Netsurion™ | EventTracker

Integrate Cybereason

EventTracker v9.x and above

Publication Date: SEP 17, 2019

Abstract

This guide provides instructions to configure/ retrieve **Cybereason** events using **EventTracker Application.** This will collect the logs from Cybereason like user activity, threat details, etc. Once EventTracker is configured to collect and parse these logs, dashboard, alerts, and reports can be configured to monitor Cybereason.

Scope

The configurations detailed in this guide are consistent with EventTracker version v9.x or above and **Cybereason** 17.3 and later.

Audience

Administrators who are assigned the task to monitor Cybereason using EventTracker.

Table of Contents

1. Overview

The Cybereason solution combines endpoint prevention, detection, and response all-in-one lightweight agent. EventTracker supports Cybereason, monitors the Cybereason and generates the alerts and reports for critical events like MALOP creation, malware or Threat detection, user activities, etc. The saved search and dashboards help to monitor critical and top activities in the Cybereason.

2. Prerequisites

- EventTracker v9.x or later should be installed.
- Cybereason 17.3 or later should be installed.
- The Firewall exception for the syslog port (default: 514) should be enabled between Cybereason and EventTracker.

3. Configuring Cybereason to send syslog to EventTracker

- The EventTracker is compatible with the syslog format available in Cybereason 17.3, or in Cybereason 17.5+ running in compatibility mode. (Syslog 17.3 format).
- You must submit a request for a syslog configuration to Cybereason's technical support. You must provide Technical Support with your IPv4 and Port number to connect the unencrypted TCP syslog to your 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 Cybereason.

4.1 Flex Reports

- **Cybereason - User login failed activities –** This report gives information about, the user who has failed to log into the console, along with user and device information like IP address, hostname, and its role.

LogTime	Computer	Event Class	Event Category	Severity	Action Status (Failed: 0 Success:1)	User Name	User Role	Machine Name	Machine IP Address
09/13/2019 02:44:54 PM	CYBEREASON	General	Login	0	0	barbarag	analyst_l3	contoso-server2dc	89.234.157.254
09/13/2019 02:44:55 PM	CYBEREASON	General	Login	0	0	matt	analyst_l3	contoso-server2dc	91.200.12.91
09/13/2019 02:44:55 PM	CYBEREASON	General	Login	1	0	maryj	sys_admin	contoso-asagw2	213.251.182.115
09/13/2019 02:44:55 PM	CYBEREASON	General	Login	1	0	frantz	sys_admin	contoso-etids	195.154.250.216
09/13/2019 02:44:55 PM	CYBEREASON	General	Login	0	0	clarkk	analyst_l3	contoso-etids	195.154.250.216
09/13/2019 02:44:55 PM	CYBEREASON	General	Login	0	0	peterp	user_admin	contoso-etids	195.154.240.176
09/13/2019 02:44:55 PM	CYBEREASON	General	Login	1	0	loisl	sys_admin	contoso-dc01.azurestack	77.247.181.165
09/13/2019 02:44:55 PM	CYBEREASON	General	Login	1	0	joeb	executive	contoso-etsb12	195.154.240.176
09/13/2019 02:44:55 PM	CYBEREASON	General	Login	0	0	System	executive	contoso-server6dc	195.154.241.119
09/13/2019 02:44:55 PM	CYBEREASON	General	Login	0	0	frantz	sys_admin	contoso-etids	201.18.18.173
09/13/2019 02:44:55 PM	CYBEREASON	General	Login	0	0	mjones	sys_admin	contoso-rhsvr1	178.137.87.242
09/13/2019 02:44:55 PM	CYBEREASON	General	Login	0	0	loisl	user_admin	contoso-etsb12	46.148.22.18

Figure 1

- **Cybereason - User login and logout activities –** This report gives information about the user login and logout activities in the console, along with user and device information like IP address, hostname, and its role.

LogTime	Event Class	Event Category	User Name	User Role	Action Status (Failed: 0 Success:1)	Machine IP Address	Machine Name
09/13/2019 02:44:55 PM	General	Logout	joe	analyst_l3	1	195.154.250.216	contoso-etids
09/13/2019 02:44:55 PM	General	Login	mjones	executive	1	195.154.243.31	contoso-filesvr6
09/13/2019 02:44:55 PM	General	Logout	clarkk	sys_admin	1	195.154.250.216	contoso-etids
09/13/2019 02:44:55 PM	General	Login	frantz	user_admin	1	37.187.129.166	contoso-asagw2
09/13/2019 02:44:55 PM	General	Logout	matt	analyst_l3	1	89.234.157.254	contoso-asagw1

Figure 2

- **Cybereason – User activities –** This report gives detailed information on user action takes places on Cybereason activities like (custom rule creation, Change in configuration settings, sensor management).

LogTime	Product	Event Category	Event Class	Severity	User Name	Action Status (Failed: 0 Success:1)	Previous Mode	New Mode
09/12/2019 11:13:25 AM	Cybereason	ChangeConfigurationSettings	General	0	admin@contoso.com	1		
09/12/2019 11:13:25 AM	Cybereason	ChangeConfigurationSettings	General	0	admin@contoso.com	1		
09/12/2019 11:13:25 AM	Cybereason	ChangeConfigurationSettings	General	0	admin@contoso.com	1		
09/12/2019 11:13:25 AM	Cybereason	PowerShellProtectionMode	Security Profile	0	admin@contoso.com	1	Off	On
09/12/2019 11:13:25 AM	Cybereason	ChangeConfigurationSettings	General	0	admin@contoso.com	1		
09/12/2019 11:13:25 AM	Cybereason	PowerShellProtectionMode	Security Profile	0	admin@contoso.com	1	On	Off

Figure 3

- **Cybereason - User malop investigation activities–** This report gives detailed information on user action on investigating malop activities like (threat remediation, change in malop state, remediation details, machine isolation details)

LogTime	Event name	Event class	Severity	Destination Hostname	Virus Name	Threat Info	Investigation URL	Malware Creation Time
09/13/2019 11:46:28 AM	Malware Created	Malware	5	contoso-server6dc	eicar.com	https://eicar.com	http://localhost:7894/d/42669814	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:28 AM	Malware Created	Malware	1	contoso-rhsvr1	eicar.com	invoke-expression	http://localhost:7894/d/25649090	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:28 AM	Malware Created	Malware	1	contoso-server2dc	AI.StaticAnalysis	invoke-expression	http://localhost:7894/d/28558771	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:28 AM	Malware Updated	Malware	5	contoso-server1dc	download & execute	https://eicar.com	http://localhost:7894/d/72400271	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:28 AM	Malware Updated	Malware	5	contoso-server6dc	malicious download	http://www.example.com/aunt/advice.html?breath=account&afterthought=army	http://localhost:7894/d/20292064	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:28 AM	Malware Created	Malware	5	contoso-server2dc	AI.StaticAnalysis	https://eicar.com	http://localhost:7894/d/94165369	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:28 AM	Malware Updated	Malware	5	contoso-filesvr6	AI.StaticAnalysis	http://www.example.com/aunt/advice.html?breath=account&afterthought=army	http://localhost:7894/d/48709325	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:28 AM	Malware Updated	Malware	1	contoso-asagw2	download & execute	https://eicar.com	http://localhost:7894/d/75044513	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:28 AM	Malware Updated	Malware	1	contoso-asagw2	eicar.com	http://www.example.com/aunt/advice.html?breath=account&afterthought=army	http://localhost:7894/d/123113752	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:28 AM	Malware Updated	Malware	5	contoso-rhsvr1	malicious command	http://www.example.com/aunt/advice.html?breath=account&afterthought=army	http://localhost:7894/d/61320046	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:28 AM	Malware Created	Malware	5	contoso-asagw2	malicious command	https://eicar.com	http://localhost:7894/d/49118045	Dec 19 2017, 15:58:14 IST

Figure 4

- **Cybereason - Malop created or updated details –** This report gives information on MALOP created or updated information along with MALOP information.

Event name	Severity	Start Time	Malop Id	Malop Activity Type	Malop Detection Type	Malop Key Suspicion	Malop Suspect	Reason	Is Signed	Malop Link	Request Context	Affected Machine Name	Affected Machines Count	Affected Users Count
Malop Created	10	Dec 19 2017, 15:58:14 IST	59.904712850	Data_Theft	MalopProcess	Credential Theft Malop	API.md	blacklist	1	localhost:8080/#/malop/54.545034625	API.md		45	3
Malop Created	10	Dec 19 2017, 15:58:14 IST	59.953052412	Scanning	MalopProcess	Credential Theft Malop	uc_FlexMeterGuage_am.ascx	blacklist	1	localhost:8080/#/malop/67.990879413	uc_FlexMeterGuage_am.ascx		68	86
Malop Created	10	Dec 19 2017, 15:58:14 IST	59.322872258	Scanning	MalopProcess	Credential Theft Malop	uc_Widget.ascx	blacklist	0	localhost:8080/#/malop/86.816018953	uc_Widget.ascx		91	78
Malop Created	10	Dec 19 2017, 15:58:14 IST	44.419719562	Privilege Escalation	MalopProcess	Credential Theft Malop	teszt.pdf	blacklist	0	localhost:8080/#/malop/39.885614423	teszt.pdf		17	63
Malop Created	10	Dec 19 2017, 15:58:14 IST	56.292623304	Privilege Escalation	MalopProcess	Credential Theft Malop	nations.html	blacklist	0	localhost:8080/#/malop/51.561718937	nations.html		81	95
Malop Created	10	Dec 19 2017, 15:58:14 IST	55.816516132	Scanning	MalopProcess	Credential Theft Malop	uc_FlexTabular.ascx	blacklist	1	localhost:8080/#/malop/58.399869412	uc_FlexTabular.ascx		81	70
Malop Created	10	Dec 19 2017, 15:58:14 IST	48.755679689	Data_Theft	MalopProcess	Credential Theft Malop	test_radial_tree.html	blacklist	0	localhost:8080/#/malop/73.933059657	test_radial_tree.html		6	52
Malop Created	10	Dec 19 2017, 15:58:14 IST	59.178681575	Scanning	MalopProcess	Credential Theft Malop	diagram-state-machine.png	blacklist	1	localhost:8080/#/malop/97.583713561	diagram-state-machine.png		14	90
Malop Created	10	Dec 19 2017, 15:58:14 IST	15.135355903	C&C	MalopProcess	Credential Theft Malop	test_constraints.html	blacklist	0	localhost:8080/#/malop/47.815584963	test_constraints.html		46	3
Malop Created	10	Dec 19 2017, 15:58:14 IST	58.941229766	Scanning	MalopProcess	Credential Theft Malop	elasticsearch.jquery.min.js	blacklist	1	localhost:8080/#/malop/50.372699663	elasticsearch.jquery.min.js		20	51

Figure 5

- **Cybereason - Malop device information details –** This report gives information on the device in which Malop incident has been detected. This report will help to investigate the malop activity when correlated with the malop created or updated details report.

