Integrate Vectra AI

EventTracker v9.x and above

Publication Date: March 30, 2020

Abstract

This guide provides instructions to configure a **Vectra AI** to send its syslog to EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker version v9.x or above and **Vectra AI.**

Audience

Administrators who are assigned the task to monitor Vectra AI 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.

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

Vectra is an AI-driven threat detection and response platform. The Cognito platform uses artificial intelligence to reveal single in-progress cyberattack on hosts and predicts the potential spread of the attack in real-time.

EventTracker helps to monitor events from **Vectra AI**. Its dashboard, alerts and reports will keep you informed about attacks, suspicious host accounts and audit activities.

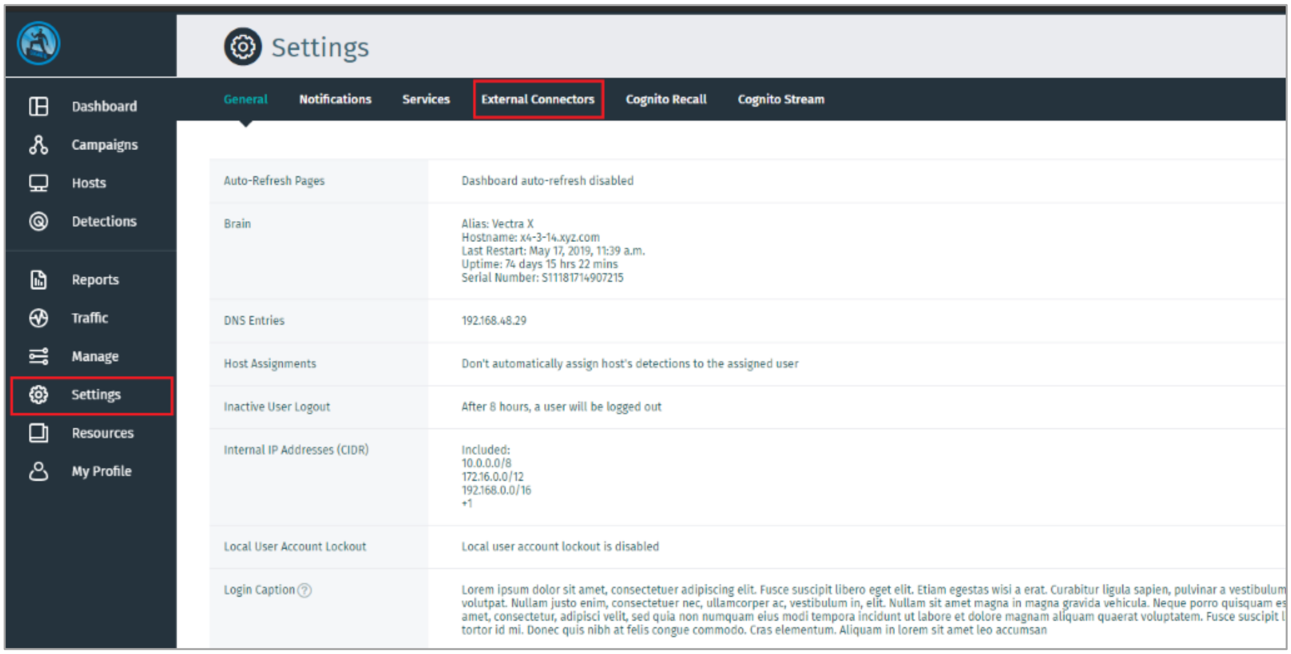
2. Prerequisites

- **EventTracker v9.x** or **above** should be installed.
- **Admin permission is** required for configuring syslog on Vectra Console.

3. Integration of Vectra AI with EventTracker

For integration, login into Vectra console

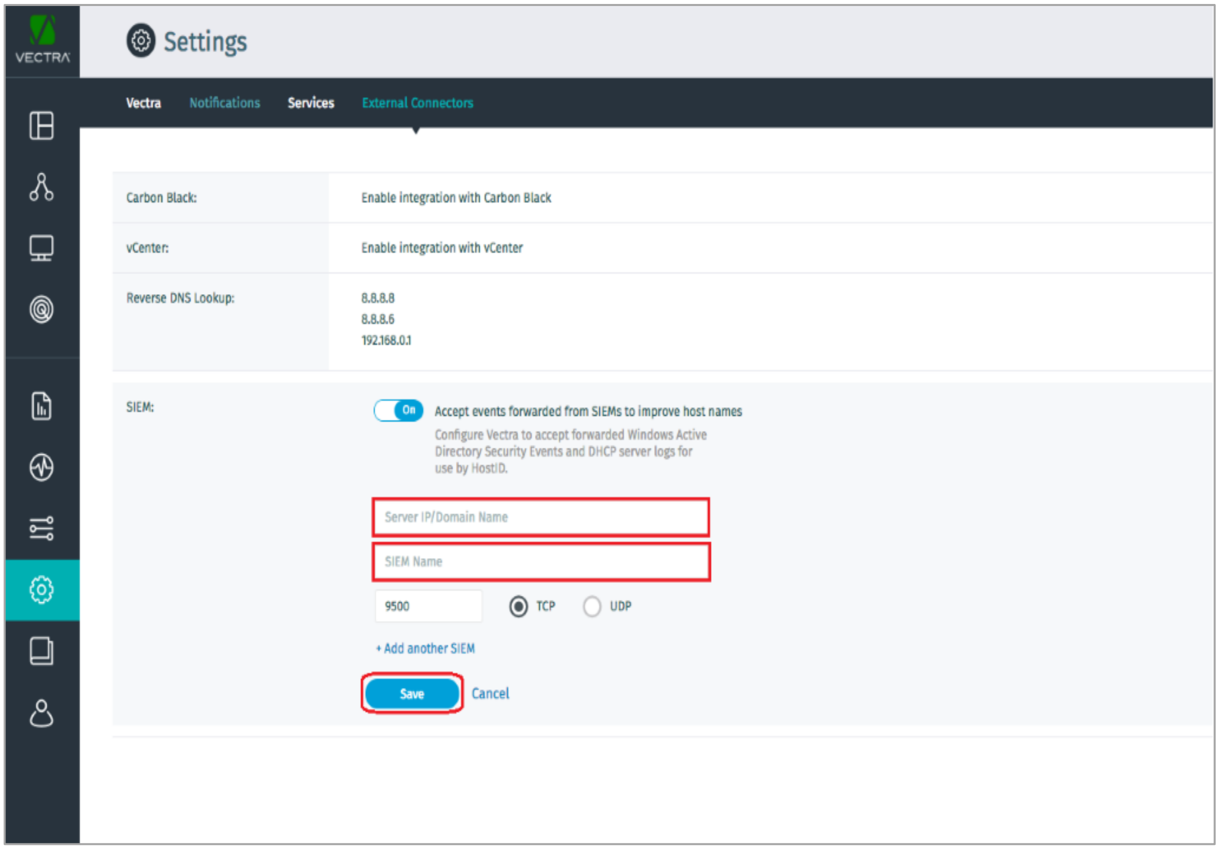
1. Go to Settings > External Connectors.



Auto-Refresh Pages	Dashboard auto-refresh disabled
Brain	Alias: Vectra X Hostname: x4-3-14.xyz.com Last Restart: May 17, 2019, 11:39 a.m. Uptime: 74 days 15 hrs 22 mins Serial Number: S11181714907215
DNS Entries	192.168.48.29
Host Assignments	Don't automatically assign host's detections to the assigned user
Inactive User Logout	After 8 hours, a user will be logged out
Internal IP Addresses (CIDR)	Included: 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 +1
Local User Account Lockout	Local user account lockout is disabled
Login Caption ?	Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Fusce suscipit libero eget elit. Etiam egestas wisi a erat. Curabitur ligula sapien, pulvinar a vestibulum volutpat. Nullam justo enim, consectetuer nec, ullamcorper ac, vestibulum in, elit. Nullam sit amet magna in magna gravida vehicula. Neque porro quisquam es amet, consectetur, adipisci velit, sed quia non numquam eius modi tempora incidunt ut labore et dolore magnam aliquam quaerat voluptatem. Fusce suscipit l tortor id mi. Donec quis nibh at felis congue commodo. Cras elementum. Aliquam in lorem sit amet leo accumsan

Figure 1

2. In external connectors. Please fill the details of EventTracker public IP and syslog port (e.g. default 514) and Save the setting.



Carbon Black: Enable integration with Carbon Black

vCenter: Enable integration with vCenter

Reverse DNS Lookup: 8.8.8.8
8.8.8.6
192.168.0.1

SIEM: On Accept events forwarded from SIEMs to improve host names

Configure Vectra to accept forwarded Windows Active Directory Security Events and DHCP server logs for use by HostID.

Server IP/Domain Name

SIEM Name

9500 ● TCP ○ UDP

+ Add another SIEM

Figure 2

The Vectra integration with EventTracker is completed and logs will be sent to EventTracker.

4. 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 Vectra AI.

4.1 Category

- **Vectra AI: Login Failed -** This category provides information related to failed login triggered by Vectra AI.

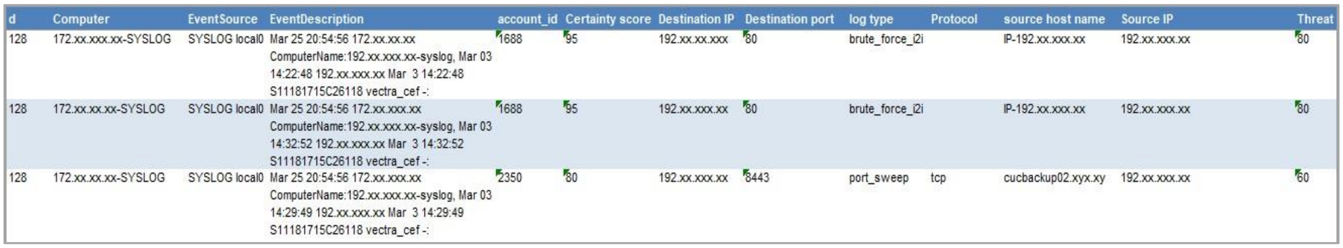
4.2 Alert

- **Vectra: Account Locked -** This alert is generated when any account lockdown is detected by Vectra AI.
- **Vectra: Login Failed –** This alert is generated when login failed is detected by Vectra AI.
- **Vectra: Suspicious account detected –** This alert is generated when suspicious account threat and certainty score detected by Vectra AI is > 60

- **Vectra: Threat Detected –** This alert is generated when threat score and certainty score detected by Vectra AI is > 30.

4.3 Report

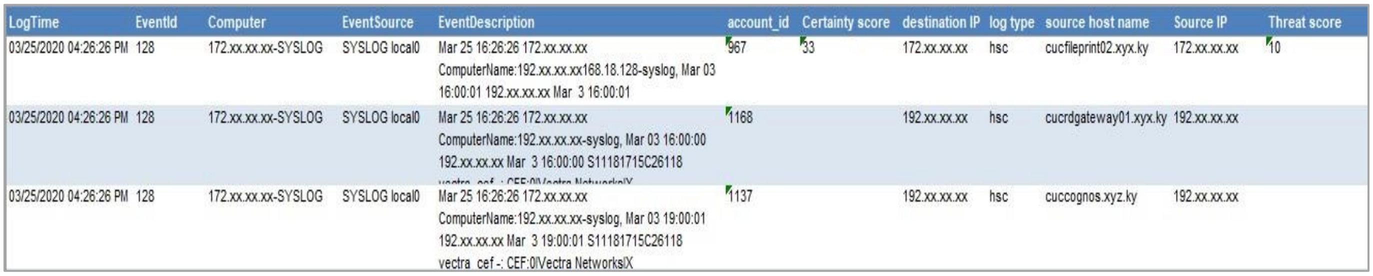
- **Vectra: Threat Detected**- This report gives the information about the threats detected by Vectra AI. This contains information about the threat name, its category, threat and certainty score and its system information which we can use to investigate.



d	Computer	EventSource	EventDescription	account_id	Certainty score	Destination IP	Destination port	log type	Protocol	source host name	Source IP	Threat
128	172.xx.xxx.xx-SYSLOG	SYSLOG local0	Mar 25 20:54:56 172.xx.xx.xx ComputerName:192.xx.xxx.xx-syslog, Mar 03 14:22:48 192.xx.xxx.xx Mar 3 14:22:48 S11181715C26118 vectra_cef -:	1688	95	192.xx.xx.xxx	80	brute_force_i2i		IP-192.xx.xxx.xx	192.xx.xxx.xx	80
128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Mar 25 20:54:56 172.xx.xxx.xx ComputerName:192.xx.xxx.xx-syslog, Mar 03 14:32:52 192.xx.xxx.xx Mar 3 14:32:52 S11181715C26118 vectra_cef -:	1688	95	192.xx.xxx.xx	80	brute_force_i2i		IP-192.xx.xxx.xx	192.xx.xxx.xx	80
128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Mar 25 20:54:56 172.xx.xxx.xx ComputerName:192.xx.xxx.xx-syslog, Mar 03 14:29:49 192.xx.xxx.xx Mar 3 14:29:49 S11181715C26118 vectra_cef -:	2350	80	192.xx.xxx.xx	8443	port_sweep	tcp	cucbackup02.xyx.xy	192.xx.xxx.xx	60

Figure 3

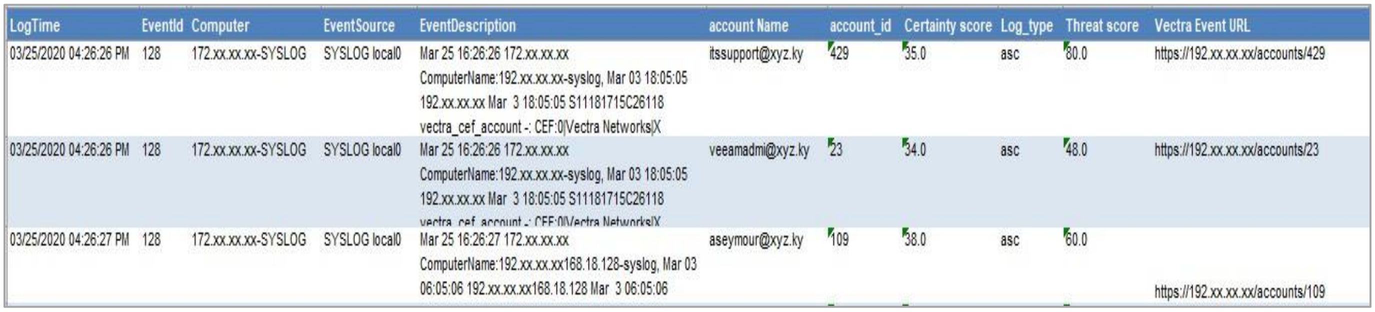
- **Vectra: Host Scoring-** This report gives the information about the host scoring detected by Vectra AI. This contains information about the host, threat score and certainty score, and other system details which will be helpful to investigate the host and its activities.



