EventTracker

Actionable Security Intelligence

Integrate CylancePROTECT

EventTracker v8.x and above

Publication Date: May 10, 2018

Abstract

This guide provides instructions to configure CylancePROTECT to generate logs for critical events. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor CylancePROTECT.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version v8.x or above and CylancePROTECT.

Audience

Administrators who are assigned the task to monitor CylancePROTECT events using EventTracker.

Table of Contents

Overview

CylancePROTECT is an integrated threat prevention solution that combines the power of artificial intelligence (AI) to block malware infections with additional security controls that safeguard against script-based, file less, memory, and external device based attacks.

With EventTracker, you can monitor CylancePROTECT events from a single view. EventTracker can generate flex reports; trigger alerts for user logon activity, configuration changes, device activity, exploitation attempt and threat detection.

Prerequisites

- EventTracker agent should be installed.
- CylancePROTECT should be configured for forwarding logs.
- Please make sure the exception for port 514 in firewall of EventTracker Manager system.

Configure CylancePROTECT to forward logs to EventTracker

To configure the CylancePROTECT to forward logs to a syslog server,

1. **Log in** to the CylancePROTECT Console.
2. Select **Settings > Application**.
3. When the page loads, scroll down to the **INTEGRATIONS** section of the page.

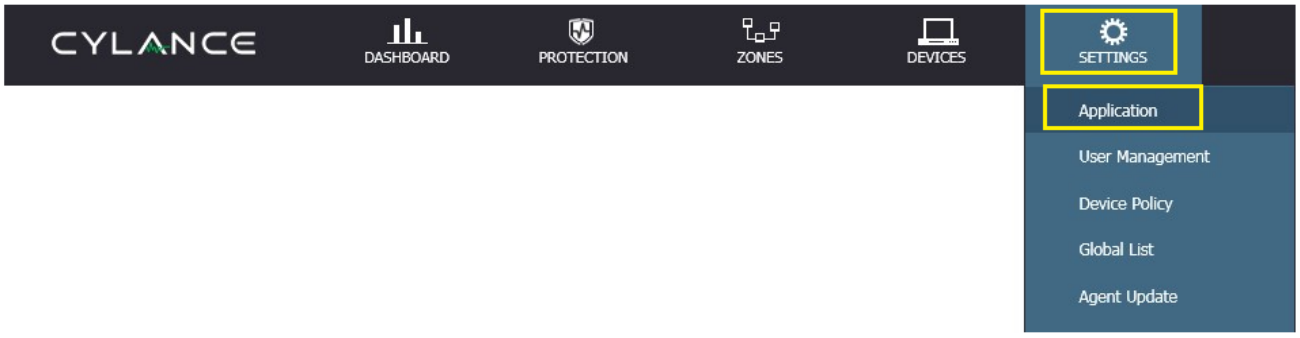

Figure 1

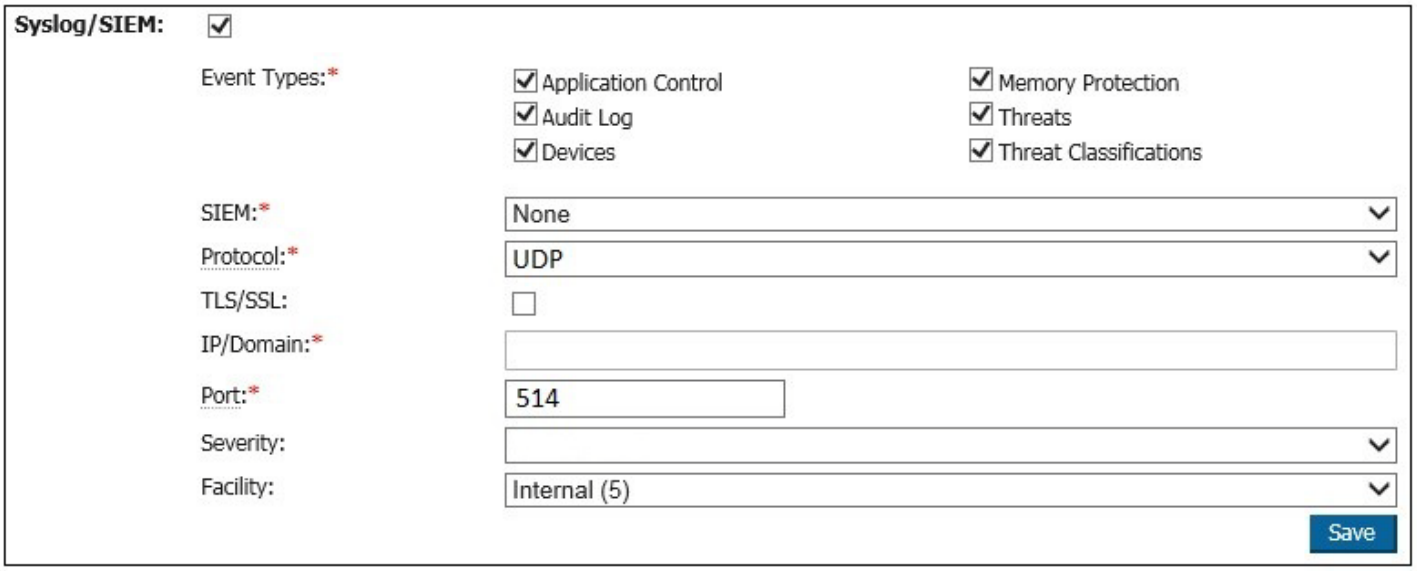

Figure 2

4. Please check the '**Syslog/SIEM'** box.
5. Under **Event Types**, select **all** available events.
6. **SIEM:** Select appropriate option.
7. **Protocol**: Select **UDP**.
8. **TLS/SSL:** Leave the box empty.
9. **IP/Domain:** Enter the IP address of the **EventTracker Manager**.
10. **Port:** Enter **514**.
11. **Severity:** Select Information option.
12. **Facility:** Select **Internal (5).**
13. Click **Save**.

NOTE: If you want to use '**TLS/SSL**' connection with protocol as **'TCP'**, additional configuration will be needed.

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 Enterprise to support CylancePROTECT.

Flex Reports

- **Cylance - Configuration changes -** This report gives the information about device configuration changes done by users.

LogTime	Computer	Event Name	User Name	Activity
05/02/2018 12:38:04 PM	NTPLDTBLR42\CYLANCE	DeviceEdit	Mara Lee (Maralee@nmkehspace.com)	Device: TSD222C; Policy Changed: "Default" to "5 Complete Protection"; Zones Added: "Everett Merril Creek"
05/02/2018 12:38:04 PM	NTPLDTBLR42\CYLANCE	DeviceRemove	Mara Lee (Maralee@nmkehspace.com)	Devices: TSD222C
05/02/2018 12:38:09 PM	NTPLDTBLR42\CYLANCE	ZoneAddDevice		The Device: LT0002229 was auto assigned to the Zone: Washington

Figure 3

Sample logs:

Time	Description
− May 07 11:11:46 AM	Apr 24 09:52:08 ETPVMDFHLMI01 Apr 24 09:52:08 **50.23.12.101** 192 <46>1 2018-04-24T14:52:08.6420000Z sysloghost CylancePROTECT - - - Event Type: A...
event_log_type	+ - Application
event_type	+ - Information
event_id	+ - 3333
event_source	+ - Syslog
event_user_domain	+ - N/A
event_computer	+ - Cylance
event_user_name	+ - N/A
event_description	Apr 24 09:52:08 ETPVMDFHLMI01 Apr 24 09:52:08 **50.23.12.101** 192 <46>1 2018-04-24T14:52:08.6420000Z sysloghost CylancePROTECT - - - Event Type: AuditLog, Event Name: ZoneAddDevice, Message: The Device: LT0002145 was auto assigned to the Zone: Cuba, User:

Figure 4

- **Cylance - Threat detection -** This report gives the information about all the threats detected by CylancePROTECT.

LogTime	Computer	Event Name	Threat Type	Threat Score	Action	Device Name	Source IP Address	File Type	File Name	File Path	MD5 Hash	Auto Run	Detected By	Is Malware	Is Running	Source Zone
05/02/2018 12:37:51 PM	NTPLDTBLR42\CYLANCE	threat[_]quarantined	PUP	57	Quarantined	TSD222C	11.10.23.125	Executable	3DVIASFX.Exe	C:\Windows.old\Program Files\Dassault Systemes\3DVIAComposer\6.11\Bin\x86\	5C586958AAC2710E4AD70C355A76F892	False	BackgroundThreatDetection	False	False	Everett Merril Creek
05/02/2018 12:37:56 PM	NTPLDTBLR42\CYLANCE	threat[_]quarantined	PUP	2	Quarantined	TSD222C	11.10.23.125	Executable	CSH[_]API.DLL		384538415DE959E971B859E83BC0B824	False	BackgroundThreatDetection	False	False	Everett Merril Creek

Figure 5

Sample logs:

Time	Description
− May 07 11:11:05 AM	Apr 24 17:41:09 ETPVMDFHLMI01 Apr 24 17:41:09 **65.23.01.23 650** <46>1 2018-04-24T22:41:08.1150000Z sysloghost CylancePROTECT - - - Event Type: T..
event_log_type	+ - Application
event_type	+ - Information
event_id	+ - 3333
event_source	+ - Syslog
event_user_domain	+ - N/A
event_computer	+ - Cylance
event_user_name	+ - N/A
event_description	Apr 24 17:41:09 ETPVMDFHLMI01 Apr 24 17:41:09**65.23.01.23 650**<46>1 2018-04-24T22:41:08.1150000Z sysloghost CylancePROTECT - - - Event Type: Threat, Event Name: threat[_]quarantined, Device Name: TSD222C, IP Address:**(11.10.23.12)**,File Name: CSH[_]API.DLL, Path: C:\Program Files (x86)\Adobe\FrameMaker9\, Drive Type: Internal Hard Drive, SHA256: 356BEF7676ADC7A71B8628B8725AA16EEE8DF7F1BF6D930C14154C20A20AA159, MD5: 384538415DE959E971B859E83BC0B824, Status: Quarantined, Cylance Score: 2, Found Date: 4/24/2018 10:41:08 PM, File Type: Executable, Is Running: False, Auto Run: False, Detected By: BackgroundThreatDetection, Zone Names: (Everett Merril Creek), Is Malware: False, Is Unique To Cylance: True, Threat Classification: PUP

Figure 6

- **Cylance - Exploitation attempt -** This report gives information about memory exploitations detected by CylancePROTECT.

