

Integration Guide

Integrate InQuest with EventTracker

Publication Date:

August 01, 2022

Abstract

This guide provides instructions to configure the Knowledge Packs in EventTracker to receive the logs from InQuest. The Knowledge Pack contains alerts, reports, dashboards, categories, and the knowledge object.

Scope

The configuration detailed in this guide is consistent with EventTracker version 9.3 or later and InQuest manager version 3.87.x or later.

Audience

This guide is for the administrators responsible for configuring the Knowledge Packs in EventTracker.



Table of Contents

1	Ov	erview	4								
2	Pre	erequisite	4								
3	Eve	tTracker Knowledge Packs4									
	3.1	Category	4								
	3.2	Alerts	4								
	3.3	Reports	5								
	3.4	Dashboard	6								
4	Imj	porting InQuest Knowledge Packs into EventTracker	8								
	4.1	Category	9								
	4.2	Alerts 1	.0								
	4.3	Token Template 1	1								
	4.4	Reports1	2								
	4.5	Knowledge Objects (KO)1	3								
	4.6	Dashboard1	.5								
5	Vei	rifying InQuest Knowledge Packs in EventTracker1	8								
	5.1	Category 1	.8								
	5.2	Alerts 1	.8								
	5.3	Token Template	9								
	5.4	Reports	0								
	5.5	Knowledge Objects (KO) 2	1								
	5.6	Dashboard 2	1								

1 Overview

InQuest focuses its analysis on identifying, processing, and inspecting files downloaded over the web or received via email to detect malicious code in transit. In addition to threat detection, InQuest encounters sensitive data in motion like confidential documents and personally identifiable information.

Netsurion facilitates monitoring events retrieved from the InQuest. The dashboard, category, alerts, and reports in Netsurion's threat protection platform, EventTracker, will benefit you in tracking possible attacks, suspicious activities, or any other threat noticed.

2 Prerequisite

- EventTracker version 9.3 or later must be installed and configured to receive logs.
- Configure InQuest to forward logs to EventTracker.

Note

Refer to <u>How-To</u> guide to configure InQuest to forward logs to EventTracker.

3 EventTracker Knowledge Packs

Configure categories and reports in EventTracker once the logs are available in EventTracker.

The following Knowledge Packs (KPs) are available in the EventTracker.

3.1 Category

InQuest - C2 engine: This category aids in finding and parsing the logs relevant to risky IP connections and DNS.

InQuest - Malware detection engine: This category aids in finding and parsing the logs related to the detection of potential malware on systems.

InQuest - Threat detection engine: This category aids in finding and parsing the logs related to risky SMTP transfers and malicious file attachments on emails.

3.2 Alerts

InQuest: Suspicious file detected: This alert gets triggered when the InQuest Malware detection engine detects a suspicious file with a high-risk score and a reasonably high Shannon entropy.

3.3 Reports

InQuest - Potential SMTP threats: This report provides details of emails or SMTP transfers that are potentially risky and may have malicious file attachments.