LogTime	EventId	Computer	EventSource	EventDescription	account_id	Certainty score	destination IP	log type	source host name	Source IP	Threat score
03/25/2020 04:26:26 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Mar 25 16:26:26 172.xx.xx.xx ComputerName:192.xx.xx.xx168.18.128-syslog, Mar 03 16:00:01 192.xx.xx.xx Mar 3 16:00:01	967	33	172.xx.xx.xx	hsc	cucfileprint02.xyx.ky	172.xx.xx.xx	10
03/25/2020 04:26:26 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Mar 25 16:26:26 172.xx.xx.xx ComputerName:192.xx.xx.xx-syslog, Mar 03 16:00:00 192.xx.xx.xx Mar 3 16:00:00 S11181715C26118 vectra_cef -: CEF:0|Vectra Networks|X	1168		192.xx.xx.xx	hsc	cucrdgateway01.xyx.ky	192.xx.xx.xx	
03/25/2020 04:26:26 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Mar 25 16:26:26 172.xx.xx.xx ComputerName:192.xx.xx.xx-syslog, Mar 03 19:00:01 192.xx.xx.xx Mar 3 19:00:01 S11181715C26118 vectra_cef -: CEF:0|Vectra Networks|X	1137		192.xx.xx.xx	hsc	cuccognos.xyz.ky	192.xx.xx.xx	

Figure 4

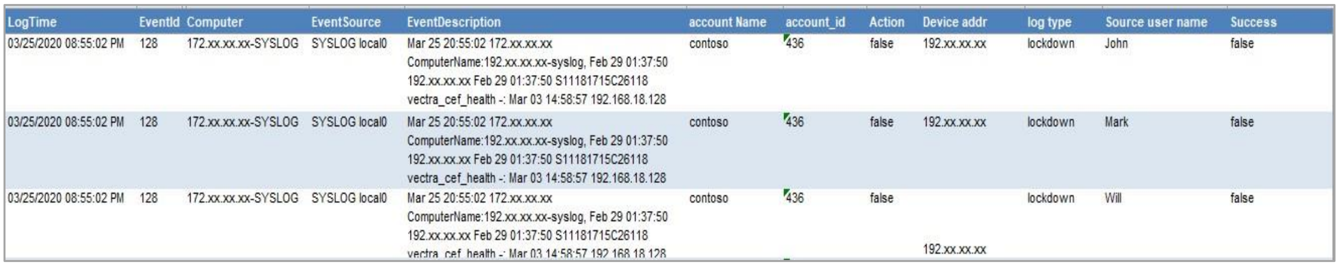
- **Vectra: Account Scoring-** This report gives the information about account scoring logs detected by Vectra AI. This contain information about the account and other system details with its threat and certainty score of the log which can help you investigate the cause.



LogTime	EventId	Computer	EventSource	EventDescription	account Name	account_id	Certainty score	Log_type	Threat score	Vectra Event URL
03/25/2020 04:26:26 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Mar 25 16:26:26 172.xx.xx.xx ComputerName:192.xx.xx.xx-syslog, Mar 03 18:05:05 192.xx.xx.xx Mar 3 18:05:05 S11181715C26118 vectra_cef_account -: CEF:0|Vectra Networks|X	itssupport@xyz.ky	429	35.0	asc	80.0	https://192.xx.xx.xx/accounts/429
03/25/2020 04:26:26 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Mar 25 16:26:26 172.xx.xx.xx ComputerName:192.xx.xx.xx-syslog, Mar 03 18:05:05 192.xx.xx.xx Mar 3 18:05:05 S11181715C26118 vectra_cef_account -: CEF:0|Vectra Networks|X	veeamadmi@xyz.ky	23	34.0	asc	48.0	https://192.xx.xx.xx/accounts/23
03/25/2020 04:26:27 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Mar 25 16:26:27 172.xx.xx.xx ComputerName:192.xx.xx.xx168.18.128-syslog, Mar 03 06:05:06 192.xx.xx.xx168.18.128 Mar 3 06:05:06	aseymour@xyz.ky	109	38.0	asc	60.0	https://192.xx.xx.xx/accounts/109

Figure 5

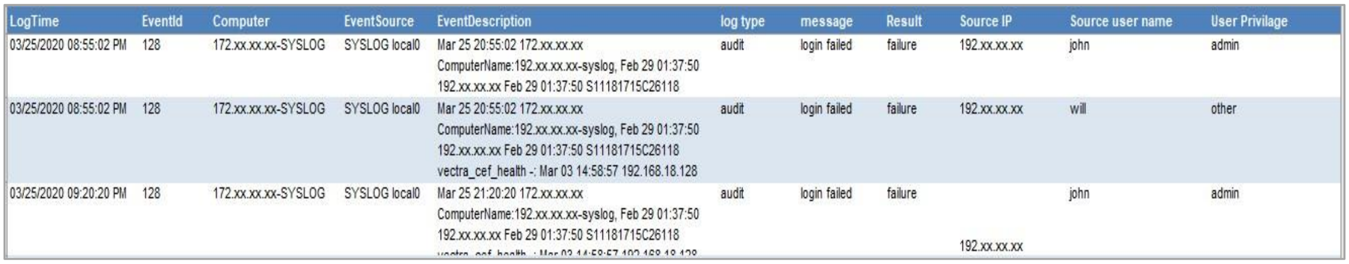
- **Vectra: Account Lockdown-** This report gives information about account lockdown detected by Vectra AI. This contains the account and username which has been locked down and its system details which can be useful to investigate.



LogTime	EventId	Computer	EventSource	EventDescription	account Name	account_id	Action	Device addr	log type	Source user name	Success
03/25/2020 08:55:02 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Mar 25 20:55:02 172.xx.xx.xx ComputerName:192.xx.xx.xx-syslog, Feb 29 01:37:50 192.xx.xx.xx Feb 29 01:37:50 S11181715C26118 vectra_cef_health -: Mar 03 14:58:57 192.168.18.128	contoso	436	false	192.xx.xx.xx	lockdown	John	false
03/25/2020 08:55:02 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Mar 25 20:55:02 172.xx.xx.xx ComputerName:192.xx.xx.xx-syslog, Feb 29 01:37:50 192.xx.xx.xx Feb 29 01:37:50 S11181715C26118 vectra_cef_health -: Mar 03 14:58:57 192.168.18.128	contoso	436	false	192.xx.xx.xx	lockdown	Mark	false
03/25/2020 08:55:02 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Mar 25 20:55:02 172.xx.xx.xx ComputerName:192.xx.xx.xx-syslog, Feb 29 01:37:50 192.xx.xx.xx Feb 29 01:37:50 S11181715C26118 vectra_cef_health -: Mar 03 14:58:57 192.168.18.128	contoso	436	false	192.xx.xx.xx	lockdown	Will	false

Figure 6

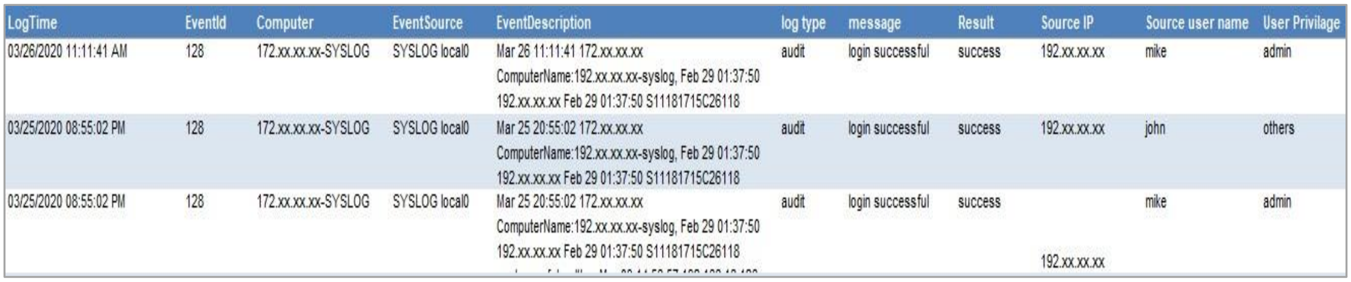
- **Vectra: Login Failed-** This report gives information about failed logins detected by Vectra AI. This contains the username, user privilege, source IP and other details of failed login attempts which will help to investigate further.



LogTime	EventId	Computer	EventSource	EventDescription	log type	message	Result	Source IP	Source user name	User Privilage
03/25/2020 08:55:02 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Mar 25 20:55:02 172.xx.xx.xx ComputerName:192.xx.xx.xx-syslog, Feb 29 01:37:50 192.xx.xx.xx Feb 29 01:37:50 S11181715C26118	audit	login failed	failure	192.xx.xx.xx	john	admin
03/25/2020 08:55:02 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Mar 25 20:55:02 172.xx.xx.xx ComputerName:192.xx.xx.xx-syslog, Feb 29 01:37:50 192.xx.xx.xx Feb 29 01:37:50 S11181715C26118 vectra_cef_health -: Mar 03 14:58:57 192.168.18.128	audit	login failed	failure	192.xx.xx.xx	will	other
03/25/2020 09:20:20 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Mar 25 21:20:20 172.xx.xx.xx ComputerName:192.xx.xx.xx-syslog, Feb 29 01:37:50 192.xx.xx.xx Feb 29 01:37:50 S11181715C26118 vectra_cef_health -: Mar 03 14:58:57 192.168.18.128	audit	login failed	failure	192.xx.xx.xx	john	admin

Figure 7

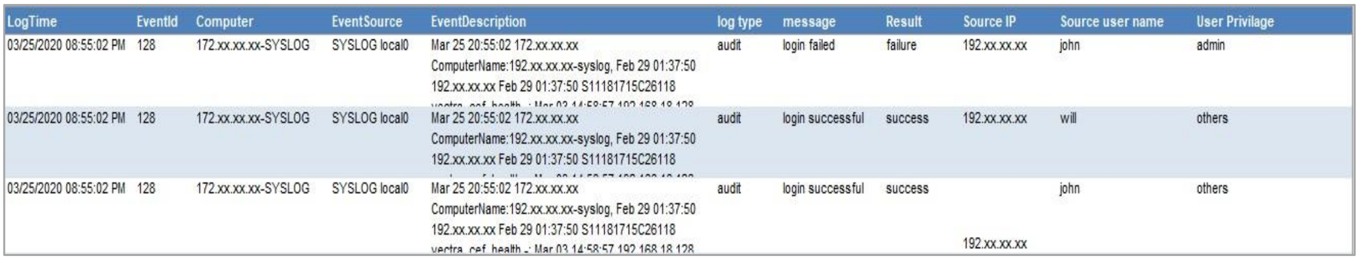
- **Vectra: Login Success-** This report gives information about successful logins detected by Vectra AI. This contains the username, user privilege, source IP and other details of successful logins to keep track of users accessing the system.



LogTime	EventId	Computer	EventSource	EventDescription	log type	message	Result	Source IP	Source user name	User Privilage
03/26/2020 11:11:41 AM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Mar 26 11:11:41 172.xx.xx.xx ComputerName:192.xx.xx.xx-syslog, Feb 29 01:37:50 192.xx.xx.xx Feb 29 01:37:50 S11181715C26118	audit	login successful	success	192.xx.xx.xx	mike	admin
03/25/2020 08:55:02 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Mar 25 20:55:02 172.xx.xx.xx ComputerName:192.xx.xx.xx-syslog, Feb 29 01:37:50 192.xx.xx.xx Feb 29 01:37:50 S11181715C26118	audit	login successful	success	192.xx.xx.xx	john	others
03/25/2020 08:55:02 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Mar 25 20:55:02 172.xx.xx.xx ComputerName:192.xx.xx.xx-syslog, Feb 29 01:37:50 192.xx.xx.xx Feb 29 01:37:50 S11181715C26118	audit	login successful	success	192.xx.xx.xx	mike	admin

Figure 8

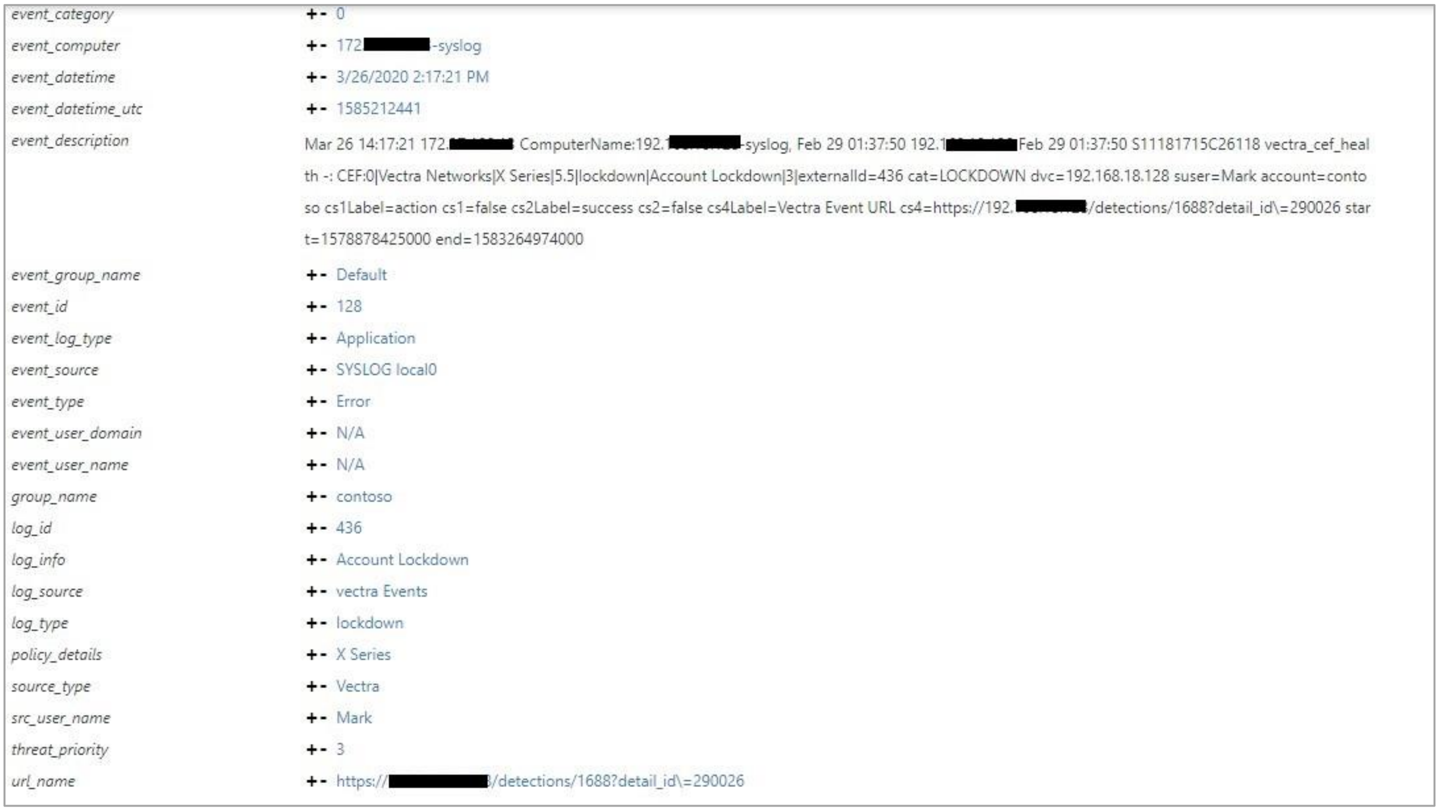
- **Vectra: Audit activities-** This report gives information about audit activities detected by Vectra AI. This contains the username, user privilege and other system details to keep track of all the audit activities performed.



