



Integration Guide

Integrate Azure Data Factory with EventTracker

Publication Date:

September 26, 2022

© Copyright Netsurion. All Rights Reserved.



Abstract

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

Scope

The configuration details in this guide are consistent with EventTracker version 9.3 or later and Azure Data Factory.

Audience

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



Table of Contents

1	Ove	erview	4
2	Pre	requisite	4
3	Eve	entTracker Knowledge Packs	4
	3.1	Alerts	4
	3.2	Categories	4
	3.3	Reports	5
	3.4	Dashboard	5
4	Imp	oorting Azure Data Factory Knowledge Packs into EventTracker	7
	4.1	Category	8
	4.2	Alerts	9
	4.3	Token Template1	0
	4.4	Reports 1	1
	4.5	Knowledge Objects (KO)1	2
	4.6	Dashboard 1	4
5	Ver	rifying Azure Data Factory Knowledge Packs in EventTracker1	7
	5.1	Category1	7
	5.2	Alerts1	7
	5.3	Token Template1	8
	5.4	Reports 1	9
	5.5	Knowledge Objects (KO)1	9
	5.6	Dashboard 2	0



1 Overview

Azure Data Factory is a cloud-based data integration service used to create data-driven workflows in the cloud for orchestrating and automating data movement and transformation. It also helps to monitor and manage workflows using both programmatic and UI mechanisms.

Netsurion facilitates monitoring events retrieved from the Azure Data Factory. The dashboard, category, alerts, and reports in Netsurion's threat protection platform, EventTracker, benefit 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 Azure Data Factory to forward logs to EventTracker.

Note

Refer to <u>How-To</u> guide to configure Azure Data Factory to forward logs to EventTracker.

3 EventTracker Knowledge Packs

After the logs are received by the EventTracker Manager, configure the Knowledge Packs into EventTracker.

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

3.1 Alerts

Azure Data Factory: Potential exfiltration detected: This alert is triggered when data transfer contains a large payload.

Azure Data Factory: Service interruption detected: This alert is triggered when a network is disrupted or if there is a DNS failure.

Azure Data Factory: Unauthorized access attempt: This alert is triggered when multiple attempts made to establish connection with data factory without proper credentials.

3.2 Category

Azure Data Factory - Activities summary: This category of the saved search allows you to parse events that are specific to the pipeline activities for Azure Data Factory.

Azure Data Factory - SSIS integration runtime summary: This category of the saved search allows you to parse events that are specific to the SQL server integration service activities for Azure Data Factory.



3.3 Reports

Azure Data Factory - Activities summary: This report provides a detailed summary of pipeline activities in Azure Data Factory. The report includes the activity type, data source, destination, error type, error message, and more.

LogTime	Client IP	Host	User Agent	InstanceID	Http Method	Http Version	Client Port	Http Status
06-22-2022 05:05:33 AM	10.207.204.44	vgw098	MozillaV5.0 (Windows NT 6.1; WOW6	appgw_2	PUT	HTTPV1.1	51886	404
06-22-2022 05:05:34 AM	10.2.2.13	appgw009	NetSystemsResearch studies the avai	appgw_5	DELETE	HTTP/1.1	37408	200
06-22-2022 05:05:34 AM	10.20.2.139	vgw098	MozillaV5.0 (Windows NT 6.1; WOW6	appgw_4	PUT	HTTPV1.1	51886	404
06-22-2022 05:05:34 AM	10.2.56.36	appgw009	NetSystemsResearch studies the avai	appgw_3	DELETE	HTTP/1.1	37408	200
06-22-2022 05:05:35 AM	192.168.155.102	vgw098	MozillaV5.0 (Windows NT 6.1; WOW6	appgw_13	PUT	HTTPV1.1	51886	404
06-22-2022 05:05:35 AM	10.55.53.144	10.55.53.144	Mozilla/5.0+(Windows+NT+10.0;+Win	ApplicationGatewayRole_	DELETE	HTTP/1.1	37408	200
06-22-2022 05:05:35 AM	192.168.162.27		NetSystemsResearch studies the avai	appgw_25	POST	HTTPV1.1	60929	402
06-22-2022 05:05:35 AM	192.168.161.37	appgw009	NetSystemsResearch studies the avai	i appgw_1	GET	HTTPV1.1	60929	502