LogTime	Computer	Event Name	Exploit Name	Action	Device Name	User Name	Source IP Address	Process Name	Source Zone
05/02/2018 12:38:07 PM	NTPLDTBLR42\CYLANCE	blocked	Remote Unmap of Memory	Blocked	LT0002151	tgeiler	10.12.22.112	C:\Windows\system32\werfault.exe	Fountain Lakes
05/02/2018 12:38:35 PM	NTPLDTBLR42\CYLANCE	blocked	Remote Unmap of Memory	Blocked	LT0002190	DWM-12	10.12.22.112	C:\Windows\system32\WerFault.exe	Fountain Lakes

Figure 7

Sample logs:

Time	Description
− May 07 11:11:40 AM	Apr 24 10:32:53 ETPVMDFHLMI01 Apr 24 10:32:53**54.23.1.128 345**<46>1 2018-04-24T15:32:53.6310000Z sysloghost CylancePROTECT - - - Event Type: Ex...

event_log_type	+- Application
event_type	+- Information
event_id	+- 3333
event_source	+- Syslog
event_user_domain	+- N/A
event_computer	+- Cylance
event_user_name	+- N/A
event_description	Apr 24 10:32:53 ETPVMDFHLMI01 Apr 24 10:32:53**54.23.1.128 345**<46>1 2018-04-24T15:32:53.6310000Z sysloghost CylancePROTECT - - - Event Type: ExploitAttempt, Event Name: blocked, Device Name: LT0002190, IP Address:(10.12.22.112),Action:Blocked, Process ID: 860, Process Name: C:\Windows\system32\WerFault.exe, User Name: DWM-12, Violation Type: Remote Unmap of Memory, Zone Names: (Fountain Lakes)

Figure 8

- **Cylance - Script execution -** This report gives information about scripts executed by the users.

LogTime	Computer	Event Name	Device Name	User Name	Script Type	File Path	Source Zone
05/02/2018 12:37:01 PM	NTPLDTBLR42\CYLANCE	Blocked	CHI1ADMIN06	SYSTEM	Powershell	[[]*COMMAND*] & C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modules\SmbShare\DisableUnusedSmb1.ps1 -Scenario Client	Managed Computers
05/02/2018 12:37:02 PM	NTPLDTBLR42\CYLANCE	Blocked	CHI1ADMIN05	SYSTEM	Powershell	[[]*COMMAND*] & C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modules\SmbShare\DisableUnusedSmb1.ps1 -Scenario Client	Managed Computers
05/02/2018 12:37:02 PM	NTPLDTBLR42\CYLANCE	Blocked	LT160028	jgeels	ActiveScript	c:\users\jgeels\appdata oaming\microsoft\windows\start menu\programs\startup\maphomedrive.vbs	Tulsa

Figure 9

Sample logs:

Time	Description
− May 07 11:11:50 AM	Apr 24 09:16:47 ETPVMDFHLMI01 Apr 24 09:16:47 **50.23.126.32** 320 <46>1 2018-04-24T14:16:47.1620000Z sysloghost CylancePROTECT - - - Event Type: Sc...

event_log_type	+- Application
event_type	+- Information
event_id	+- 3333
event_source	+- Syslog
event_user_domain	+- N/A
event_computer	+- Cylance
event_user_name	+- N/A
event_description	Apr 24 09:16:47 ETPVMDFHLMI01 Apr 24 09:16:47 **50.23.126.32** 320 <46>1 2018-04-24T14:16:47.1620000Z sysloghost CylancePROTECT - - - Event Type: ScriptControl, Event Name: Alert, Device Name: DT0001329, File Path: c:\program files (x86)\microsoft office\office16\ospp.vbs, Interpreter: ActiveScript, Interpreter Version: 5.812.10586.0, Zone Names: (Washington), User Name: jordanaubin

Figure 10

- **Cylance - Device activities -** This report gives information about device activity in agent systems.

LogTime	Computer	Event Name	Device Name	Device OS	Agent Version	User Name	Source IP Address	Source MAC Address	Source Zone
05/02/2018 11:32:09 AM	NTPLDTBLR42 \CYLANCE	SystemSecurity	SUR0001201	Microsoft Windows 10 Pro x64 10.0.16299	2.0.1470.17	NMKEHSPACE\ bbues	11.23.25.125 NMKEHSPACE	0025:96FF:FE12:3456	Vista
05/02/2018 11:32:09 AM	NTPLDTBLR42 \CYLANCE	SystemSecurity	61LEAD8	Microsoft Windows 7 Professional Service Pack 1 x64 6.1.7601	2.0.1470.17	NMKEHSPACE\ ssaller	11.23.25.100	7856:45JK:GH45:4579	Tulsa
05/02/2018 11:32:09 AM	NTPLDTBLR42 \CYLANCE	SystemSecurity	LT0001344	Microsoft Windows 10 Pro x64 10.0.15063	2.0.1470.17	NMKEHSPACE\ Lee	11.23.25.101	2525:89KF:JE59:5451	Tulsa
05/02/2018 11:32:09 AM	NTPLDTBLR42 \CYLANCE	SystemSecurity	LT0000226	Microsoft Windows 7 Professional Service Pack 1 x64 6.1.7601	2.0.1470.17	NMKEHSPACE\ Rjaz	11.23.25.98	6515:56BV:LE89:5674	Fountain Lakes
05/02/2018 11:32:09 AM	NTPLDTBLR42 \CYLANCE	SystemSecurity	LT0000943	Microsoft Windows 7 Professional Service Pack 1 x64 6.1.7601	2.0.1470.17	NMKEHSPACE\ Althen	11.23.25.124, 11.23.25.129	22NN:85EE:MD45:0987, 9825:OJ67:NM56:0012	Washington

Figure 11

Sample logs:

Time	Description
− May 08 10:59:17 AM	Apr 24 09:17:25 ETPVMDFHLMI01 Apr 24 09:17:25 65.23.12.125 333 <46>1 2018-04-24T14:17:25.6780000Z sysloghost CylancePROTECT - - - Event Type: D...
event_log_type	+- Application
event_type	+- Information
event_id	+- 3333
event_source	+- Syslog
event_user_domain	+- N/A
event_computer	+- Cylance
event_user_name	+- N/A
event_description	Apr 24 09:17:25 ETPVMDFHLMI01 Apr 24 09:17:25 65.23.12.125 333 <46>1 2018-04-24T14:17:25.6780000Z sysloghost CylancePROTECT - - - Event Type: Device, Event Name: SystemSecurity, Device Name: LT0001685, Agent Version: 2.0.1470.17, IP Address: (11.23.159.3), MAC Address: 0025:96FF:FE12:3456,Logged On Users: (NMKEHSPACE\Ejusseller), OS: Microsoft Windows 10 Pro x64 10.0.10586, Zone Names: (Mexicali)

Figure 12

- **Cylance - User logon -** This report gives information about successful user logon.

LogTime	Computer	Event Name	Source IP Address	User Name	Activity
05/02/2018 12:38:11 PM	NTPLDTBLR42\CYLANCE	LoginSuccess	183.198.155.32	Mara Lee (Maralee@nmkehspace.com)	Provider: CylancePROTECT
05/02/2018 12:38:32 PM	NTPLDTBLR42\CYLANCE	LoginSuccess	183.198.155.32	Mara Lee (Maralee@nmkehspace.com)	Provider: CylancePROTECT
05/02/2018 12:38:41 PM	NTPLDTBLR42\CYLANCE	LoginSuccess	183.198.155.32	Mara Lee (Maralee@nmkehspace.com)	Provider: CylancePROTECT

Figure 13

Sample logs:

Time	Description
− May 08 10:59:12 AM	Apr 24 09:45:40 ETPVMDFHLMI01 Apr 24 09:45:40 66.36.125.36 229 <46>1 2018-04-24T14:45:33.2000000Z sysloghost CylancePROTECT - - - Event Type: A...
event_log_type	+- Application
event_type	+- Information
event_id	+- 3333
event_source	+- Syslog
event_user_domain	+- N/A
event_computer	+- Cylance
event_user_name	+- N/A
event_description	Apr 24 09:45:40 ETPVMDFHLMI01 Apr 24 09:45:40 66.36.125.36 229 <46>1 2018-04-24T14:45:33.2000000Z sysloghost CylancePROTECT - - - Event Type: AuditLog, Event Name: LoginSuccess, Message: Provider: CylancePROTECT, Source IP: 185.198.155.32, User: Mara Lee (Maralee@nmkehspace.com)

Figure 14

Alerts

- **Cylance: Configuration changed -** This alert will be generated when device configuration is changed.
- **Cylance: Exploitation attempt -** This alert will be generated when a memory exploitation is detected.
- **Cylance: Script executed -** This alert will be generated when a script is executed by user.
- **Cylance: Threat detected -** This alert will be generated when a threat is detected on Cylance agent system.
- **Cylance: User logon succeeded -** This alert will be generated when a successful user logon happens.

Categories and Saved searches

- **Cylance: Configuration changes -** This category provides information related to device configuration changes.
- **Cylance: Device activities -** This category provides information related to device activities on agent systems.
- **Cylance: Exploitation attempt -** This category provides information related to memory exploitations detected on agent systems.
- **Cylance: Script execution -** This category provides information related to scripts executed by users.
- **Cylance: Threat detection -** This category provides information related to threats detected on agent systems.
- **Cylance: User logon -** This category provides information related to successful user logon.

Knowledge Objects

- **Cylance - Configuration changes -** This knowledge object helps to analyze logs related to device configuration changes.
- **Cylance - Device activities -**This knowledge object helps to analyze logs related to device activities.
- **Cylance - Exploitation attempt -** This knowledge object helps to analyze logs related to memory exploitations detected in agent systems.
- **Cylance - Script execution -** This knowledge object helps to analyze logs related to scripts executed by users.
- **Cylance - Threat detection -** This knowledge object helps to analyze logs to threats detected on agent systems.
- **Cylance - User logon -** This knowledge object helps to analyze logs related to successful user logon.