LogTime Source IP	Source por	t Destination IP	Destination port	t Severity	Risk score	Message	SMTP recipient	HTTP header	SMTP sender	File path	File type	File name	File MD5 hash	SHA1 hash	Shannon entropy
06-07-2022 07:07:22 AM 10.10.15.1	37957	192.168.30.144	25	8	1	HA_Email_Heade rs with None or									
06-07-2022 07:07:22 AM 10.10.15.1	22877	192.168.30.144	25	1	1	HA_Email_Heade									
06-07-2022 07:07:22 AM 10.10.15.1	60075	192.168.30.144	25	1	7	FC_PDF_Version _1_3	jack@contoso.co m	crs - security interest approved	noreply.crs@conto so.com	/opt/inquest/se nsors/c2b8b32 4-4c11-4202- 8087-	application/pdf	2022-492683.pdf	34c9196180508be 26b67e87eb4388e bb	7295fa8ace103a 611acbc3d6b130 b3fb80e2085b	7.131
06-07-2022 07:07:22 AM 10.10.15.1	16644	192.168.30.144	25	1	1	HA_Email_Heade rs with None or									
06-07-2022 07:07:22 AM 10.10.15.1	12661	192.168.30.144	25	1 0	1	HA_Email_Heade									
06-07-2022 07:07:24 AM 10.10.15.1	5 0077	192.168.30.144	25	1	1	FC_PDF_Version _1_3	anu@contoso.co m	crs - security interest approved	noreply.crs@conto so.com	o /opt/inquest/se nsors/c2b8b32 4-4c11-4202- 8087-	application/pdf	2022-492687.pdf	a219c61a7c2a60e ecd7269dba91f5a 00	12cba072202620 3a809d44231d48 0d7cb57606f2	7.131
06-07-2022 07:07:24 AM 10:10.15.1	60075	192.168.30.144	25	1	1	FC_PDF_Version _1_3	dave@contoso.co m	crs - security interest approved	noreply.crs@conto so.com	/opt/inquest/se nsors/c2b8b32 4-4c11-4202- 8087-	application/pdf	2022-492683.pdf	34c9196180508be 26b67e87eb4388e bb	7295fa8ace103a 611acbc3d6b130 b3fb80e2085b	7.131

InQuest - Malware and suspicious files: This report provides details related to potential malware on systems based on the InQuest Malware Detection Engine.

LogTime	Protocol	First detection			Destination IP	Destination port	Risk score	Shannon entropy	File path	File name	File type	File MD5 hash	SHA1 hash	SHA256 hash
06-06-2022 09:18:43 PM	smtp	May 16 2022 18:09:27 UTC	15406	10.164.233.243	192.168.30.144	25	10	6.129	/opt/inquest/sensors/c2 b8b324-4c11-4202- 8087-	Electronic form 05.16.2022 from	application/vn d.ms-excel	bf85ba636b07f62 4bb8e86601d122 0f9	25500cabff996a b31d602039989 8984d5612672f	40b992c809254620ab92e8b5 beaf9d08470bc512d8159167 5ee67498a6a1706d
06-06-2022 09:18:43 PM	smtp	May 16 2022 18:09:27 UTC	54815	10.212.219.24	192.168.30.144	25	* 10	6.129	/opt/inquest/sensors/c2 b8b324-4c11-4202- 8087- 7ac4629a7a23/files/202	Electronic form 05.16.2022 from Polic.gov.xls	application/vn d.ms-excel	bf85ba636b1d122 0f9	25500ca020399 898984d561267 2f	40b992c809254620a8159167 5ee67498a6a1706d
06-06-2022 09:18:43 PM	smtp	May 16 2022 18:09:27 UTC	54815	10.212.219.24	192.168.30.144	25	10	6.129	/opt/inquest/sensors/c2 b8b324-4c11-4202- 8087- 7ac4629a7a23/files/202	Electronic form 05.16.2022 from Polic.gov.xls	application/vn d.ms-excel	bf85ba636b07f62 4bb8e86601d122 0f9	25500cabff996a b31d602039989 8984d5612672f	40b992c809254620ab92e8b5 beaf9d08470bc512d8159167 5ee67498a6a1706d
06-06-2022 09:18:46 PM	smtp	May 16 2022 18:09:27 UTC	15406	10.164.233.243	192.168.30.144	25	10	6.129	/opt/inquest/sensors/c2 b8b324-4c11-4202- 8087- 7ac4629a7a23/files/202	Electronic form 05.16.2022 from Polic.gov.xls	application/vn d.ms-excel	bf85ba636b07f62 4bb8e86601d122 0f9	25500cabff996a b31d602039989 8984d5612672f	40b992c809254620ab92e8b5 beaf9d08470bc512d8159167 5ee67498a6a1706d
06-06-2022 09:18:46 PM	smtp	May 16 2022 18:09:27 UTC	54815	10.212.219.24	192.168.30.144	25	10	6.129	/opt/inquest/sensors/c2 b8b324-4c11-4202- 8087- 7ac4629a7a23/files/202	Electronic form 05.16.2022 from Polic gov xls	application/vn d.ms-excel	bf85ba636b07f62 4bb8e86601d122 0f9	25500cabff996a b31d602039989 8984d5612672f	40b992c809254620ab92e8b5 beaf9d08470bc512d8159167 5ee67498a6a1706d