LogTime	EventId	Computer	EventSource	EventDescription	log type	message	Result	Source IP	Source user name	User Privilage
03/25/2020 08:55:02 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Mar 25 20:55:02 172.xx.xx.xx ComputerName:192.xx.xx.xx-syslog, Feb 29 01:37:50 192.xx.xx.xx Feb 29 01:37:50 S11181715C26118 vectra_cef_health -: Mar 03 14:58:57 192.168.18.128	audit	login failed	failure	192.xx.xx.xx	john	admin
03/25/2020 08:55:02 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Mar 25 20:55:02 172.xx.xx.xx ComputerName:192.xx.xx.xx-syslog, Feb 29 01:37:50 192.xx.xx.xx Feb 29 01:37:50 S11181715C26118	audit	login successful	success	192.xx.xx.xx	will	others
03/25/2020 08:55:02 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Mar 25 20:55:02 172.xx.xx.xx ComputerName:192.xx.xx.xx-syslog, Feb 29 01:37:50 192.xx.xx.xx Feb 29 01:37:50 S11181715C26118 vectra_cef_health -: Mar 03 14:58:57 192.168.18.128	audit	login successful	success	192.xx.xx.xx	john	others

Figure 9

Logs Considered



event_category	+-	0
event_computer	+-	172[redacted]-syslog
event_datetime	+-	3/26/2020 2:17:21 PM
event_datetime_utc	+-	1585212441
event_description		Mar 26 14:17:21 172.[redacted] ComputerName:192.[redacted]-syslog, Feb 29 01:37:50 192.1[redacted]Feb 29 01:37:50 S11181715C26118 vectra_cef_health -: CEF:0|Vectra Networks|X Series|5.5|lockdown|Account Lockdown|3|externalId=436 cat=LOCKDOWN dvc=192.168.18.128 suser=Mark account=contoso cs1Label=action cs1=false cs2Label=success cs2=false cs4Label=Vectra Event URL cs4=https://192.[redacted]/detections/1688?detail_id\=290026 start=1578878425000 end=1583264974000
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
group_name	+-	contoso
log_id	+-	436
log_info	+-	Account Lockdown
log_source	+-	vectra Events
log_type	+-	lockdown
policy_details	+-	X Series
source_type	+-	Vectra
src_user_name	+-	Mark
threat_priority	+-	3
url_name	+-	https://[redacted]/detections/1688?detail_id\=290026

