

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.

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

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

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

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

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

© 2019 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



Table of Contents

1.	Overview	. 3
2.	Prerequisites	. 3
3.	Configuring Cybereason to send syslog to EventTracker	. 3
4.	EventTracker Knowledge Pack 4.1 Flex Reports	. 3 . 3
	4.2 Alerts	. 7
	4.3 Saved Searches	. 7
	4.4 Dashboards	. 8
5.	Importing Cybereason knowledge pack into EventTracker 5.1 Alerts	14 15
	5.2 Token Template	16
	5.3 Knowledge Object	17
	5.4 Flex Reports	18
	5.5 Category	20
	5.6 Dashboard	21
6.	Verifying Cybereason knowledge pack in EventTracker 6.1 Alerts	22 22
	6.2 Token Template	23
	6.3 Knowledge Object	24
	6.4 Flex Reports	24
	6.5 Category	25



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.



				-	Action Status (Failed: 0	-			
LogTime	Computer	Event Class	Event Category	Severity	Success:1)	User Name	User Role	Machine Name	Machine IP Address
09/13/2019 02:44:54 PM	CYBEREASON	General	Login	0	5	barbarag	analyst_13	contoso-server2dc	89.234.157.254
09/13/2019 02:44:55 PM	CYBEREASON	General	Login	0	5	matt	analyst_13	contoso-server2dc	91.200.12.91
09/13/2019 02:44:55 PM	CYBEREASON	General	Login	1	5	maryj	sys_admin	contoso-asagw2	213.251.182.115
09/13/2019 02:44:55 PM	CYBEREASON	General	Login	1	5	frantz	sys_admin	contoso-etids	195.154.250.216
09/13/2019 02:44:55 PM	CYBEREASON	General	Login	5	5	clarkk	analyst_13	contoso-etids	195.154.250.216
09/13/2019 02:44:55 PM	CYBEREASON	General	Login	0	5	peterp	user_admin	contoso-etids	195.154.240.176
09/13/2019 02:44:55 PM	CYBEREASON	General	Login	1	5	loisl	sys_admin	contoso-dc01.azurestack	77.247.181.165
09/13/2019 02:44:55 PM	CYBEREASON	General	Login	1	5	joeb	executive	contoso-etsb12	195.154.240.176
09/13/2019 02:44:55 PM	CYBEREASON	General	Login	0	5	System	executive	contoso-server6dc	195.154.241.119
09/13/2019 02:44:55 PM	CYBEREASON	General	Login	0	5	frantz	sys_admin	contoso-etids	201.18.18.173
09/13/2019 02:44:55 PM	CYBEREASON	General	Login	0	5	mjones	sys_admin	contoso-rhsvr1	178.137.87.242
09/13/2019 02:44:55 PM	CYBEREASON	General	Login	0	5	loisl	user_admin	contoso-etsb12	46.148.22.18

• **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.

					Action Status (Failed: 0		
LogTime	Event Class	Event Category	User Name	User Role	Success:1)	Machine IP Address	Machine Name
09/13/2019 02:44:55 PM	General	Logout	joe	analyst_l3	5	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	5	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	Cybereaso n	ChangeCon figurationSe ttings	General	ъ	admin@contoso.com	٩		
09/12/2019 11:13:25 AM	Cybereaso n	ChangeCon figurationSe ttings	General	ъ	admin@contoso.com	4		
09/12/2019 11:13:25 AM	Cybereaso n	ChangeCon figurationSe ttings	General	ъ	admin@contoso.com	٩		
09/12/2019 11:13:25 AM	Cybereaso n	PowerShell ProtectionM ode	Security Profile	5	admin@contoso.com	4	Off	On
09/12/2019 11:13:25 AM	Cybereaso n	ChangeCon figurationSe ttings	General	ъ	admin@contoso.com	٩		
09/12/2019 11:13:25 AM	Cybereaso n	PowerShell ProtectionM ode	Security Profile	ზ 	admin@contoso.com	1	On	Off



