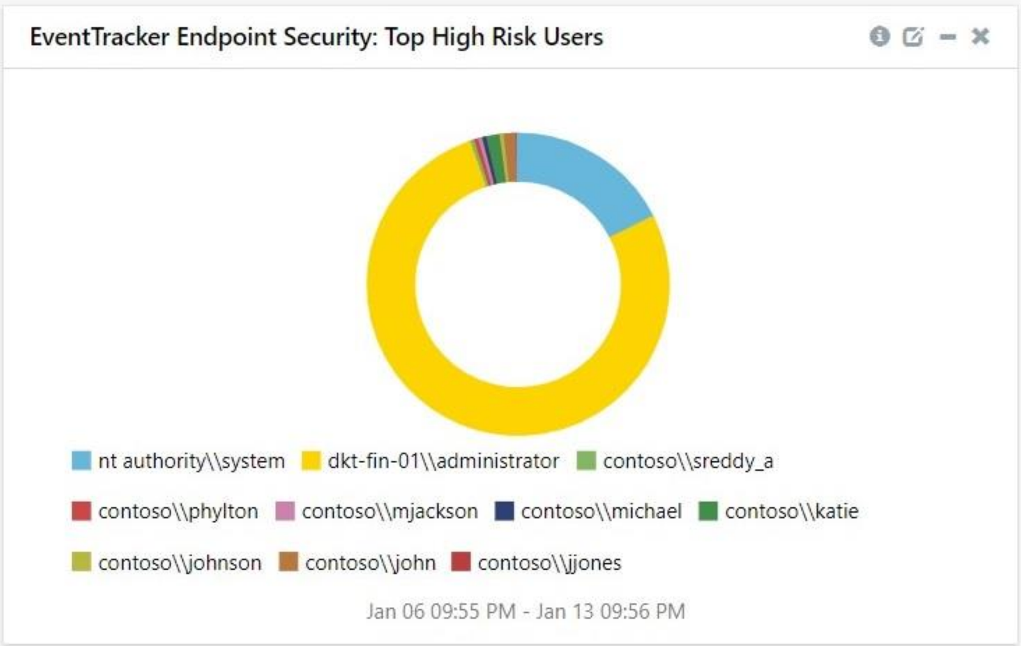


Figure 14

- **EventTracker Endpoint Security: Top High-Risk Host**

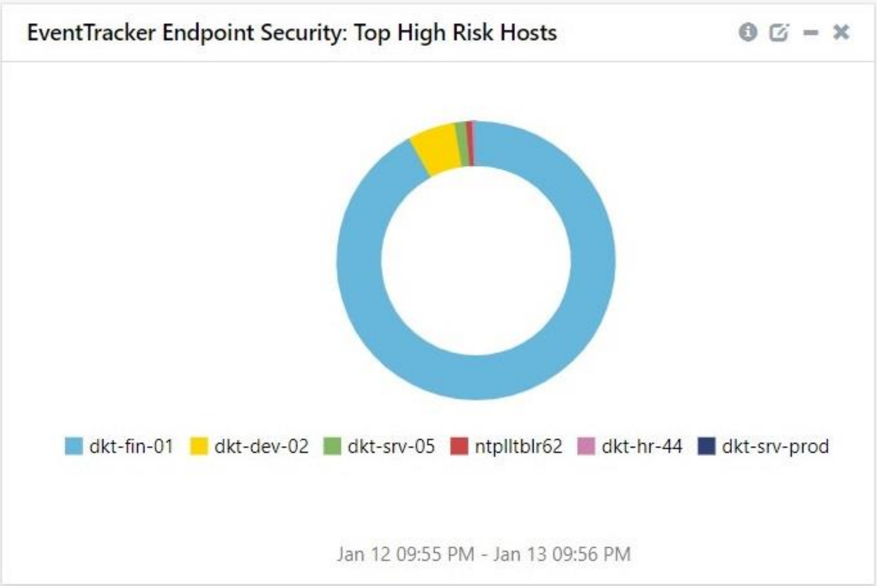

EventTracker Endpoint Security: Top High Risk Hosts
dkt-fin-01
dkt-dev-02
dkt-srv-05
ntplltblr62
dkt-hr-44
dkt-srv-prod
Jan 12 09:55 PM - Jan 13 09:56 PM