Azure Data Factory – SSIS integration runtime summary: This report provides a detailed summary of SQL server integration services runtime activities in Azure Data Factory. The report includes the source component, destination component, package name, package path. and more.

LogTime	TransactionId	Client IP	Client Port	Hostname	Requested URI	Requested Query	RuleID	Rule Type	Rule Version	Message
06-22-2022 05:05:35 AM	0a830da0e1da0d5f6b268deb0bce3152	192.168.155.102	51886	vm000003	V	AzureApplicationGateway-CACHE-HIT	942150	OWASP_CRS	3.0	SQL Injection Attack: SQL Tautology Detected
06-22-2022 05:05:35 AM	16861477007022634343	10.55.53.144	37408	vm000004	٨	AzureApplicationGateway-CACHE-HIT	920350	OWASP	3.0	SQL Injection Attack: SQL Tautology Detected.
06-22-2022 05:05:35 AM	c6d4051cd01960334279f645b2a6be1b	192.168.162.27	60929	vm000003	V	AzureApplicationGateway-CACHE-HIT	942150	OWASP_CRS	3.0	SQL Injection Attack: SQL Tautology Detected.
06-22-2022 05:05:35 AM	c6d4051cd01960334279f645b2a6be1b	192.168.161.37	60929	vm000004	V	AzureApplicationGateway-CACHE-HIT	920350	OWASP	3.0	SQL Injection Attack: SQL Tautology Detected.
06-22-2022 05:05:35 AM	AcAcAcAcAKH@AcAcAcAcAyAt	31.58.237.148	17270	vm000003	1	AzureApplicationGateway-CACHE-HIT	942150	OWASP_CRS	3.0	SQL Injection Attack: SQL Tautology Detected
06-22-2022 05:05:36 AM	AcAcAcAcAKH@AcAcAcAcAyAt	192.168.248.32	59338	vm000004	1	AzureApplicationGateway-CACHE-HIT	920350	OWASP	3.0	SQL Injection Attack: SQL Tautology Detected.
06-22-2022 05:05:36 AM	0a830da0e1da0d5f6b268deb0bce3152	10.14.248.32	59338	vm0002	1	AzureApplicationGateway-CACHE-HIT	920350	OWASP	3	Host header is a numeric IP address
06-22-2022 05:05:37 AM	16861477007022634343	10.168.10.147	0	127.0.0.1	1	AzureApplicationGateway-CACHE-HIT	920350	OWASP	3.0	Host header is a numeric IP address
06-22-2022 05:05:37 AM	16861477007022634343	10.161.109.147	.0	127.0.0.1	1	AzureApplicationGateway-CACHE-HIT	920350	OWASP	3.0	Host header is a numeric IP address

3.4 Dashboard

Azure Data Factory - Failed events by activities: This dashlet displays the failed activities of the request made to access the data factory.





Azure Data Factory - Failed SSIS IR activities: This dashlet displays the failed activities made to data factory.



Azure Data Factory - Failed SSIS package execution: This dashlet displays the failed package execution in SQL server integration services.





Azure Data Factory - Failed events by error codes: This dashlet displays the error codes of the failed events along with data source and destination.

Azure Data Factory	- Failed ev	vents by error codes	0) (; - x
application_category	dest_path	src_device_name	threat_info	Count
load files	databricks	azureblobstoragereadsettings	2505	1
load files	databricks	azureblobstoragereadsettings	2711	1
load files	databricks	azureblobstoragereadsettings	3251	1
load files	databricks	azureblobstoragereadsettings	sftpauthenticationfailur	re 1

4 Importing Azure Data Factory Knowledge Packs into EventTracker

Import the Knowledge Pack items in the following sequence.