InQuest - C2 engine detections: This report provides details of suspicious detections by the InQuest C2 engine.

LogTime	C2 category	C2 hit	Destination IP	Destination port	Source IP	Source port	Risk score
06-24-2022 04:33:24 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	53975	10
06-24-2022 04:33:24 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	52745	1 0
06-24-2022 04:33:24 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	53393	* 10
06-24-2022 04:33:24 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	56450	*1 0
06-24-2022 04:33:24 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	53426	1 0
06-24-2022 04:33:24 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	53521	*1 0
06-24-2022 04:33:24 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	56497	*1 0
06-24-2022 04:33:24 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	53422	* 10
06-24-2022 04:33:25 AM	C2_DNS_Alert	contoso.com	8.8.8.8	53	10.191.98.66	2891	* 10
06-24-2022 04:33:25 AM	C2_IP_Alert	192.168.98.124	192.168.30.114	22	192.168.98.14	16869	* 10
06-24-2022 04:33:25 AM	C2_IP_Alert	192.168.98.124	192.168.30.118	22	192.168.98.12	33772	*1 0
06-24-2022 04:33:25 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	52835	5
06-24-2022 04:33:26 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	56457	*1 0
06-24-2022 04:33:26 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	53336	*1 0
06-24-2022 04:33:26 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	54132	*1 0
06-24-2022 04:33:26 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	55970	*1 0
06-24-2022 04:33:26 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	52805	*1 0
06-24-2022 04:33:26 AM	C2_DNS_Alert	contoso.com	8.8.8.8	53	10.191.98.66	2891	* 10
06-24-2022 04:33:26 AM	C2_DNS_Alert	contoso.com	8.8.8.8	53	10.191.98.66	2891	*1 0
06-24-2022 04:33:26 AM	C2_DNS_Alert	contoso.com	8.8.8.8	53	10.191.98.66	2891	* 10
06-24-2022 04:33:26 AM	C2_DNS_Alert	contoso.com	8.8.8.8	53	10.191.98.66	2891	* 10

3.4 Dashboard



InQuest - Threats by geolocation: This dashlet displays the details of the active threat detected by InQuest based on the geolocation.

InQuest - Risky DNS connections by source: This dashlet displays the log information for risky DNS connections based on the Shannon entropy risk score.

Note

The higher the risk score, the higher the risk associated with a particular DNS connection.





InQuest - High risk events by priority: This dashlet displays the high-risk alert details detected by the malware detection engine.



InQuest - Risk assessment: This dashlet displays the average risk score of all the alerts associated with InQuest. The **Average** displays the average risk score of all the alerts, and the **Latest** displays the current risk score of the latest alert.

Note

A risk score above 8 must be reported.



InQuest - Risky domain and IP connections trend: This dashlet displays the risk status of the DNS and the IP alert traffic.



4 Importing InQuest Knowledge Packs into EventTracker

Import the InQuest Knowledge Pack items in the following sequence.

- Category
- Alerts
- Reports and templates
- Knowledge Objects
- Dashboards
- 1. Launch EventTracker Control Panel.
- 2. Double click Export-Import Utility and click the Import tab.