Figure 15

- **EventTracker Endpoint Security: Security Event Detected on Host**

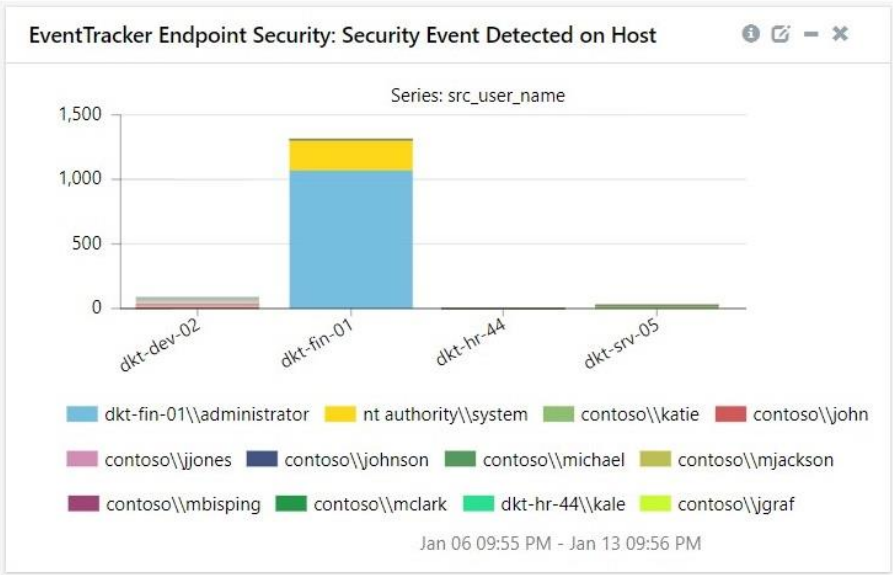


Figure 16

- **EventTracker Endpoint Security: File Type Detected by Security Events**

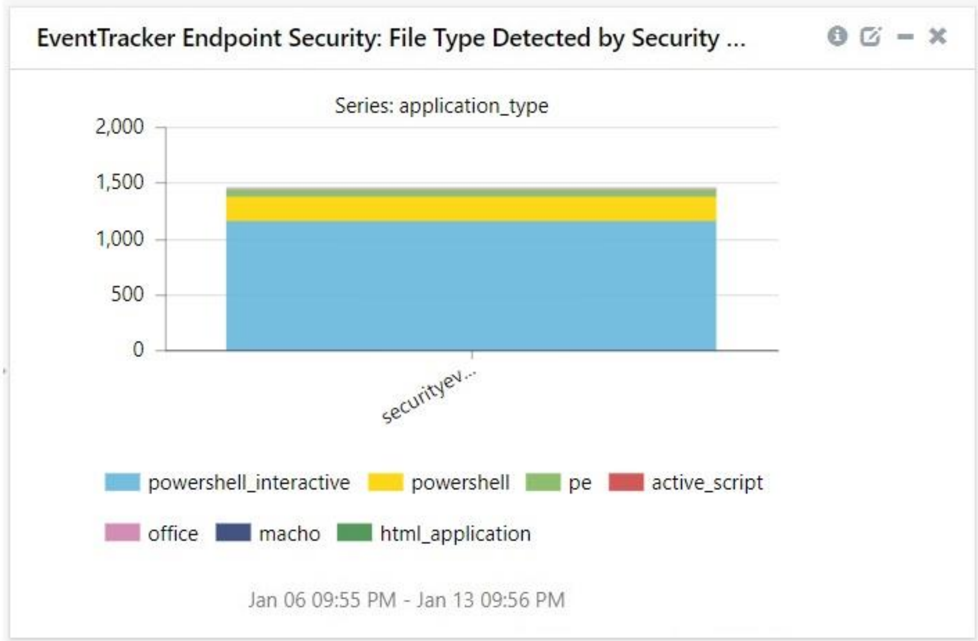


Figure 17

- **EventTracker Endpoint Security: Malware Family Detected on Hostname**

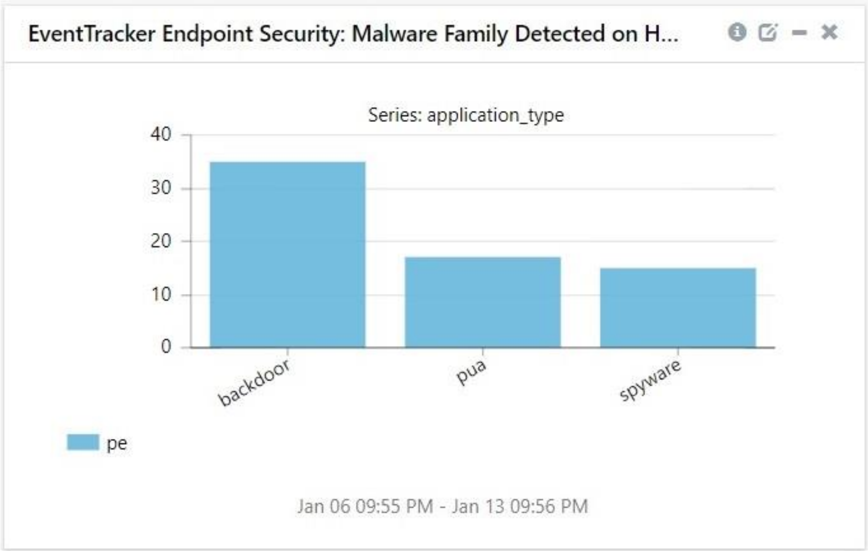

EventTracker Endpoint Security: Malware Family Detected on H...
Series: application_type
40
30
20
10
0
backdoor
pua
spyware
pe
Jan 06 09:55 PM - Jan 13 09:56 PM

Figure 18

5. Importing EventTracker Endpoint Security knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Category
- Alert
- Token template
- Knowledge Object
- Report
- Dashboard

1. Launch **EventTracker Control Panel**.

2. Double click **Export Import Utility**.

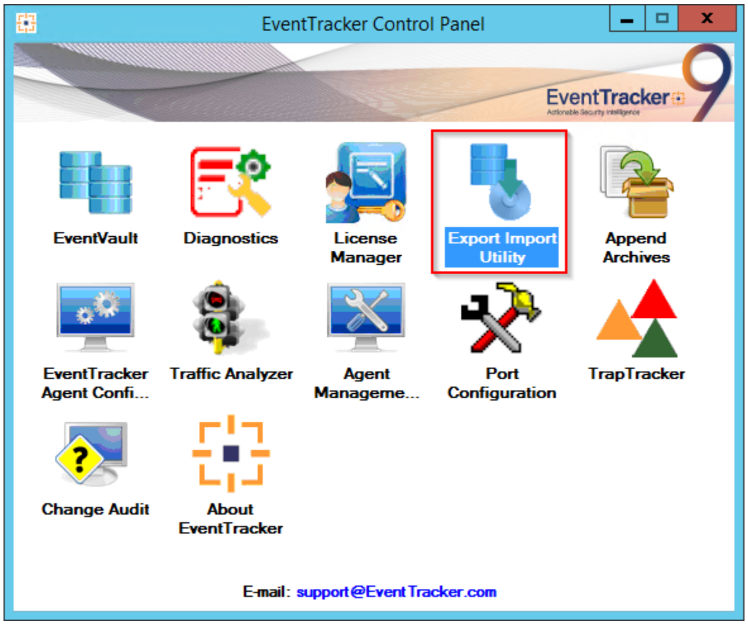
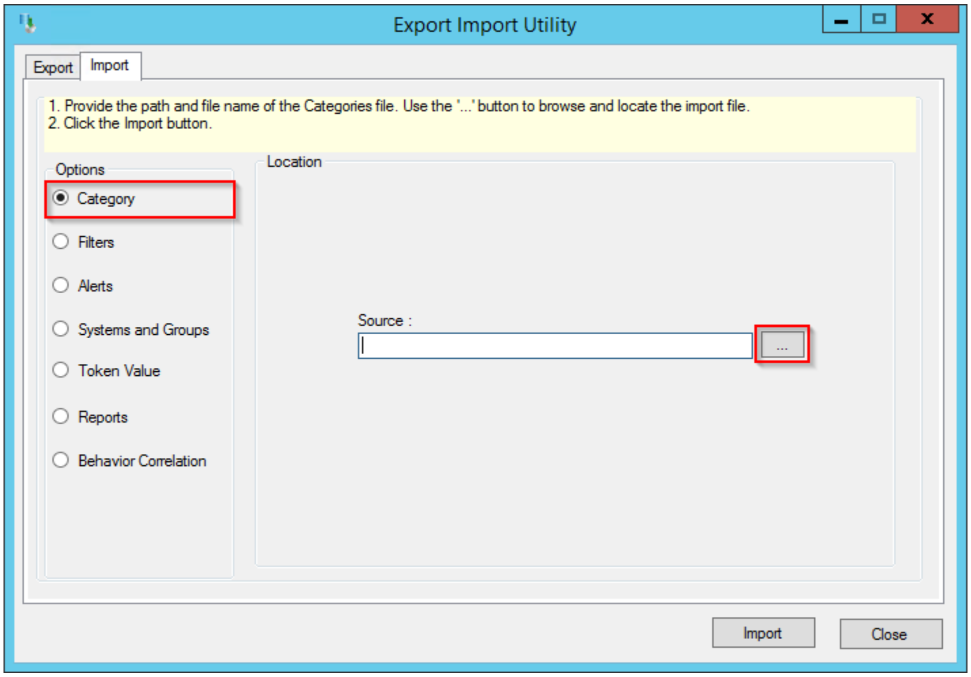


Figure 19

3. Click the **Import** tab.

5.1 Category

1. Click **Category** option and click **Browse** ... .



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

Options

● Category

○ Filters

○ Alerts

○ Systems and Groups

○ Token Value

○ Reports

○ Behavior Correlation

Location

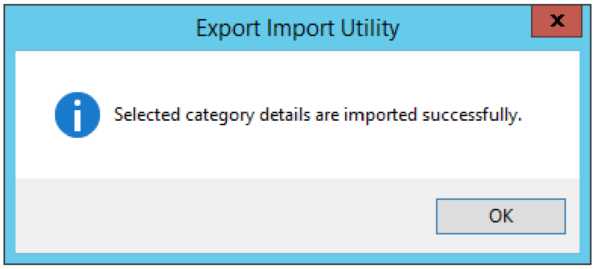
Source :

Figure 20

2. Locate **Categories_EventTracker Endpoint Security.iscat** file and click **Open**.

3. To import categories, click **Import**.

   EventTracker displays success message.