- Categories
- Alerts
- Token Template
- Reports
- Knowledge Objects
- Dashboards
- 1. Launch the 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.

Ч У	Export Import Utility	-		x
Export Import				
1. Provide the path and file nam 2. Click the Import button.	e of the Categories file. Use the '' button to browse and locate the import file.			
Options	Location			
 Category 				
○ Filters				
⊖ Alerts				
O Systems and Groups	Source :			
O Token Value				
O Reports				
O Behavior Correlation				
	Import		Close	•

- 2. In the Browse window, locate the Categories_Azure Data Factory.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.

<u>ц</u>	Export Ir	nport Utility		-		x
Export Import						
1. Provide the path and file name 2. Click the Import button.	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 import Alert files. For v7, the active status will b	s from Legacy be set based c	(v6x) on		
 Alerts 	 By default 	"Active" key available in the configurat	ion section.			
 Systems and Groups 	Watchlist Configuration					
O Token Value	Import Watchlist configuration	on				
O Breata	I his setting is applicable only f Note: If this option is enabled t	or alerts which have Advanced watchlist of ne user should make sure the watchlist group are imported.	configured. oups are avail	able		
	on the console where the alert	are imported.				
 Behavior Correlation 						
	Source :					
	*.isalt					
			Import		Clos	e

- 2. In the Browse window, locate the Alerts_ Azure Data Factory.isalt file, and then click Open button.
- **3.** To import the alerts, click the **Import** button.
- 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 Manager console, hover over the Admin menu and click Parsing Rules.

	🔎 Admir	n ↓ Tools ↓
ers	😥 Parsing Rules	† /
lt Contain	s set of rules which tell what kin	d of data you want
Configuration	Systems	

2. In the Parsing Rules interface, click the Template tab and then click Import Configuration.

Parsing Rules			🔶 / Admin / Parsing Rules
Parsing Rule Template			
Groups	+	Group :	C 1 I
Default	Î	Tranch	Import configuration
Azure Intune	0	Templa	Active

- **3.** In the **Import** window, click **Browse** to search and locate for the file name with **".ettd"** extension (example, **Templates_Azure Data Factory.ettd**).
- **4.** It takes few seconds to load the templates and once you see the list of templates, click the appropriate templates, and click **Import**.

Import	
Select file	🗁 Browse
Note: Pleas	e select file of type *.ettd (eventtracker template dashlets).

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

Template(s) imported successfully	
	ОК



4.4 Reports

1. In the Import tab, click **Reports** and then click **New (*.etcrx)**.

4	Export Import Utility	-		x
Export Import	Export Import Utility me of Schedule Report file. Use the '' button to browse and locate the import file. Date, first import template and proceed with exportimport utility. Location Legacy (*issch) New (*.etcx) Source : *issch			x
	Import		Clos	e