• **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 Hame	Threat Info	Investigation URL	Mahware Creation Time
09/13/2019 11:46:28 AM	Malware Created	Malware	6	contoso-server6dc	eicar.com	https://eicar.com	http://localhost.7894/id/42669814	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:28 AM	Malware Created	Malware	5	contoso-rhsvr1	eicer.com	invoke-expression	http://localhost.7894/ks/25649090	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:28 AM	Malware Created	Malware	5	contoso-server2dc	Al Static Analysis	invoke-expression	http://localhost.7894/ki/28558771	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:28 AM	Malware Updated	Malware	15	contoso-server1dc	download & execute	https://eicar.com	http://localhost.7894/ld/72400271	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:26 AM	Malware Updated	Malware	5	contoso-server6dc	malicious download	http://www.example.com/aunt/adv ice.html?breath=account&aftertho upth=armv	http://localhost.7894/kd/20292064	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:28 AM	Malware Created	Malware	5	contoso-server2dc	Al StaticAnalysis	https://eicar.com	http://localhost.7894/ld/94165369	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:28 AM	Malware Updated	Malware	8	contoso-filesvr6	Al Static Analysis	http://www.example.com/aunt/adv ice.html?breath=account&aftertho uptt=army	http://localhost.7894/id/48709325	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:28 AM	Malware Updated	Malware	٩	contoso-asagw2	download 8 execute	https://eicar.com	http://localhost.7894Ad/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/adv ice.html?breath=account&aftertho upht=army	http://localhost.7894/id/123113752	Dec 19 2017, 15:58:14 IST
09/13/2019 11:46:28 AM	Malware Updated	Malware	6	contoso-rhsvr1	malicious command	http://www.example.com/aunt/adv ice.html?breathwaccount&aftertho	http://localhost.7894/id/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/ld/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.

												Affected		
					Malop Detection	Malop Key						Machine	Affected	Affected Users
Event name	Severity	Start Time	Malop Id	Malop Activity Type	Туре	Suspicion	Malop Suspect	Reason	Is Signed	Malop Link	Request Context	Name	Machines Count	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/54.545034 625	API.md		45	5
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/67.990879 413	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	5	localhost:8080/#/malop/86.816018 953	uc_Widget.ascx		51	78
Malop Created	10	Dec 19 2017, 15:58:14 IST	44.419719562	Privilege Escalation	MalopProcess	Credential Theft Malop	teszt.pdf	blacklist	5	localhost:8080/#/malop/39.885614 423	teszt.pdf		17	63
Malop Created	10	Dec 19 2017, 15:58:14 IST	36.292623304	Privilege Escalation	MalopProcess	Credential Theft Malop	nations.html	blacklist	5	localhost:8080/#/malop/51.561718 937	nations.html		81	95
Malop Created	10	Dec 19 2017, 15:58:14 IST	85.816516132	Scanning	MalopProcess	Credential Theft Malop	uc_FlexTabular.ascx	blacklist	1	localhost:8080/#/malop/58.399869 412	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	5	localhost:8080/#/malop/73.933059 657	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	٩	localhost:8080/#/malop/97.583713 561	diagram-state- machine.png		14	50
Malop Created	10	Dec 19 2017, 15:58:14 IST	15.135355903	C&C	MalopProcess	Credential Theft Malop	test_constraints.html	blacklist	5	localhost:8080/#/malop/47.815584 963	test_constraints.html		46	3
Malop Created	10	Dec 19 2017, 15:58:14 IST	98.941229766	Scanning	MalopProcess	Credential Theft Malop	elasticsearch.jquery.min.js	blacklist	٦	localhost:8080/#/malop/50.372699 663	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.