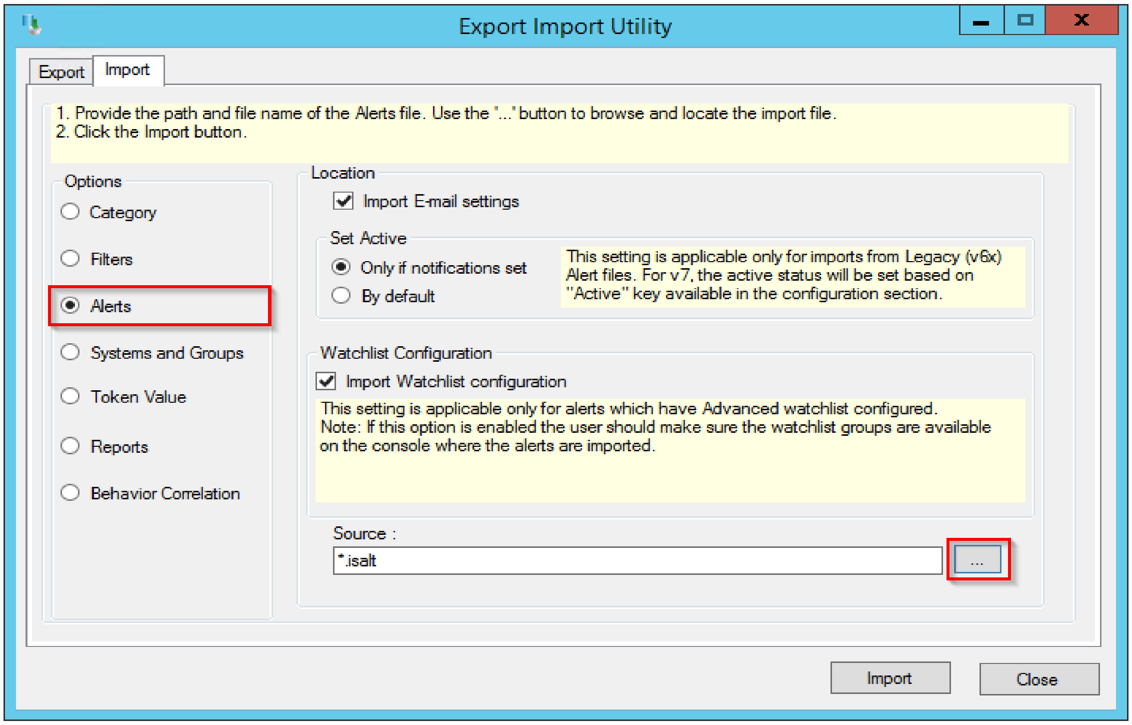
Selected category details are imported successfully.

Figure 21

4. Click **OK** and click **Close**.

5.2 Alert

1. Click **Alert** option and click **Browse** [...].



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
- ○ Token Value
- ○ Reports
- ○ Behavior Correlation

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.

Watchlist Configuration
- ☑ Import Watchlist configuration

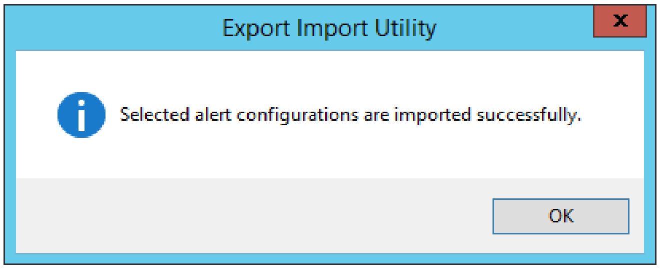
This setting is applicable only for alerts which have Advanced watchlist configured.
Note: If this option is enabled the user should make sure the watchlist groups are available on the console where the alerts are imported.

Source : *.isalt [...]

Figure 22

2. Locate **Alerts_EventTracker Endpoint Security.isalt** file and click **Open**.
3. To import alerts, click **Import**.

EventTracker displays success message.



Selected alert configurations are imported successfully.

Figure 23

4. Click **OK** and click **Close**.

5.3 Token template

1. Click **Parsing rule** under **Admin** option in the EventTracker manager page.

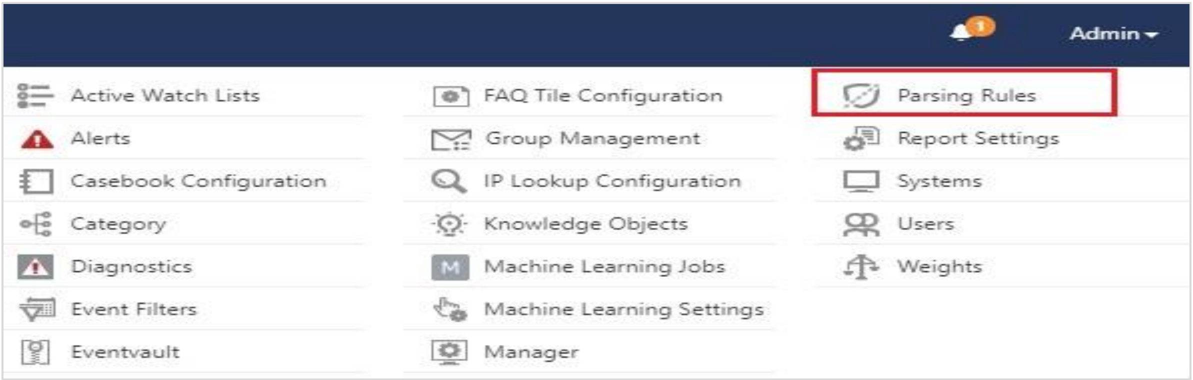


Figure 24

2. Click **Template.**

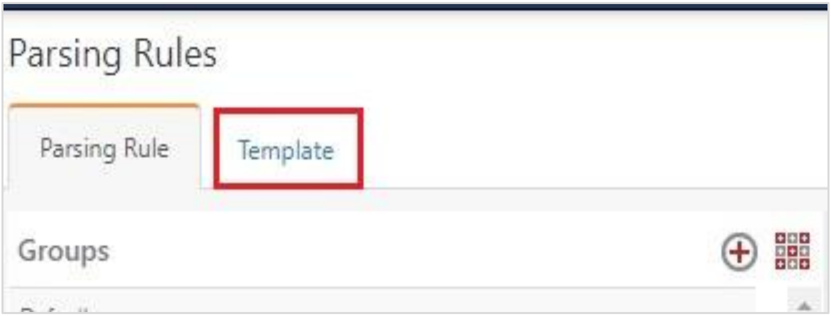


Figure 25

3. To import token template, click **Import**.

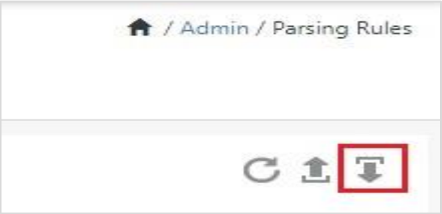
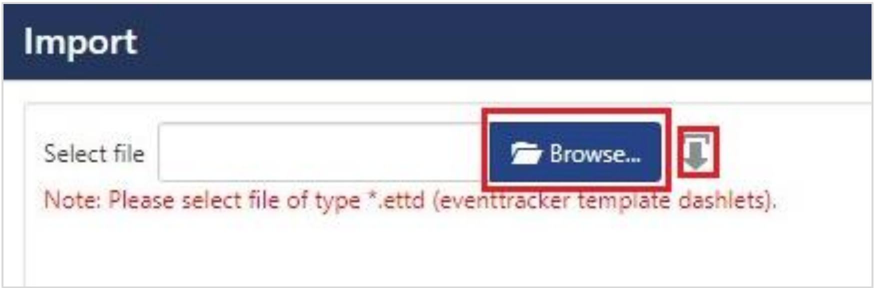


Figure 26

4. Locate the **Templates_EventTracker Endpoint Security.ettd** type file by clicking **Browse** button, enable all the templates and click **import**.