Import CylancePROTECT knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Token Templates
- Knowledge Objects
- Flex Reports
- Dashboards

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

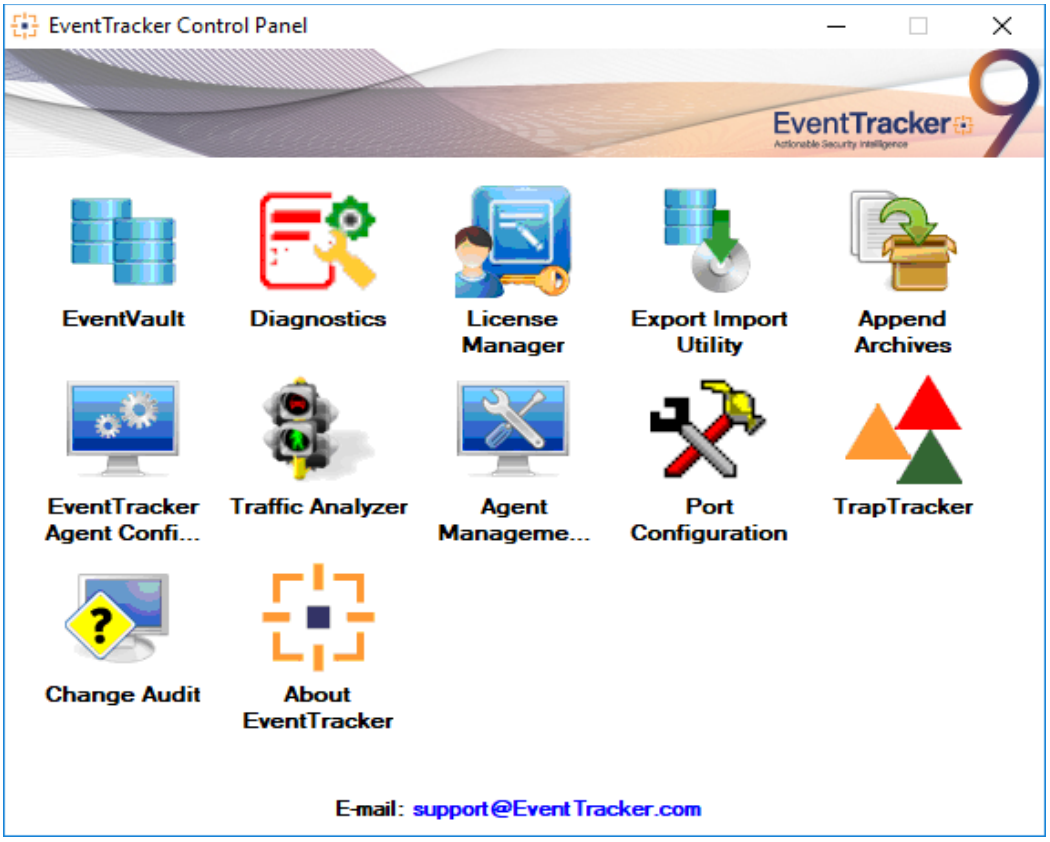

Figure 15

3. Click the **Import** tab.

Category

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

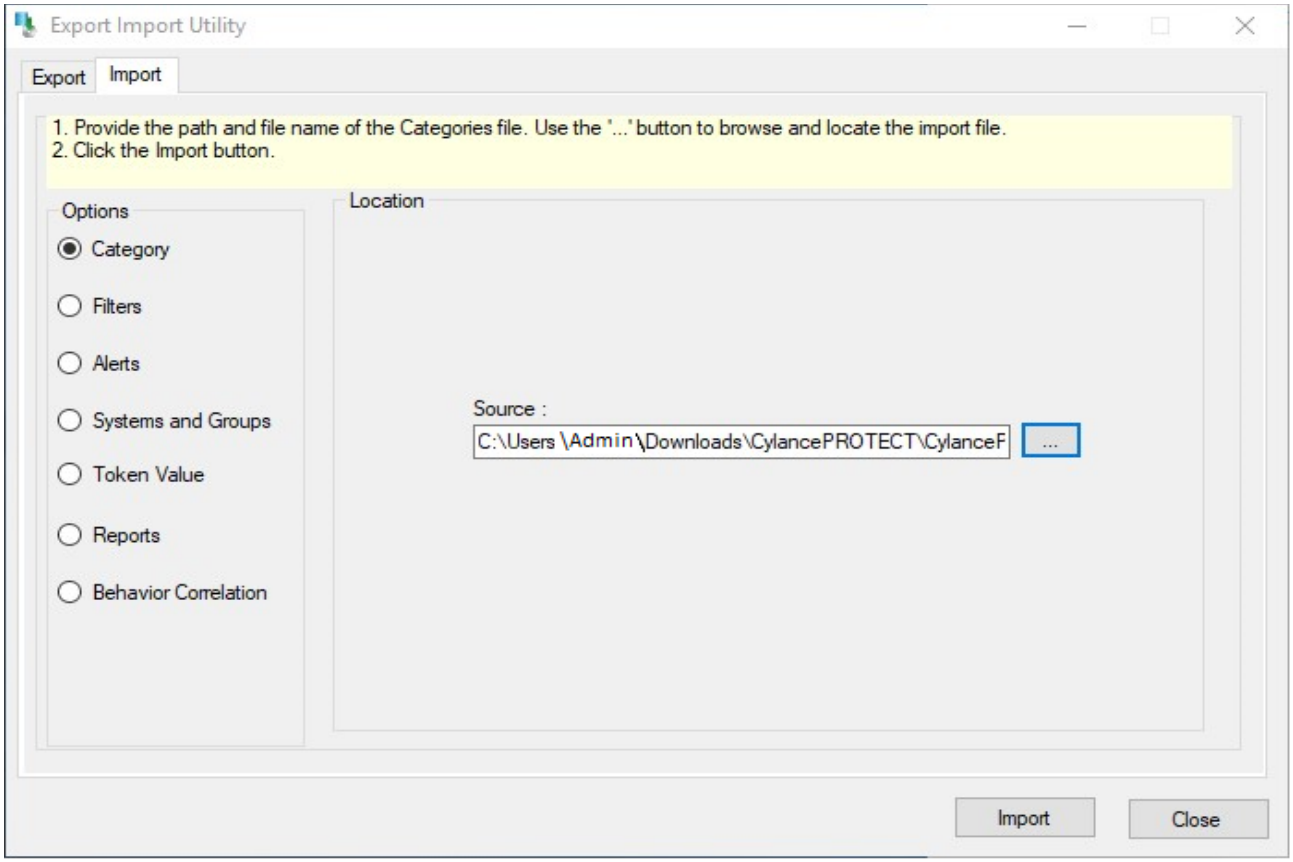

Figure 16

2. Locate **Category_CylancePROTECT.iscat** file, and then click the **Open** button.

3. To import categories, click the **Import** button. EventTracker displays success message.

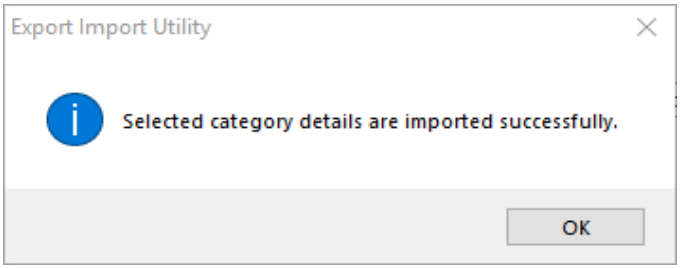

Figure 17

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

Alerts

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

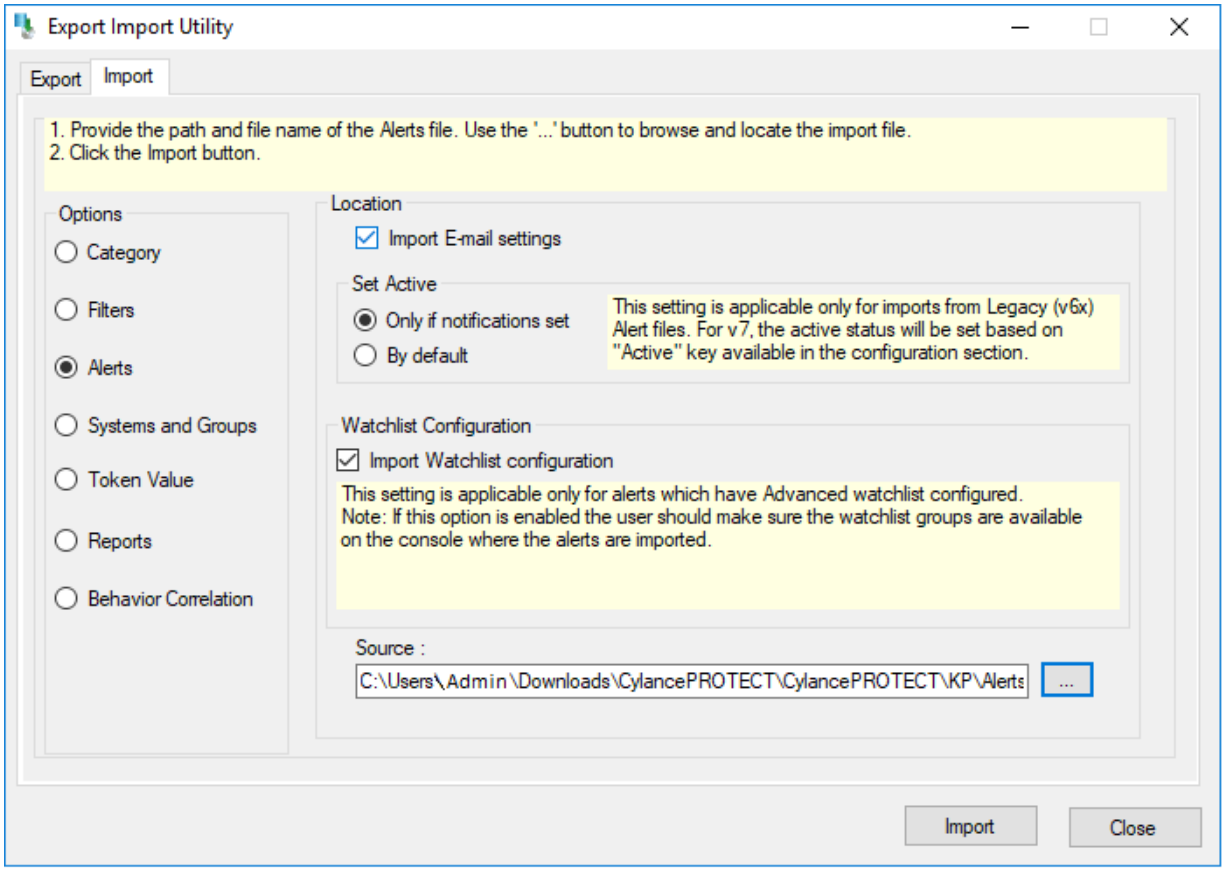

Figure 18

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

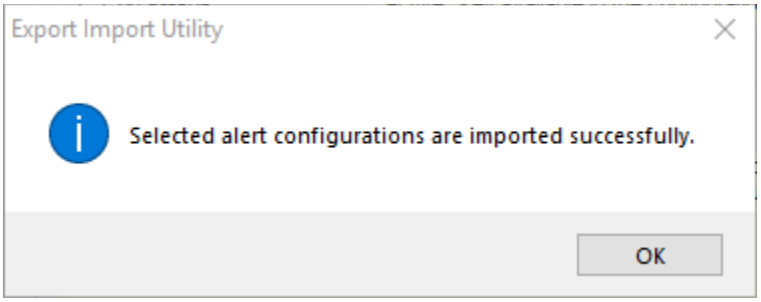

Figure 19

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

Token Templates

1. Click **Parsing rules** under **Admin** option in the EventTracker manager page.
2. Move to **Template** and click on import configuration icon on the top right corner.
3. In the popup window browse the file named **Token Template_ CylancePROTECT.ettd**.