LogTime	Severity	Event name	Malop Id	Affected Machines Count	Destination Hostname	Parent Process	ChildrenProcess	OS Version	User Name	Online Status
09/13/2019 11:46:29 AM	10	Malop Machine Information	13.837687851	12	10.0.0.25	SISIDSService	smss	Windows_10	System	
09/13/2019 11:46:29 AM	10	Malop Machine Information	69.867300583	14	10.25.2.1	Microsoft.Photos	iexplore	Windows_10	frantz	
09/13/2019 11:46:29 AM	10	Malop Machine Information	21.126999488	27	contososerver	smss	mmc	Windows_10	clarkk	
09/13/2019 11:46:29 AM	10	Malop Machine Information	92.688107116	59	contososerver	EventTracker.Reporter	Microsoft.Photos	Windows_7	frantz	
09/13/2019 11:46:29 AM	10	Malop Machine Information	54.900108218	90	10.25.2.1	lync	cmd	Windows_10	frantz	
09/13/2019 11:46:29 AM	10	Malop Machine Information	94.739722606	59	contososerver	UcMapi	SISIPSService	Windows_10	polo	
09/13/2019 11:46:29 AM	10	Malop Machine Information	50.697752353	44	10.25.2.1	UcMapi	smss	Windows_8	gary	
09/13/2019 11:46:29 AM	10	Malop Machine Information	59.262759465	97	contososerver	EtScheduler	vmware-usbarbitrator64	Windows_8	brucew	
09/13/2019 11:46:29 AM	10	Malop Machine Information	81.775880625	48	10.25.2.1	EventTracker.Reporter	smss	Windows_8	polo	
09/13/2019 11:46:29 AM	10	Malop Machine Information	90.998397327	11	contososerver	mmc	brkrprcs64	Windows_10	matt	
09/13/2019 11:46:29 AM	10	Malop Machine Information	25.576340879	42	10.25.2.1	Expresso	iexplore	Windows_8	maya	
09/13/2019 11:46:29 AM	10	Malop Machine Information	68.297060039	58	contososerver	notepad	smss	Windows_7	peterp	
09/13/2019 11:46:29 AM	10	Malop Machine Information	39.436108213	68	10.25.2.1	Expresso	SISIDSService	Windows_8	System	
09/13/2019 11:46:29 AM	10	Malop Machine Information	94.559264978	22	contososerver	Expresso	System	Windows_10	System	
09/13/2019 11:46:29 AM	10	Malop Machine Information	20.313244031	48	10.25.2.1	SISIDSService	EtScheduler	Windows_7	System	
09/13/2019 11:46:29 AM	10	Malop Machine Information	18.857816535	31	contososerver	EventTracker.Reporter	scheduler	Windows_8	loisl	
09/13/2019 11:46:29 AM	10	Malop Machine Information	79.274651621	64	10.25.2.1	iexplore	SISIDSService	Windows_7	peterp	
09/13/2019 11:46:29 AM	10	Malop Machine Information	23.940710621	28	contososerver	mmc	smss	Windows_7	System	

Figure 6

- **Cybereason - Threat detected and updated details –** This report gives detailed information on malware or threat (fileless, ai analytics or known malware) detected or suspected by the Cybereason. And contains information on resolved threat information can be identified by the severity 1 in case of completed, 5 in case of threat detected.

LogTime	Event name	Event class	Severity	Destination Hostname	Virus Name	Threat Info	Investigation URL	Malware Creation Time
09/13/2019 11:46:26 AM	Malware Created	Malware	10	contoso-server2dc	malicious command	https://eicar.com	http://localhost:7894/id/50395866	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:26 AM	Malware Created	Malware	10	contoso-server2dc	malicious download	http://www.example.com/aunt/advice.html?breath=account&afterthought=army	http://localhost:7894/id/98625694	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:26 AM	Malware Created	Malware	10	contoso-etsb12	eicar.com	https://eicar.com	http://localhost:7894/id/71487702	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:26 AM	Malware Updated	Malware	10	contoso-filesvr6	download & execute	https://eicar.com	http://localhost:7894/id/118388624	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:26 AM	Malware Updated	Malware	10	contoso-asagw2	AI.StaticAnalysis	https://eicar.com	http://localhost:7894/id/124212492	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:28 AM	Malware Created	Malware	10	contoso-rhsvr1	download & execute	https://eicar.com	http://localhost:7894/id/21565572	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:28 AM	Malware Created	Malware	10	contoso-asagw2	malicious download	http://www.example.com/aunt/advice.html?breath=account&afterthought=army	http://localhost:7894/id/23032040	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:28 AM	Malware Created	Malware	10	contoso-asagw1	AI.StaticAnalysis	invoke-expression	http://localhost:7894/id/61852049	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:28 AM	Malware Created	Malware	10	contoso-etsb12	AI.StaticAnalysis	invoke-expression	http://localhost:7894/id/24476609	Dec 19 2017, 15:58:14 IST

Figure 7

- **Cybereason - Not mitigated threat details -**This report gives information on the critical threat which failure to act by Cybereason.

Event name	Event class	Severity	Destination Hostname	Virus Name	Threat Info	Investigation URL	Malware Creation Time
Malware Updated	Malware	10	contoso-etsb12	malicious download	http://www.example.com/aunt/advice.html?breath=account&afterthought=army	http://localhost:7894/id/61567803	Dec 19 2017, 15:58:14 IST
Malware Updated	Malware	10	contoso-server1dc	AI.StaticAnalysis	https://eicar.com	http://localhost:7894/id/62358927	Dec 19 2017, 15:58:14 IST
Malware Created	Malware	10	contoso-asagw2	malicious download	http://www.example.com/aunt/advice.html?breath=account&afterthought=army	http://localhost:7894/id/23032040	Dec 19 2017, 15:58:14 IST
Malware Created	Malware	10	contoso-asagw1	AI.StaticAnalysis	invoke-expression	http://localhost:7894/id/61852049	Dec 19 2017, 15:58:14 IST
Malware Created	Malware	10	contoso-etsb12	AI.StaticAnalysis	invoke-expression	http://localhost:7894/id/24476609	Dec 19 2017, 15:58:14 IST
Malware Updated	Malware	10	contoso-asagw1	malicious download	invoke-expression	http://localhost:7894/id/34563513	Dec 19 2017, 15:58:14 IST
Malware Updated	Malware	10	contoso-dc01.azurestack	download & execute	https://eicar.com	http://localhost:7894/id/35010313	Dec 19 2017, 15:58:14 IST
Malware Updated	Malware	10	contoso-server1dc	malicious command	https://eicar.com	http://localhost:7894/id/111886297	Dec 19 2017, 15:58:14 IST
Malware Created	Malware	10	contoso-rhsvr1	download & execute	https://eicar.com	http://localhost:7894/id/21565572	Dec 19 2017, 15:58:14 IST
Malware Updated	Malware	10	contoso-asagw2	malicious command	invoke-expression	http://localhost:7894/id/62844374	Dec 19 2017, 15:58:14 IST
Malware Created	Malware	10	contoso-etsb12	malicious download	http://www.example.com/aunt/advice.html?breath=account&afterthought=army	http://localhost:7894/id/49039444	Dec 19 2017, 15:58:14 IST
Malware Created	Malware	10	contoso-dc01.azurestack	malicious command	https://eicar.com	http://localhost:7894/id/40892476	Dec 19 2017, 15:58:14 IST

Figure 8

4.2 Alerts

- **Cybereason - Malop Created –** This alert is generated when new malop is created on Cybereason.
- **Cybereason - Malop Updated –** This alert is generated when an existing malop event is updated.
- **Cybereason - Malware detected –** This alert is generated when malware or suspicious threat detected by Cybereason.
- **Cybereason - Malware Updated –** This alert is generated when an existing malware state has been updated.
- **Cybereason - Threat not mitigated –** This alert is generated when malware detected and failed to mitigate.
- **Cybereason - User login failed** -This alert is generated when user login failed to log into the console event occurs.

4.3 Saved Searches

- **Cybereason - Malop events**– This saved search will help you to search malop created and updated along with machine information.
- **Cybereason - Malop investigation events** – This saved search will help you to search user action events on malop investigation.
- **Cybereason - Malware events–** This saved search will help you to search malware detected and malware state updated events.
- **Cybereason - Non-mitigated threats**– This saved search will help you to search not mitigate threat details.
- **Cybereason - Threat detected**– This saved search will help you to detected threat and its information.
- **Cybereason - User action events**– This saved search will help you to user action like configuration changes.

- **Cybereason - User failed login activities**– This saved search will help you to search user information whose login got failed.
- **Cybereason - User login and logout activities** – This saved search will help you to search user login and logout details.