Figure 10

4.4 Dashboards

Vectra- Accounts Locked

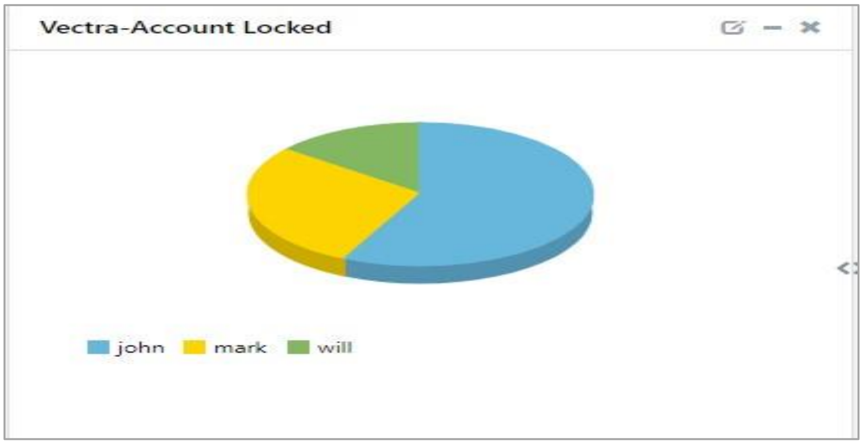


Figure 11

Vectra- Login Failed

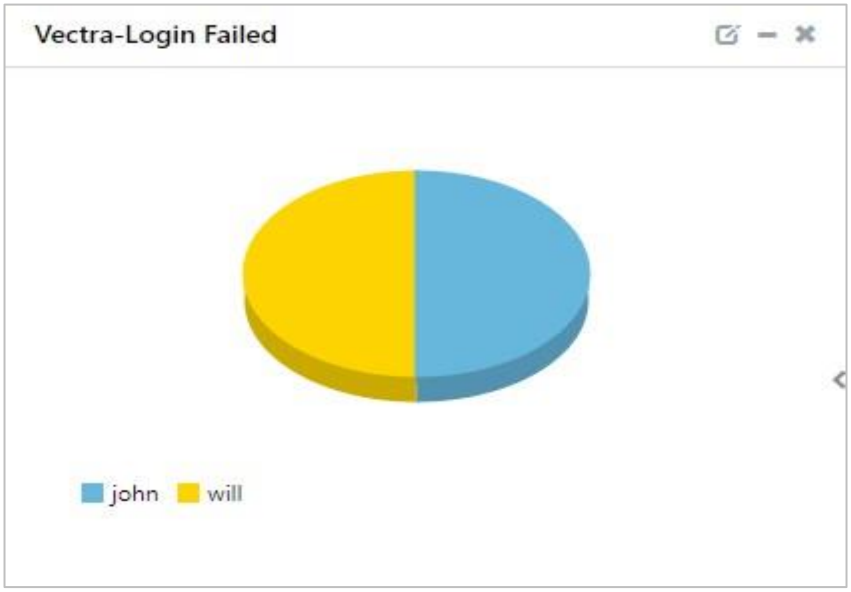


Figure 12

Vectra- Audit activities by user

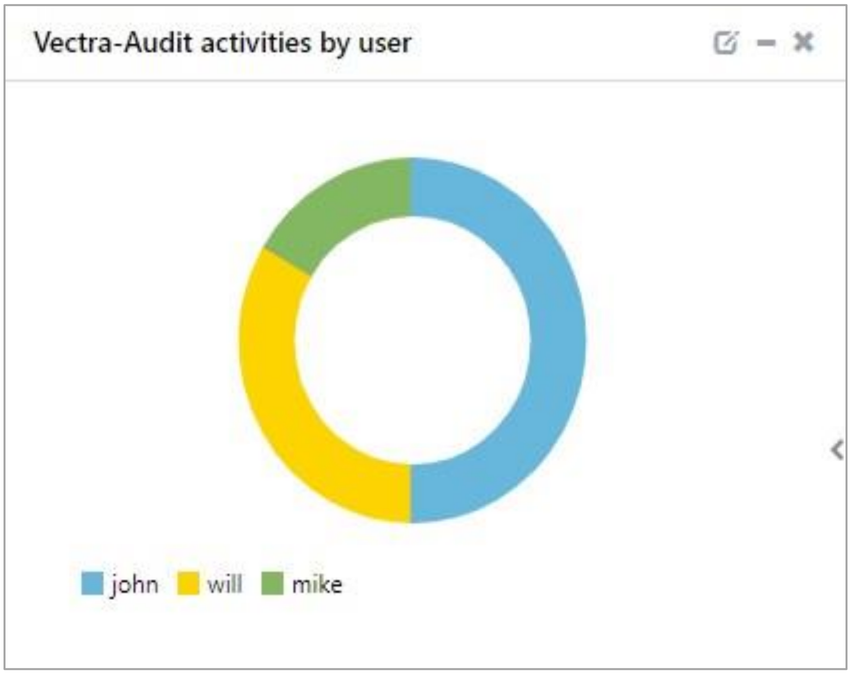


Figure 13

Vectra-Top high scored host

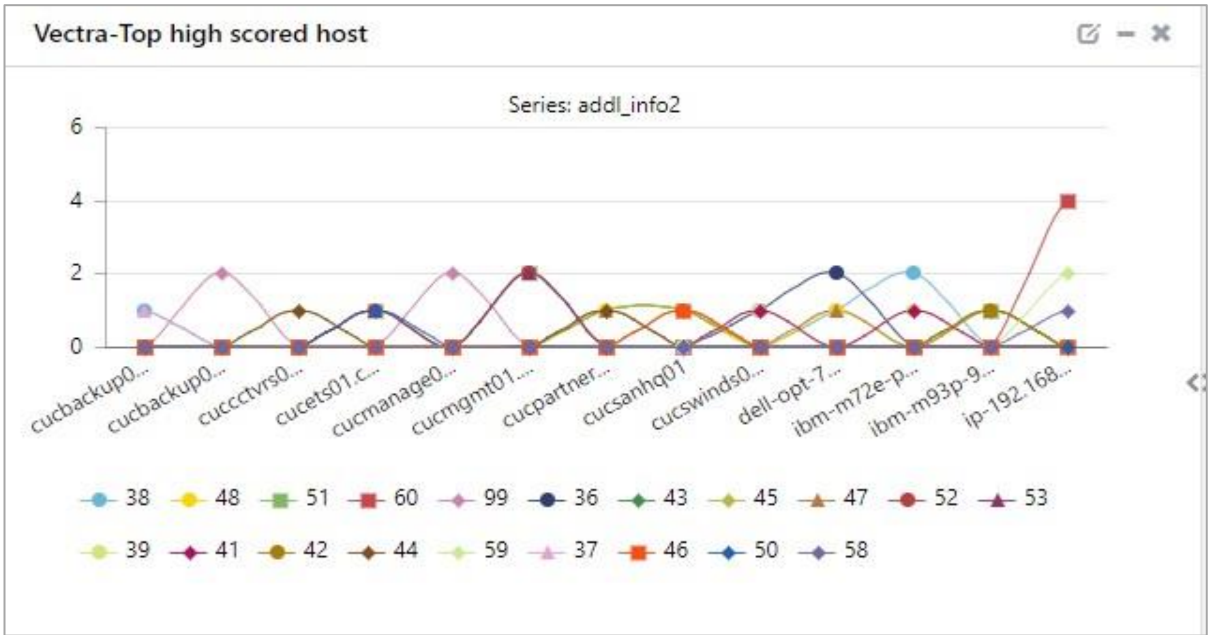


Figure 14

Vectra-Suspicious account detected by category

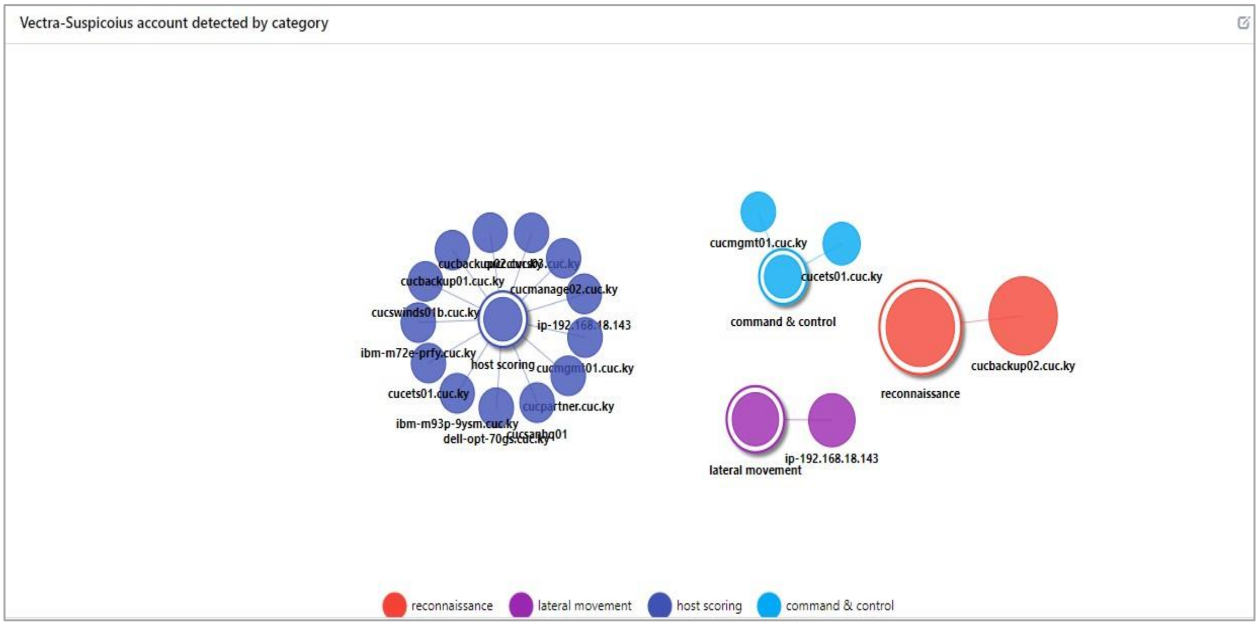

Vectra-Suspicoius account detected by category

Figure 15

Vectra-Threats detected by category

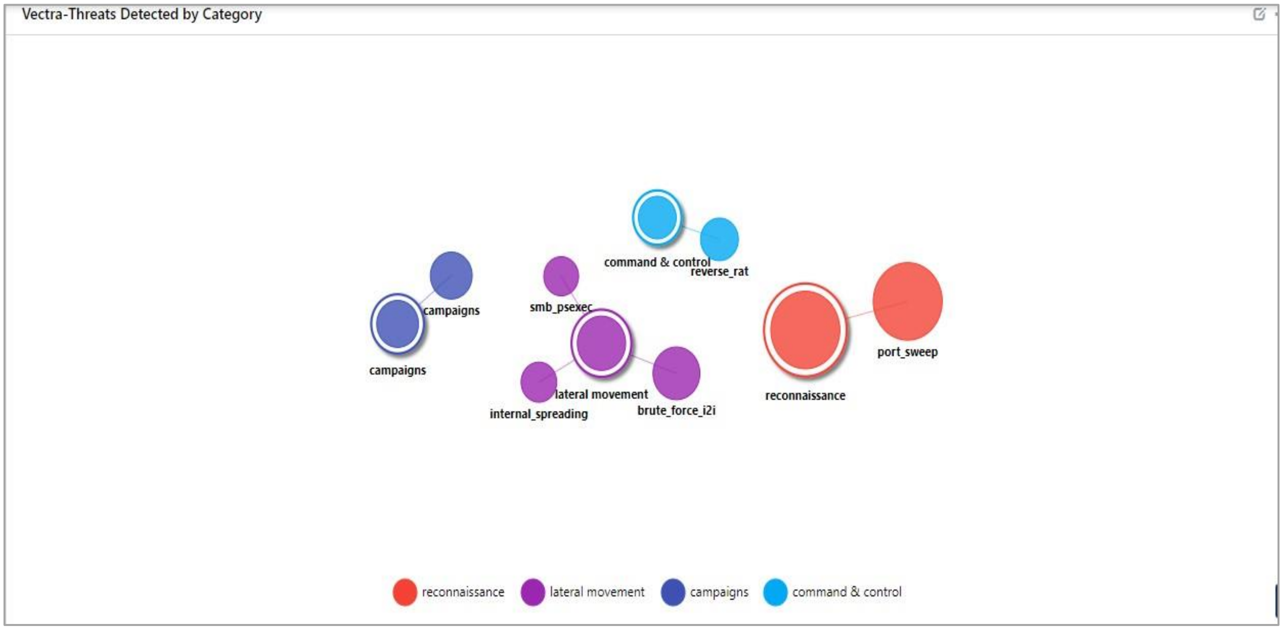

Vectra-Threats Detected by Category

Figure 16

Vectra- Threat detected by host

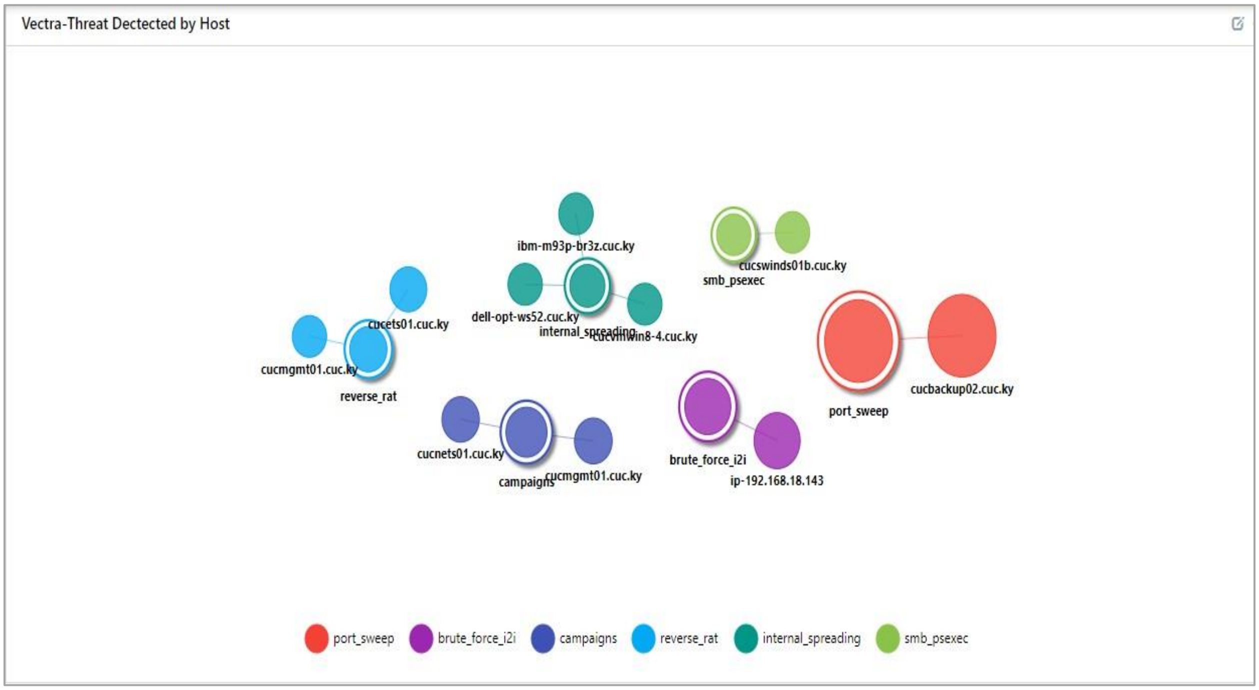


Figure 17

Vectra-Threat score by category

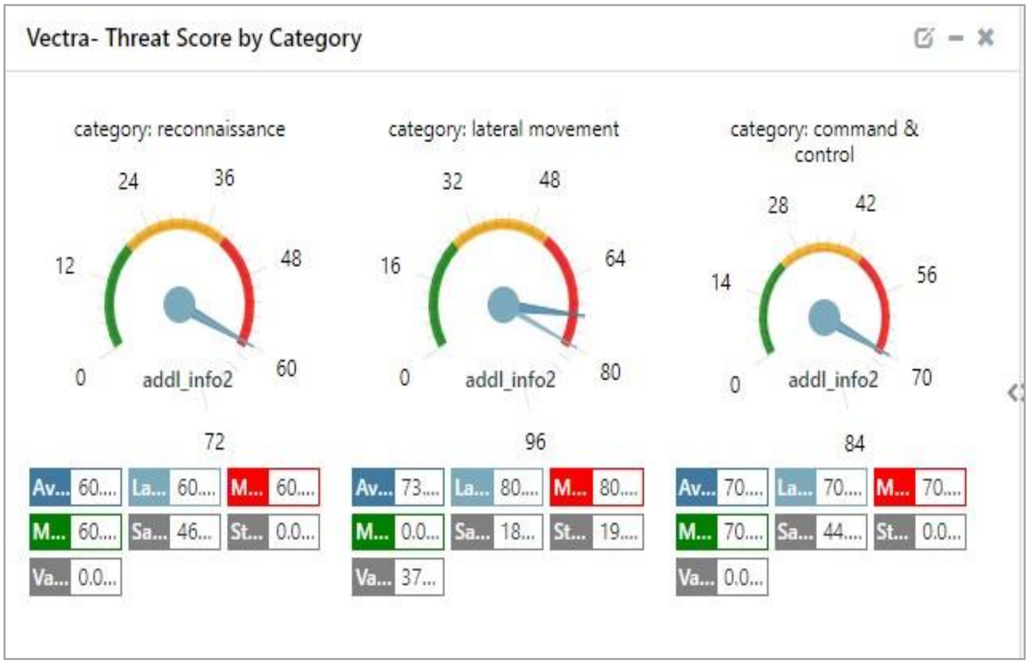

Vectra- Threat Score by Category
category: reconnaissance
0
12
24
36
48
60
72
addl_info2
category: lateral movement
0
16
32
48
64
80
96
addl_info2
category: command & control
0
14
28
42
56
70
84
addl_info2
Av... 60.... La... 60.... M... 60....
M... 60.... Sa... 46.... St... 0.0....
Va... 0.0....
Av... 73.... La... 80.... M... 80....
M... 0.0.... Sa... 18.... St... 19....
Va... 37....
Av... 70.... La... 70.... M... 70....
M... 70.... Sa... 44.... St... 0.0....
Va... 0.0....

Figure 18

Vectra-Certainty score by category

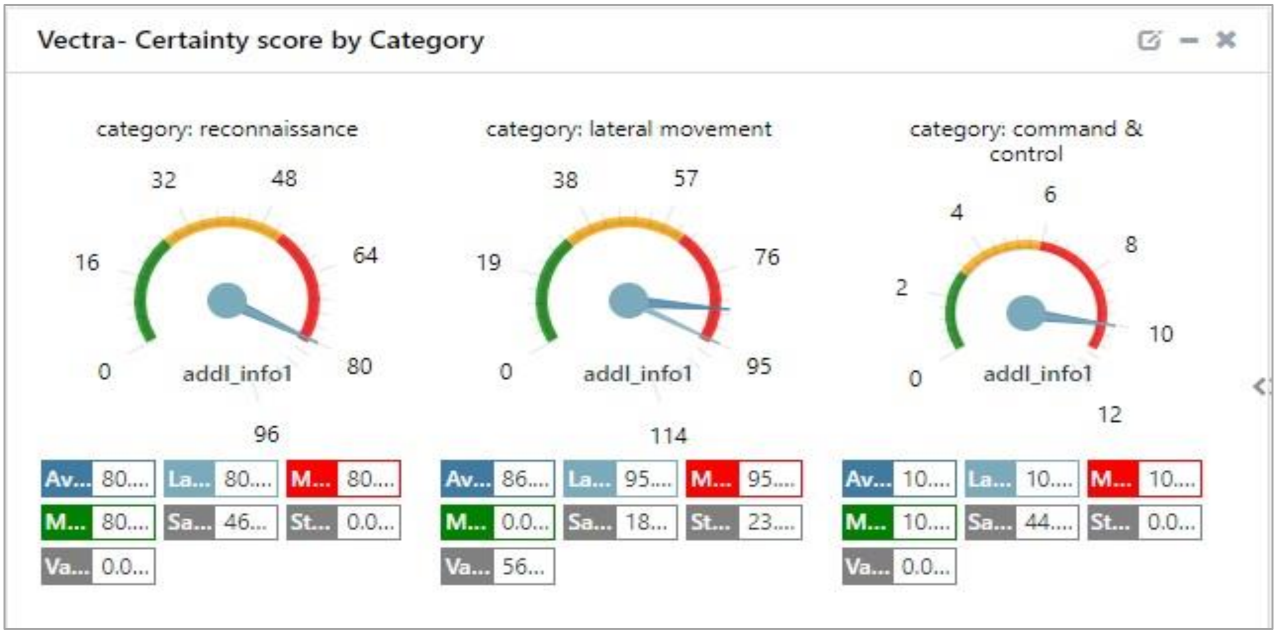


Figure 19

5. Importing Vectra AI knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

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

1. Launch **EventTracker Control Panel**.

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

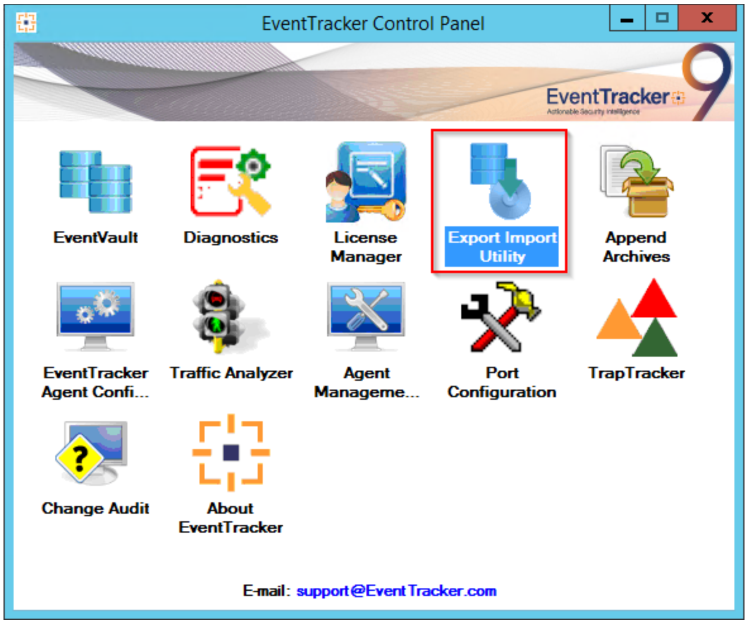
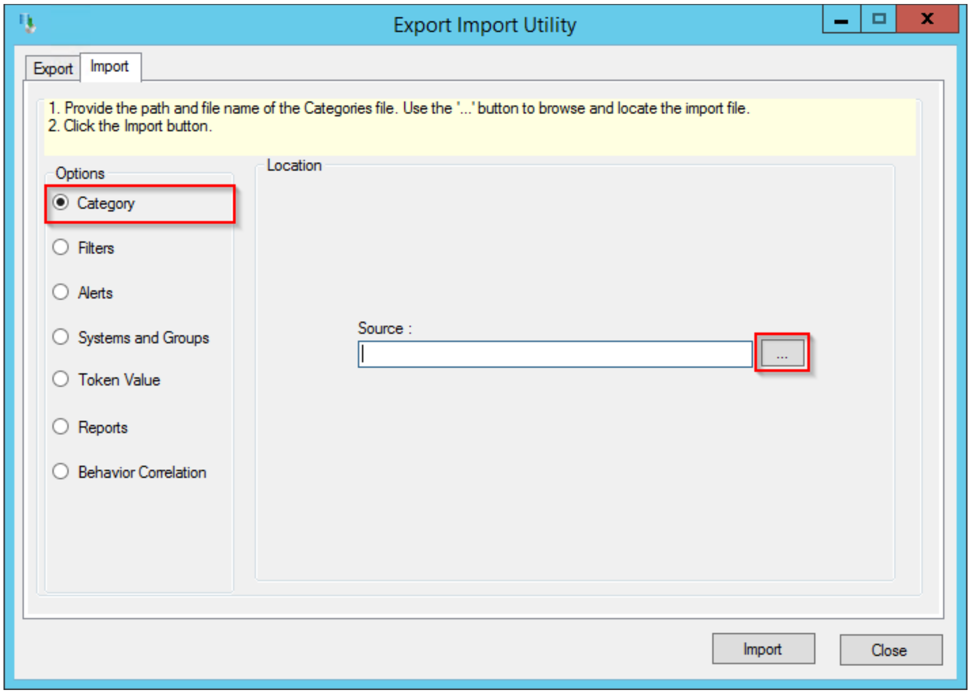


Figure 20

3. Click the **Import** tab.

5.1 Category

1. Click **Category** option, and then 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.

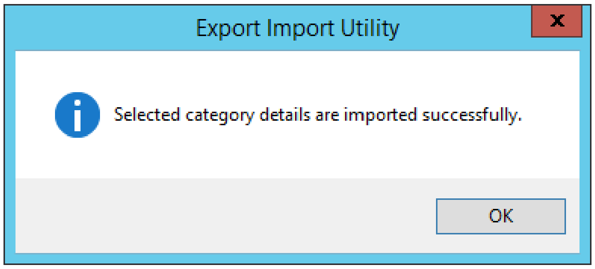
● Category
○ Filters
○ Alerts
○ Systems and Groups
○ Token Value
○ Reports
○ Behavior Correlation

Figure 21

2. Locate **Category_Vectra.iscat** file, and then click **Open**.

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

   EventTracker displays success message.