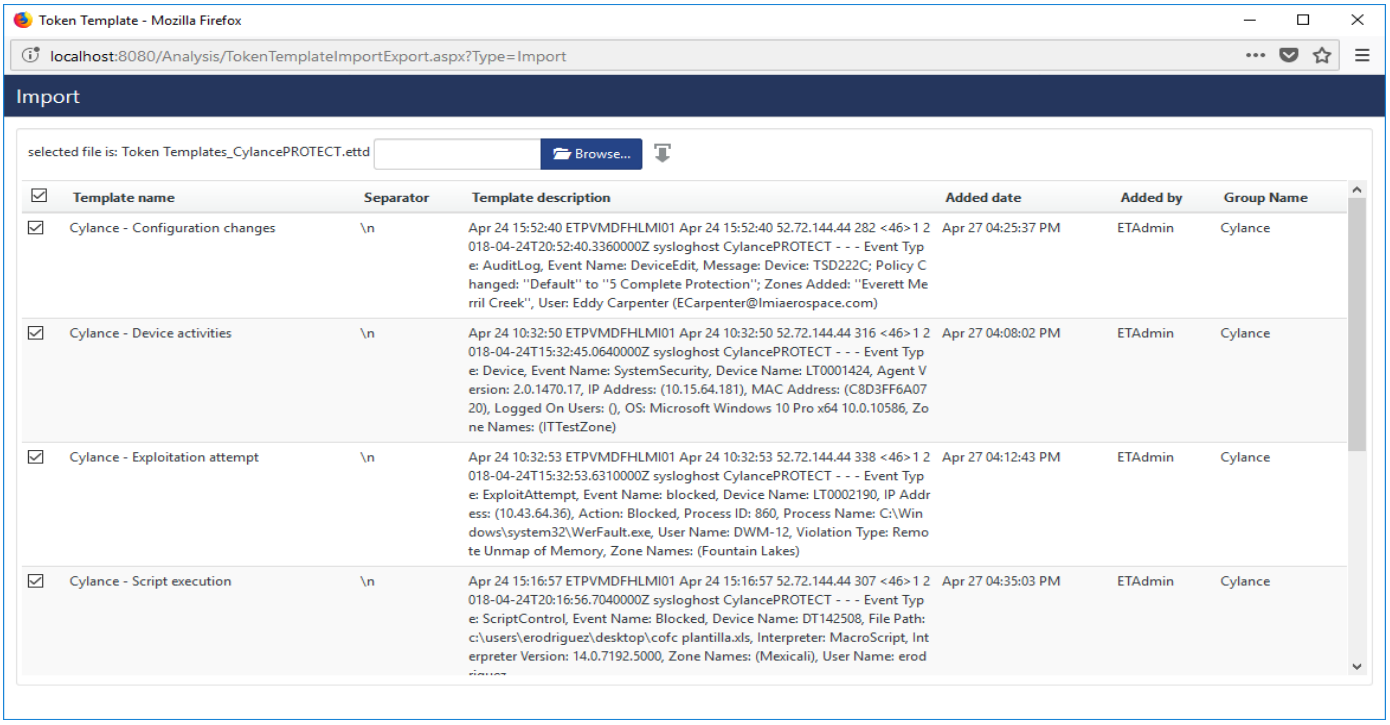

Figure 20

4. Now select all the check box and then click on **Import** option. EventTracker displays success message.

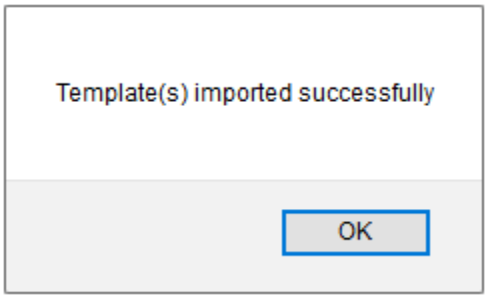

Figure 21

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

Knowledge Objects

1. Click **Knowledge objects** under **Admin** option in the EventTracker manager page.
2. Locate the **KO_CylancePROTECT.etko** file.