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

Figure 27

5. Click **OK**.

5.4 Knowledge Object

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

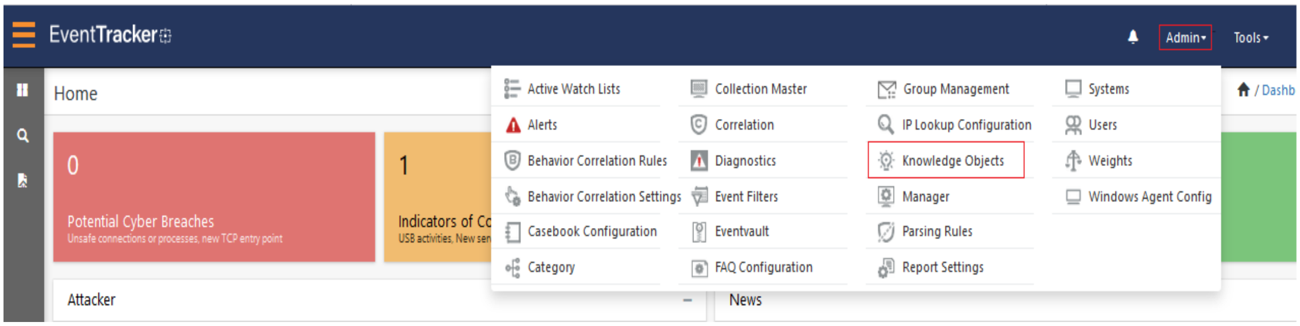


Figure 28

2. Click **Import** as highlighted in the below image:

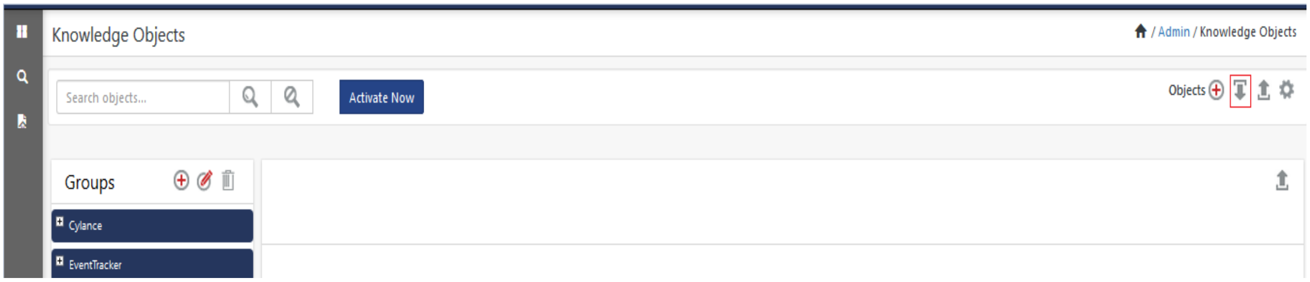


Figure 29

3. Click **Browse**.

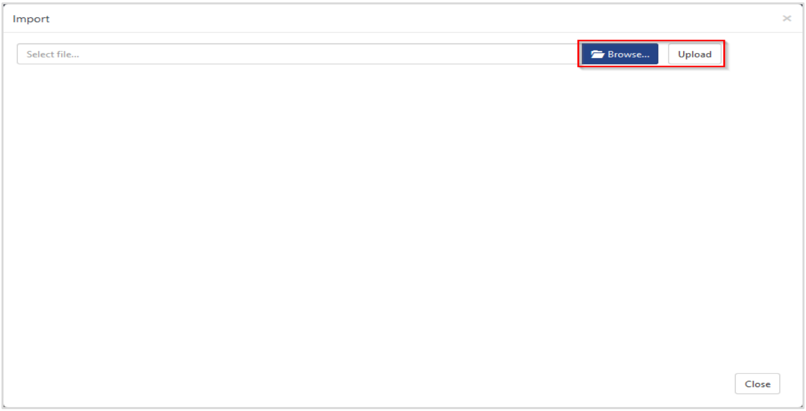
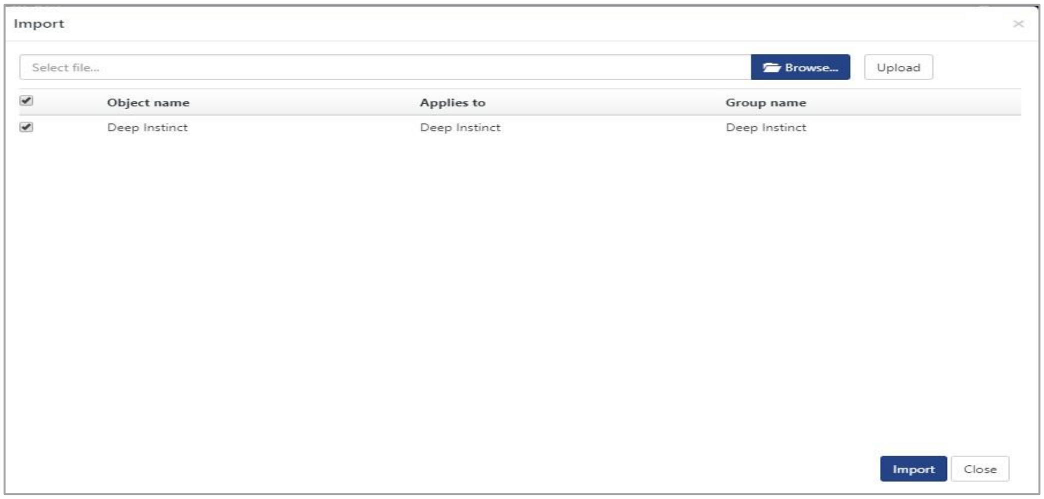


Figure 30

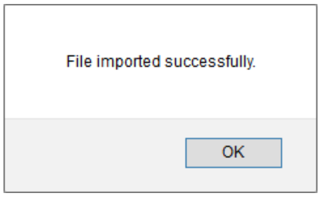
4. Locate the file named **KO_EventTracker Endpoint Security.etko**.
5. Now select the check box and click **Import**.



☑	Object name	Applies to	Group name
☑	Deep Instinct	Deep Instinct	Deep Instinct

Figure 31

6. Knowledge objects are now imported successfully.

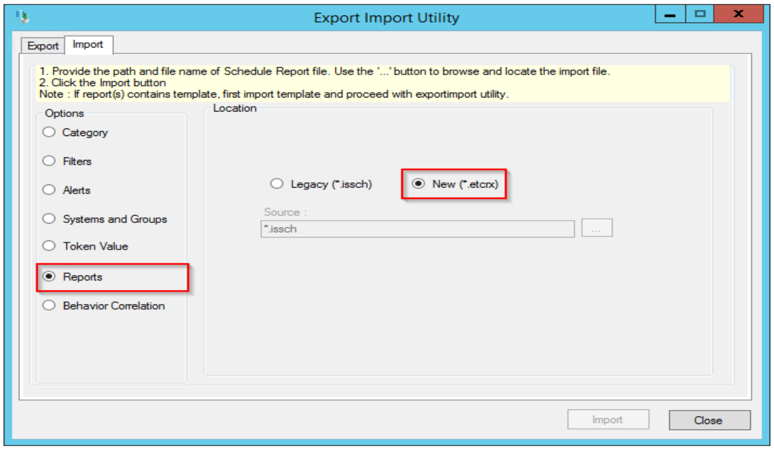


File imported successfully.

Figure 32

5.5 Report

1. Click **Reports** option and select **New (*.etcrx)** option.



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.

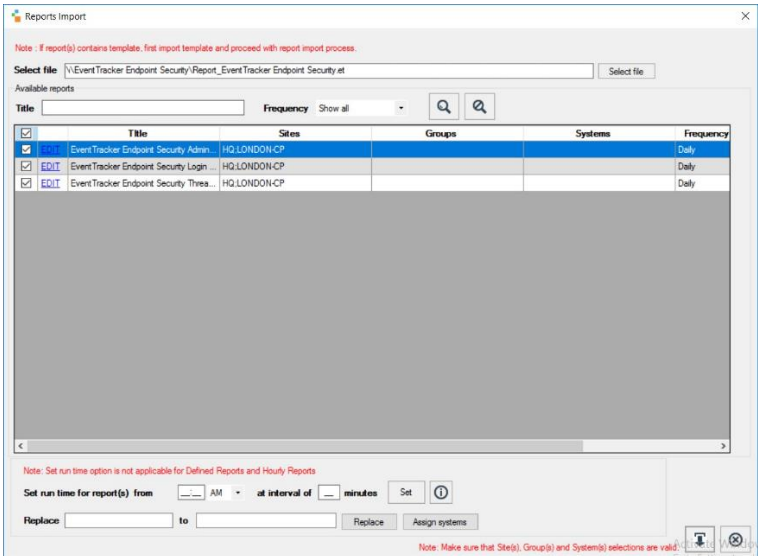
Options
○ Category
○ Filters
○ Alerts
○ Systems and Groups
○ Token Value
● Reports
○ Behavior Correlation

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

Source :
*.issch

Figure 33

2. Locate the file named **Reports_ EventTracker Endpoint Security.etcrx** and select the check box.



Note : If report(s) contains template, first import template and proceed with report import process.