2. In the **Reports Import** window, click **Select file** to locate **Reports_Azure Data Factory.etcrx** file.

Conception of the product of th	Stars time option is not applicable for Defred Reports and Hourly Reports Admin for report(s) from Admin + at interval of maintees Set	Tible Sites Groups Systems Propare Abure Data Factory - Attivity summary Undefined Undefined Solt Abure Data Factory - SSIS integration r Undefined Solt Abure Data Factory - SSIS integration r Undefined	due reporte	free area Store of			
e Set out time option is not applicable for Colored Reports and Houly Reports	Accer Data Factory - Activity summary Undefined Exit: Accer Data Factory - SSIS integration r Undefined Cat out time option is not applicable for Defined Reports and Hourly Reports run times for report(s) from Integration of and the interval of Integrates Set D	Access Data Factory - Addrey summary Undefined EDIX Access Data Factory - SSIS integration r Undefined Undefined Undefined Undefined Ext sum time ration is not applicable for Defined Reports and Houty Reports Image: Address Set Image: Address Set Lace to Reprinte Access Set Image: Access A	TBle	Sites	Groups	Systems	Frequenc
EXX (Adure Data Factory - 5313 integration f (Underne	Set on the option is not applicable for Defred Reports and Houry Reports non time for report(s) from AM * at interval of maintages	Ext: Adver Data Hactory - Solds integration if Undervice Ext: Adver Data Hactory - Solds integration if Undervice Ext: Adver Data Hactory - Solds integration if Undervice Ext: Adver Data Hactory - Solds integration if Undervice Ext: Adver Data Hactory - Solds integration if Undervice Ext: Adver Data Hactory - Solds integration if Undervice Ext: Adver Data Hactory - Solds integration if Undervice Ext: Adver Data Hactory - Solds integration if Undervice Ext: Adver Data Hactory - Solds integration if Ext: Ext: Adver Data Hactory - Solds integration if Ext: Ext: Adver Data Hactory - Solds integration if Ext: Ext: Adver Data Hactory - Solds integration if Ext: Ext: Adver Data Hactory - Solds integration if Ext: Ext: Adver Data Hactory - Solds integration if Ext: Ext: Adver Data Hactory - Solds integration if Ext: Ext: Adver Data Hactory - Solds integration if Ext: Ext: Adver DataHactory - Solds integrati	LOT Asure Data Factory - Activity summary				Undefined
Set run time option is not applicable for Ordinad Reports and Houry Reports	(Set out time option is not applicable for Defined Reports and Hourly Reports nan times for report(s) from AM * at interval of maintales Set	Set run time option is not applicable for Celored Reports and Houry Reports nan time for report(s) from AM * at informal of animates Lace to Repire Reports and Houry Reports					
Set we take option is not applicable for Defined Reports and Houry Reports	(Set out time option is not applicable for Defred Reports and Hourly Reports num times for report(s) from AM * at interval of minutes Set	Set sun time option is not applicable for Cellned Reports and Houly Reports nan time for report(s) from AM * at interval of minutes face to Replace					
Stat up the option is not applicable for Cafned Reports and Houly Reports	Set un time option is not applicable for Defined Reports and Hourly Reports num times for report(s) from AM * at interval of minutes	Set run time option is not applicable for Colored Reports and Houry Reports nan time for report(s) from AM * at interval of minutes for Reprise					
Set out tree option is not applicable for Codined Reports and Houly Reports	Set num time option is not applicable for Cellned Reports and Houly Reports nan time for respont(a) from AM at interval of minutes	Set run time option is not applicable for Defined Reports and Hourly Reports num time for report(a) from AM * at interval of minutes tace to Replace					
Ser cun time option is not applicable for Defined Reports and Hourly Reports	Set can time option is not applicable for Calined Reports and Houly Reports an time for report(p) from AM - at interval of minutes	Set run tone option is not applicable for Collevel Reports and Houly Reports un times for respont(p) from AM = at interval of minutes sce to Region: Ansyn systems					
In success registers a not applicable for Certined Reports and Hourly Reports	iet sun time option is not applicable for Cellned Reports and Houly Reports in time for resport(p) from AM * at interval of minutes 5rt	let un time option is not applicable for Defined Reports and Hourly Reports in times for resport(s) from AM * at interval of minutes Set ce to Replace					
t sur time option is not applicable for Catheol Reports and Houty Reports	t run time option is not applicable for Defined Reports and Hourly Reports times for report(s) fromAM * at interval ofminutes 5rt	fruit time option is not applicable for Defined Reports and Hourly Reports times for report(ju) from AM * at interval of minutes m for Reports Reports					
Set run time option is not applicable for Defined Reports and Houdy Reports	Set run time option is not applicable for Defined Reports and Hourly Reports an time for report(a) from AM * at interval of minutes Set	Set run time option is not applicable for Defined Reports and Hourly Reports an time for respont(a) from AM × at interval of minutes Set co to Regime. Assign systems					
Set out two option is not applicable for Defined Reports and Hourly Reports	Set run time option is not applicable for Cellned Reports and Houly Reports nan time for respont(p) from AM = at interval of minutes	Set sur time option is not applicable for Collined Reports and Houty Reports nan time for report(p) from AM × at interval of minutes 5tt tace to Replace Assign systems					
Set run time option is not applicable for Cafined Reports and Houly Reports	Set our time option is not applicable for Selfned Reports and Hourly Reports nan time for respon(s) from AM * at interval of minutes	Set run time option is not applicable for Cellned Reports and Houry Reports nun times for report(s) from AM * at interval of minutes lace to Replace					