4.1 Category

1. In the **Import** tab, click **Category**, and then click the **Browse** button to locate the file.

3	Export Import Utility		x
Export Import Provide the path and fi Click the Import button Options Category Filters Alerts Systems and Groups Token Value Reports Behavior Correlation	e name of the Categories file. Use the '' button to browse and locate the import file.		
	Import	Clo	se

- 2. In the Browse window, locate the Categories_InQuest.iscat file and click Open.
- **3.** To import the categories, click **Import**.
- 4. EventTracker displays a success message on successfully importing the selected file in **Category**.



5. Click **OK** or the **Close** button to complete the process.



4.2 Alerts

1. In the **Import** tab, click **Alerts**, and then click the **Browse** button to locate the file.

ц. Э	Export Ir	nport Utility	-		х						
Export Import											
1. Provide the path and file name 2. Click the Import button.	e of the Alerts file. Use the '' butt	on to browse and locate the import file.									
Options	Location										
Category	 Import E-mail settings 										
⊖ Filters	Set Active Only if notifications set	This setting is applicable only for imports from Leg Alert files. For v7, the active status will be set bas	acy (v6x) ed on	cy (v6x) d on							
 Alerts 	 By default 	1.									
O Systems and Groups	roups Watchlist Configuration										
O Token Value	 Import Watchlist configurati This setting is applicable only f 										
O Reports	on the console where the alert	Valiable									
O Behavior Correlation											
	Source :										
	*.isalt										
			_								
		Import		Clos	e						

- 2. In the Browse window, locate the Alerts_InQuest.isalt file, and then click Open.
- **3.** To import the alerts, click **Import**.
- 4. EventTracker displays a success message on successfully importing the selected file in Alerts.



5. Click **OK** or the **Close** button to complete the process.

4.3 Token Template

1. In the EventTracker Web interface, hover over the Admin menu and click Parsing Rules.

		🔎 Admin v
Active Watch Lists	FAQ Tile Configuration	Manager
▲ Alerts	Group Management	MITRE ATT&CK Rules
Casebook Configuration	Q IP Lookup Configuration	🧭 Parsing Rules
Category	Knowledge Objects	Report Settings
Diagnostics	M Machine Learning Jobs	Systems
Event Filters	🐁 Machine Learning Settings	📿 Users
Eventvault	🄎 Manage API keys	The Weights

- 2. In the **Parsing Rules** interface, click the **Template** tab and then click the **Import Configuration I** button.
- 3. In the Import window, click Browse to search and locate for the Templates_InQuest.ettd file.
- 4. It takes few seconds to load the templates and once you see the list of templates, select the appropriate templates, and click **Import**.

Impo	rt						
select	ed file is: Templates_InQuest.ettd		🖆 Browse				
	Template name	Separator	Template description				
	InQuest C2	N	CEF:0 InQuest C2 Engine 1.0 100 C2_JP_Alert 10 cn3Label=vlan src=10.83.2 16.232 spt=443 dst=10.4.7.101 dpt=62978 cn3=0 msg=c2 hit: 10.83.216.2 32 cat=default policy cn1=10 cn1Label=Threat Score end=Nov 16 2020 0 4:34:49 UTC				
	InQuest MDE	N	CEF:0 InQuest mde 1.0 200 valyria 10 cd1Label=First Seen src=127.0.0.1 fl exString2=ef96ef23c0a71bd1beedd95ca44c61bf0726703b cn2=0 cn3=0 ileHash=7b93902926791f6ce56c9bc5efb59a99 filePath=/opt/inquest/sen sors/4d78db4a-2c437/files/20220211/01/6f-eb8d7f0ef4ba spt=0 fileType =application/vnd.ms-excel fsize=123904 cs1Label=AV Engine cn3Label= VLAN dpt=0 cd1=Feb 09 2022 06:44:52 UTC fname=PO 02.xls cn2Label=L nique Submissions msg=valyria sha256=bdd174dcc6dc046eeacf975c335 b849f8 cs1=InQuest MDE app=smtp dst=127.0.0.1 cn1=9 cn1Label=Threat t Score externalId=52887 cfp1=6.497 cfp1Label=File Entropy cs5=https:// 10.0.1.77/session/52 cs5Label=InQuest URL end=Feb 09 2022 06:44:52 UTC				
	InQuest TDE	M	Jun 24 01:40:37 10.101.102.108 Jun 24 01:40:57 acc-vm-xlmanager syslogg er[2274]: CEF:0 InQuest Threat Discovery Engine 3.91.57 100 Data Loss 5 fl exString1=??: ??? src=192.168.20.18 flexString2=7d07178fef312c7c5 sever ity=5 fileHash=ae9a86222697be5c08e6 filePath=/opt/inquest/sensors/2d be71fb-e0b2-41e80c/files/20220621/09/fbb5501b-8281-4359-a18e-9a8a da0ce4dd spt=48062 dst=10.47.18.202 fsize=4409297 fileType=applicati on/pdf cn3Label=VLAN flexString2Label=SHA1 flexString1Label=Subject dpt=25 fname=doc04692020220621090538.pdf suser=john@contoso.co				