				Affected						
LogTime	Severity	Event name	Malop Id	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	sms-s	Windows_10	System	1
09/13/2019 11:46:29 AM	٩0	Malop Machine Information	69.867300583	14	10.25.2.1	Microsoft.Photos	iexplore	Windows_10	frantz	1
09/13/2019 11:46:29 AM	10	Malop Machine Information	21.126999488	27	contososerver	smss	mmc	Windows_10	clarkk	1
09/13/2019 11:46:29 AM	10	Malop Machine Information	92.688107116	59	contososerver	EventTracker.Reporter	Microsoft.Photos	Windows_7	frantz	1
09/13/2019 11:46:29 AM	10	Malop Machine Information	54.900108218	90	10.25.2.1	lync	cmd	Windows_10	frantz	1
09/13/2019 11:46:29 AM	٩0	Malop Machine Information	94.739722606	59	contososerver	UcMapi	SISIPSService	Windows_10	polo	٩
09/13/2019 11:46:29 AM	10	Malop Machine Information	50.697752353	44	10.25.2.1	UcMapi	smiss	Windows_8	gary	1
09/13/2019 11:46:29 AM	10	Malop Machine Information	59.262759465	97	contososerver	EtScheduler	vmware-usbarbitrator64	Windows_8	brucew	1
09/13/2019 11:46:29 AM	10	Malop Machine Information	81.775880625	48	10.25.2.1	EventTracker Reporter	smss	Windows_8	polo	1
09/13/2019 11:46:29 AM	10	Malop Machine Information	90.998397327	11	contososerver	mmc	brkrprcs64	Windows_10	matt	1
09/13/2019 11:46:29 AM	10	Malop Machine Information	25.576340879	42	10.25.2.1	Expresso	iexplore	Windows_8	maya	1
09/13/2019 11:46:29 AM	10	Malop Machine Information	68.297060039	58	contososerver	notepad	smss	Windows_7	peterp	1
09/13/2019 11:46:29 AM	10	Malop Machine Information	39.436108213	68	10.25.2.1	Expresso	SISIDSService	Windows_8	System	1
09/13/2019 11:46:29 AM	10	Malop Machine Information	94.559264978	22	contososerver	Expresso	System	Windows_10	System	٩
09/13/2019 11:46:29 AM	10	Malop Machine Information	20.313244031	48	10.25.2.1	SISIDSService	EtScheduler	Windows_7	System	1
09/13/2019 11:46:29 AM	10	Malop Machine Information	18.857816535	31	contososerver	EventTracker Reporter	scheduler	Windows_8	loisl	1
09/13/2019 11:46:29 AM	10	Malop Machine Information	79.274651621	64	10.25.2.1	iexplore	SISIDSService	Windows_7	peterp	1
09/13/2019 11:46:29 AM	10	Malop Machine Information	23.940710621	28	contososerver	mmc	smss	Windows_7	System	1

 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/adv ice.html?breath=account&aftertho ught=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/ld/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/adv ice.html?breath=account&aftertho ught=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	Al.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/adv ice.html?breath=account&aftertho ught=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	۹0	contoso-asagw2	malicious download	http://www.example.com/aunt/adv ice.html?breath=account&aftertho ught=army	http://localhost:7894/id/23032040	Dec 19 2017, 15:58:14 IST
Malware Created	Malware	10	contoso-asagw1	Al.StaticAnalysis	invoke-expression	http://localhost:7894/id/61852049	Dec 19 2017, 15:58:14 IST
Malware Created	Malware	10	contoso-etsb12	Al.StaticAnalysis	invoke-expression	http://localhost:7894/id/24476609	Dec 19 2017, 15:58:14 IST
Malware Updated	Malware	٩0	contoso-asagw1	malicious download	invoke-expression	http://localhost:7894/id/34563513	Dec 19 2017, 15:58:14 IST
Malware Updated	Malware	٩0	contoso-dc01.azurestack	download & execute	https://eicar.com	http://localhost:7894/id/35010313	Dec 19 2017, 15:58:14 IST
Malware Updated	Malware	٩0	contoso-server1dc	malicious command	https://eicar.com	http://localhost:7894/id/111886297	Dec 19 2017, 15:58:14 IST
Malware Created	Malware	٩0	contoso-rhsvr1	download & execute	https://eicar.com	http://localhost:7894/id/21565572	Dec 19 2017, 15:58:14 IST
Malware Updated	Malware	٩0	contoso-asagw2	malicious command	invoke-expression	http://localhost:7894/id/62844374	Dec 19 2017, 15:58:14 IST
Malware Created	Malware	۹0	contoso-etsb12	malicious download	http://www.example.com/aunt/adv ice.html?breath=account&aftertho ught=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

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







Sep 06 04:28 PM - Sep 13 04:29 PM



Cybereason - Malop events

🖾 – 🗶

log_type	object_name re	eason 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	Ŧ	
4					•		



Figure 12





Figure 13



Figure 14









Figure 16





Figure 17



Figure 18

Netsurion... EventTracker







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

🥾 Expo	rt Import	Utility	
Export	Import		
1. Pro 2. Cli	ovide the p ck the Imp	ath and file nar ort button.	ne of the Categories file. Use the '' button to
Opti	ions		Location
•	Category		

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.