Select file \\EventTracker Endpoint Security\Report_EventTracker Endpoint Security.et

Available reports

Title ______ Frequency Show all

☑		Title	Sites	Groups	Systems	Frequency
☑	EDIT	EventTracker Endpoint Security Admin...	HQ;LONDON-CP			Daily
☑	EDIT	EventTracker Endpoint Security Login ...	HQ;LONDON-CP			Daily
☑	EDIT	EventTracker Endpoint Security Threa...	HQ;LONDON-CP			Daily

Note: Set run time option is not applicable for Defined Reports and Hourly Reports

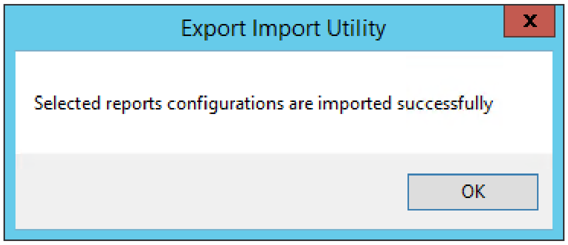
Set run time for report(s) from __:__ AM at interval of __ minutes

Replace ______ to ______

Note: Make sure that Site(s), Group(s) and System(s) selections are valid.

Figure 34

3. Click **Import** to import the report. EventTracker displays success message.


Export Import Utility

Selected reports configurations are imported successfully

Figure 35

5.6 Dashboards

NOTE: Below steps given are specific to EventTracker 9 and later.

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

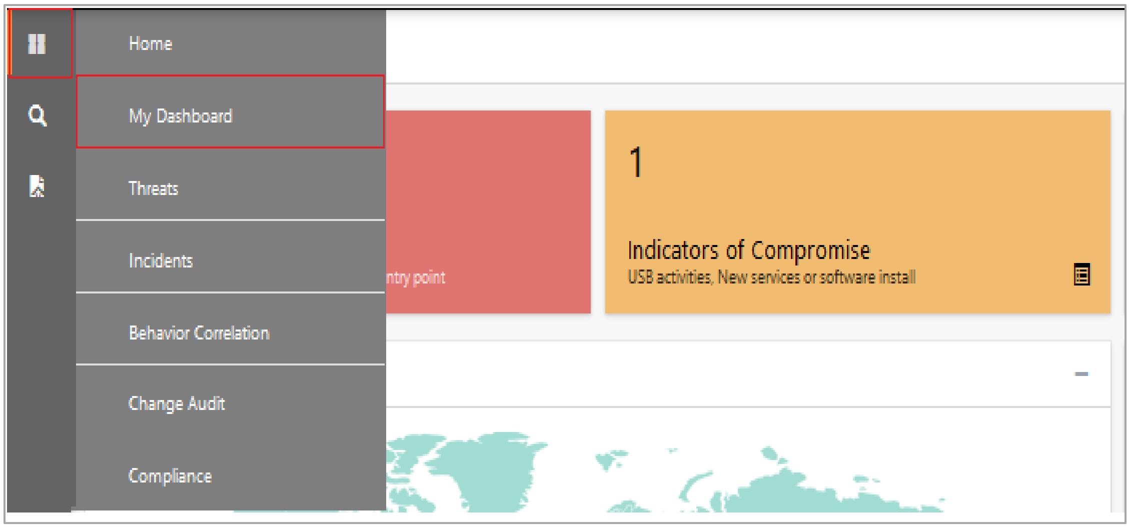


Figure 36

2. Navigate to **My Dashboard** option as shown above.
3. Click **Import** as show below:

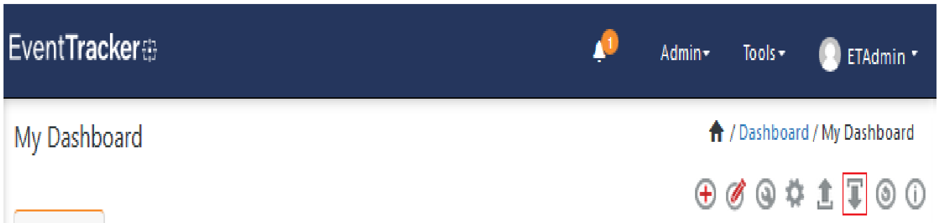
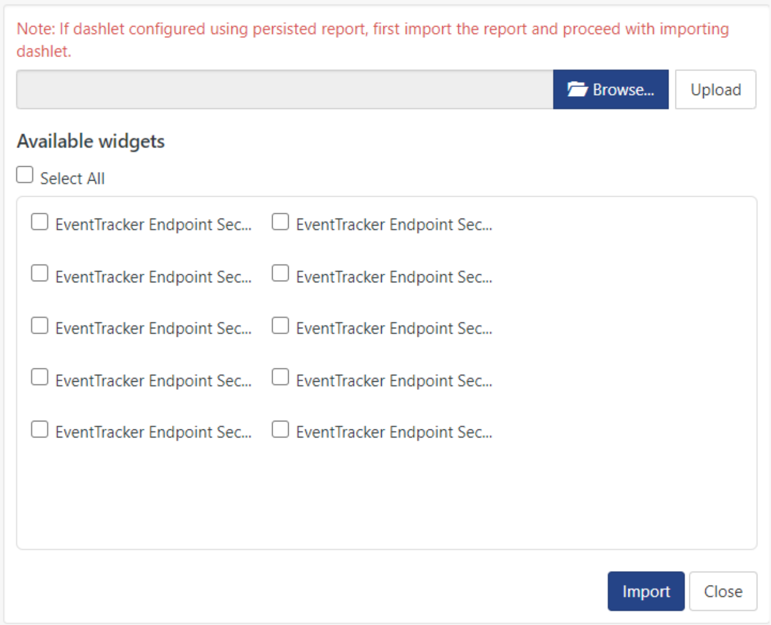


Figure 37

4. Import dashboard files **Dashboard_EventTracker Endpoint Security.etwd, Dashboard_Endpoint Security** and select **Select All** checkbox.
5. Click **Import** as shown below:



Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.

Available widgets

□ Select All

□ EventTracker Endpoint Sec... □ EventTracker Endpoint Sec...

□ EventTracker Endpoint Sec... □ EventTracker Endpoint Sec...

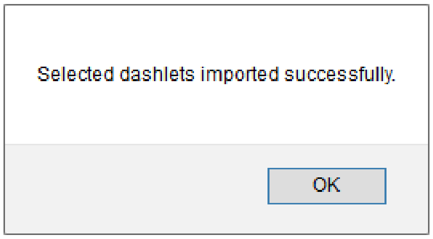
□ EventTracker Endpoint Sec... □ EventTracker Endpoint Sec...

□ EventTracker Endpoint Sec... □ EventTracker Endpoint Sec...

□ EventTracker Endpoint Sec... □ EventTracker Endpoint Sec...

Figure 38

6. Import is now completed successfully.



Selected dashlets imported successfully.