Figure 22

3. Click the '**Upload'** option.
4. Now select all the check box and then click on '**Import**' option.

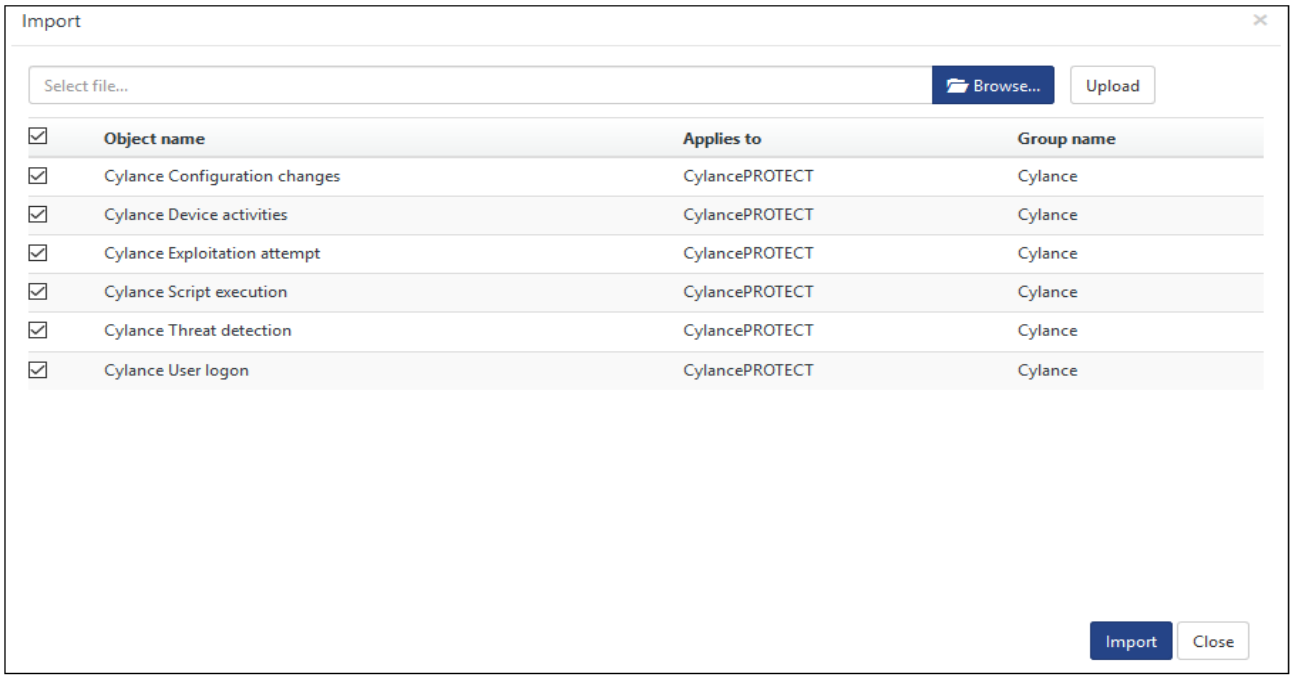

Figure 23

5. Knowledge objects are now imported successfully.

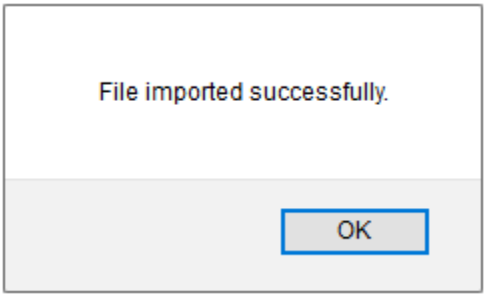

Figure 24

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

Flex Reports

On EventTracker Control Panel,

1. Click **Reports** option, and select new (*.etcrx) from the option.

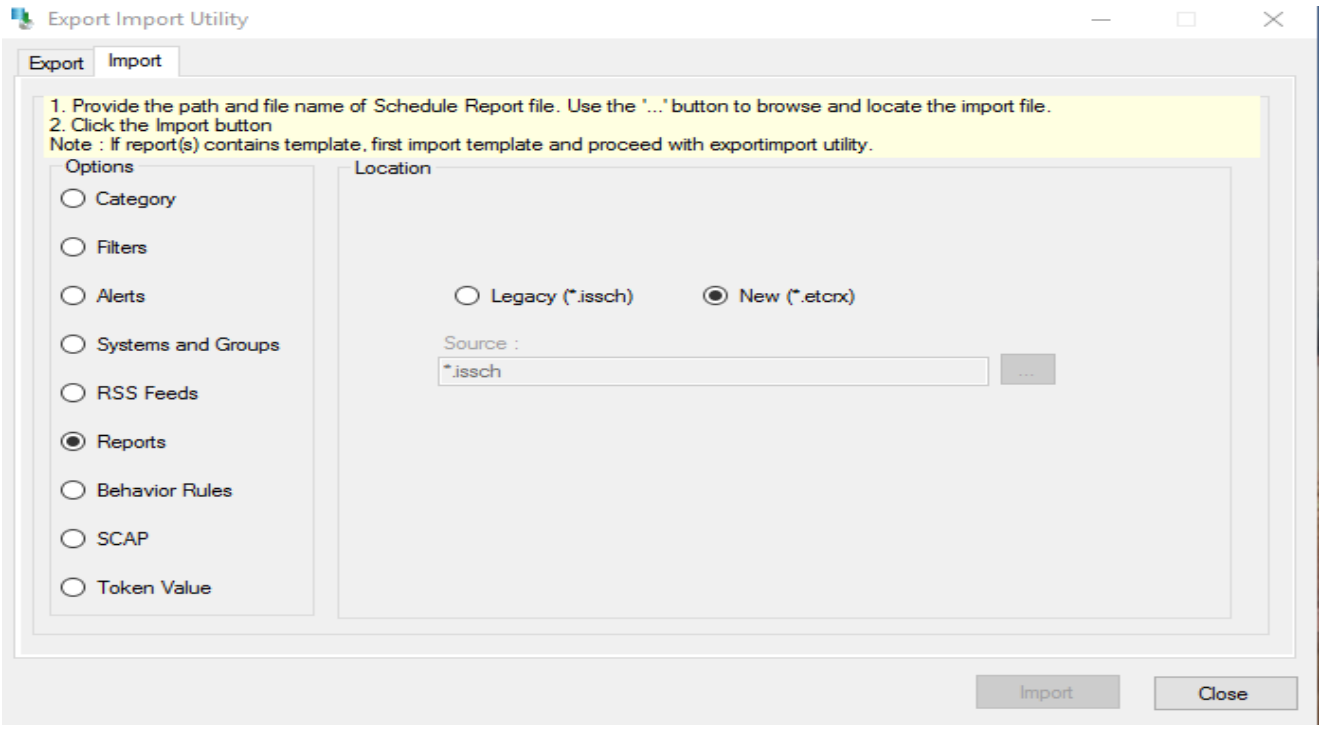

Figure 25

2. Locate the **Reports_CylancePROTECT.etcrx** file, and select all the check box.

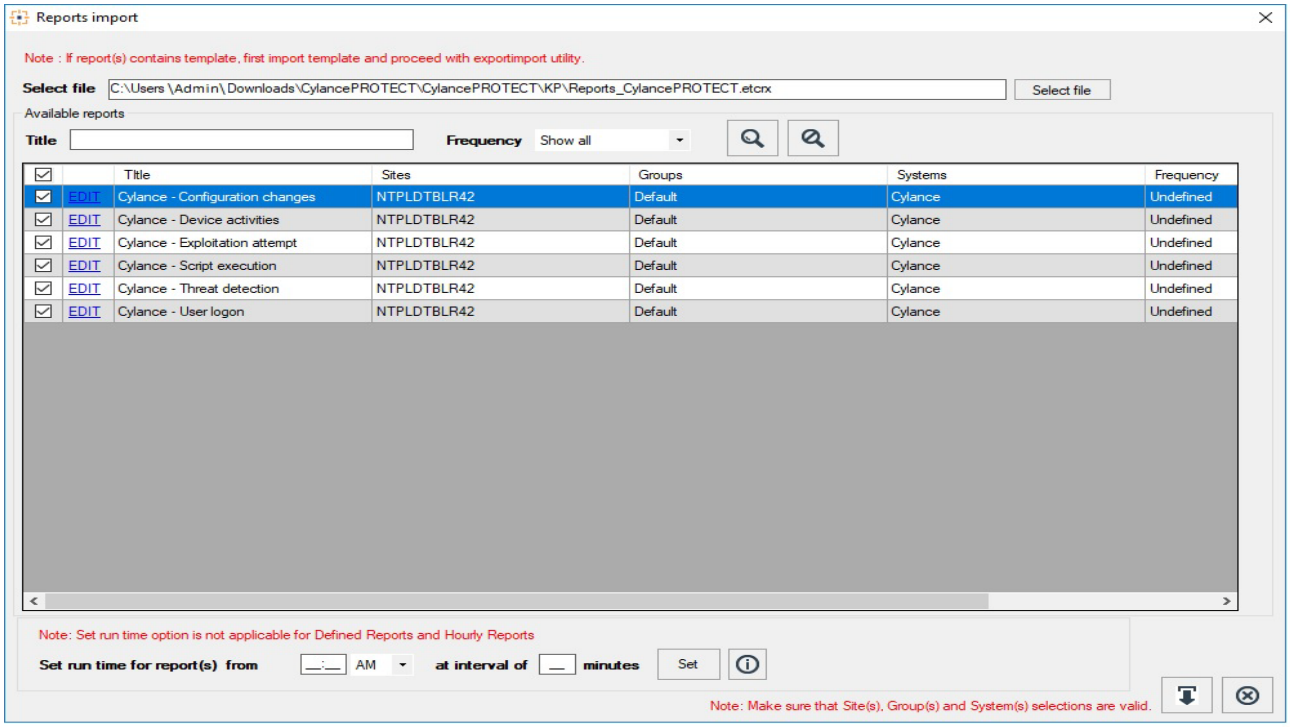

Figure 26

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

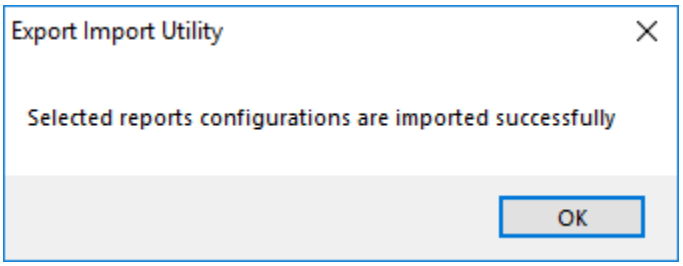

Figure 27

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

Dashboards

Note: If you have EventTracker Enterprise version **v9.0**, you can import dashboards.