Set run time option is not applicable for Calined Reports and Houly Reports	(Set run time option is not applicable for Cellned Reports and Hourly Reports nan time for respon(s) from AM * at interval of minutes	Set on time option is not applicable for Cellined Reports and Houly Reports nan time for report(s) from AM × at interval of minutes tace to Replace					
Set run time option is not applicable for Cafined Reports and Houly Reports	Set run time option is not applicable for Setined Reports and Hourly Reports nan time for respon(s) from AM * at interval of minutes	Set run time option is not applicable for Cellned Reports and Hourly Reports nun time for report(a) from AM * at interval of minutes 5H lace to Replace Assign systems					
Set run time option is not applicable for Calined Reports and Houly Reports	(Set run time option is not applicable for Defined Reports and Hourly Reports nan time for report(s) from AM * at interval of minutes	Set run time option is not applicable for Cellned Reports and Houty Reports nan time for report(s) from AM × at interval of minutes lace to Replace Assign systems					
Set run time option is not applicable for Celfred Reports and Houly Reports	Set run time option is not applicable for Sefred Reports and Hourly Reports nan time for report(a) from AM * at interval of minutes	Set run time option is not applicable for Cellned Reports and Houty Reports num times for report(p) fromAM * at interval ofminutes lacetoRepiaceRepinystems					
Set run time option is not applicable for Cellined Reports and Houly Reports	Set run time option is not applicable for Cellned Reports and Hourly Reports num time for report(s) from AM * at interval of minutes Set	Set run time option is not applicable for Defined Reports and Hourly Reports num time for report(s) from AM = at interval of minutes lace to ReplaceRepring					
Set run time option is not applicable for Cellined Reports and Houly Reports	Set run time option is not applicable for Sefred Reports and Houly Reports nan time for report(a) from AM * at interval of minutes	Set run time option is not applicable for Cellned Reports and Houty Reports num time for report(p) from AM + at interval of minutes lace toReplaceReplace					
Set run time option is not applicable for Cellined Reports and Hourly Reports	Set run time option is not applicable for Cellned Reports and Hourly Reports num time for report(s) from AM - at interval of minutes Set	Set run time option is not applicable for Defined Reports and Houry Reports nun time for report(s) from AM * at interval of minutes lace to Replace					
Set run time option is not applicable for Carlined Reports and Hourly Reports	Set run time option is not applicable for Cellned Reports and Houly Reports Internations for responsive from AM * at interval of minutes	Set sun time option is not applicable for Cellned Reports and Houty Reports nun time for report(p) from AM * at interval of minutes Set acce to Replace					
Set run time option is not applicable for Cellined Reports and Houly Reports	Set run time option is not applicable for Defined Reports and Hourly Reports num time for report(s) from AM + at interval of minutes Set	Set run time option is not applicable for Defined Reports and Hourly Reports nun time for report(s) from AM * at interval of minutes 5st acce to Replace Assign systems					
Set run time option is not applicable for Cellined Reports and Hourly Reports	Set run time option is not applicable for Cellned Reports and Hourly Reports num time for report(s) from AM * at interval of minutes Set	Set run time option is not applicable for Defined Reports and Houty Reports num time for report(s) from AM * at interval of minutes lace to ReplaceReplace					
Set run time option is not applicable for Defined Reports and Hourly Reports	Set run time option is not applicable for Cellined Reports and Houly Reports num time for report(s) from AM + at interval of minutes Set	Set sur time option is not applicable for Cellined Reports and Houty Reports nan time for report(s) from AM * at interval of minutes lace toReplaceReplace					
Set run time option is not applicable for Defined Reports and Houly Reports	Set run time option is not applicable for Defined Reports and Hourly Reports num time for report(s) from	Set run time option is not applicable for Celned Reports and Hourly Reports num time for report(s) from AM * at interval of minutes lace to ReplaceRespin systems					
Set run time option is not applicable for Defined Reports and Hourly Reports	Set will tree option is not applicable for Defined Reports and Houry Reports num time for report(s) from AM + ot interval of minutes	Set sur time option is not applicable for Cellined Reports and Houty Reports nun time for report(s) from AM * at interval of minutes. Set lace to ReplaceAssign systems					
Set run time option is not applicable for Defined Reports and Hourly Reports	Set sur time option is not applicable for Defined Reports and Hourly Reports nun time for report(s) from AM * at interval of minutes Set	: Set un time option is not applicable for Defined Reports and Hourly Reports nun time for report(s) from AM * at interval of minutes lace toReplaceReplace					
	nun time for report(s) from AM + at interval of minutes Set	nun time for report(s) from AM + at interval of minutes 5rt Asce to Replace Assyn systems					
	tun time for report(s) from An * at interval of minutes on U	lace to Replace Assign systems	Set run time option is not applicable for Defined Re	ports and Hourly Reports			
and time for monthly from 111 x of interest of 111 x 11		lace to Replace Assign systems	Set run time option is not applicable for Defined Re	ports and Houty Reports			
		Topass Topass	Set run time option is not applicable for Defined Fir run times for respon(a) from AM	ports and Houty Reports • at interval of minutes	5 5 D		
	Barlana Assim sutana		Set run time option is not applicable for Colored Re run time for report(a) from AM	ports and Houty Reports * at interval ofminutes	54 O		
		The big on the first fir	Set not tree option is not applicable for Defined Re un time for report(a) from AM	ports and Houdy Reports • at Interval ofmemutes	- 54 O		