4.4 Dashboards

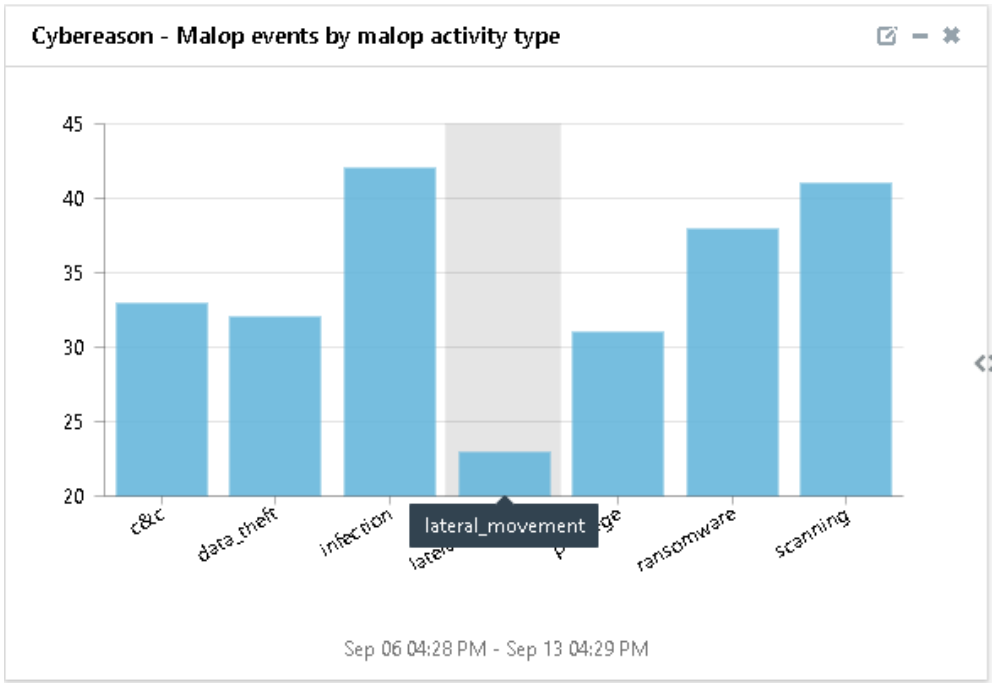

Figure 9

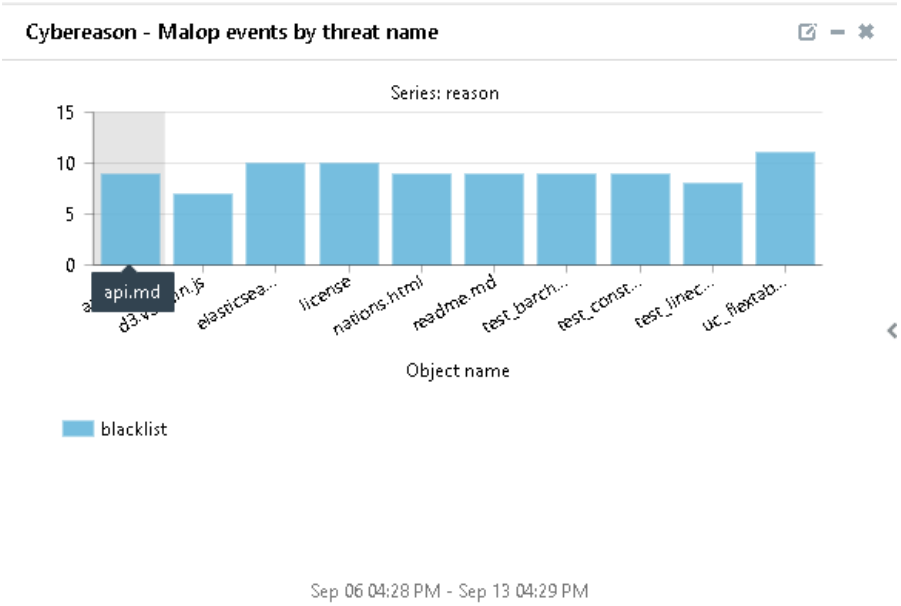

Figure 10

Cybereason - Malop events

log_type	object_name	reason	threat_category	threat_id	threat_name	threat_type	tota
Malop	iexplore			0			14
Malop	brkrprcs64			0			85
Malop	lync			0			94
Malop	SISIPSService			0			80
Malop	scheduler			0			31
Malop	System			0			22
Malop	smss			0			12
Malop	Microsoft.Photos			0			59
Malop	igfxTray			0			34
Malop	notepad			0			65