1. Open **EventTracker Enterprise**.

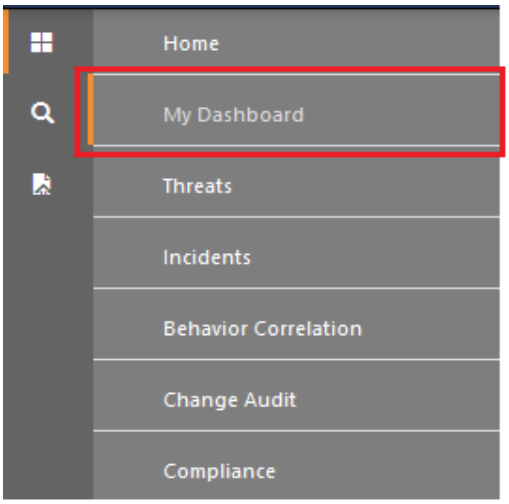

Figure 28

2. Navigate to **Dashboard>My Dashboard**.
   My Dashboard pane is shown.

3. Click the **'Import'** button to import the dashlets.

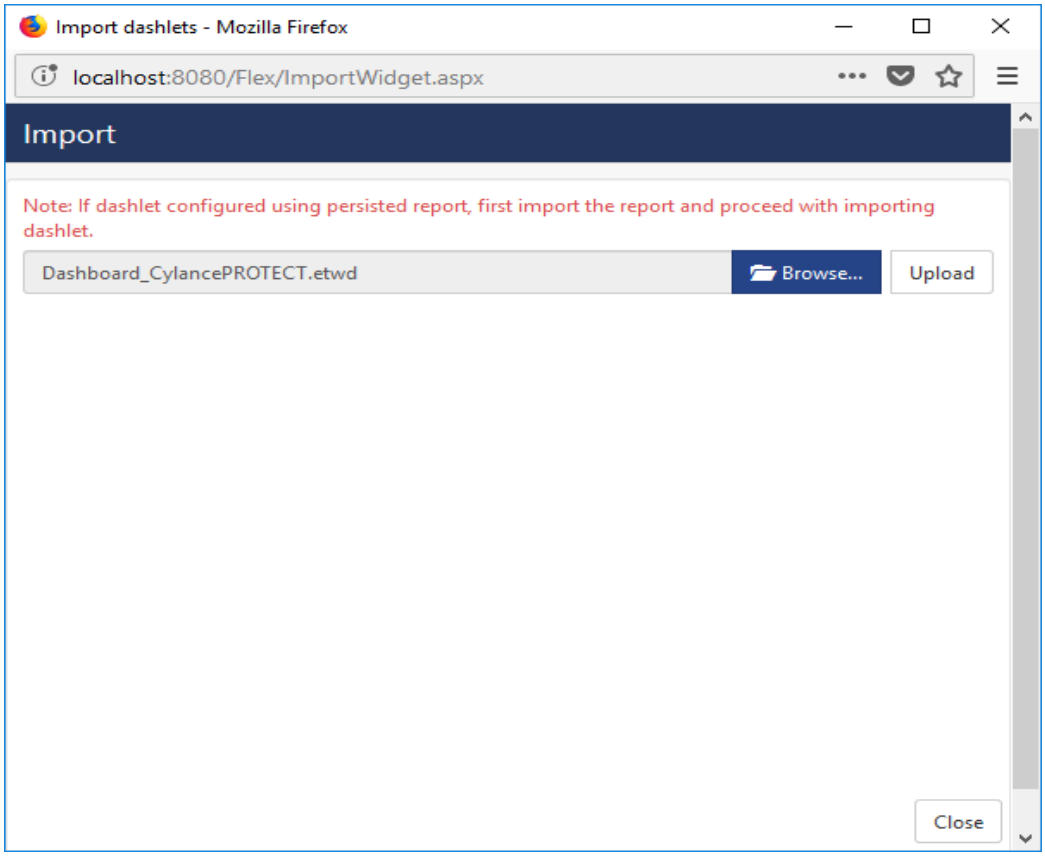

Figure 29

4. Locate the **Dashboard_CylancePROTECT.etwd** file.
5. Click the '**Upload'** option.

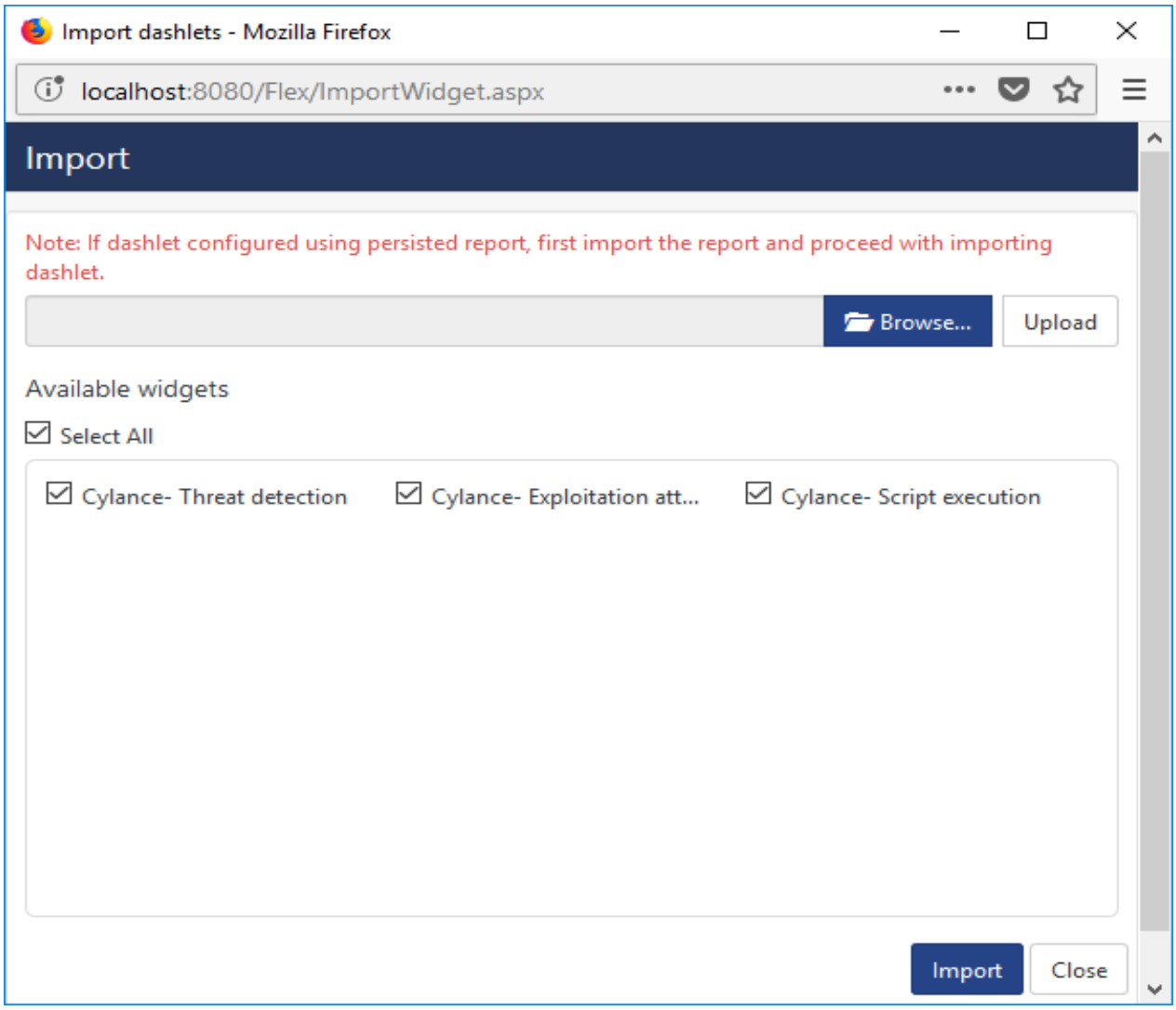

Figure 30

6. Now select all the check box and then click on '**Import**' option.
   Dashlets are now imported successfully.
7. Click the '**Add'** button to create a new dashlets.

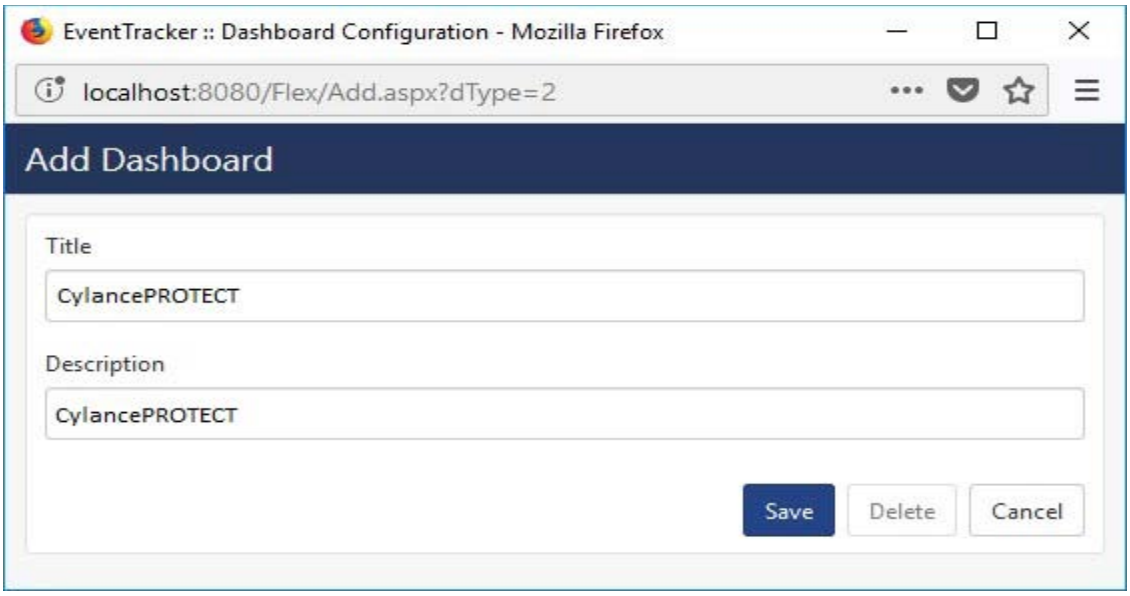

Figure 31

8. Fill suitable Title and Description and click **Save** button.
9. Click **'Customize'** to locate **Cylance** dashlets and choose all created dashlets for **Cylance** and choose all created dashlets.

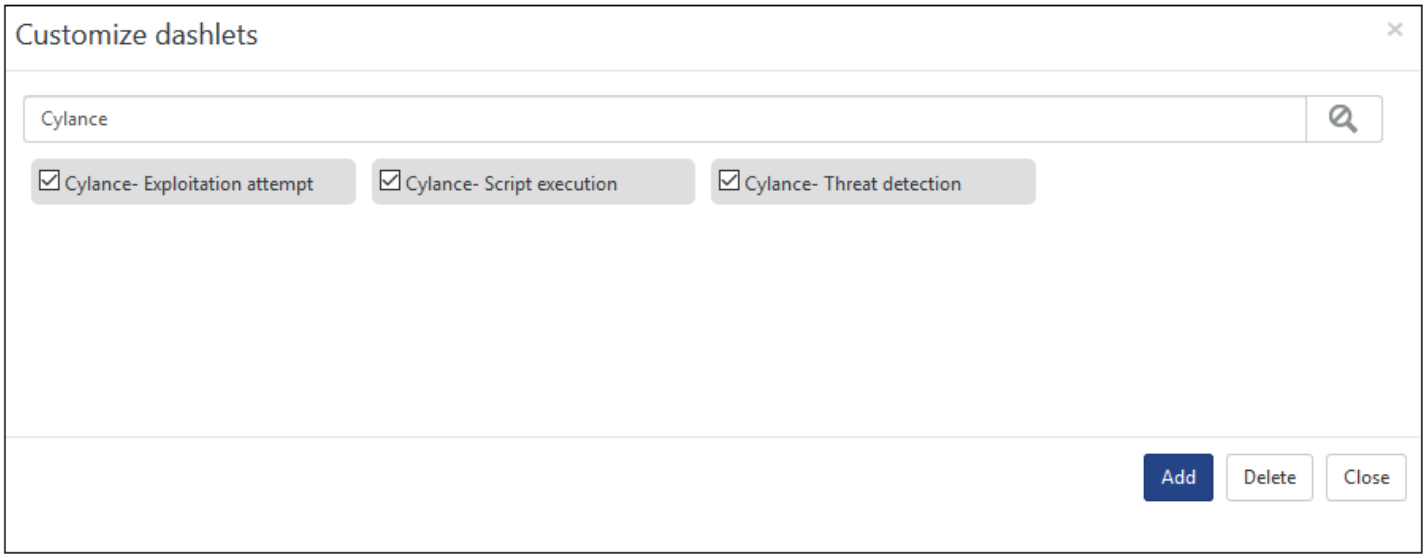

Figure 32

10. Click '**Add'** dashlet to create dashboard.

Verify CylancePROTECT knowledge pack in EventTracker

Categories

1. Logon to **EventTracker Enterprise**.
2. Click **Admin** dropdown, and then click **Categories**.
3. In **Category Tree** to view imported categories, scroll down and expand **Cylance** group folder to view the imported categories.