Export Import Utility

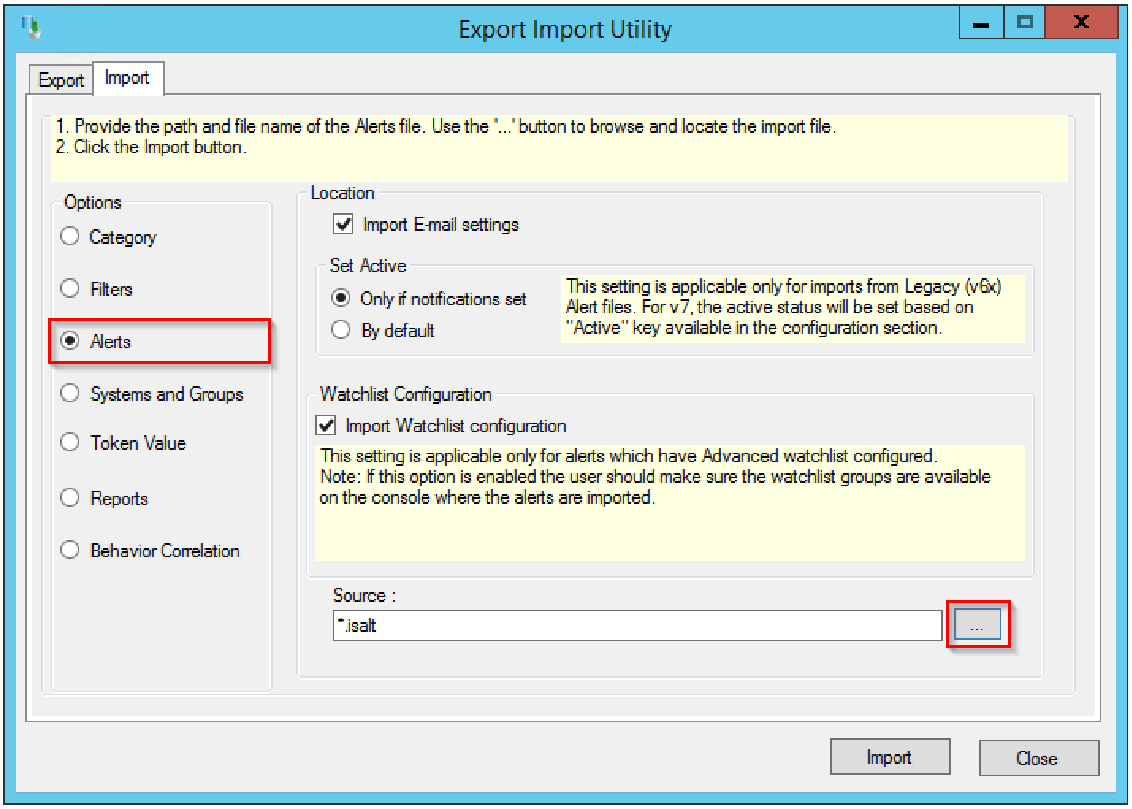
Selected category details are imported successfully.

Figure 22

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

5.2 Alert

1. Click **Alert** option, and then click **Browse** ... .



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

○ 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

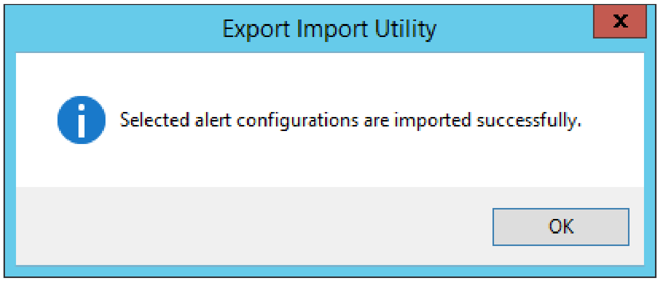
This setting is applicable only for alerts which have Advanced watchlist configured.
Note: If this option is enabled the user should make sure the watchlist groups are available on the console where the alerts are imported.

Source : *.isalt

Figure 23

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

   EventTracker displays success message.



Export Import Utility

Selected alert configurations are imported successfully.

Figure 24

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

5.3 Token Template

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

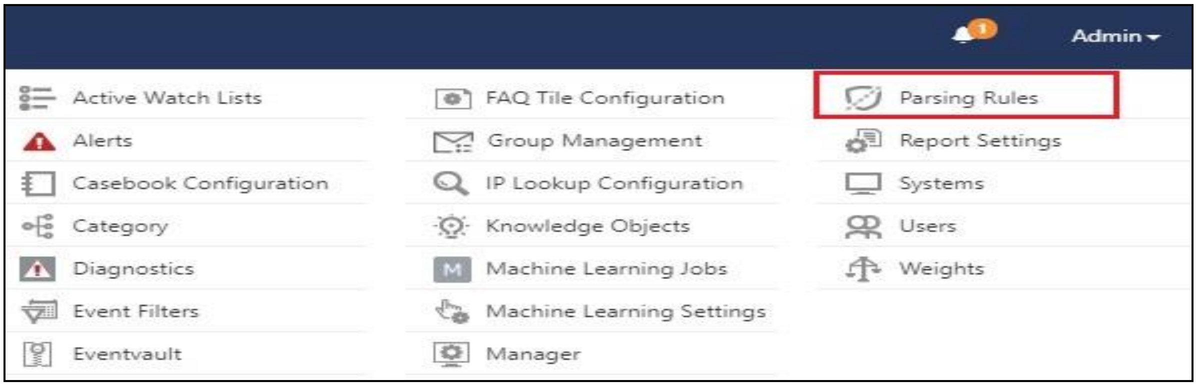


Figure 25

2. Click **Template.**

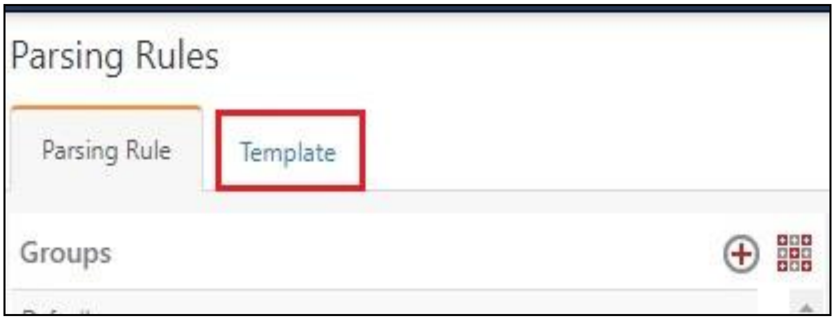


Figure 26

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

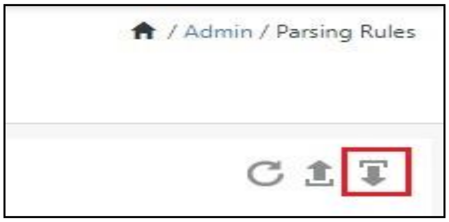
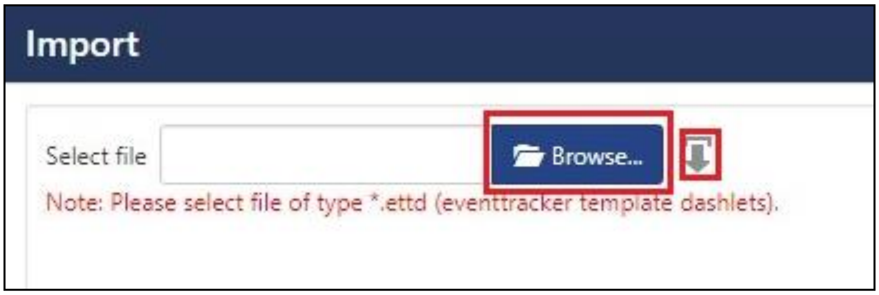


Figure 27

4. Locate the **Templates_Vectra.ettd** type file by clicking **Browse**, enables all the templates and click **import**.



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

Figure 28

5. Click **OK**.

5.4 Knowledge Object

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

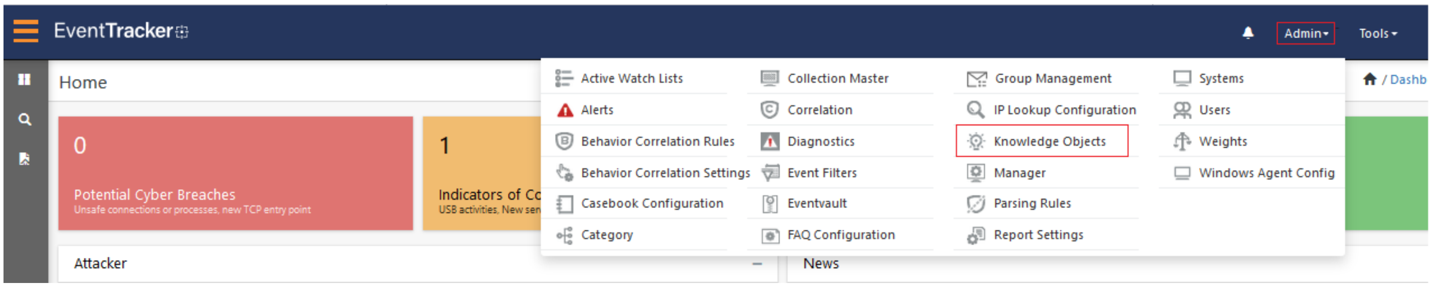


Figure 29

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

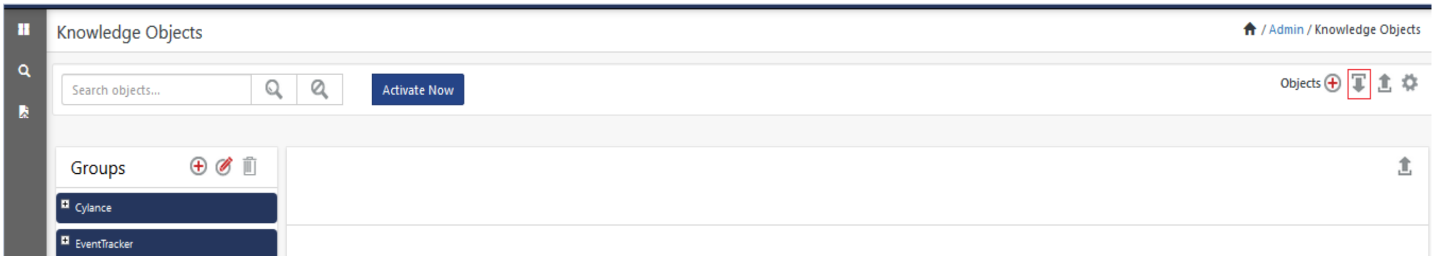


Figure 30

3. Click **Browse**.

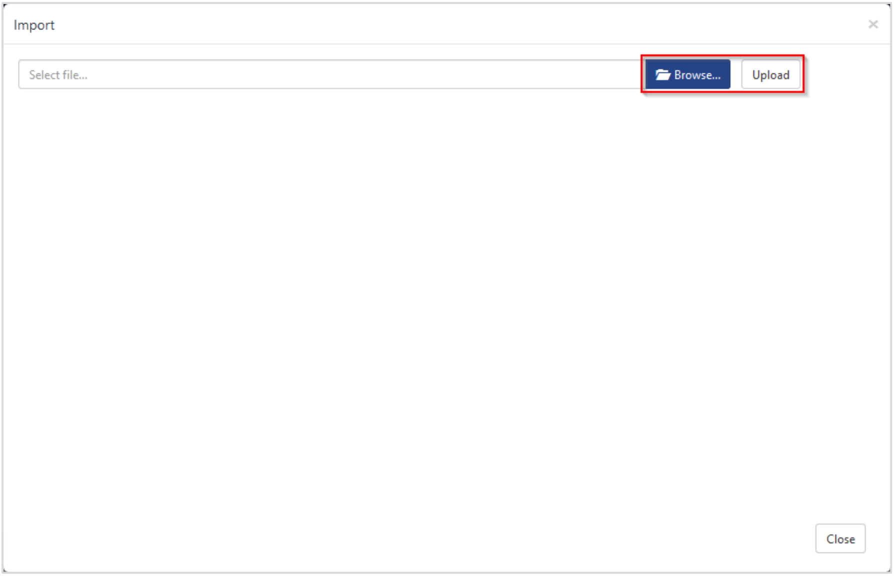
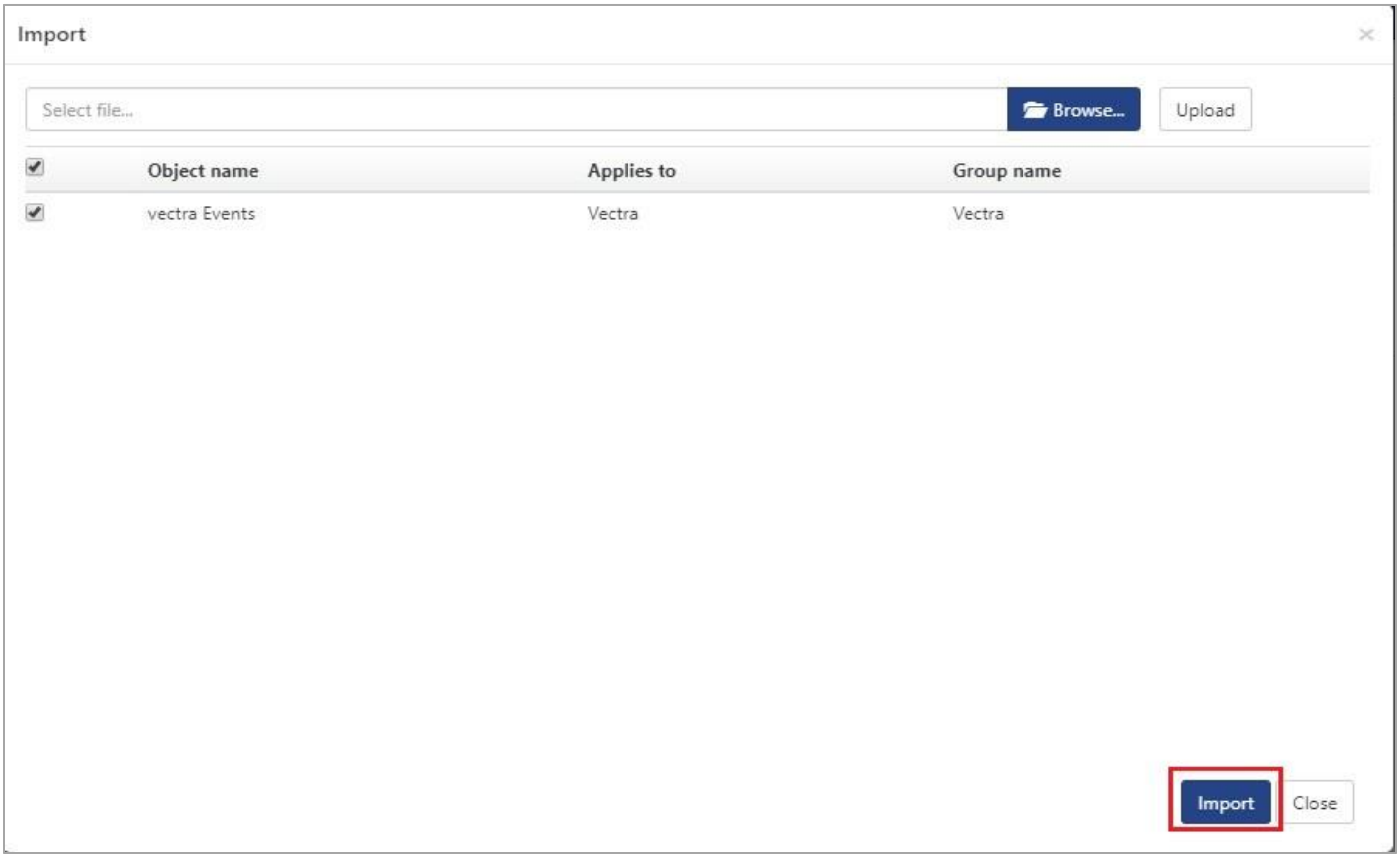


