Netsurion. EventTracker*

Integrate Heroku

EventTracker v9.3 and above

Publication Date: February 22, 2021

Abstract

This guide helps you in configuring **Heroku** with EventTracker to receive **Heroku** events. In this guide, you will find the detailed procedures required for monitoring **Heroku**.

Scope

The configuration details in this guide are consistent with EventTracker version v9.3 or above and Heroku.

Audience

Administrators, who are assigned the task to monitor and manage Heroku events 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.

© 2021 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.	Ov	erview	. 3
2.	Pre	erequisites	. 3
3.	Int 3.1	egrating Heroku with EventTracker EventTracker uses syslog drain to receive logs from Heroku	. 3 . 3
	3.2	System Licensing	. 4
4.	Eve 4.1	entTracker Knowledge Pack Category	. 7 . 7
	4.2	Alert	. 7
	4.3	Report	. 7
	4.4	Dashboards	. 9
5.	Im	porting Heroku knowledge pack into EventTracker	13
	5.1	Category	14
	5.2	Alert	15
	5.3	Knowledge Object	16
	5.4	Report	18
	5.5	Dashboards	19
6.	Ve	rifying Heroku knowledge pack in EventTracker	22
	6.1	Category	22
	6.2	Alert	22
	6.3	Knowledge Object	23
	6.4	Report	24
	6.5	Dashboards	25

1. Overview

Heroku is a container-based cloud platform as a service (PaaS) that is used to build, deploy, manage, and scale modern applications. Heroku Enterprise provides services to large companies which help them to improve collaboration among different teams. It provides a set of features like fine-grained access controls, identity federation, and private spaces to manage their enterprise application development process, resources, and users.

This guide helps you in configuring **Heroku** with EventTracker to receive **Heroku** events. Once Heroku is configured to send logs to EventTracker, EventTracker's knowledge pack will help in monitoring events from **Heroku**.

EventTracker's knowledge pack consists of dashboard (graphical representation of events), alerts (near realtime notification of important events), saved searches (for searching specific category of logs with a single click) and reports (structured and details info of events) to help you correct problems long before a disastrous failure occurs.

EventTracker's built-in knowledge pack enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

2. Prerequisites

- EventTracker v9.3 or above should be installed.
- Heroku should be configured.
- Heroku Command Line Interface (CLI) must be installed.

3. Integrating Heroku with EventTracker

3.1 EventTracker uses syslog drain to receive logs from Heroku.

- 1. Create an app in Heroku.
- 2. Login to Heroku CLI.
- 3. Turn on debug and runtime logging.
 - Turn on debug logging:
 - \$ heroku config:add LOG_LEVEL=DEBUG --app <YOUR_APP_NAME>
 - Turn on runtime logging:
 - \$ heroku labs:enable log-runtime-metrics --app <YOUR_APP_NAME>
- 4. Restart your app to apply changes:

• **Restart your app**:

- \$ heroku restart -- app <YOUR_APP_NAME>
- 5. Using command line, add syslog URL (which contains the host and port) as a syslog drain.

TLS Syslog
<pre>\$ heroku drains:add syslog+tls://logs.example.com:12345 -a myapp</pre>
Plain text Syslog
\$ heroku drains:add syslog://logs.example.com -a myapp

Figure 1

Here, myapp = the name of your Heroku application

e.g. heroku drains:add syslog://<EventTracker Manager IP>:<port> --app <YOUR APP NAME>

EventTracker will receive events/logs of applications for which syslog drain has been created.

3.2 System Licensing

1. Click on Manager under Admin.

		🔎 Admin 🗸
Active Watch Lists	FAQ Tile Configuration	包,MITRE ATT&CK Rules
Alerts	Group Management	🧭 Parsing Rules
Casebook Configuration	Q IP Lookup Configuration	Report Settings
🚭 Category	·☆ Knowledge Objects	Systems
Diagnostics	M Machine Learning Jobs	Q Users
Event Filters	🗞 Machine Learning Settings	reights
Eventvault	Manager	



2. Go to syslog/Virual Collection Point tab.



Netsurion	EventTracker ⁻						<u>,</u> 2	Admin -	Tools 🗸	💽 gurmukh 🗸
Manager									† 7	Admin / Manager
Configuration	syslog / Virtual Collection Po	oint Direct Log Archiver	Agent Settings	Email	Collection Master Ports	Elasticsearch				
syslog										
🗹 Enable sys	log receiver 🗌 Do not resolv	ve sender's IP address to host na	me			Total av	/ailable: Unlim	ited		
Port numbe	r Description	Cache path			Purge frequency (days)	Archive path				
514	All Syslog Systems (UDP)	D:\Program Files (x86)\Prism N	vlicrosystems\EventTra	acker\Cache	0	D:\Program Files (x86)\Prism I	Microsystems\	EventTracker\A	rchives	\$
6514		D:\Program Files (x86)\Prism N	vlicrosystems\EventTra	acker\Cache	0	D:\Program Files (x86)\Prism 1	Microsystems\	EventTracker\A	rchives	\$
									Add Edit	Remove