5. EventTracker displays a success message on successfully importing the selected file in **Template**.

4.4 Reports

1. In the EventTracker Control Panel > Export-Import Utility > Import tab, click Reports, and then click New (*.etcrx).

9	Export Import Utility
Export Import 1. Provide the path and file nam 2. Click the Import button Note : if report(s) contains temping Options Category Filters Alerts Systems and Groups Token Value Reports Behavior Correlation 	e of Schedule Report file. Use the '' button to browse and locate the import file. ate, first import template and proceed with exportimport utility. Location C Legacy (*.issch) New (*.etcnx) Source : *
	Import Close

2. In the Reports Import window, click Select file to locate the Reports_InQuest.etcrx file.

te : If repo	Import ort(s) contains template, first import template and p	roceed with report import process.			
lect file	C:\Users\amishra\Desktop\Reports_InQuest.et	crx		Select file	
ailable rep	ports				
tle		Frequency Show all	- Q Q		
2	Title	Sites	Groups	Systems	Frequency
EDIT	InQuest - C2 engine detections				Undefined
	InQuest - Malware and suspicious files				Undefined
EDIT	InQuest - Potential SMTP threats				Undefined
Note: Set r Set run ti	run time option is not applicable for Defined Repo time for report(s) from	at interval of minute	ss Set		
Replace	to	Repl	ace Assign systems		
					· · · · · · · · · · · · · · · · · · ·



- **3.** Select the check box of all the files and click the **Import I** button to import the selected files.
- 4. EventTracker displays a success message on successful importing of the selected files in **Reports.**



5. Click OK or the Close button to complete the process.

4.5 Knowledge Objects (KO)

1. In the EventTracker Manager console, hover over the Admin menu and click Knowledge Objects.

≡	Event Tracker ⊕					Admin-	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
٩		_	Alerts	Correlation	🔍 IP Lookup Configuration	🛱 Users	_
	0	1	Behavior Correlation Rules	Diagnostics	💮 Knowledge Objects	r Weights	
			🗞 Behavior Correlation Settings	Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Co USB activities, New sen	Casebook Configuration	Seventvault	🧭 Parsing Rules		
				FAQ Configuration	Report Settings		
	Attacker		- News				

2. In the Knowledge Objects interface, click the Import I button as shown in the below image.

	Knowledge Obj	jects			🔶 / Admin / Y	Knowledge Objects
Q R	Search objects	Q	Q,	Activate Now	Object	s 🕀 耳 🏦 🌣
	Groups	🕀 🗭 🗓				Ĺ
	E Cylance					
	EventTracker					



3. In the Import window, click Browse and locate the KO_InQuest.etko file.

Import	×
Select file	vse Upload
	Close

4. Select the check box next to the browsed file, and then click the **Import** button.

Impoi	rt		×
Sele	ect file		🖆 Browse Upload
	Object name	Applies to	Group name
V	InQuest	InQuest Manager version 3.87.x and above	InQuest
			Import