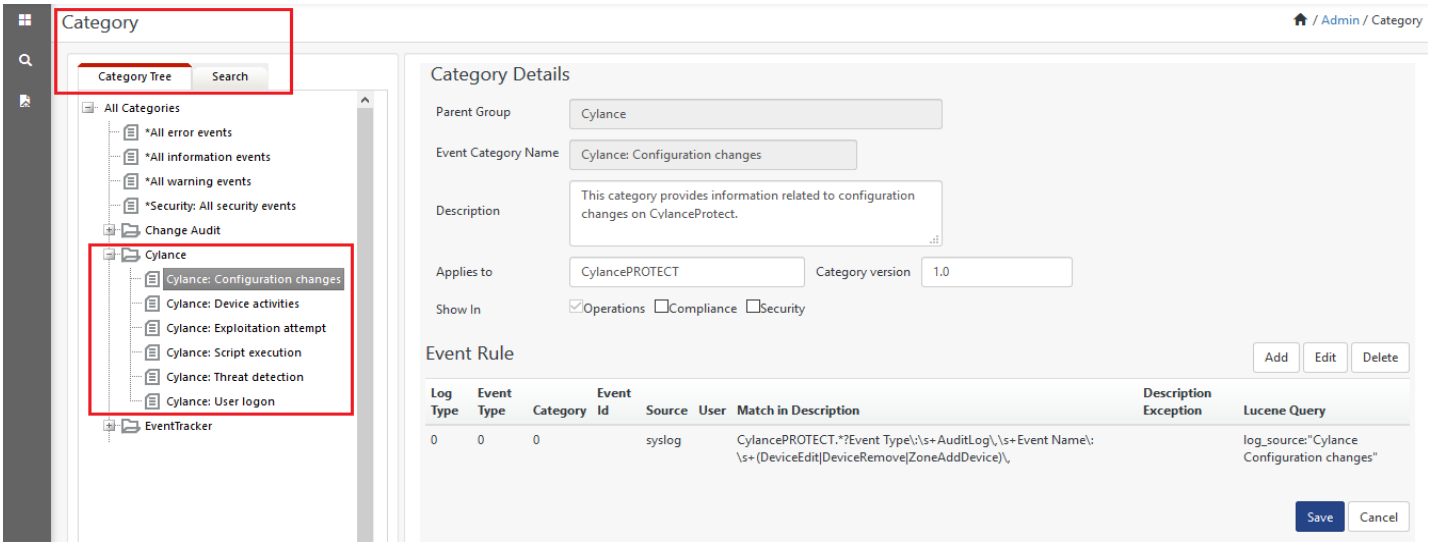

Figure 33

Alerts

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Alerts.**
2. In search box, enter **Cylance** and then click the **Search** button.
   EventTracker displays alert of **Cylance.**

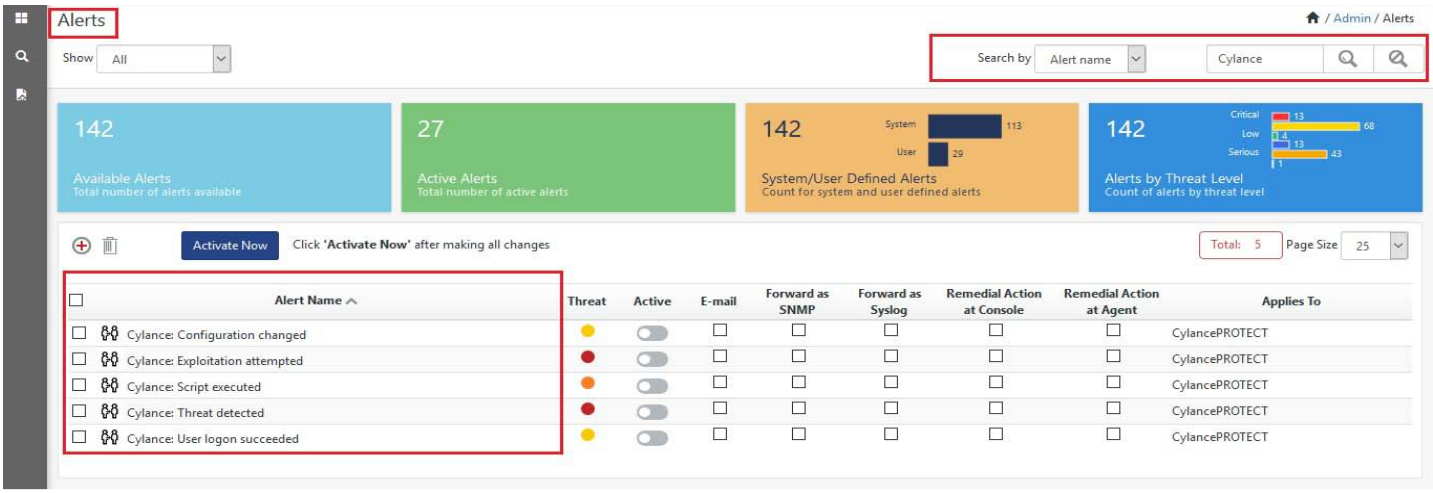

Figure 34

Token Templates

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Parsing rules.**
2. On **Template** tab, click on the **Cylance** group folder to view the imported Token Values.

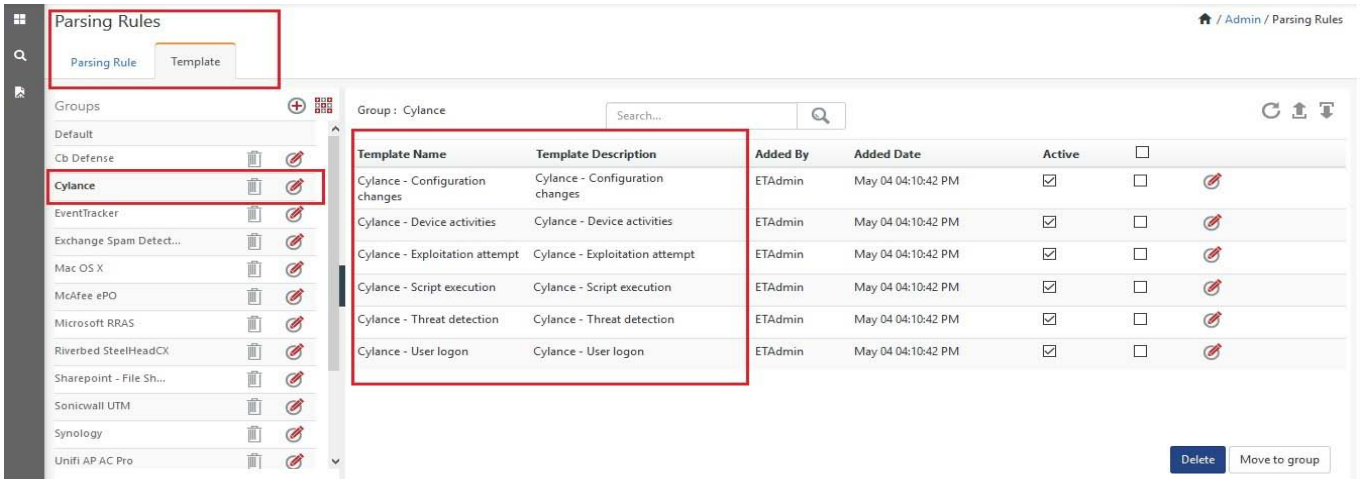

Figure 35

Knowledge Objects

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Knowledge Objects.**
2. In the **Knowledge Object** tree, expand **Cylance** group folder to view the imported Knowledge objects.

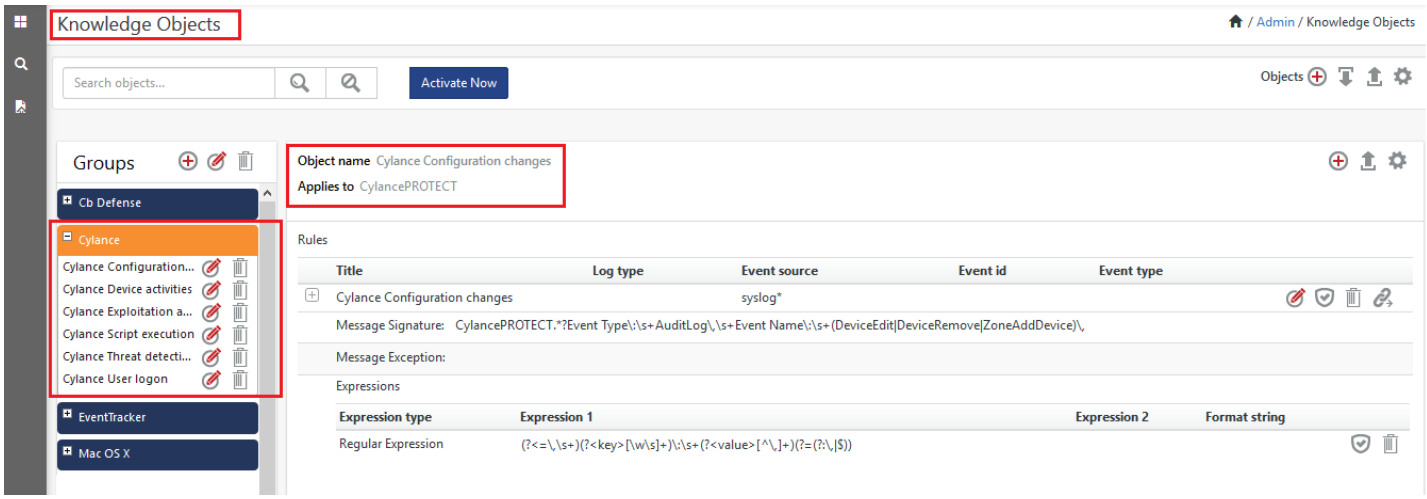

Figure 36

Flex Reports

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

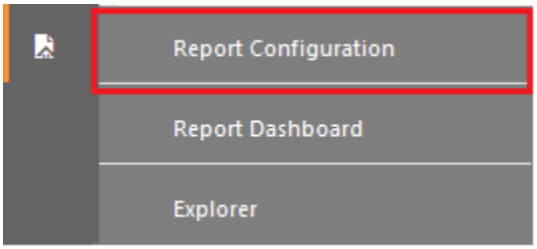

Figure 37

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

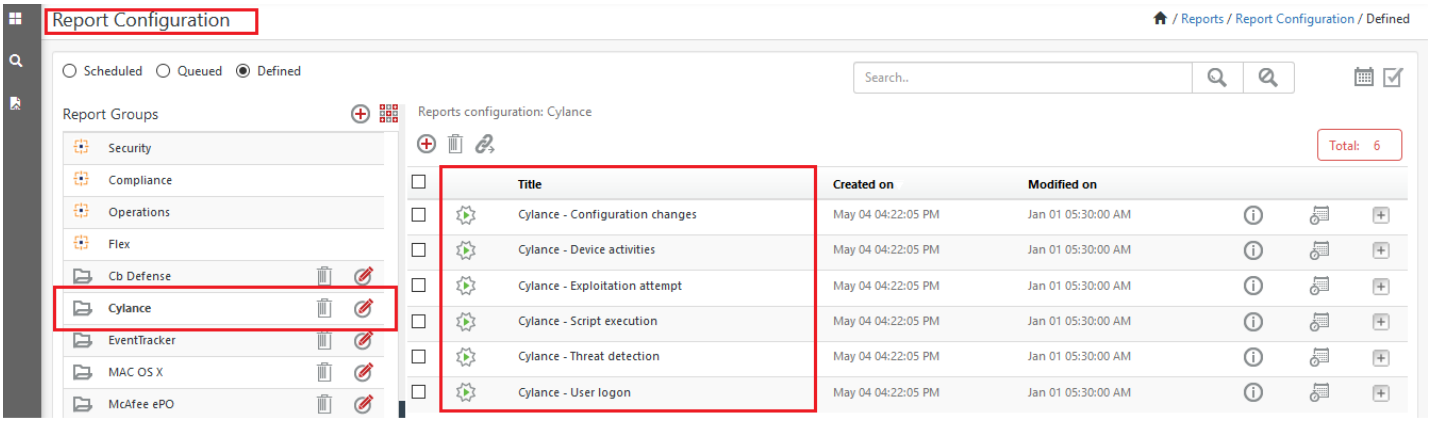

Figure 38

Dashboards

1. Open **EventTracker Enterprise** in browser and logon.
2. Navigate to **Dashboard>My Dashboard**.
   My Dashboard pane is shown.