Figure 39

7. In **My Dashboard** page select ⊕ to add dashboard.

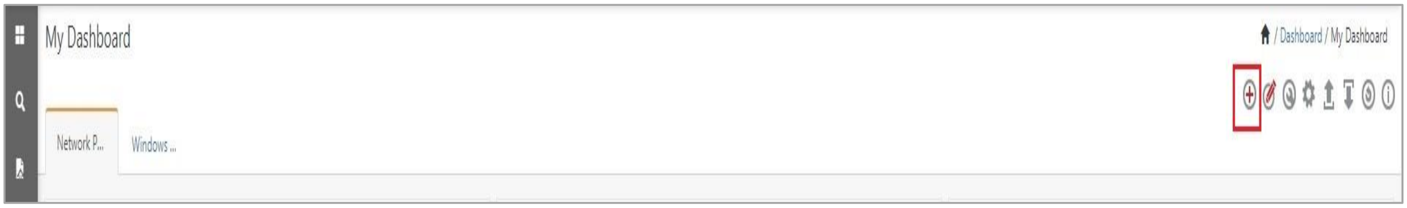
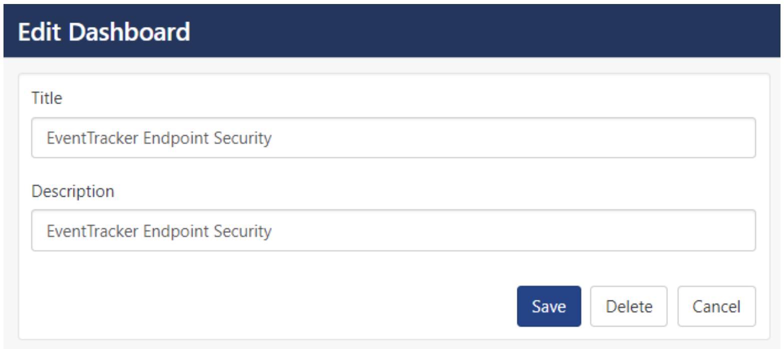


Figure 40

8. Choose appropriate name for **Title** and **Description**. Click **Save**.



Edit Dashboard

Title

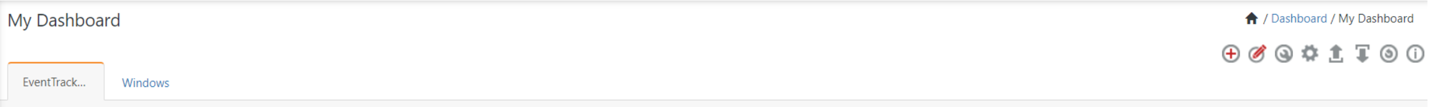
EventTracker Endpoint Security

Description

EventTracker Endpoint Security

Figure 41

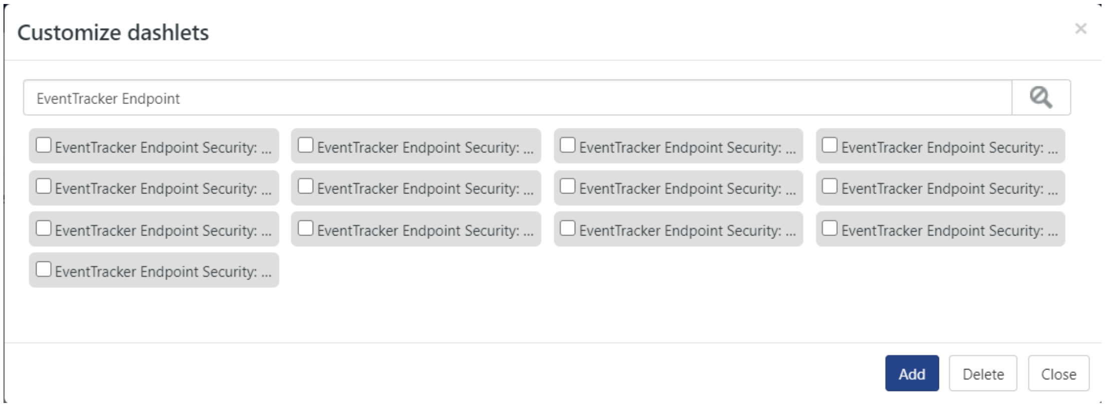
9. In **My Dashboard** page select ◎ to add dashlets.



My Dashboard

Figure 42

10. Select imported dashlets and click **Add**.



Customize dashlets

EventTracker Endpoint

☐ EventTracker Endpoint Security: ...
☐ EventTracker Endpoint Security: ...
☐ EventTracker Endpoint Security: ...
☐ EventTracker Endpoint Security: ...
☐ EventTracker Endpoint Security: ...
☐ EventTracker Endpoint Security: ...
☐ EventTracker Endpoint Security: ...
☐ EventTracker Endpoint Security: ...
☐ EventTracker Endpoint Security: ...
☐ EventTracker Endpoint Security: ...
☐ EventTracker Endpoint Security: ...
☐ EventTracker Endpoint Security: ...
☐ EventTracker Endpoint Security: ...

Figure 43

6. Verifying EventTracker Endpoint Security knowledge pack in EventTracker

6.1 Category

1. Logon to **EventTracker**.

2. Click **Admin** dropdown and click **Category**.

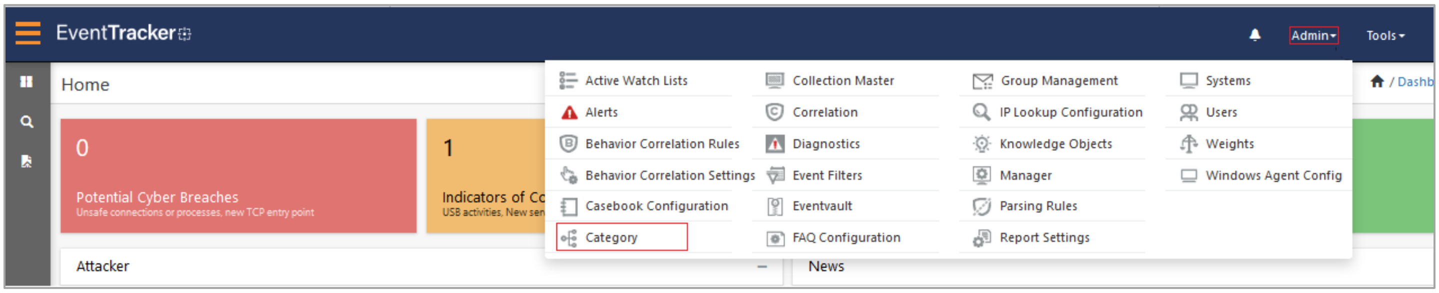
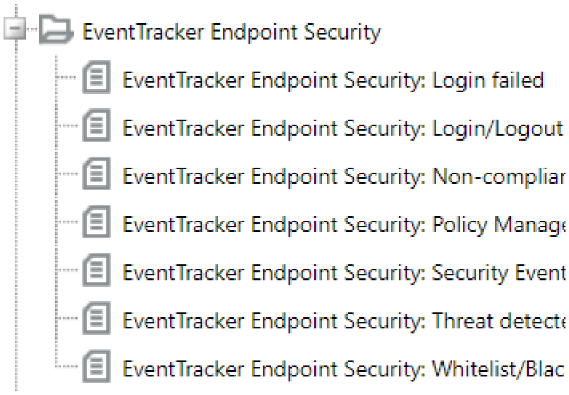


Figure 44

3. In **Category Tree** to view imported category, scroll down and expand **EventTracker Endpoint Security** group folder to view the imported category.