		🐥 Admin -	Tools 🗸
Active Watch Lists	Event Filters	🧭 Parsing Rules	
Alerts	Ventvault	Report Settings	÷
m 🖲 Behavior Correlation Rules	FAQ Tile Configuration	Systems	
behavior Correlation Settings	Group Management	Q Users	
Casebook Configuration	Q IP Lookup Configuration	r Weights	
● Category	· 🔆 Knowledge Objects	Windows Agent Config	
Diagnostics	D Manager		

Figure 25

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

Parsing Rules			🔶 / Admin / Parsing Rules
Parsing Rule T	Template		
Groups	Group : All	Search Q	C 1 T
Default	^		

Figure 26

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

Impor	nport								
selected	elected file is: Template_Cybereason.ettd 🗃 Browsc								
	Template name	Separator	Template description	Added date	Added by	Group Name			
	Cybereason - Malop events	N	$\label{eq:constraints} CEF:I[Cyberesson]7.6.0]Malop[Malop Created]10] cs1Label= malopAtityType cs2=MalopProcess cs3Label= malopAtityType cs3=LATRAL_MOVEMENT cs4Label=malopAtityType cs3=LATRAL_MOVEMENT cs4Label=malopAtityType cs3=LATRAL_MOVEMENT cs4Label=malopAtityType cs3=LATRAL_MOVEMENT cs4Label=malopAtityType cs3=LatRaL_MOVEMENT cs4Label=malopAtityType cs4Label=malopAtityType cs3=LatRaL_MOVEMENT cs4Label=malopAtityType cs4Label=malopAtityType cs3=LatRaL_MOVEMENT cs4Label=malopAtityType cs4Label=malopAtityType cs3=LatRaL_MOVEMENT cs4Label=malopAtityType cs4Label=malopAtityType cs4LatRaL_MOVEMENT cs4L$	Sep 11 10:55:18.AM		Cyberesson			
	Cybereason - Malware created or updated	M	CEFII(bydereason)Cybereason 17.6.0]Mahware/Mahware Created]1Qeventid =102353df dvchost=contos_energe cILabel=vius/Name ci=download & exocute c324bel=context c32=http://cicar.com visit.s1abel=imset/sgaton c3ahttp://localhost:80gf deviceCustomDate1Label=mahwareCreationTi me deviceCustomDate1_jum520911222111UC	Sep 11 07:13:35 PM		Cybereason			
	Cyberrason -User action events	N	SyslogLogger CEF-QCybereason/Cybereason/UserAction/General/Logout Qrs1Label=username cs1= cm1Label=act cm2cesscn31 edwsiceCustomDate1Label=userActionTime deviceCust omDate1=Jul 09 2019; 2020;57 UTC cs2Label=userActionPlane cs2= admin/sys_admin/analyst_J3 cs3Label=machineName cs3= cs2Label=QueryOetails cs2=User > P rocess > Connection	Sep 12 02:44:34 PM		Cyberesson			



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.

		🔎 Admin -	Tools 👻 🌔
Active Watch Lists	💭 Event Filters	🧭 Parsing Rules	🔒 / Da
Alerts	Eventvault	Report Settings	
Behavior Correlation Rules	FAQ Tile Configuration	Systems	
🗞 Behavior Correlation Settings	Group Management	QQ Users	
ni sc 🚺 Casebook Configuration	🔍 IP Lookup Configuration	T Weights	Systems since the last 24 hou
କଟ୍ଟି Category	·☆ Knowledge Objects	Windows Agent Config	
A Diagnostics	💁 Manager		



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"



	Integrate Cybe	reason
Import	×	
KO_Cybereason.etko	🗯 Browse Upload	



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

Import	nport						
Select f	ile	-	Browse Upload				
	Object name	Applies to	Group name				
«	Cybereason malop events	cyberversion	Cybereason				
•	Cybereason malware events	cyberversion	Cybereason				
	Cybereason user events	cyberversion	Cybereason				



Figure 32

5.4 Flex Reports

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



Export Import Utility	-		×
Export Import			
1. Provide the path and file na 2. Click the Import button Note : If report(s) contains ten	ame of Schedule Report file. Use the '' button to browse and locate the import file. uplate, first import template and proceed with exportimport utility.		
Options	Location		
Category			
 Filters 			
 Alerts 	O Legacy (*.issch) New (*.etcnx) 2		
O Systems and Groups	Source : *issch		
O Token Value			
Reports 1			
O Behavior Correlation			
		_	
	Import		Close
		_	_