Figure 11

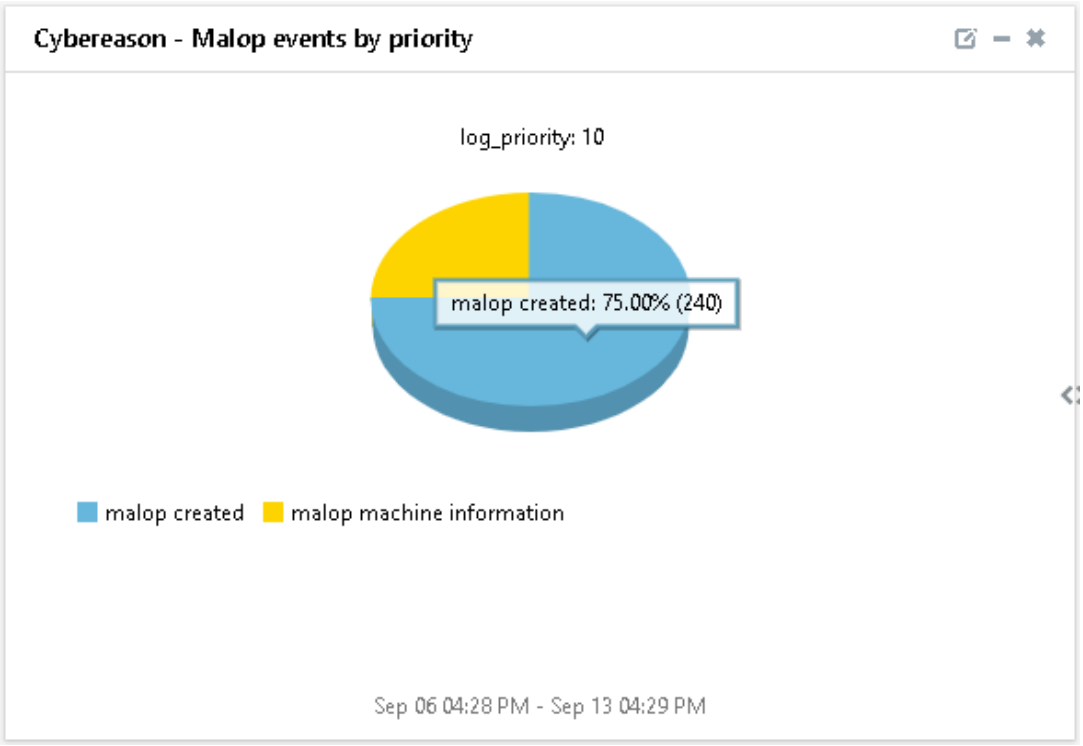

Figure 12

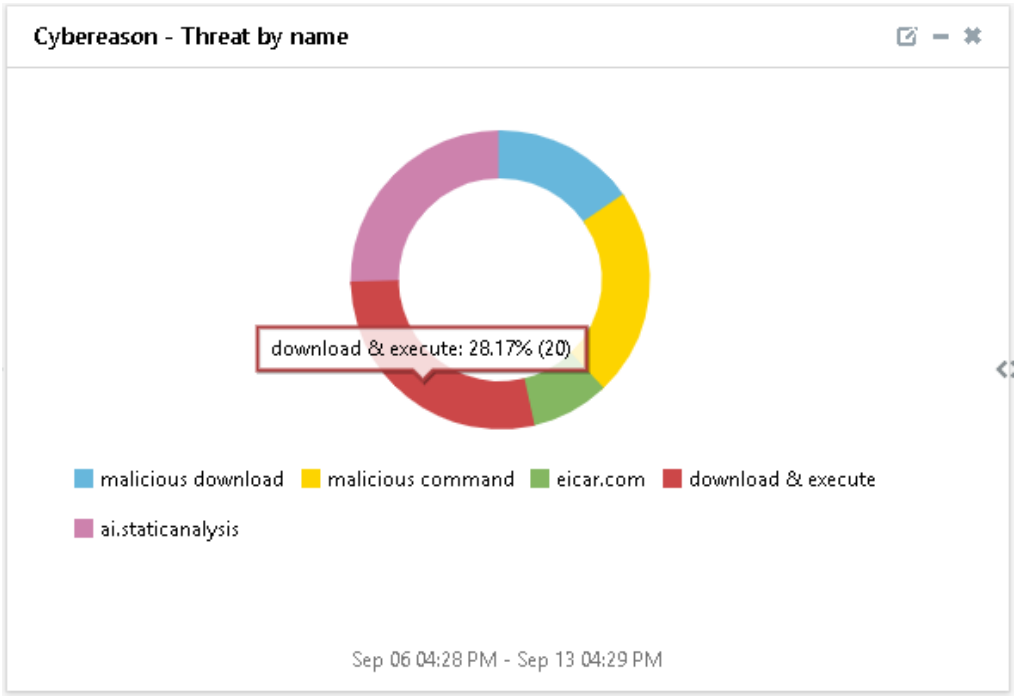

Figure 13

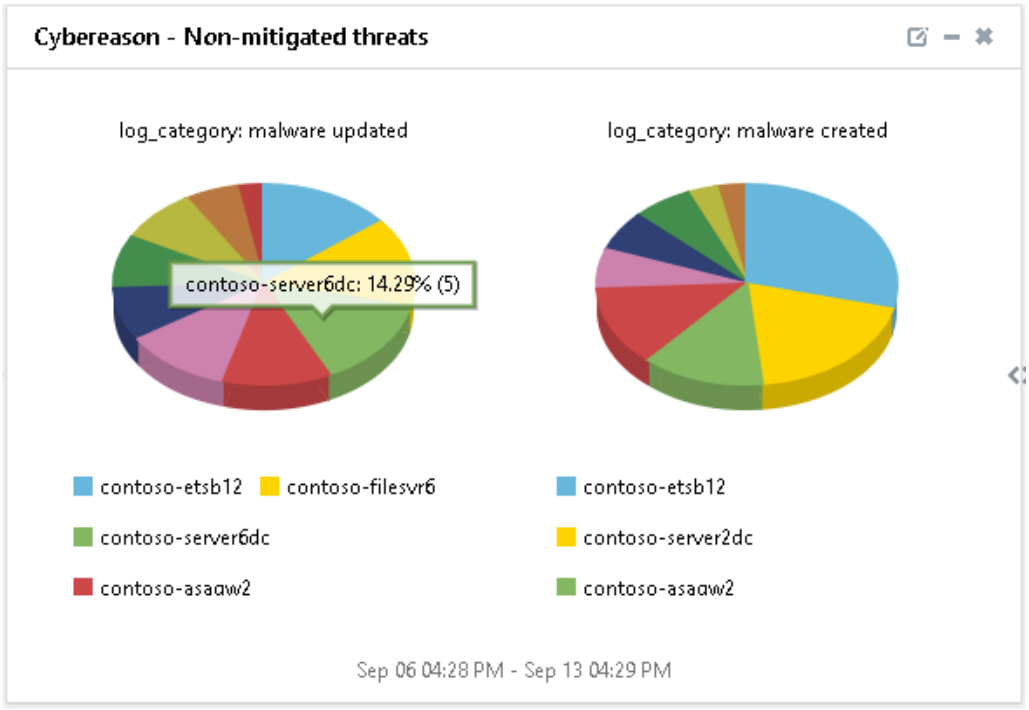

Figure 14

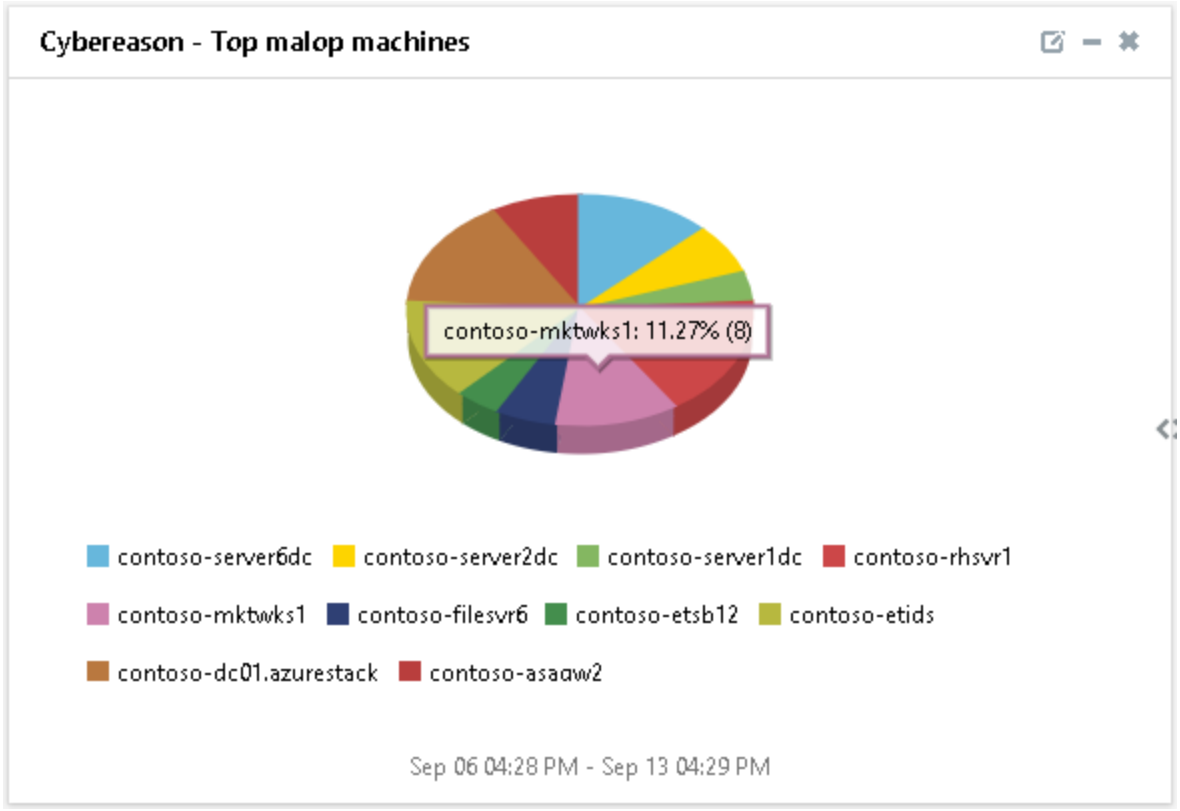

Figure 15

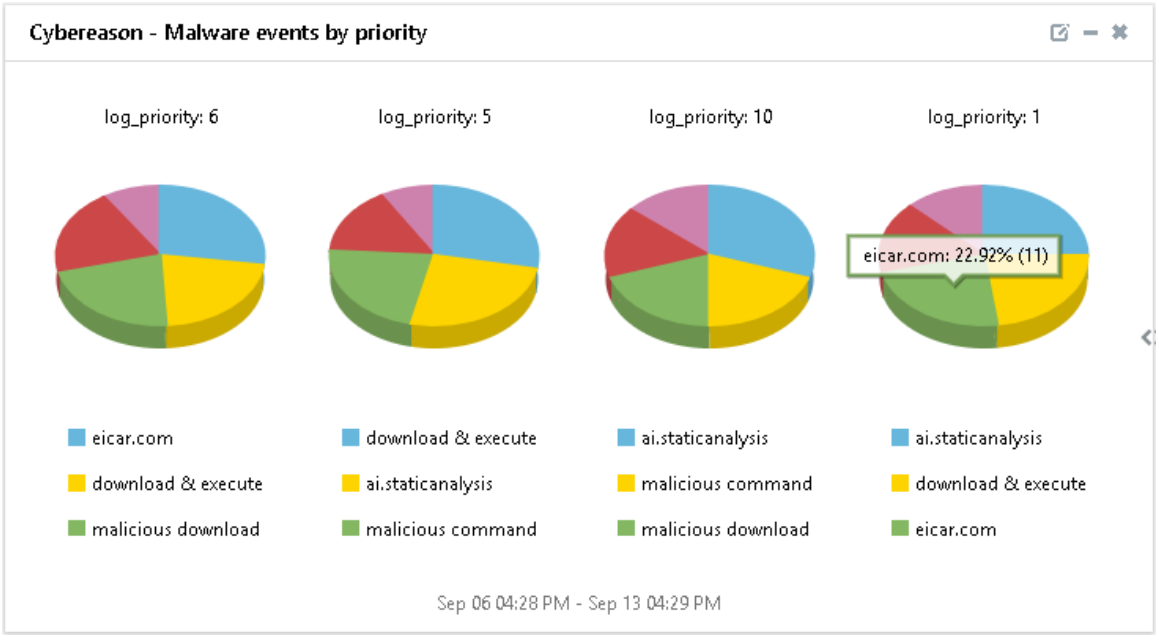

Figure 16

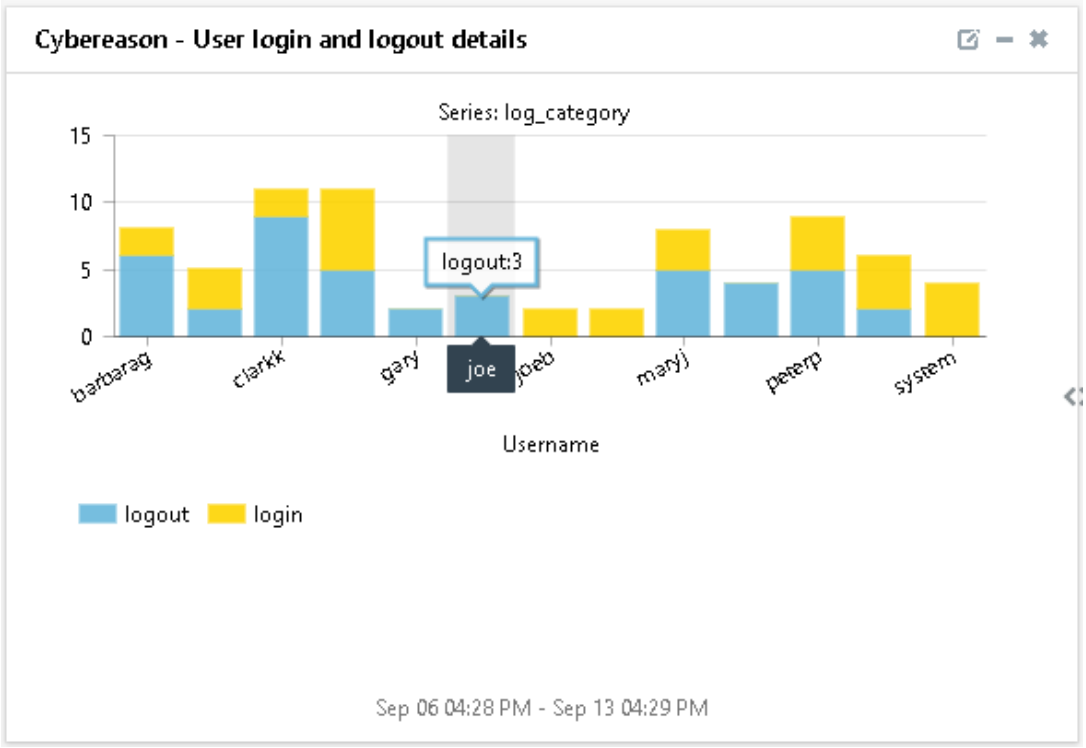

Figure 17

Figure 18

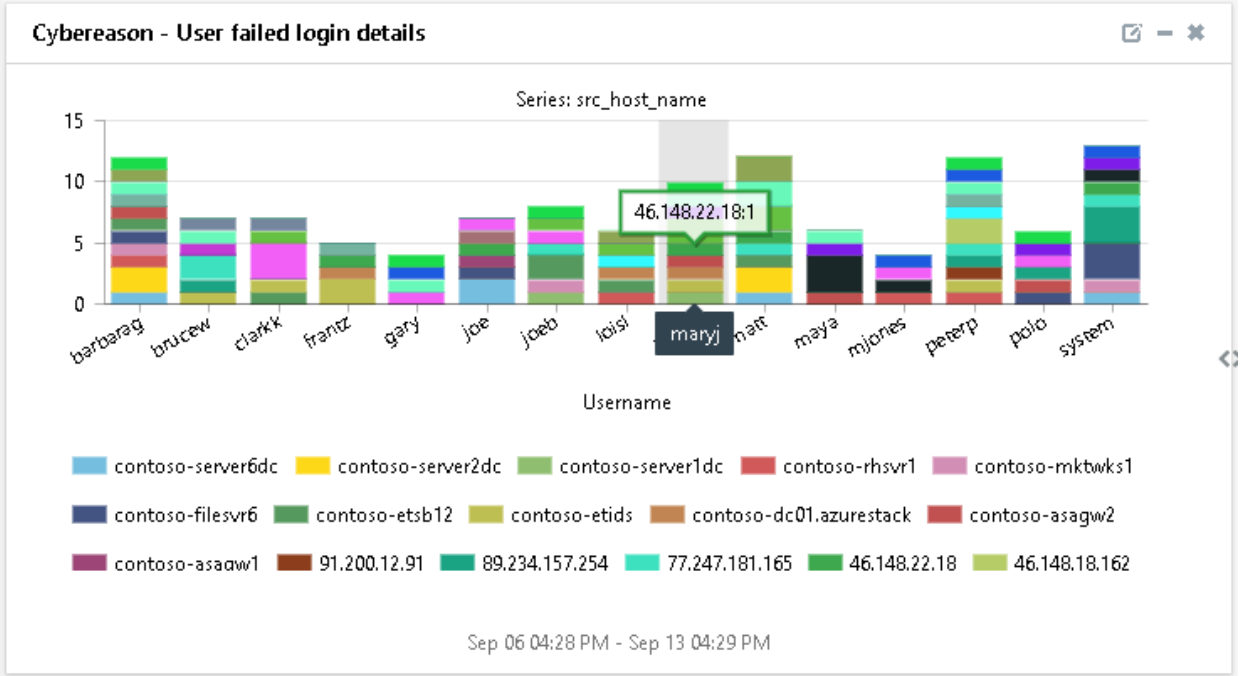

Figure 19

Figure 20

5. Importing Cybereason knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Alerts.
- Knowledge Object.
- Token templates.
- Flex Reports.
- Categories.
- Dashboard.