5. EventTracker displays a success message on successfully importing the selected file in Knowledge Objects.

File imported successfully.
ОК

4.6 Dashboard

1. Log in to the EventTracker web interface and go to Dashboard > My Dashboard.

88	Home		
٩	My Dashboard		
R	Threats	1	
	Incidents	ntry point USB activities, New services or software install	
	Behavior Correlation		
	Change Audit		-
	Compliance		

2. In the My Dashboard interface, click the Import I button to import the InQuest files.

Event Tracker ⊕	Ç	Admin -	Tools -	💽 ETAdmin 🝷
My Dashboard		A	/ Dashboar	d / My Dashboard
		+	🧭 🎱 🌣	1 3 0

3. In the **Import** window, click **Browse** to locate the **Dashboards_InQuest.etwd** dashboard file, and then click **Upload**.



4. Select the **Select All** checkbox for all the dashlet files and click **Import** to import the InQuest dashlet files.

Import
Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.
🗁 Browse Upload
Available widgets Select All
✓ InQuest - Threats by geol ✓ InQuest - Risky DNS conne
✓ InQuest - High risk event ✓ InQuest - Risky domain an
✓ InQuest - Risk assessment
Import

5. The EventTracker displays a success message on successful import of the dashlet files.

Selected	I dashlets imported successfully.
	ОК

6. Then, in the My Dashboard interface, click the Add \oplus button to add the dashboard.





7. In the Edit Dashboard interface, specify the Title and Description and click Save.

Edit I	Dashboard
Title	
InQ	luest
Descr	ription
This	s dashboard has all the dashlets relevant to InQuest products.
	Save Delete Cancel

- 8. From the newly created dashboard interface (for example, InQuest), click the Configuration Solution to add the InQuest dashlets.
- 9. Search and select the newly imported dashlets and click Add.

Customize dashlets			×
Inquest			Q
✓ InQuest - High risk events by pri	☑ InQuest - Risk assessment	✓ InQuest - Risky DNS connection	✓ InQuest - Risky domain and IP c
✓ InQuest - Threats by geolocation			
			Add Delete Close



5 Verifying InQuest Knowledge Packs in EventTracker

5.1 Category

1. In the EventTracker web interface, hover over the Admin menu and click Category.

≡	Event Tracker ⊕					🔶 🗚 Admin-	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
q		_	Alerts	C Correlation	🔍 IP Lookup Configuration	QQ Users	
	0	1	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	T Weights	
			🗞 Behavior Correlation Settings	⊽ Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Co USB activities, New sen	Casebook Configuration	C Eventvault	🧭 Parsing Rules		
			oe Category	FAQ Configuration	Report Settings		
	Attacker			- News			

2. In the **Category** interface, under the **Category Tree** tab, click the **InQuest** group folder to expand and see the imported categories.

Category Tree	Search
InQuest	ne
🔤 InQuest - Malware	edetection engine
🛄 InQuest - Threat d	etection engine

5.2 Alerts

1. In the EventTracker web interface, hover over the Admin menu and click Alerts.

	Event Tracker ⊕					🔎 🗚 Admin-	Tools +
	Home		E Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dasht
•			Alerts	Correlation	Q IP Lookup Configuration	QQ Users	
	0	2	Behavior Correlation Rules	A Diagnostics	· Knowledge Objects	∯ Weights	
~			🗞 Behavior Correlation Settings	🗟 Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Co USB activities, New sen	Casebook Configuration	Eventvault	🧭 Parsing Rules		
			● Category	FAQ Configuration	Report Settings		
	Attacker			- News			1

2. In the Alerts interface, type InQuest in the search field, and click the Search Search button.



3. The Alerts interface will display all the imported InQuest alerts.

⊕ <u>∭</u>	Activate Now	Click 'Activate Now' after making all changes		
		Alert Name 🔨	Threat	Active
🗌 ဇို့နို InQuest	: Suspicious file detec	ted	•	

- **4.** To activate the imported alert, click to toggle the **Active** switch, which is available next to the respective alert name.
- 5. EventTracker displays success message on successfully configuring the alert.