- 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

	D:\localrepowc\product\cybereason\RSA SecurID\	Configuration\Re	ports_Cybereason.etcrx		Select file	
ailable rep	orts	Frequency	Show all	Q Q		
]	Title	S	iites	Groups	Systems	Fr
EDIT	Cybereason - Malop created or updated details	NTPLDTBLR47				Und
EDIT	Cybereason - Not mitigated threat details	NTPLDTBLR47				Und
EDIT	Cybereason - Threat detected and updated details	NTPLDTBLR47				Und
EDIT	Cybereason - User login and logout activities	NTPLDTBLR47				Und
EDIT	Cybereason - User login failed activities	NTPLDTBLR47				Und
EDIT	Cybereason - User malop investigation activities	NTPLDTBLR47				Und
						>

Figure 34



4. EventTracker displays a success message:





5.5 Category

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

🤱 Export Import Utility		_		\times
Export Import				
1. Provide the path and file n 2. Click the Import button.	ame of the Categories file. Use the '' button to browse and locate the	e import file.		
 Options Category Filters Alerts Systems and Groups Token Value Reports Machine learning 	Location Source : 	ason.iscat		
		Import	Clos	e

- 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.





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

5.6 Dashboard

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





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:







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

/bereason			Q
Cybereason - Malop events	Cybereason - Malop events by	Cybereason - Malop events by	Cybereason - Malop events by t
Cybereason - Malware events b	Cybereason - Malware events b	Cybereason - Non-mitigated th	🗹 Cybereason - Threat by name
Cybereason - Top malop machi	Cybereason - User failed login d	Cybereason - User failed login d	Cybereason - User failed login d
Cybereason - User login and log	Cybereason - User login by geo		
			Add Delete Clo

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":

Alerts Show All						Search by Alert nam	e V	Admin / Alerts
								Critical 💼 10
132	29			132	User 13	119	132	Low 4 17 Serious 4
Available Alerts Total number of alerts available	Active Alerts Total number of active alerts			System/User Def Count for system and	fined Alerts d user defined alerts		Alerts by Thr Count of alerts	reat Level by threat level
Activate Now Click 'Activate Now' after makin	g all changes							Total: 6 Page Size 25 ▼
Alert Name A	Threat	Active	Email	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
🔲 🚯 Cybereason - Malop Created	•							cybereasonversion
ββ Cybereason - Malop Updated	•							cybereasonversion
ββ Cybereason - Malware created	•							cybereasonversion
ββ Cybereason - Malware Updated	•							cybereasonversion
🔲 🚯 Cybereason - Threat not mitigated	•							cybereasonversion
ββ Cybereason - User login failed	•							cybereasonversion

Figure 42

6.2 Token Template

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

		🐥 Admin v	Tools -
Active Watch Lists	Event Filters	😥 Parsing Rules	
Alerts	Eventvault	Report Settings	÷
m 🖲 Behavior Correlation Rules	FAQ Tile Configuration	Systems	
🗞 Behavior Correlation Settings	Group Management	Q Users	
Casebook Configuration	Q IP Lookup Configuration	r Weights	
● Category	·☆ Knowledge Objects	Windows Agent Config	
Diagnostics	Manager		



3. Click on Template and search for Cybereason.

Parsing Rules Parsing Rule Template									† 7 A	udmin / Parsing Rules
Groups Default		÷ #	Group : Cybereason	Search	Q					C 1 T
Cybereason	Ĩ	۲	Iemplate Name Iemplate Des	cription	Added By	Added Date	Active	-	~*	
EventTracker	Ē	0	Cybereason - Malop events		Jenish.r	Sep 11 10:55:18 AM	×		0	
RSA SecuriD	Û	1	Cybereason - Malware created or updated		jenish.r	Sep 11 07:13:35 PM	•		1	
Windows	Û	8	Cybereason -User action events		jenish.r	Sep 12 02:44:34 PM	×		Ø	
									Delete	Move to group



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.