1. Launch the **EventTracker Control Panel**.
2. Double click **Export-Import Utility**.

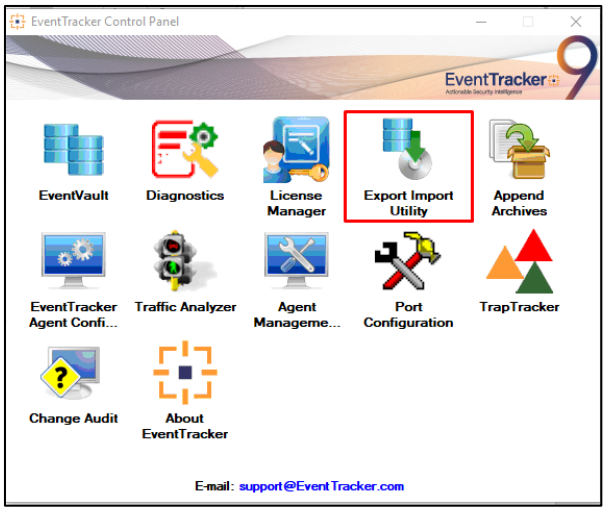

Figure 21

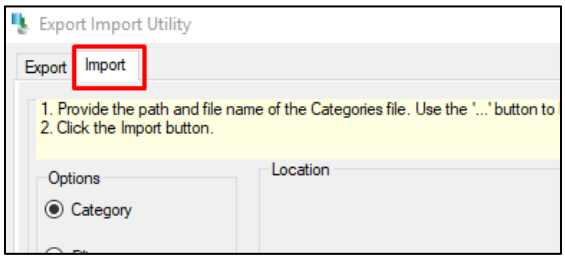

Figure 22

3. Click the **Import** tab.

5.1 Alerts

1. Click **Alert** option, and then click the browse ... button
2. Navigate to the location having a file with the extension **".isalt**" and then click on the "**Import**" button:

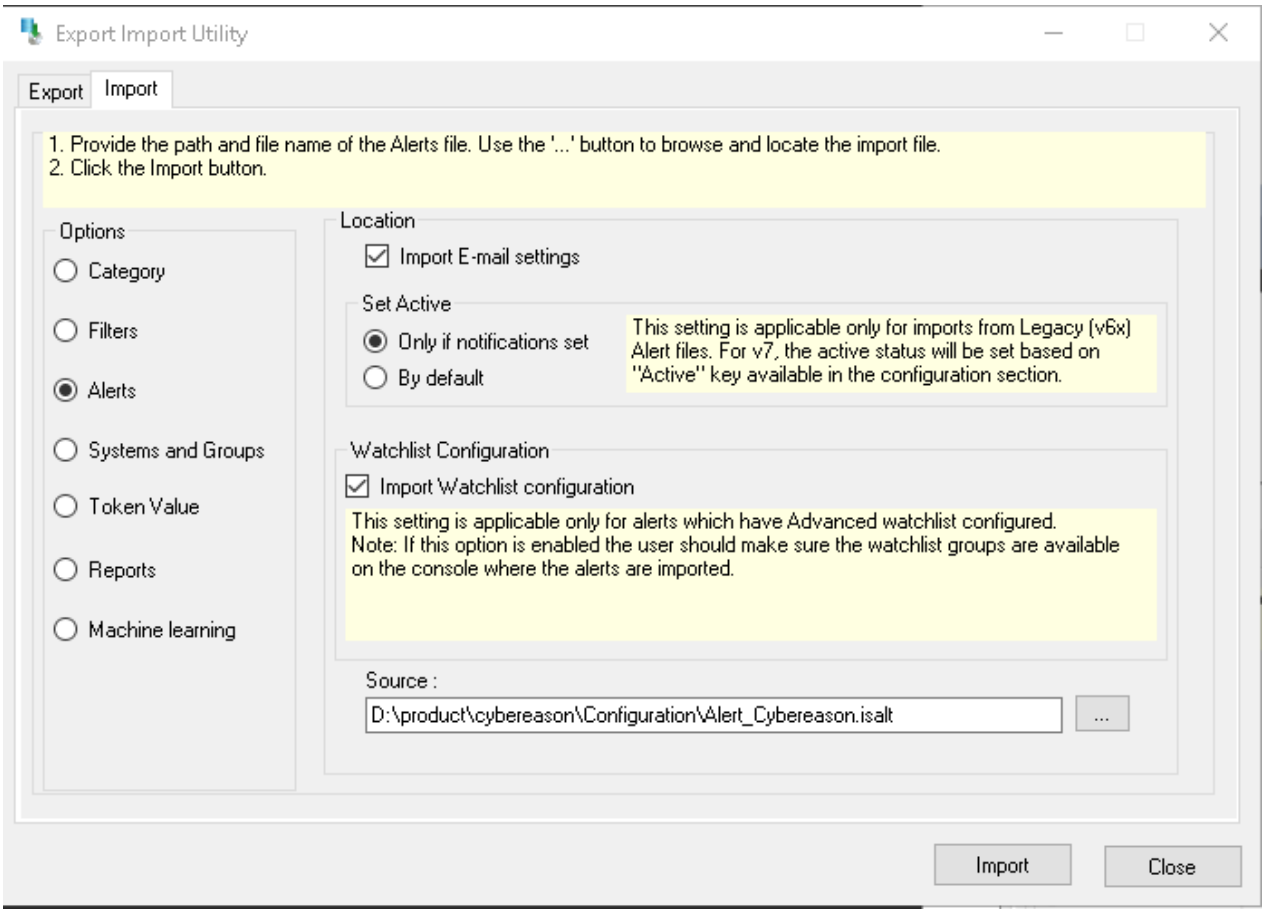

Figure 23

EventTracker displays a success message:

Figure 24

5.2 Token Template

1. Login to the **EventTracker Console**.
2. Click on **Admin >> Parsing Rules**.

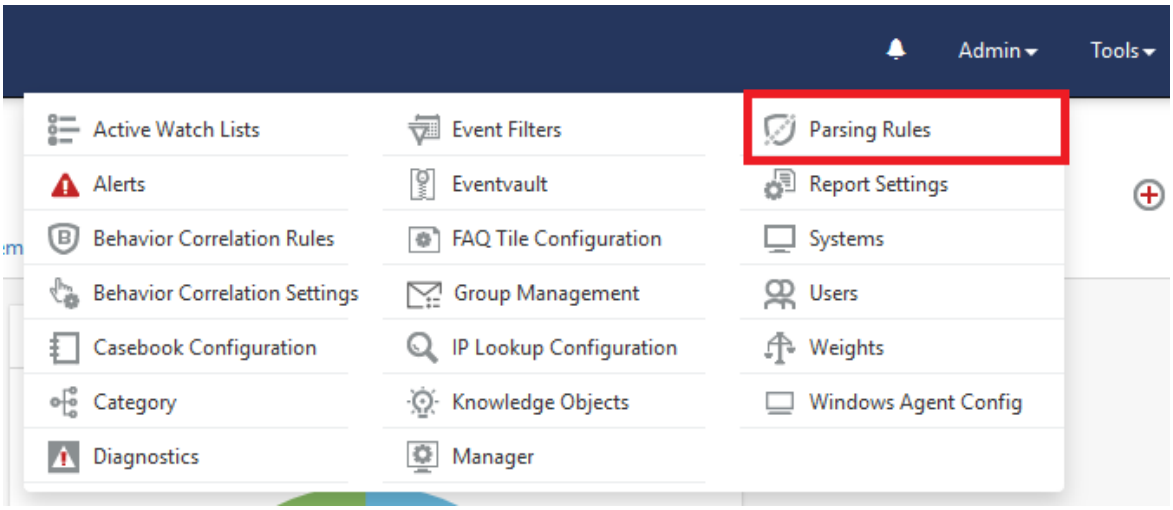

Figure 25

3. Click on **Template** and click **import configuration** Symbol.

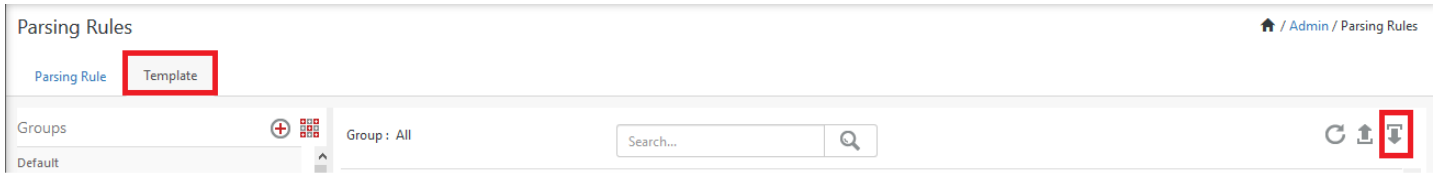

Figure 26

4. Locate the **".ettd"** file and click on **import**.

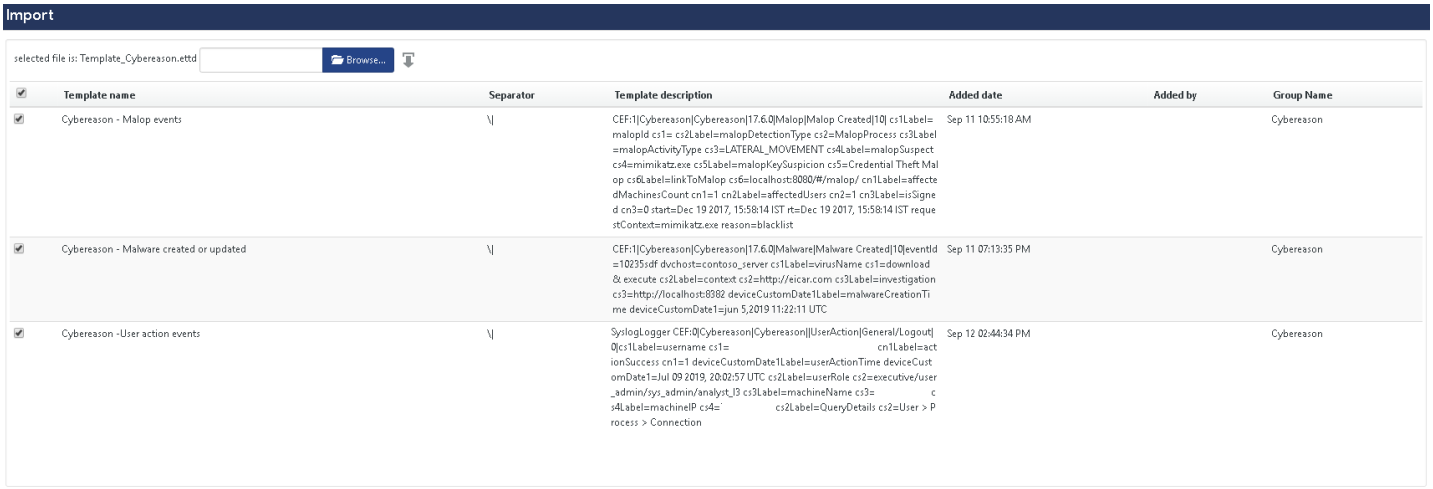

Figure 27

5. Templates are imported now successfully.

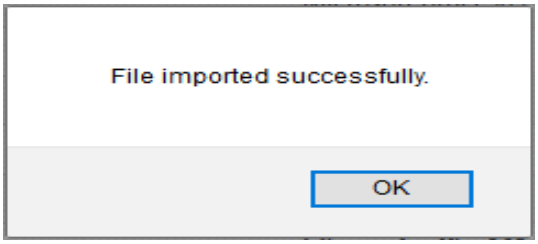

Figure 28

5.3 Knowledge Object

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

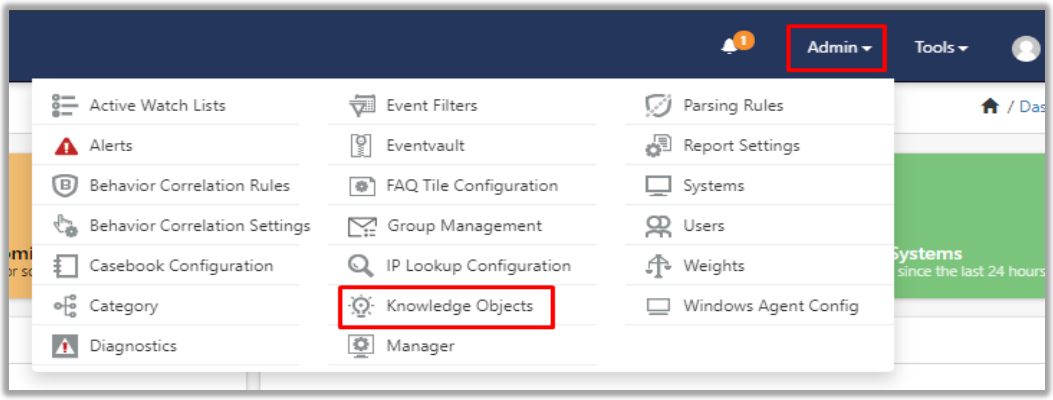

Figure 29

2. Next, click on the "import object" icon:

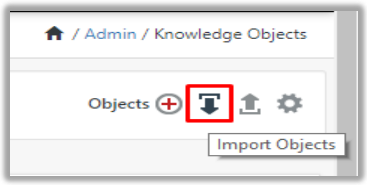

Figure 30

3. A pop-up box will appear, click "**Browse**" in that and navigate to the file path with extension **".etko"** button"

Figure 31

4. A list of available knowledge objects will appear. Select the relevant files and click on “Import” button:

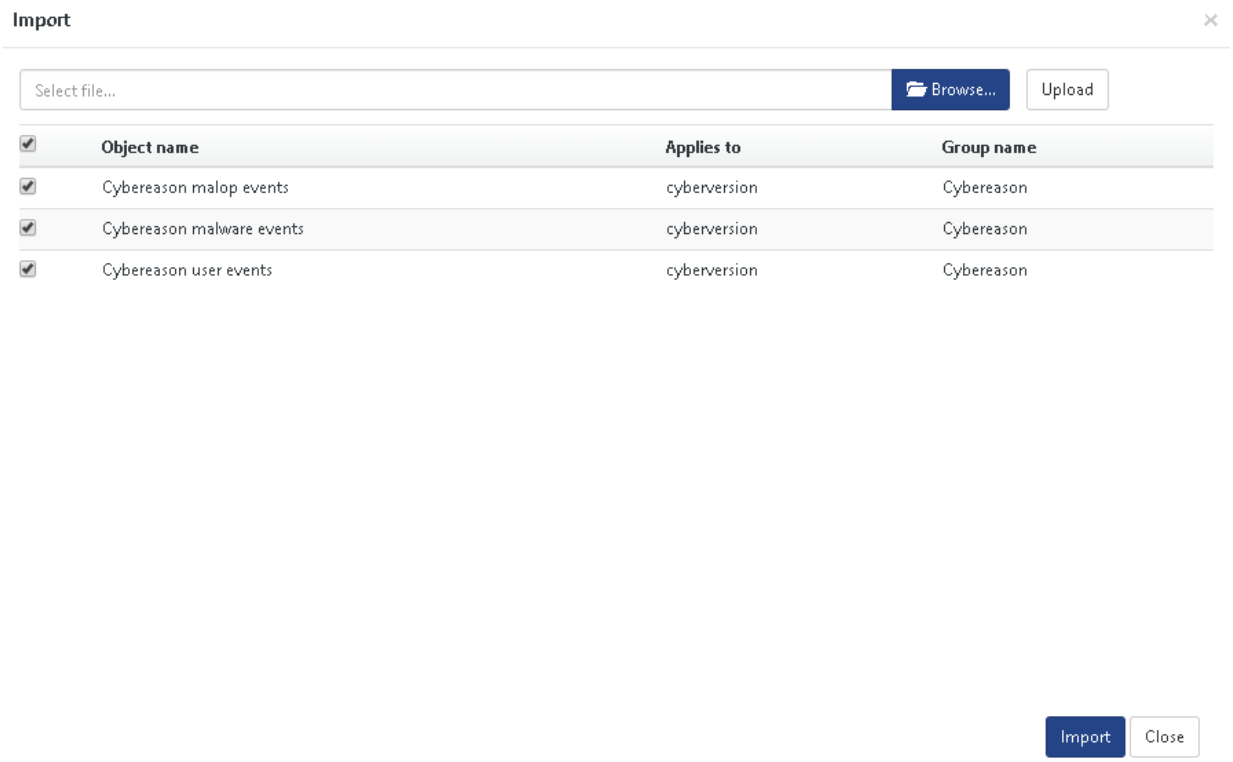

Figure 32

5.4 Flex Reports

1. In EventTracker Control Panel, select “**Export/ Import utility**” and select the “**Import tab**”. Then, click **Reports** option, and Choose “**New (*.etcrx)**”:

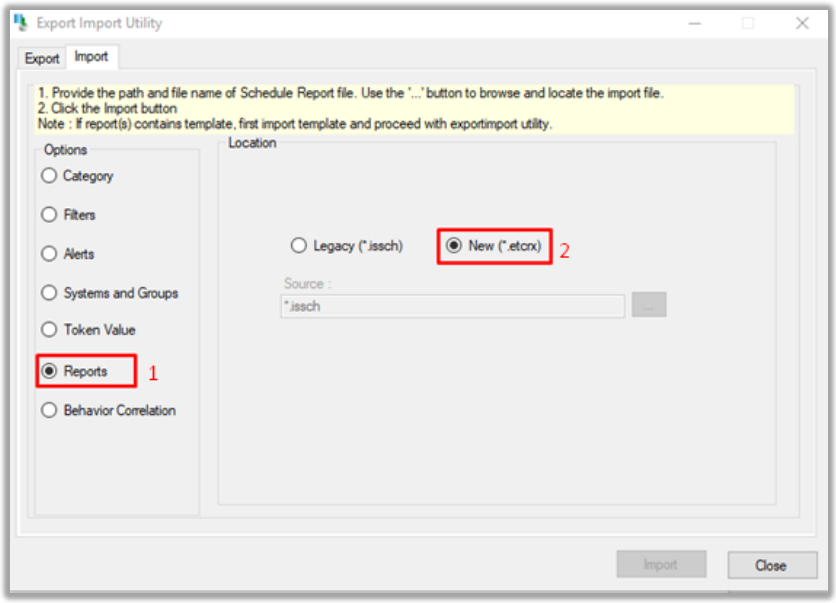

Figure 33

2. Once you have selected "**New (*.etcrx)**", a new pop-up window will appear. Click on the "**Select File**" button and navigate to the file path with a file having the extension **".etcrx**".
3. Select all the relevant files and then click on the **Import** button  .