EventTracker Endpoint Security
- EventTracker Endpoint Security: Login failed
- EventTracker Endpoint Security: Login/Logout
- EventTracker Endpoint Security: Non-compliar
- EventTracker Endpoint Security: Policy Manage
- EventTracker Endpoint Security: Security Event
- EventTracker Endpoint Security: Threat detecte
- EventTracker Endpoint Security: Whitelist/Blac

Figure 45

6.2 Alert

1. Logon to **EventTracker**.
2. Click the **Admin** menu, and then click **Alerts**.

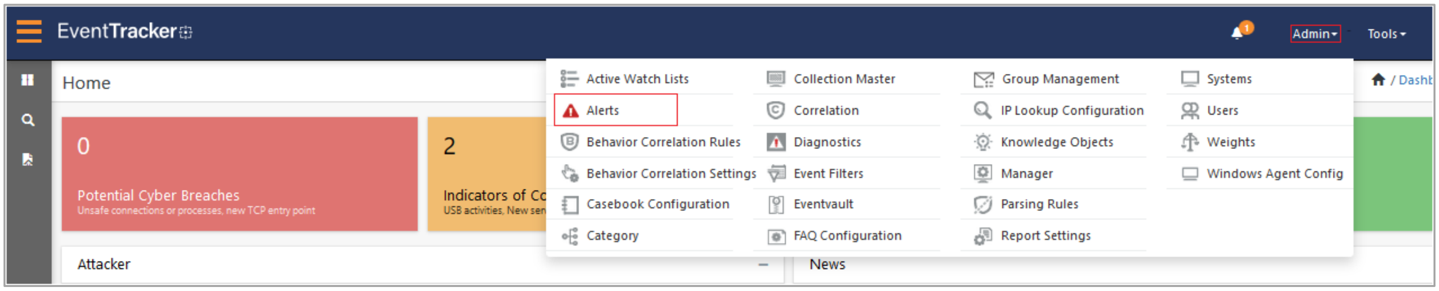
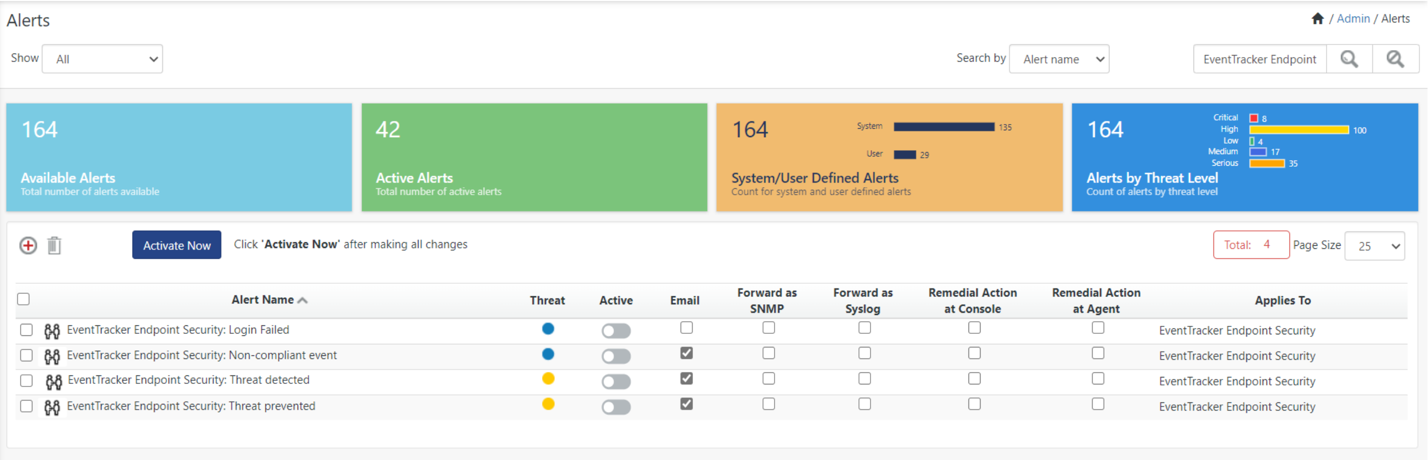


Figure 46

3. In the **Search** box, type **EventTracker Endpoint Security** and click **Go**.
   Alert Management page will display the imported alert.

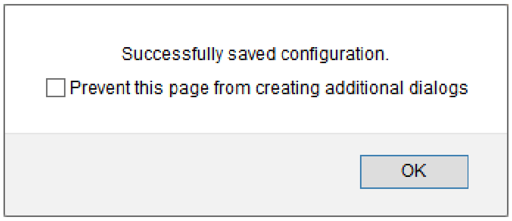


☐	Alert Name	Threat	Active	Email	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
☐	EventTracker Endpoint Security: Login Failed	●		☐	☐	☐	☐	☐	EventTracker Endpoint Security
☐	EventTracker Endpoint Security: Non-compliant event	●		☑	☐	☐	☐	☐	EventTracker Endpoint Security
☐	EventTracker Endpoint Security: Threat detected	●		☑	☐	☐	☐	☐	EventTracker Endpoint Security
☐	EventTracker Endpoint Security: Threat prevented	●		☑	☐	☐	☐	☐	EventTracker Endpoint Security

Figure 47

4. To activate the imported alert, toggle the **Active** switch.

   EventTracker displays message box.



Successfully saved configuration.

☐ Prevent this page from creating additional dialogs

Figure 48

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

NOTE: Specify appropriate **system** in **alert configuration** for better performance.

6.3 Token templates

1. In the **EventTracker** web interface, click the **Admin** dropdown, and click **Parsing rules.**

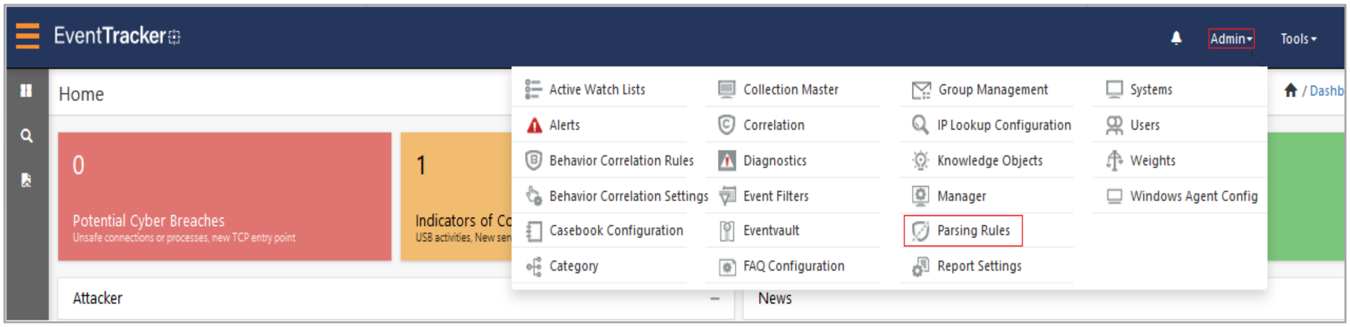
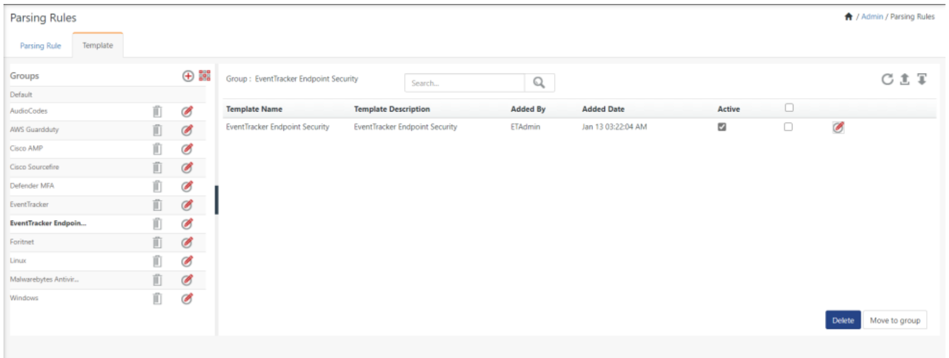


Figure 49

2. On **Template** tab, click on the **EventTracker Endpoint Security** group folder to view the imported token values.



Group : EventTracker Endpoint Security

Template Name	Template Description	Added By	Added Date	Active	□	
EventTracker Endpoint Security	EventTracker Endpoint Security	ETAdmin	Jan 13 03:22:04 AM	☑	□	