Figure 31

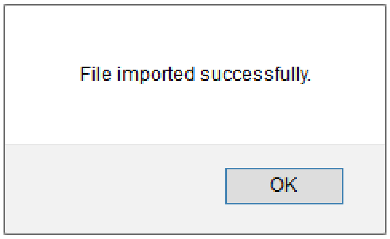
4. Locate the file named **KO_Vectra.etko**.
5. Now select the check box and then click **Import** option.



☑	Object name	Applies to	Group name
☑	vectra Events	Vectra	Vectra

Figure 32

6. Knowledge objects are now imported successfully.



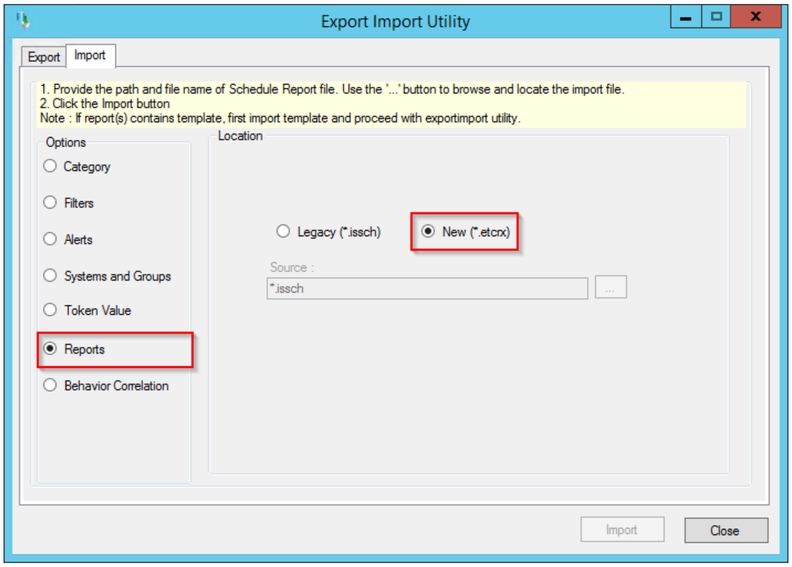
File imported successfully.

Figure 33

5.5 Report

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

2. Locate the file named **Reports_ Vectra.etcrx** and select the check box.



Export Import Utility

Export | Import

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

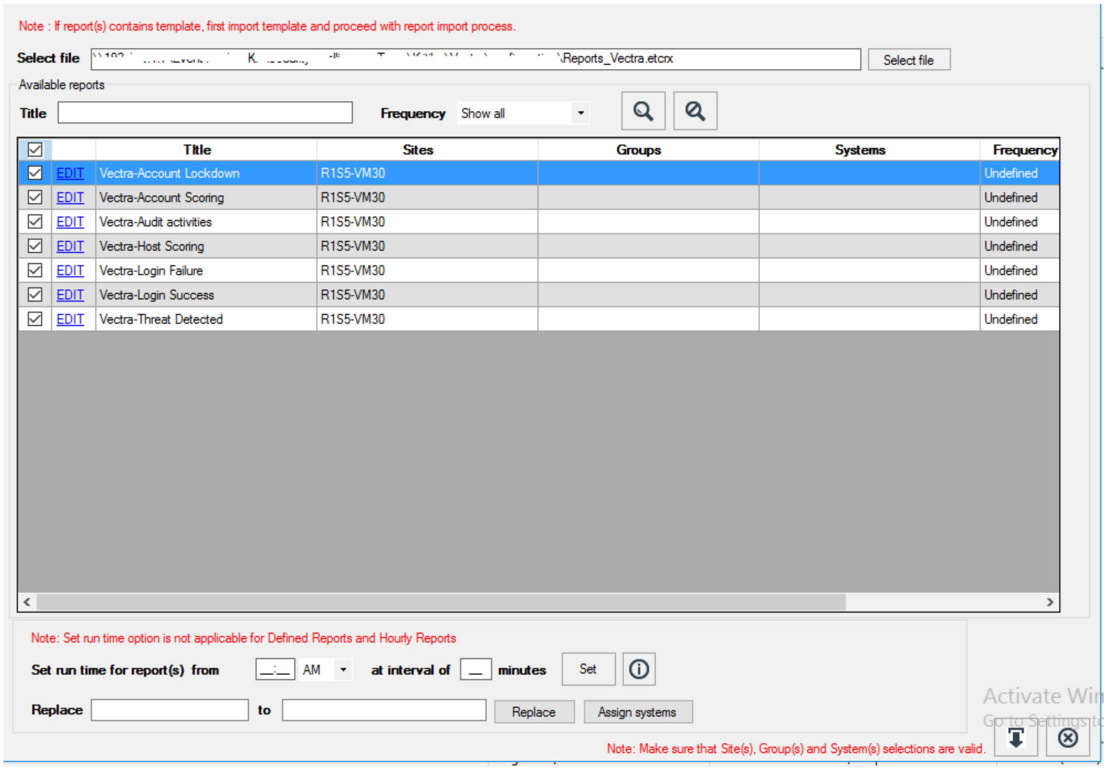
Location

○ Legacy (*.issch) ● New (*.etcrx)

Source : *.issch

Import Close

Figure 34



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

Select file [illegible]\Reports_Vectra.etcrx Select file

Available reports

Title **Frequency** Show all

☑		Title	Sites	Groups	Systems	Frequency
☑	EDIT	Vectra-Account Lockdown	R1S5-VM30			Undefined
☑	EDIT	Vectra-Account Scoring	R1S5-VM30			Undefined
☑	EDIT	Vectra-Audit activities	R1S5-VM30			Undefined
☑	EDIT	Vectra-Host Scoring	R1S5-VM30			Undefined
☑	EDIT	Vectra-Login Failure	R1S5-VM30			Undefined
☑	EDIT	Vectra-Login Success	R1S5-VM30			Undefined
☑	EDIT	Vectra-Threat Detected	R1S5-VM30			Undefined

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

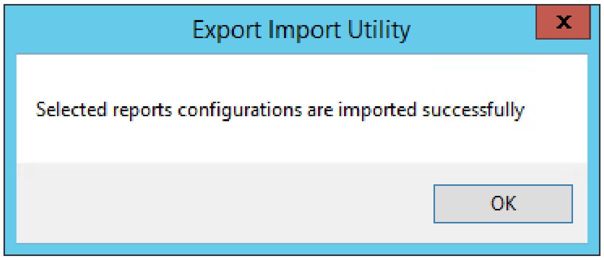
Set run time for report(s) from __:__ AM **at interval of** __ **minutes** Set

Replace **to** Replace Assign systems

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

Figure 35

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



Selected reports configurations are imported successfully

Figure 36

5.6 Dashboards

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

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

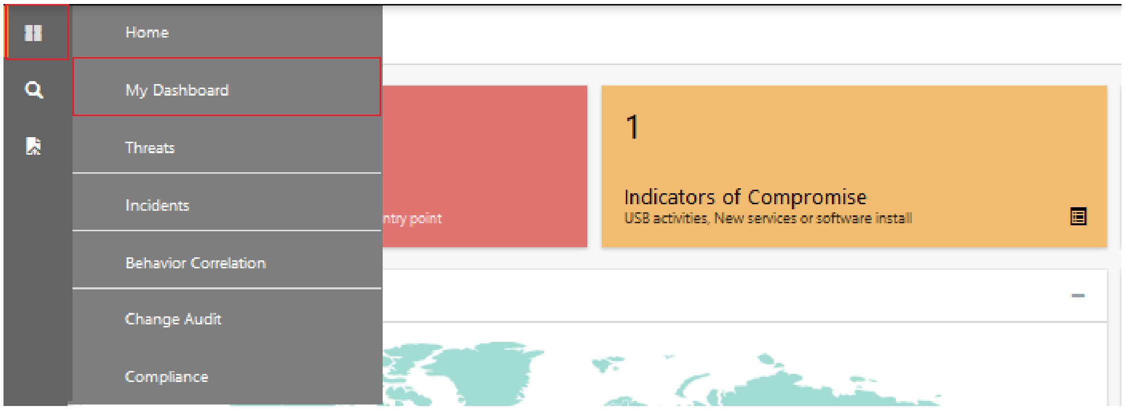


Figure 37

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

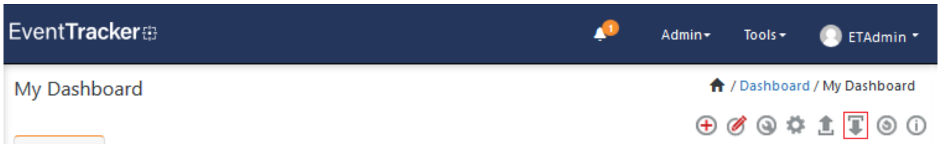


Figure 38

4. Import dashboard file **Dashboard_Vectra.etwd** and select **Select All** checkbox**.**
5. Click **Import** as shown below:

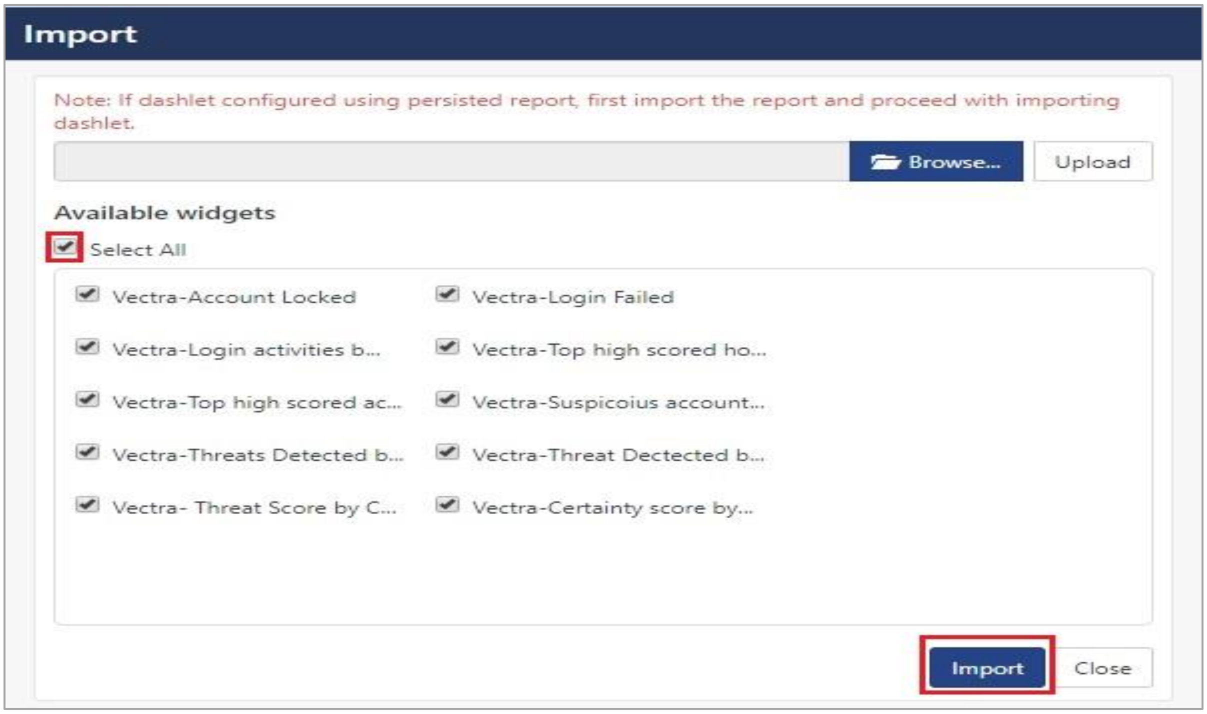

Import
Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.
Browse...
Upload
Available widgets
☑ Select All
☑ Vectra-Account Locked
☑ Vectra-Login Failed
☑ Vectra-Login activities b...
☑ Vectra-Top high scored ho...
☑ Vectra-Top high scored ac...
☑ Vectra-Suspicoius account...
☑ Vectra-Threats Detected b...
☑ Vectra-Threat Dectected b...
☑ Vectra- Threat Score by C...
☑ Vectra-Certainty score by...
Import
Close

Figure 39

6. Import is now completed successfully.

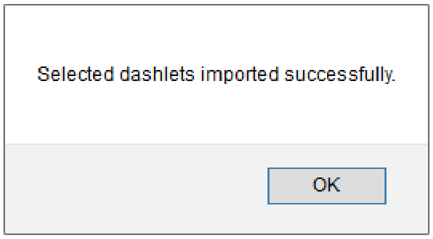

Selected dashlets imported successfully.