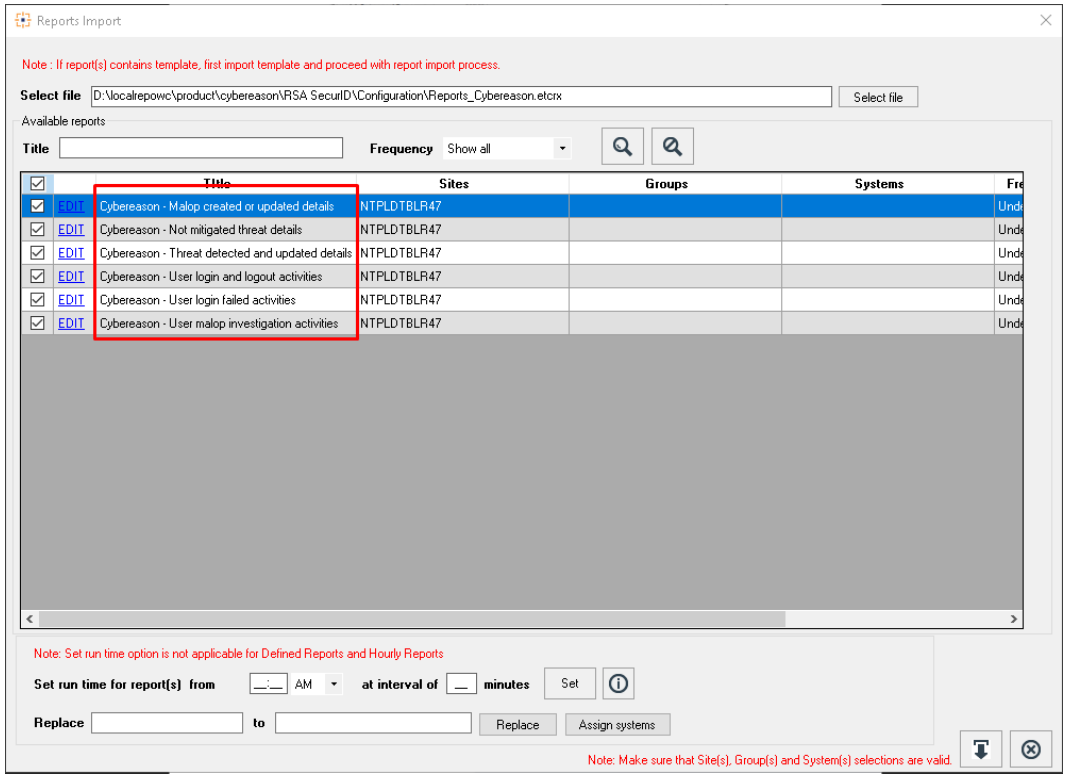

Figure 34

4. EventTracker displays a success message:

Figure 35

5.5 Category

1. Click the category option, and then click the browse ... button.

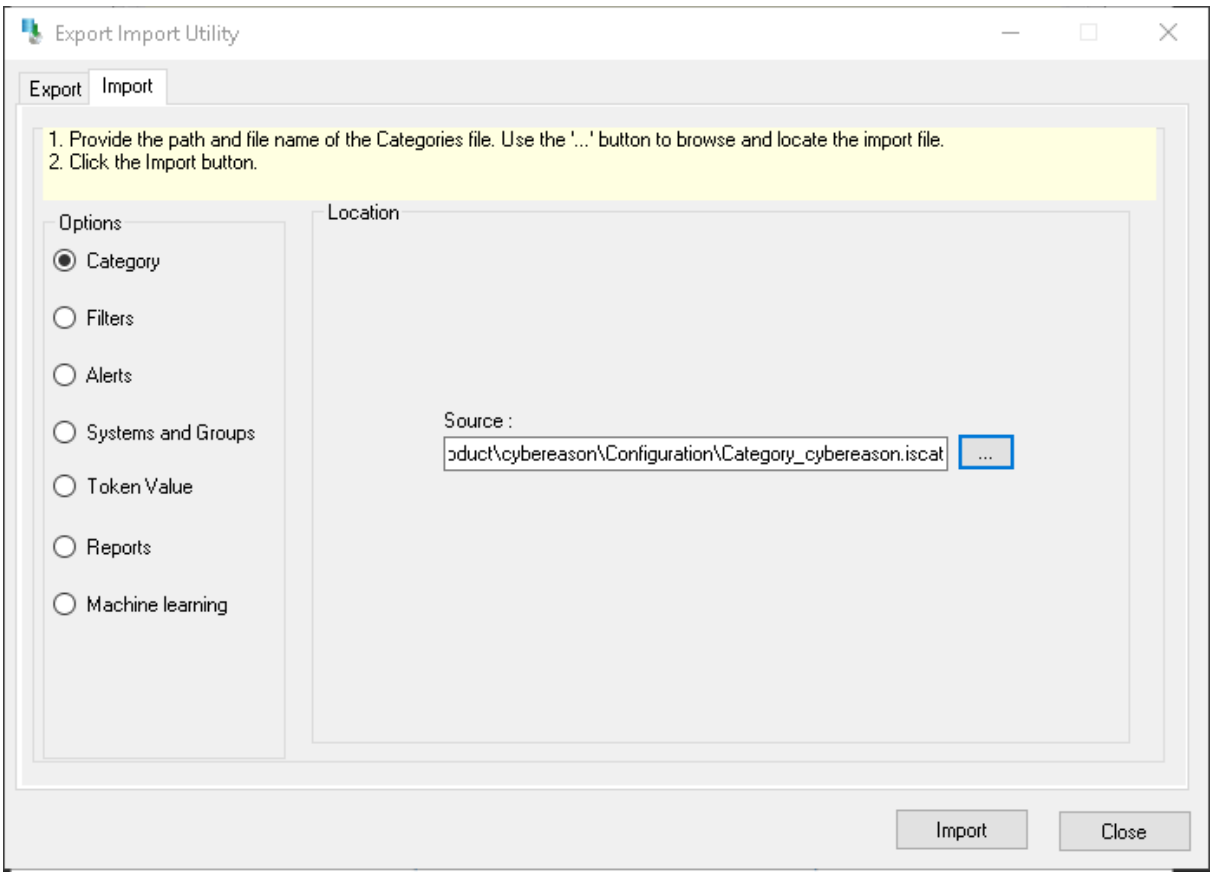

Figure 36

2. Locate the. iscat file, and then click the open button.
3. To import category, click the Import button.
4. EventTracker displays a success message.

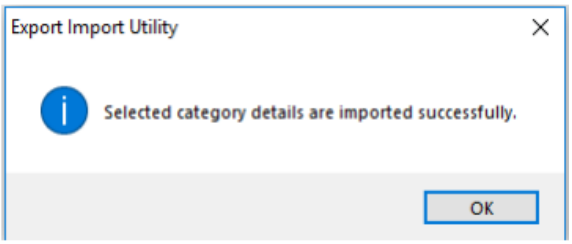

Figure 37

5. Click the OK button, and then click the Close button.

5.6 Dashboard

1. Login to **EventTracker**.
2. Navigate to **Dashboard → My Dashboard**.
3. In "My Dashboard", Click **Import Button**:

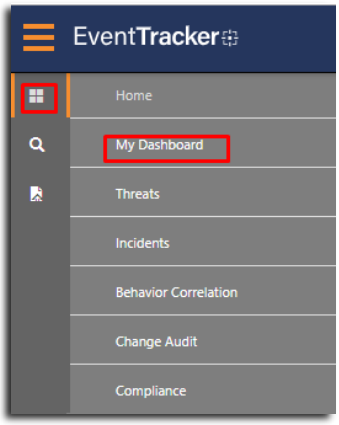

Figure 38

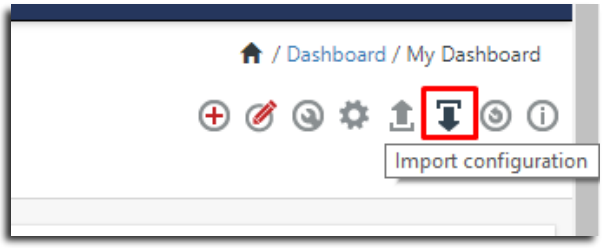

Figure 39

4. Select the **browse** button and navigate to the file path where the Dashboard file is saved and click on the "**Upload**" button.
5. Once completed, choose "**Select All**" and click on **"Import"** Button.
6. Next, Click "**Customize dashlet**" button as shown below:

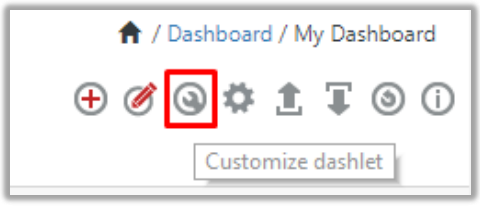

Figure 40

7. Now, put a text on the **Search bar: "Cybereason"** and then select the Cybereason Dash-lets and then click **"Add"** button.

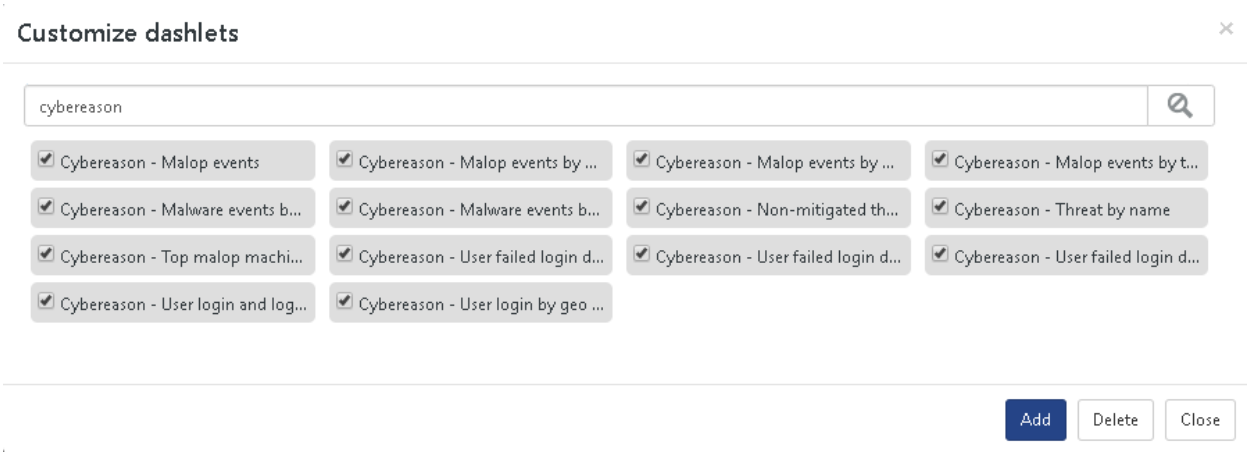

Figure 41

6. Verifying Cybereason knowledge pack in EventTracker

6.1 Alerts

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Alerts.**
2. In search box enter "**Cybereason"** and then click the **Search** button.

EventTracker displays an alert related to "**Cybereason**":