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



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
Q			Alerts	Correlation	🔍 IP Lookup Configuration	🛱 Users	_
	0	1	Behavior Correlation Rules	Diagnostics	·@ Knowledge Objects	T Weights	
			🇞 Behavior Correlation Settings	対 Event Filters	Manager	🔲 Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	USB activities, New sen	Casebook Configuration	Seventvault	Parsing Rules		
			● Category	FAQ Configuration	Report Settings		
	Attacker			 News 			

2. In the Knowledge Objects interface, click the Import \blacksquare button to import the KO files.

	Knowledge Obj	iects		🕈 / Admin / Knowledge Objects
Q 	Search objects	Q	Q Activate Now	Objects 🕀 📳 🏦 🌣
	Groups	🕀 🗭 🗓		Î
	Cylance			
	• EventTracker			



3. In the **Import** window, click **Browse** and locate the **KO_ Azure Data Factory.etko** file.

Import		×
Select file	🖆 Browse Upload	
	Clo	ose

4. Select the check box next to the browsed KO file and then click the \mathbb{T} Import button.

Import	t		×
Selec	t file		🗁 Browse Upload
	Object name	Applies to	Group name
	Azure Data factory	Azure Data factory	Microsoft Azure
			Import Close



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



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

4.6 Dashboard

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

	Home		
٩	My Dashboard		
R	Threats	1	
	Incidents	Indicators of Compromise 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 dashlet files.