Figure 50

6.4 Knowledge Object

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then select **Knowledge Objects.**

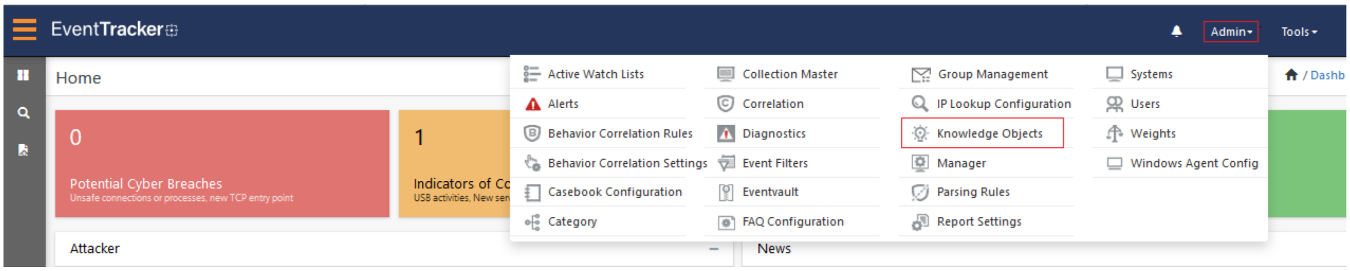
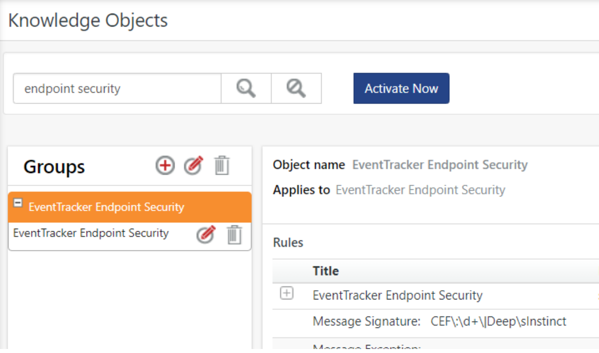


Figure 51

2. In the Knowledge Object tree, expand **EventTracker Endpoint Security** group folder to view the imported knowledge object.



Object name EventTracker Endpoint Security
Applies to EventTracker Endpoint Security

EventTracker Endpoint Security
Message Signature: CEF\:\d+\|Deep\sInstinct

Figure 52

3. Click **Activate Now** to apply imported knowledge objects.

6.5 Report

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

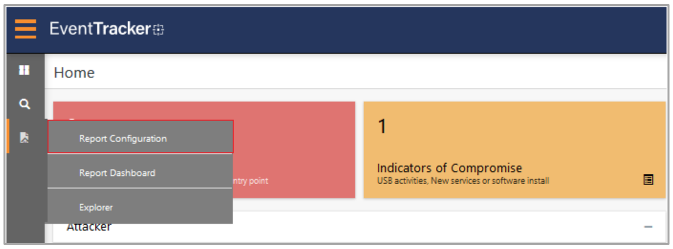
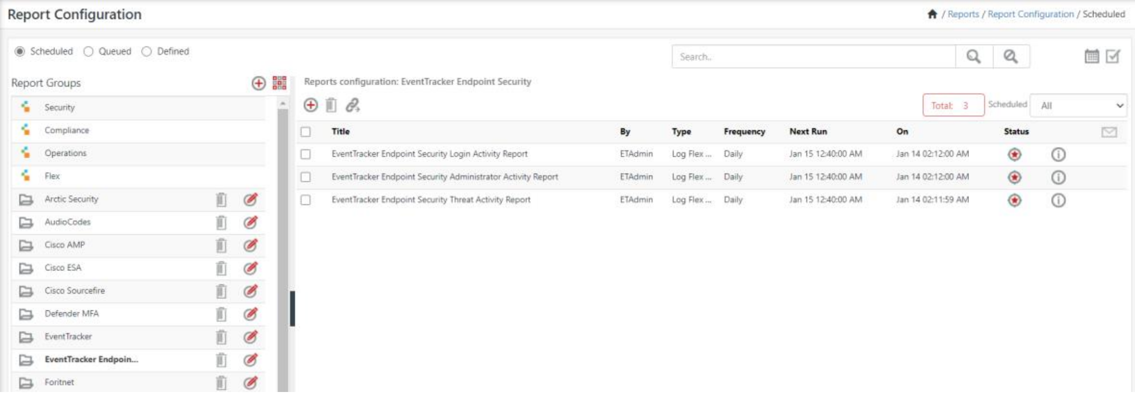


Figure 53

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



Report Configuration

/ Reports / Report Configuration / Scheduled

● Scheduled ○ Queued ○ Defined

Search..

Report Groups

- Security
- Compliance
- Operations
- Flex
- Arctic Security
- AudioCodes
- Cisco AMP
- Cisco ESA
- Cisco Sourcefire
- Defender MFA
- EventTracker
- **EventTracker Endpoin...**
- Foritnet

Reports configuration: EventTracker Endpoint Security

Total: 3 Scheduled All

□	Title	By	Type	Frequency	Next Run	On	Status
□	EventTracker Endpoint Security Login Activity Report	ETAdmin	Log Flex ...	Daily	Jan 15 12:40:00 AM	Jan 14 02:12:00 AM	● ⓘ
□	EventTracker Endpoint Security Administrator Activity Report	ETAdmin	Log Flex ...	Daily	Jan 15 12:40:00 AM	Jan 14 02:12:00 AM	● ⓘ
□	EventTracker Endpoint Security Threat Activity Report	ETAdmin	Log Flex ...	Daily	Jan 15 12:40:00 AM	Jan 14 02:11:59 AM	● ⓘ

Figure 54

6.6 Dashboards

1. In the EventTracker web interface, Click **Home** and select **My Dashboard**.

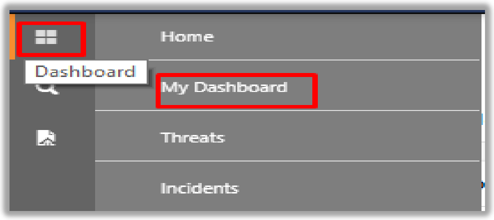
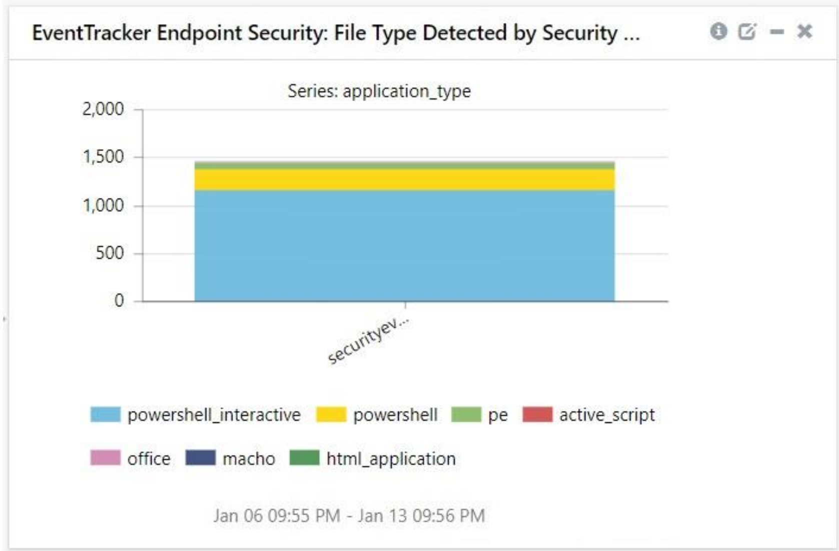


Figure 55

2. In the **EventTracker Endpoint Security** dashboard the following screen displays.



EventTracker Endpoint Security: File Type Detected by Security ...

Figure 56