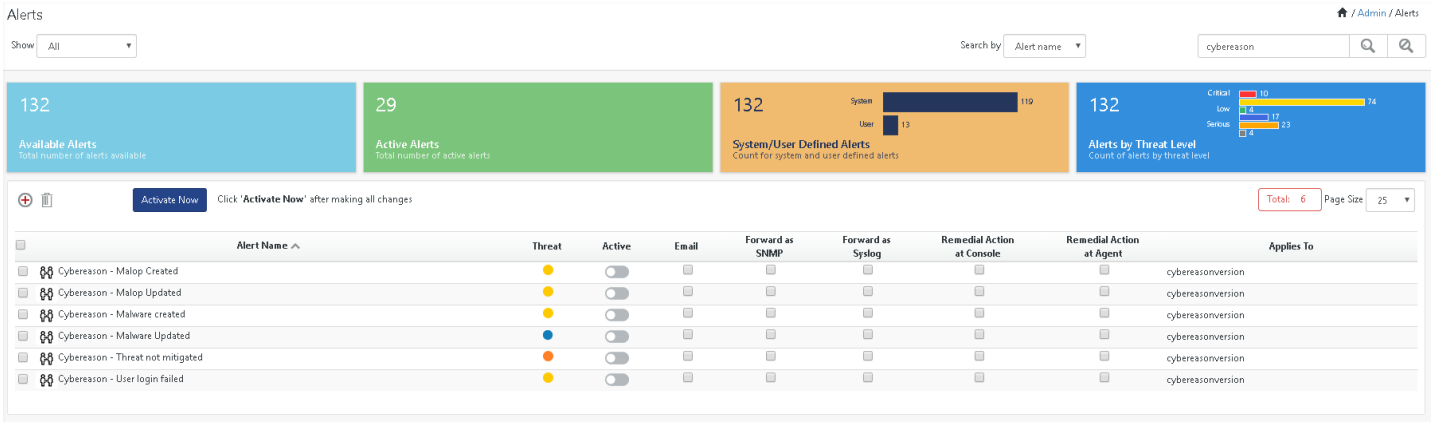

Figure 42

6.2 Token Template

1. Login to the **EventTracker.**
2. Click on **Admin >> Parsing Rules**.

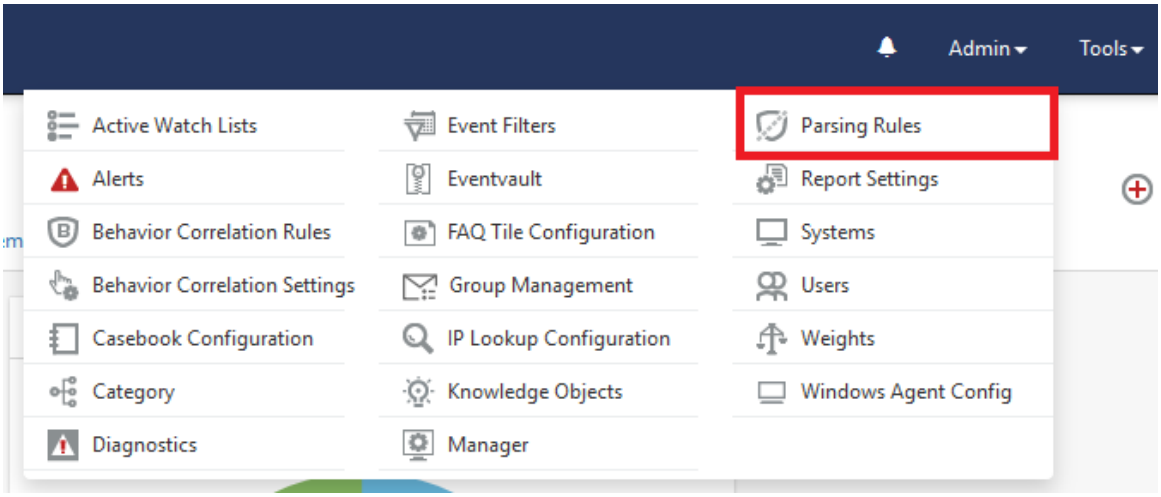

Figure 43

3. Click on **Template** and search for **Cybereason.**

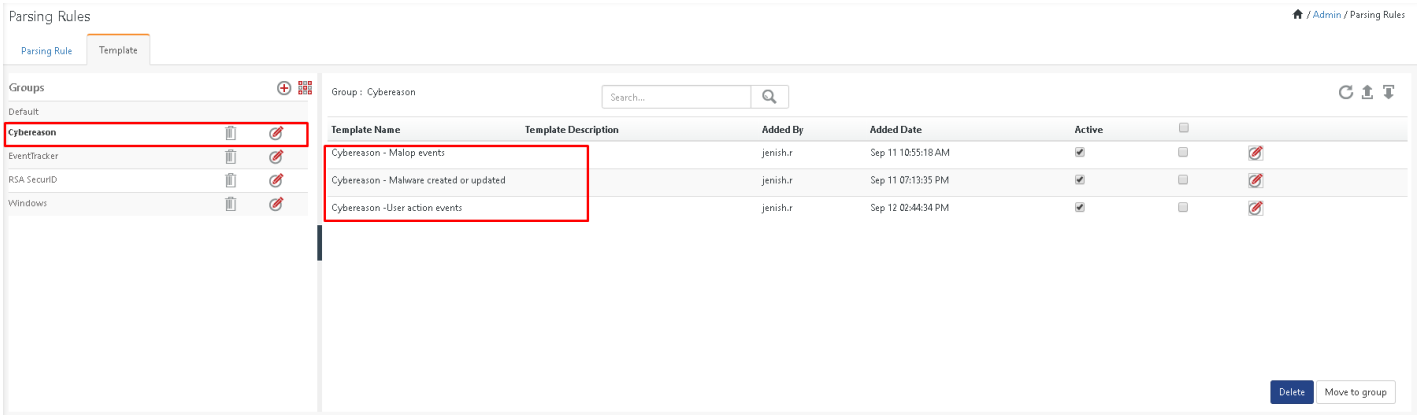

Figure 44

6.3 Knowledge Object

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

In the **Knowledge Object** tree, expand the **"Cybereason"** group folder to view the imported Knowledge objects.

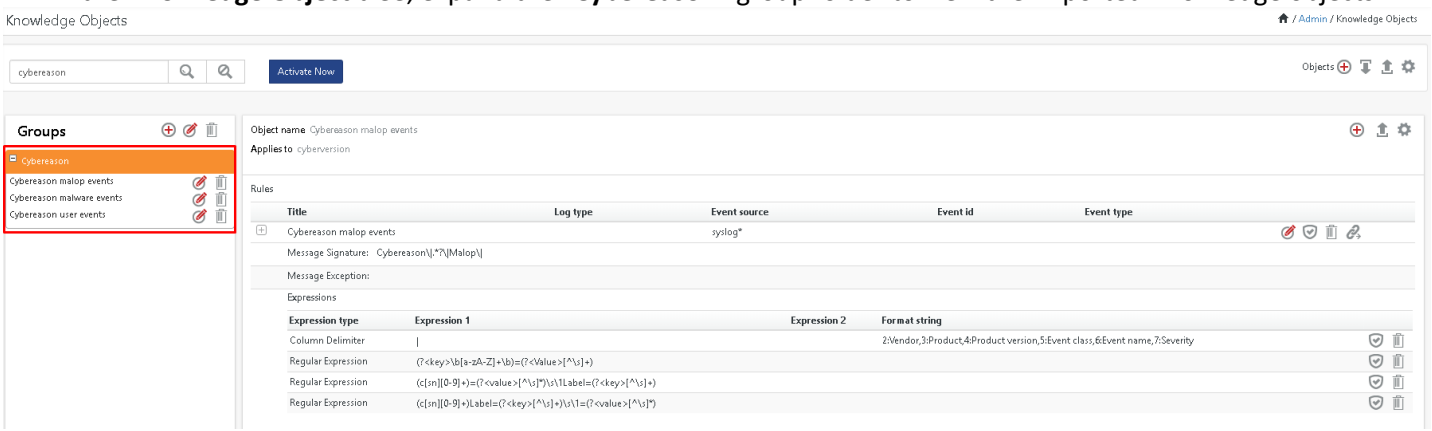

Figure 45

6.4 Flex Reports

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

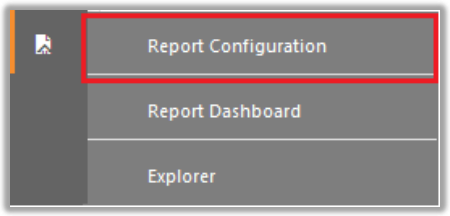

Figure 46

2. In **Reports Configuration** pane, select the **Defined** option.

3. Click on the **Cybereason** group folder to view the imported reports.

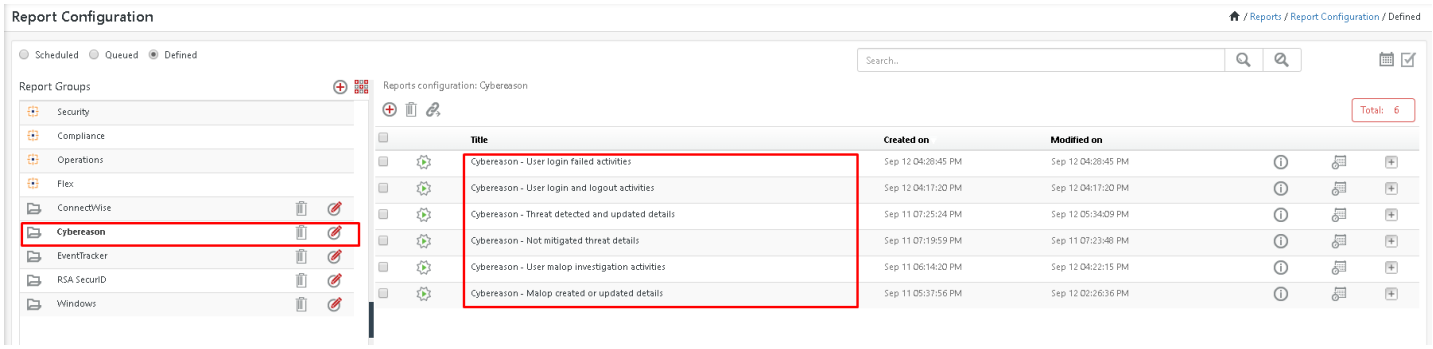

Figure 47

6.5 Category

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

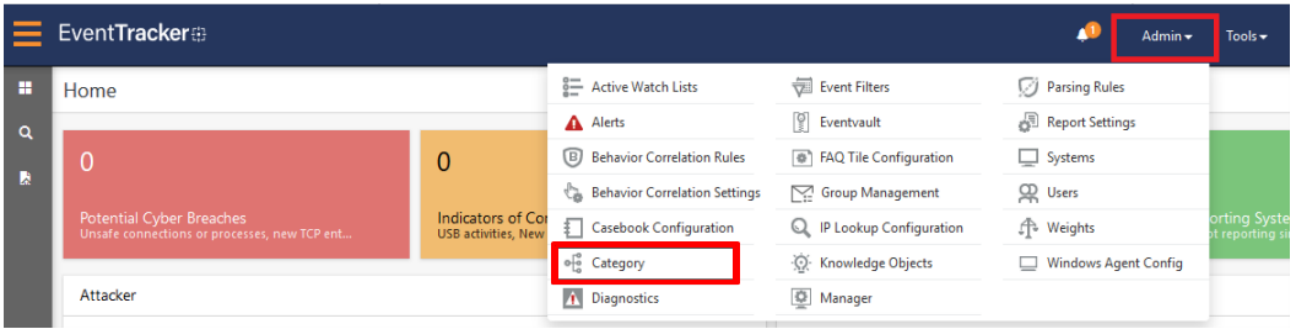

Figure 48

3. Click the search, and then search with Cybereason.

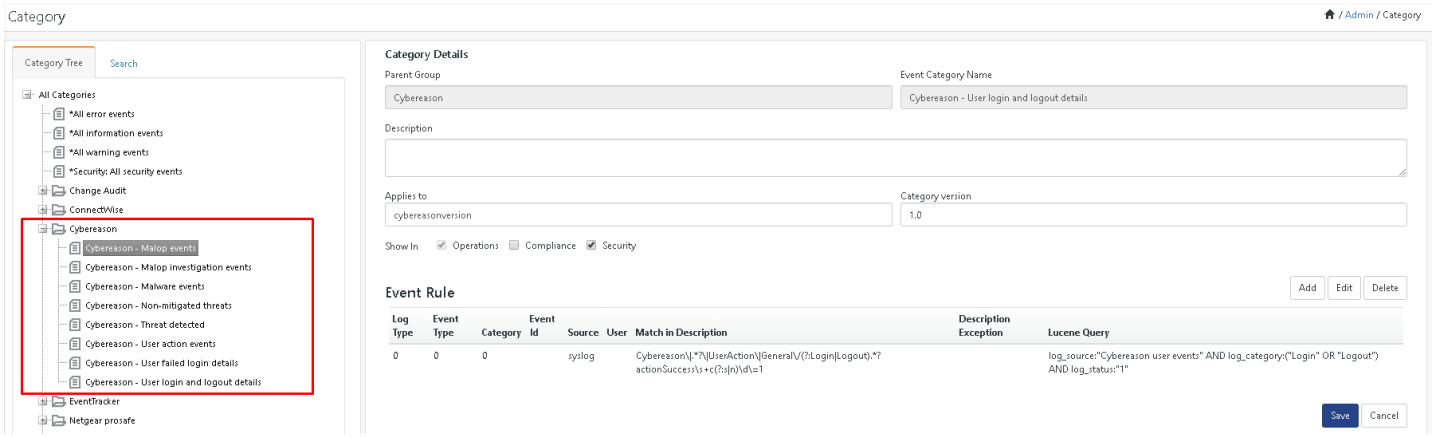

Figure 49