Figure 40

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

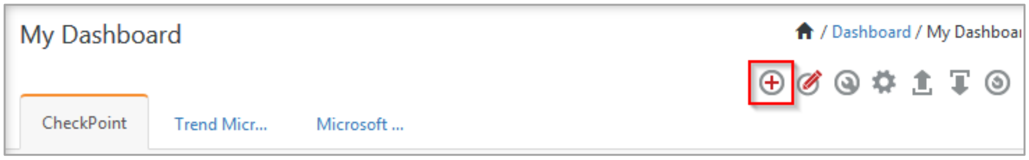
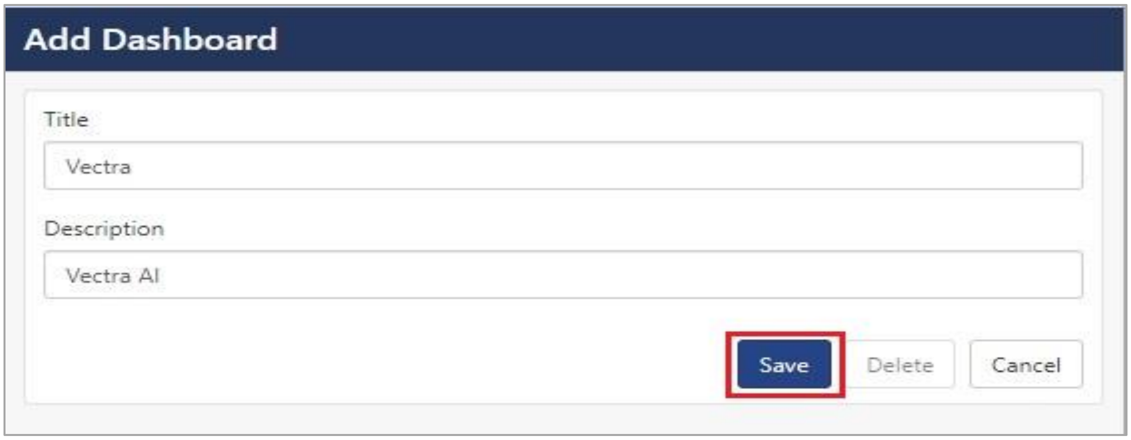


Figure 41

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



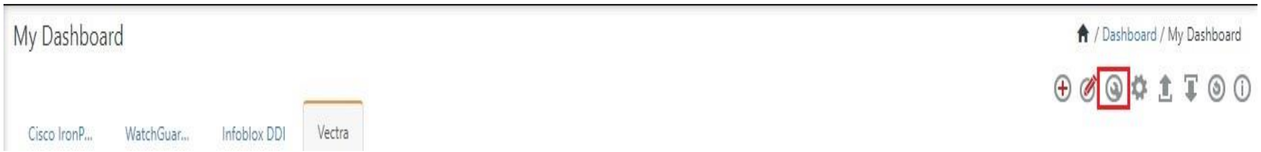
Add Dashboard

Title: Vectra

Description: Vectra AI

Figure 42

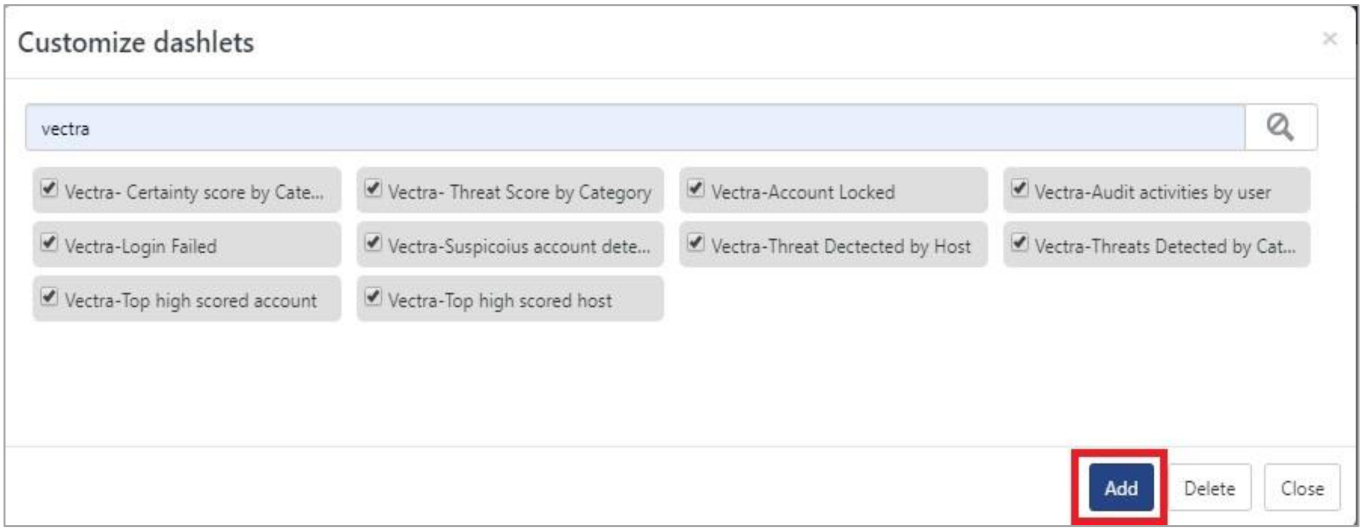
9. In **My Dashboard** page select to add dashlets.



My Dashboard

Figure 43

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



Customize dashlets

vectra

☑ Vectra- Certainty score by Cate...
☑ Vectra- Threat Score by Category
☑ Vectra-Account Locked
☑ Vectra-Audit activities by user
☑ Vectra-Login Failed
☑ Vectra-Suspicoius account dete...
☑ Vectra-Threat Dectected by Host
☑ Vectra-Threats Detected by Cat...
☑ Vectra-Top high scored account
☑ Vectra-Top high scored host

Figure 44

6. Verifying Vectra AI knowledge pack in EventTracker

6.1 Category

1. Logon to **EventTracker**.

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

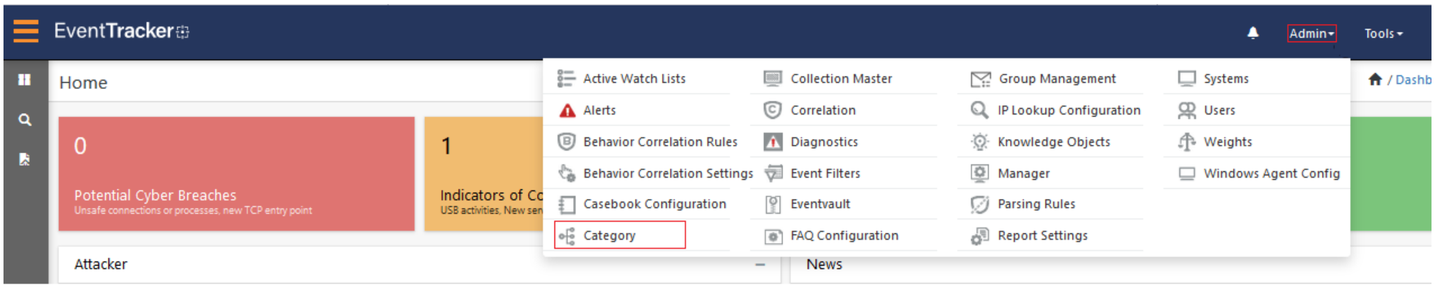


Figure 45

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

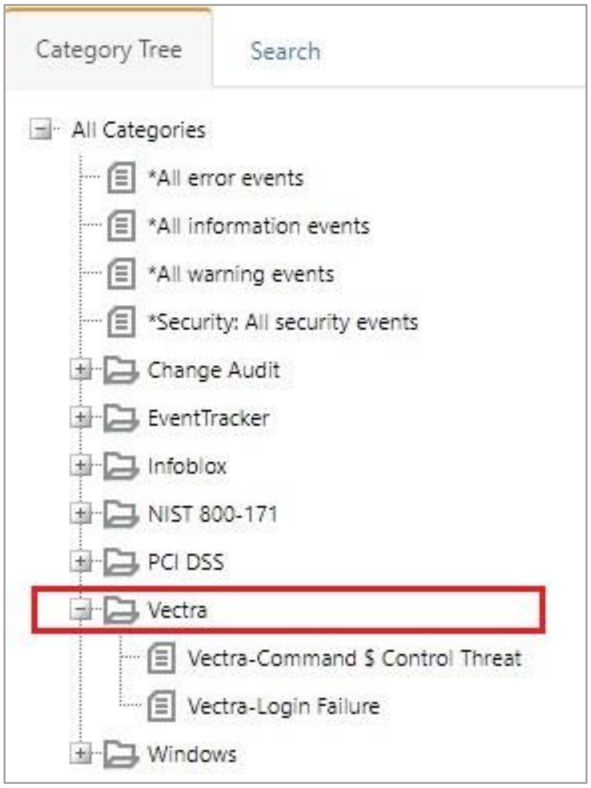


Figure 46

6.2 Alert

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

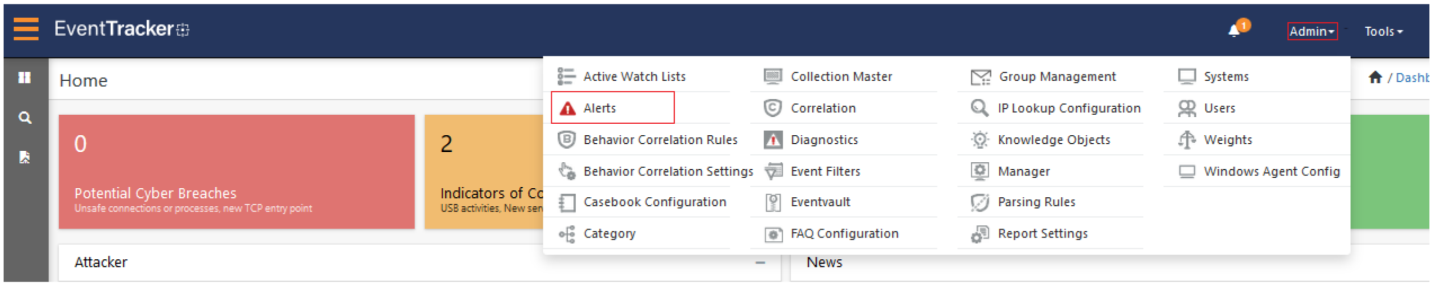
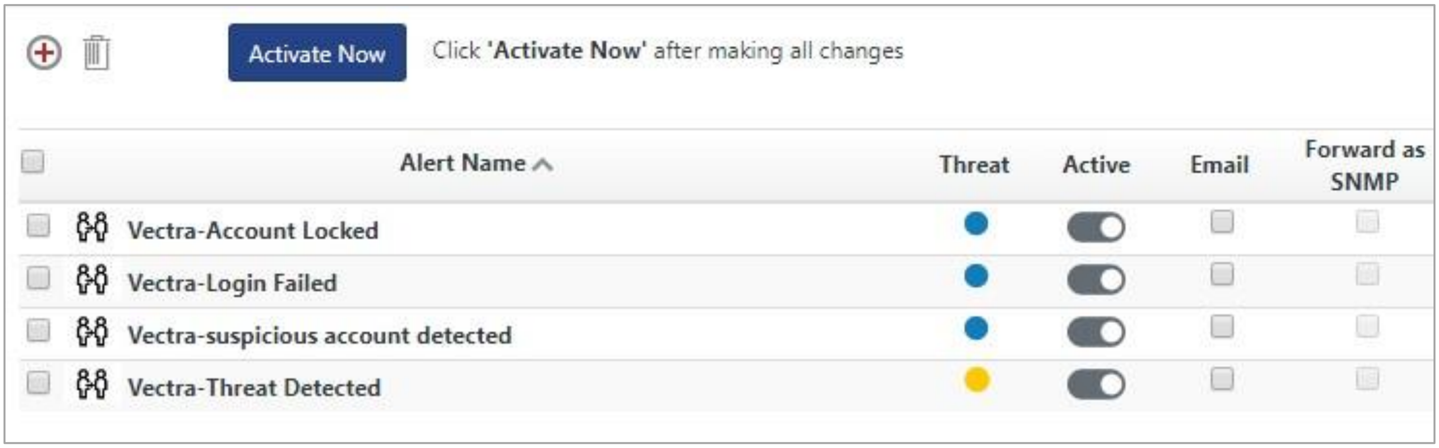


Figure 47

3. In the **Search** box, type '**Vectra**, and then click **Go**.
   Alert Management page will display the imported alert.

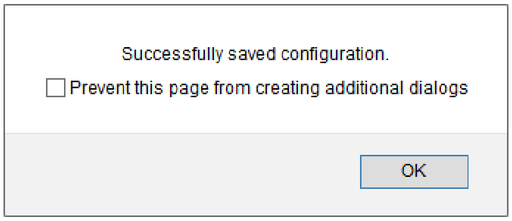


□	Alert Name	Threat	Active	Email	Forward as SNMP
□	Vectra-Account Locked	●	●	□	□
□	Vectra-Login Failed	●	●	□	□
□	Vectra-suspicious account detected	●	●	□	□
□	Vectra-Threat Detected	●	●	□	□

Figure 48

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

   EventTracker displays message box.



Successfully saved configuration.