cybereason	Q Q		Activate Now						Objects 🕀 ፒ 🏦 🌣	
Current	A 🧥 🗊	ON	ert name. Orkereason malon -	would a					A * *	
Cybereason		Object name Cybelesson malop events Applies to cybelversion								
Cybereason malop events Cybereason malware events	0 Î 1	Rub	25							
Cybereason user events	<i>i</i> 1		Title	Log type	Event source		Event id	Event type		
	V E	+	Cybereason malop event	ŝ	syslog*				⊘ ⊇ <u>n</u> 2 ,	
			Message Signature: Cyb	ereason\(.*?\ Malop\						
			Message Exception:							
			Expressions							
			Expression type	Expression 1		Expression 2	Format string			
			Column Delimiter	I			2:Vendor, 3:Product, 4:Product version	,5:Event class,6:Event name,7:Severity	🕑 🗓	
			Regular Expression	$(? < key > b[a-zA-Z]+b)=(? < Value > [^\s]+)$						
			Regular Expression	(c[sn][0-9]+)=(? <value>[^\s]*)\s\1Label=(?<key>[^</key></value>	\s]+)				☑	
			Regular Expression	(c[sn][0-9]+)Label=(? <key>[^\s]+)\s\1=(?<value>[^</value></key>	\\s]*)				🗵 🗹	



6.4 Flex Reports

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





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



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

Report Configuration 👘 / Reports / Re								
Scheduled Queued Defined			Search					
Report Groups 🕒 🔡	Reports configurat	ion: Cybereason				_		
🔁 Security	🕀 🗓 🔗			L.	otal: 6			
Compliance		Title	Created on	Modified on				
Operations	■ (\$)	Cybereason - User login failed activities	Sep 12 04:28:45 PM	Sep 12 04:28:45 PM	(j)	<u>a</u>	Ŧ	
🕀 Flex	□ ②	Cybereason - User login and logout activities	Sep 12 04:17:20 PM	Sep 12 04:17:20 PM	(i)	5	+	
🔁 ConnectWise 📋 🧭	• 🔅	Cybereason - Threat detected and updated details	Sep 11 07:25:24 PM	Sep 12 05:34:09 PM	()	8	+	
🕞 Cybereason 📋 🧭	. 🔅	Cybereason - Not mitigated threat details	Sep 11 07:19:59 PM	Sep 11 07:23:48 PM	(j)	<u></u>	+	
🕞 EventTracker		Cybereason - User malop investigation activities	Sep 11 06:14:20 PM	Sep 12 04:22:15 PM	()	5	+	
RSA SecuriD		Cybereason - Malop created or updated details	Sep 11 05:37:56 PM	Sep 12 02:26:36 PM	()	<i>[</i>]	+	
🔁 Windows 📗 🧭			1		Ū	-		

Figure 47

6.5 Category

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

≡	Event Tracker @				🔎 🛛 Admin 🗸	Tools ↓
	Home		Active Watch Lists	Event Filters	🧭 Parsing Rules	
٩			Alerts	Ventvault	Report Settings	_
	0	0	Behavior Correlation Rules	FAQ Tile Configuration	Systems	
			🗞 Behavior Correlation Settings	Group Management	QQ Users	
	Potential Cyber Breaches Unsafe connections or processes, new TCP ent	Indicators of Cor USB activities, New	Casebook Configuration	Q IP Lookup Configuration	1 Weights	orting Syste
		● Category	· Knowledge Objects	Windows Agent Config		
	Attacker	Diagnostics	Q Manager			



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

Category								🔒 / Admin / Categor
Category Tree Search	Category Detail	ls			Front Cotogon (No			
- All Categories	Cybereason				Cybereason - Use	er login and l	ogout details	
	Description							
	Applies to cybereasonversion				Lategory version			
Gereason - Malop events Gereason - Malop investigation events Gereason - Malop investigation events	Show In 🖉 O	perations 🔲 Compli	ance 🗷 Secu	ity				
Gybereason - Malware events Gybereason - Non-mitigated threats	Event Rule							Add Edit Delete
	Log Event Type Type	Event Category Id	Source Use	r Match in Description	Desc	cription eption	Lucene Query	
Cyberesson - User failed login details E Cyberesson - User login and logout details	0 0	D	syslog	Cybereason\ ,*?\ UserAction\ ,General\/(?:Login Logout).*? actionSuccess\s+c(?:s n)\d\=1			log_source:"Cybereason user events" AND log AND log_status:"1"	category:("Login" OR "Logout")
🖶 🔁 EventTracker								Save Cancel