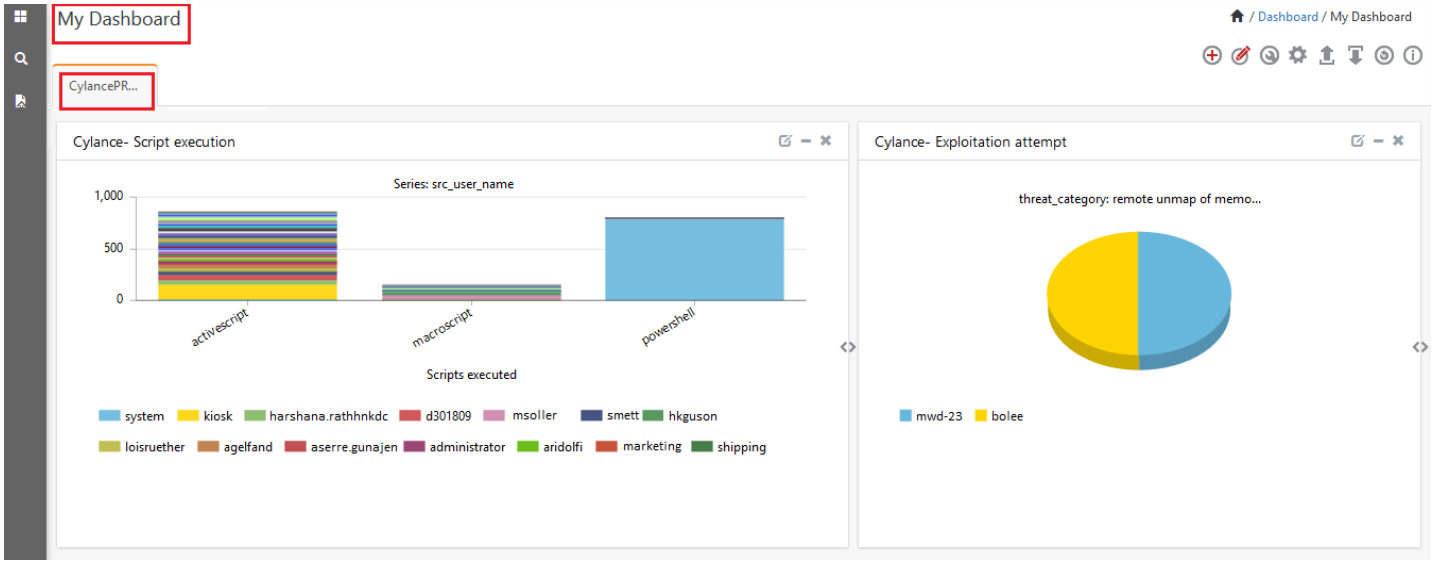

Figure 39

Sample Flex Dashboards

1. **Cylance- Threat detection**: This dashboard provides information related to threats detected on agent systems.

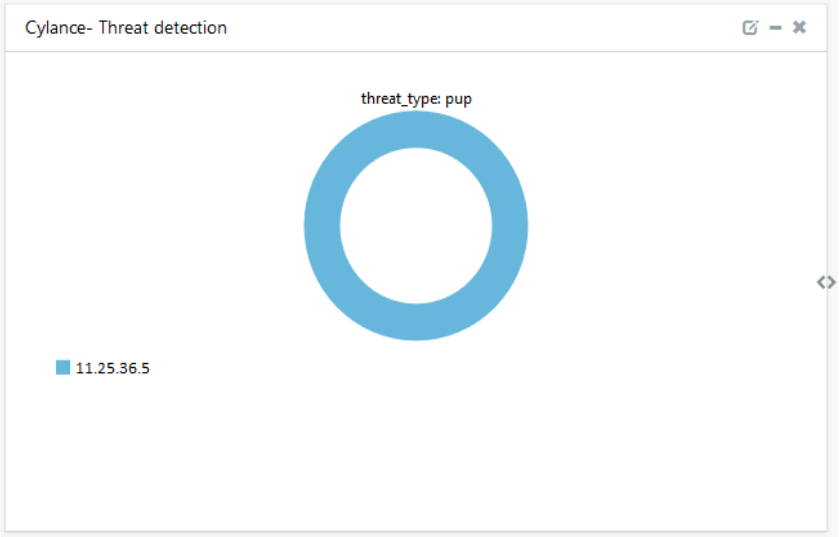

Figure 40

2. **Cylance- Script execution**: This dashboard provides information related to all the scripts executed by users.

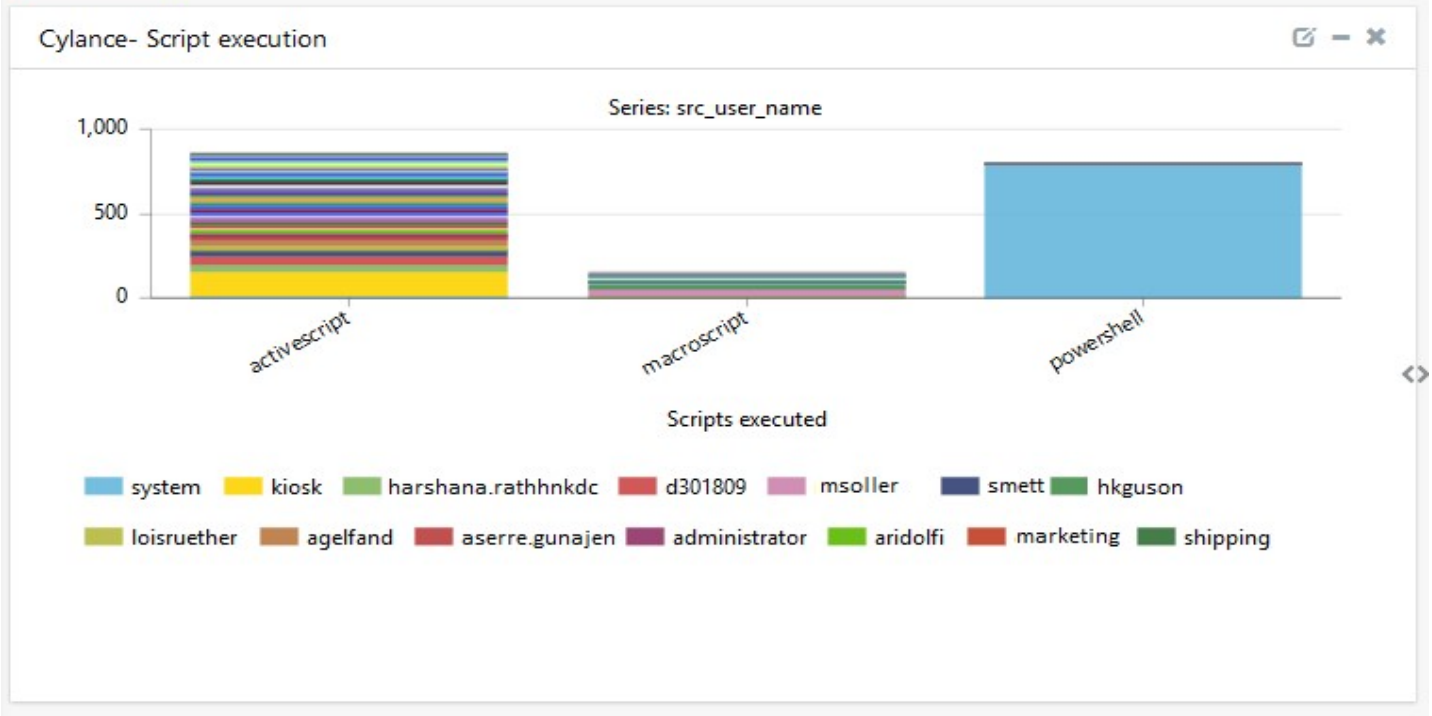

Figure 41

3. **Cylance- Exploitation attempt**: This dashboard provides information related to memory exploitations detected on agent systems.

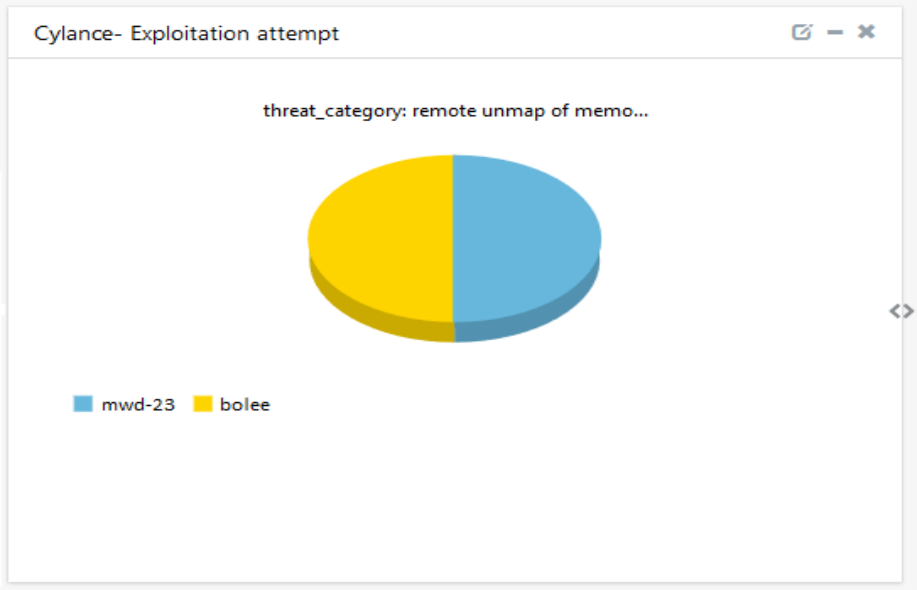

Figure 42