□ Prevent this page from creating additional dialogs

OK

Figure 49

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

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

6.3 Parsing Rules

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

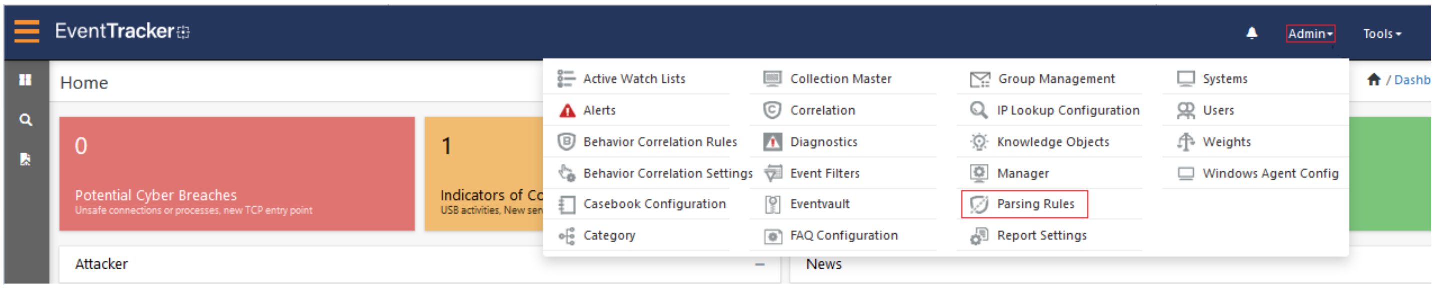
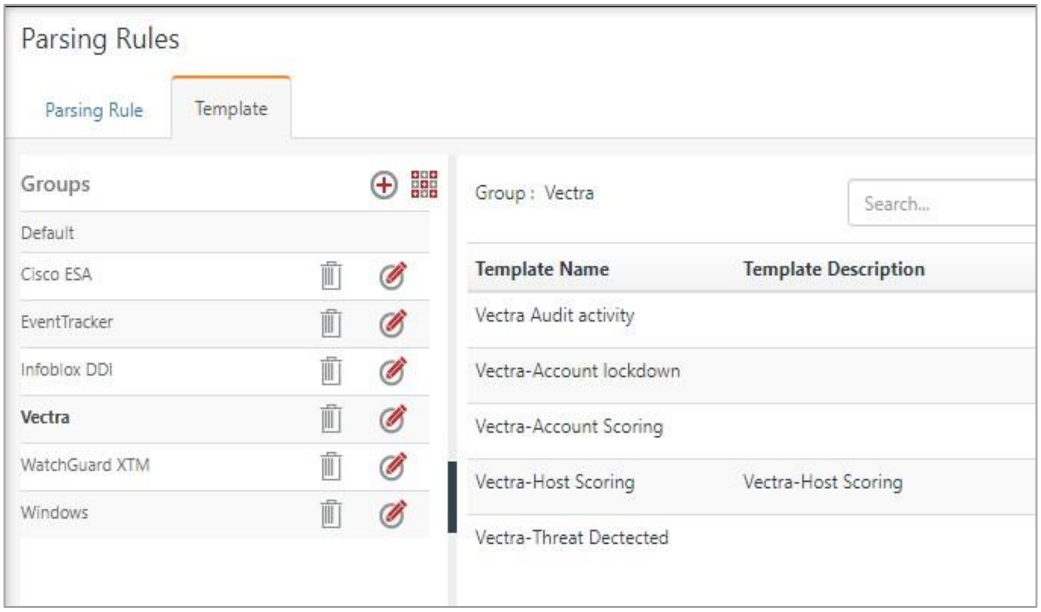


Figure 50

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



Groups:

- Default
- Cisco ESA
- EventTracker
- Infoblox DDI
- **Vectra**
- WatchGuard XTM
- Windows

Group : Vectra

Template Name	Template Description
Vectra Audit activity	
Vectra-Account lockdown	
Vectra-Account Scoring	
Vectra-Host Scoring	Vectra-Host Scoring
Vectra-Threat Dectected	

Figure 51

6.4 Knowledge Object

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

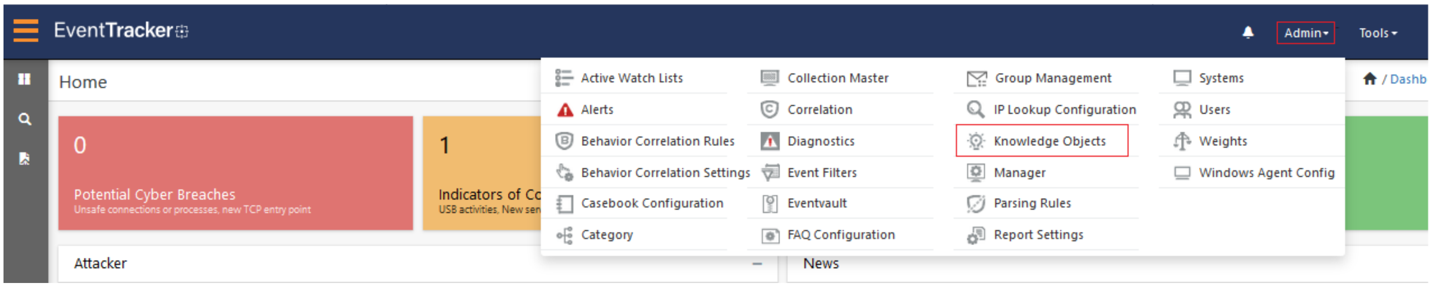
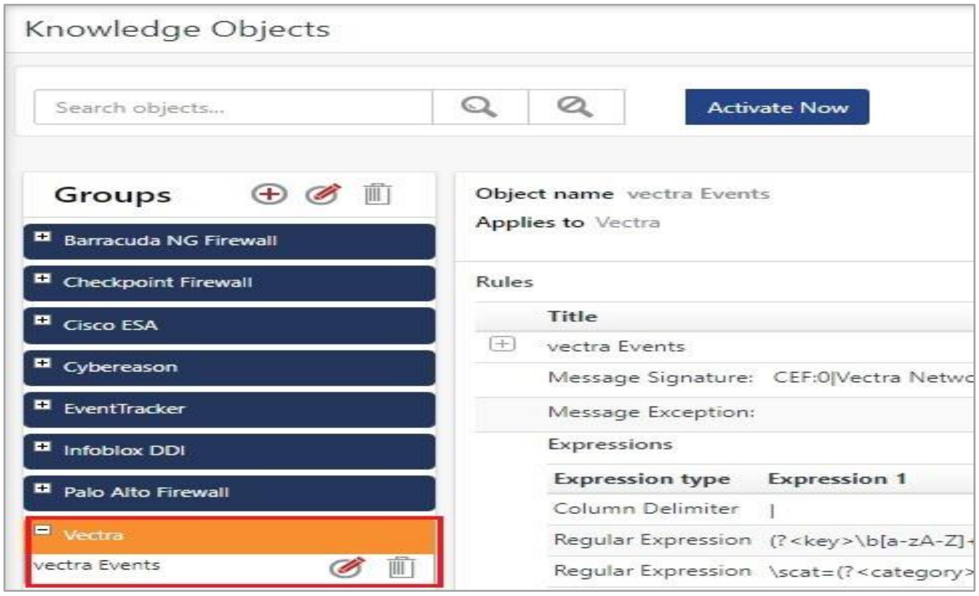


Figure 52

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



Object name vectra Events
Applies to Vectra

Rules

Title	
vectra Events	
Message Signature:	CEF:0|Vectra Netwo
Message Exception:	
Expressions	

Expression type	Expression 1
Column Delimiter	|
Regular Expression	(?<key>\b[a-zA-Z]
Regular Expression	\scat=(?<category>

Figure 53

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**.

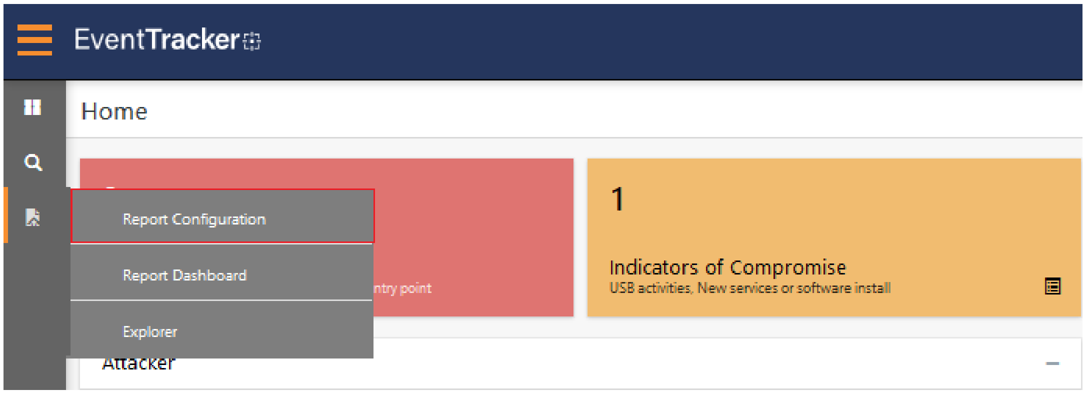
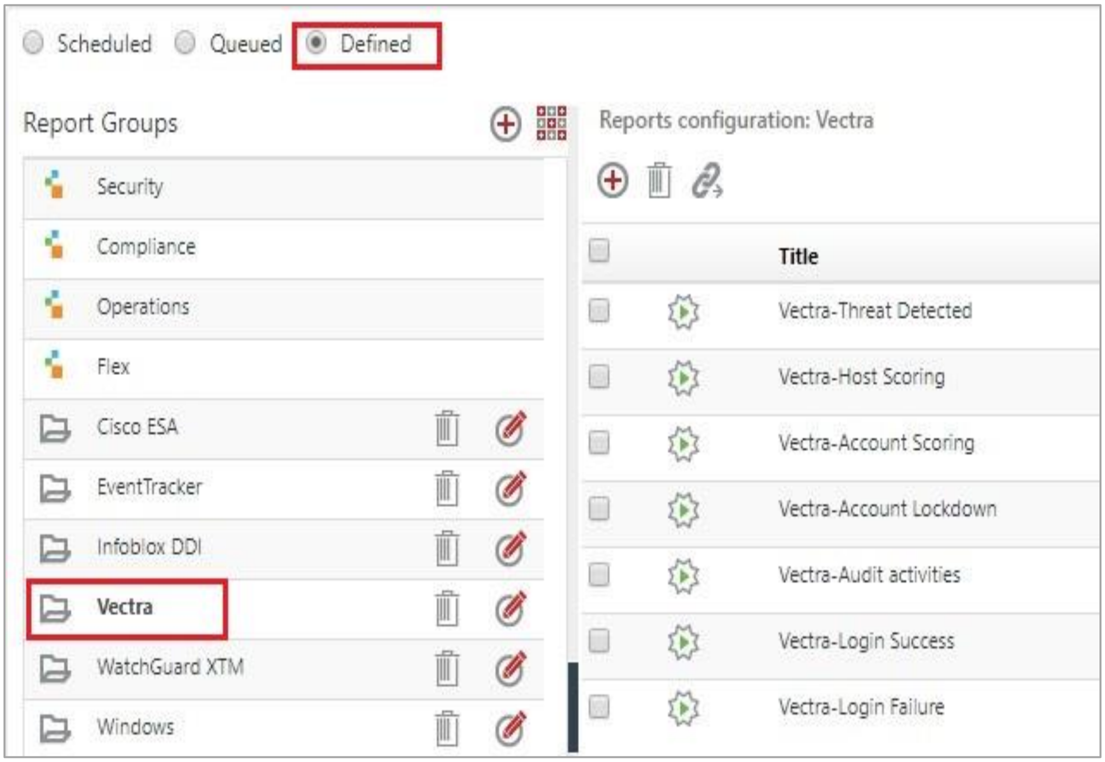


Figure 54

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



○ Scheduled ○ Queued ● Defined

□	Title
□	Vectra-Threat Detected
□	Vectra-Host Scoring
□	Vectra-Account Scoring
□	Vectra-Account Lockdown
□	Vectra-Audit activities
□	Vectra-Login Success
□	Vectra-Login Failure

Figure 55

6.6 Dashboards

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

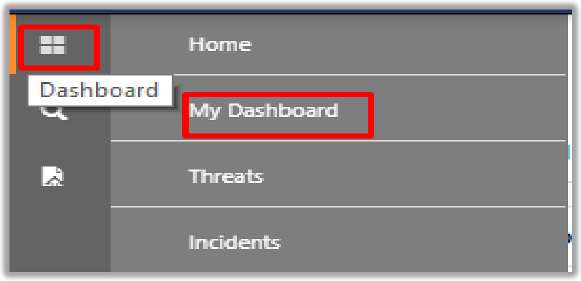


Figure 56

2. In the "**Vectra**" dashboard you should be now able to see something like this.

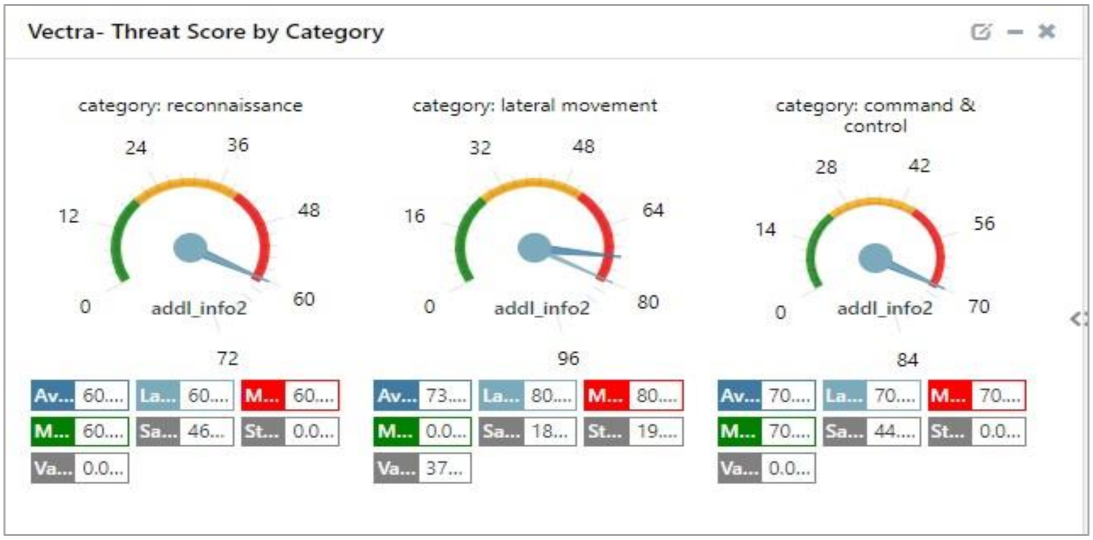

Vectra- Threat Score by Category
category: reconnaissance
0
12
24
36
48
60
72
addl_info2
Av... 60....
La... 60....
M... 60....
M... 60....
Sa... 46...
St... 0.0...
Va... 0.0...
category: lateral movement
0
16
32
48
64
80
96
addl_info2
Av... 73....
La... 80....
M... 80....
M... 0.0...
Sa... 18...
St... 19....
Va... 37...
category: command & control
0
14
28
42
56
70
84
addl_info2
Av... 70....
La... 70....
M... 70....
M... 70....
Sa... 44....
St... 0.0...
Va... 0.0...

Figure 57