Succes	sfully saved configuration.
Prevent this part of the pa	age from creating additional dialogs
	ОК

6. Click OK and click Activate now to activate the alerts after making the required changes.

Note

You can modify the required alert separately, and select the respective alert name check box, and then click **Activate Now** to save the alert modifications.

Note

In **Alert configuration** interface, select the appropriate **System** name for better performance.

5.3 Token Template

1. In the EventTracker web interface, hover over the Admin menu and click Parsing Rules.

		🔎 🛛 Admin 🚽
Active Watch Lists	FAQ Tile Configuration	Manager
Alerts	Group Management	MITRE ATT&CK Rules
Casebook Configuration	Q IP Lookup Configuration	🕖 Parsing Rules
Category	Knowledge Objects	Report Settings
1 Diagnostics	M Machine Learning Jobs	Systems
Event Filters	👆 Machine Learning Settings	QQ Users
Eventvault	🏓 Manage API keys	Heights

2. Go to the **Template** tab and click the **InQuest** group folder to view the imported Token template.

5.4 Reports

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

	Event Tracker ⊕			
	Home			
٩		_	1	
k	Report Configuration		1	
	Report Dashboard	ntry point	Indicators of Compromise USB activities, New services or software install	
	Explorer AttacKer			_

2. In the **Report Configuration** interface, click **Defined**.

Report Configuration	
○ Scheduled ○ Queued Defined	

- 3. In the search field, type **InQuest** and click **Search** to search for the InQuest files.
- 4. EventTracker displays the reports for InQuest.

Repo	orts configura	ation: InQuest
Ð	Ü ∂,	
		Title
	2	InQuest - Potential SMTP threats
	£\$3	InQuest - Malware and suspicious files

5.5 Knowledge Objects (KO)

1. In the EventTracker web interface, hover over the Admin menu and click Knowledge Objects.

≡	Event Tracker ⊕					🐥 🛛 Admin-	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
٩			Alerts	C Correlation	🔍 IP Lookup Configuration	였 Users	_
	0	1	Behavior Correlation Rules	A Diagnostics	·@- Knowledge Objects	r Weights	
			🗞 Behavior Correlation Settings	🐨 Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	Seventvault	Parsing Rules		
		_	o-[o Category	FAQ Configuration	Report Settings		
	Attacker			 News 			

2. In the Knowledge Object interface, under Groups tree, expand the InQuest group to view the imported Knowledge objects.

InQuest		
InQuest	Ø	Ē

3. Click Activate Now to apply the imported Knowledge Objects.

5.6 Dashboard

1. In the EventTracker web interface, go to Home > My Dashboard.

	Home
Dashb	My Dashboard
Å	Threats
	Incidents

2. The My Dashboard interface displays all the dashlets related to InQuest.





About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's managed cybersecurity platforms enable companies to deliver on both. Netsurion <u>Managed</u> <u>Threat Protection</u> combines our ISO-certified security operations center (SOC) with our own award-winning cybersecurity platform to better predict, prevent, detect, and respond to threats against your business. Netsurion <u>Secure Edge Networking</u> delivers our purpose-built edge networking platform with flexible managed services to multi-location businesses that need optimized network security, agility, resilience, and compliance for all branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit <u>netsurion.com</u> or follow us on <u>Twitter</u> or <u>LinkedIn</u>.

Contact Us Corporate Headquarters

Netsurion Trade Centre South 100 W. Cypress Creek Rd Suite 530 Fort Lauderdale, FL 33309

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2) EventTracker Enterprise for MSPs SOC: 877-333-1433 (Option 3) EventTracker Essentials SOC: 877-333-1433 (Option 4) EventTracker Software Support: 877-333-1433 (Option 5) https://www.netsurion.com/eventtracker-support