3. In the Import window, click Browse to locate the Dashboards_ Azure Data Factory.etwd file and then click Upload.



4. Select the **Select All** checkbox to select all the dashlet files and click **Import** to import the selected dashlet files.

Note: If dashlet configured using a	persisted report first import the report and proceed with imp	orting
dashlet.	bersisted report, inst import the report and proceed with imp	orting
	🗁 Browse	Upload
Available widgets		
Select All		
Azure Data Factory - Fail	Azure Data Factory - Fail	
Azure Data Factory - Fail	Azure Data Factory - Fail	

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



6. Then, in the My Dashboard interface click on the Add ⊕ button to add dashboard.





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

dit Dashboard				
Title				
Azure Data Factory				
Description				
Azure Data Factory				
		Save	Delete	Cancel

- From the newly created dashboard interface (for example, Azure Data Factory), click the Configuration Sutton to add the Azure Data Factory dashlets.
- 9. Search and select the newly imported dashlets and click Add.

Cı	ustomize dashlets				×
	azure data factory				Q
	Azure Data Factory - Failed Acti	Azure Data Factory - Failed SSIS	Azure Data Factory - SSIS IR acti		
				Add Delete	Close



5 Verifying Azure Data Factory 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
٩	·		Alerts	C Correlation	🔍 IP Lookup Configuration	QQ 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 Co USB activities, New sen	Casebook Configuration	Eventvault	🧭 Parsing Rules		
			el [®] Category	FAQ Configuration	Report Settings		
	Attacker			 News 			

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

Category Tree	Search	
Microsoft A	Azure Data Factory - Activities summary Data Factory - SSIS integration runtime s	ummary

5.2 Alerts

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

≡	Event Tracker ⊕					🔎 🛛 Admin-	Tools +
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dasht
a		_	Alerts	Correlation	🔍 IP Lookup Configuration	QQ Users	
	0	2	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	♠ Weights	
~			🇞 Behavior Correlation Settings	🐨 Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	USB activities, New sen	Casebook Configuration	Seventvault	🧭 Parsing Rules		
			● Category	FAQ Configuration	Report Settings		
	Attacker			 News 			

2. In the Alerts interface, type Azure Data Factory in the Search field and click the Search button.



3. The Alerts interface will display all the imported Azure Data Factory alerts.



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

Successfully saved configu	ration. dditional 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 the Alert Configuration interface, specify the appropriate System for better performance.

5.3 Token Template

- 1. In the EventTracker web interface, hover over the Admin menu and click Parsing Rules.
- 2. Go to the **Template** tab and click the **Azure Data Factory** 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**.

EventTracker					
	Home				
Q 	 Report Configuration		1		
	Report Dashboard	ntry point	Indicators of Compromise USB activities, New services or software install		
	Explorer Attacker			-	

- 2. In the Reports Configuration interface, select the Defined option.
- 3. In the search field, type Microsoft Azure and click Search to search for the Azure Data Factory files.
- 4. EventTracker displays the reports for Azure Data Factory.

Reports configuration: Microsoft Azure			
Ð	İ 2,		
		Title	
	€3	Azure Data Factory - SSIS integration runtime summary	
	2	Azure Data Factory - Activity summary	

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	Q IP Lookup Configuration	였 Users	
	0	1	Behavior Correlation Rules	1 Diagnostics	· Knowledge Objects	The 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, click the Microsoft Azure group to expand and view the imported Knowledge objects.



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

5.6 Dashboard

1. In the EventTracker console, go to Home > My Dashboard, and click the Customize dashlets.

		Home
Dashb	oard	My Dashboard
Å		Threats
		Incidents

- 2. In the **Customize dashlets** interface, search for **Azure Data Factory** in the search field.
- 3. The following Azure Data Factory dashlet files will get displayed

×
2



About Netsurion

Netsurion[®] delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's managed offering includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers Managed Threat Protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection and Response (MDR) and a Top 25 Global MSSP. Learn more at <u>netsurion.com</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