Figure 3

3. Click on the symbol and then select **Extract device Id**.

	Netsurion Even	tTracker				🔎 Ad	min 	Tools 🕶 🌔 🕶
•	Manager						† /	Admin / Manager
۹	Configuration syslo	y / Virtual Collection Point Direct Log	Archiver Agent Settings Email Elasticsearch					
2	and a							
	sysiog				Total confliction (Information			
	Enable syslog recei	ver 📋 Do not resolve sender s IP addres:	s to nost name		iotai available: Uniimited			
	Port number	Description	Cache path	Purge frequency (days)	Archive path	Extract de	vice id	
	514	All Syslog Systems (UDP)	C\\Program Files (x86)\Prism Microsystems\EventTracker\Cache	0	C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives	Assign de	vice type	3
						_	_	
						A	ld Edit	Remove



4. Provide below **Regex** in Regular Expression space.

 $+\d+\:\d+\s(\P<\Computer>d\.[^\s]+)$

5. Provide below value in Token name.

Computer

- 6. Check Active box.
- 7. Click Add and then close.

lote: Adding multiple regular expression fo	r extracting device id or name may cause the EventTracker re	eceiver performance degradation
Regular expression	Token name	Active
		Delete
Regular expression (1)		
Token name 🕕		Active 🔲 Ignore syslog message if regular
Token name () Note: The provided token must be same at	s Named Capture Group given in the regular	Active Ignore syslog message if regular expression does not match

Figure 5

8. Click Save.

slog					
Enable syslog rei	ceiver 🗌 Do not resolve	sender's IP address to host name		Total available: Unlimited	
Port number	Description	Cache path	Purge frequency (days)	Archive path	
514	All Syslog Systems (UD	P) D:\Program Files (x86)\Prism Microsystems\EventTracker\Cache	0	D:\Program Files (x86)\Prism Microsystems\EventTracker\Archives	۵
1514		D:\Program Files (x88)\Prism Microsystems\EventTracker\Cache	0	D\Program Files (x86)\Prism Microsystems\EventTracker\Archives	٥
					Add Edit Remove
tual Collectio	n Points				
				Total available: Unlimited	
Port number	Description	Carbo nath	Purps frequency (days)	Archiva nath	
14606	All Custome	Cacille Parti	Turge mequeincy (usys)	Automet path	
	AND SOLUTION	D/Drogram Files (v86)/Drism Microsystems/SuentTracker/Cache	0	Phyrogram Files (vShi) Vrism Microsystems) Event (radver) Archives	
14525	ADACHE	D1Program Files (x86)(Prism Microsystems)EventTracker(Cache	0	D:\Program Hies (x80)\Prism Microsystems\Event Iracker\Archives	
14525	APACHE	D\Program Files (x88)(Prism Microsystems)EventTracker(Cache D\Program Files (x88)(Prism Microsystems)EventTracker(Cache	0	Di Program Files (1880),Prism Microsystems)Event Tracker,Archives Di Program Files (1880),Prism Microsystems)EventTracker,Archives	
14525	APACHE	Di Program Files (#88)/Prism Microsystems(EventTracker/Cache Di Program Files (#88)/Prism Microsystems(EventTracker/Cache	0	Di Vingram Files (x00) Union Microsystemisissent fracken Archives Di Program Files (x00) (Prism Microsystemisissent Tracken Archives	
14525	APACHE	DiPlogram Files (48) (Prinn Microsoftem ElverTinder (Carbe DiPlogram Files (48) (Prinn Microsoftem ElverTinder (Carbe	0	Univegran Hiel (1989)/Hem MicrogrammEvent Inder Ardnives Di/Program Files (1989)/Hem MicrogrammEventTinder/Ardhives	
14525	АЛ Зузынть АЛАСНЕ	DiPlogram Files (98) (Prinn Morogstems ElverTinder (Carbe DiPlogram Files (98) (Prinn Morogstems ElverTinder (Carbe	0	Uringgan - His (188) (Plan Microgramd)sert Tacar-Vories Di (Program File (188) (Plan Microgramd)Sert Tacar Archives	
14525	APACHE	D/Program Files (98) (Priors Microsystem) ElverTradee/Cache D/Program Files (98) (Priors Microsystem) ElverTradee/Cache	0	Urogan nis (98) /Pion Moogandoseri face/Vore	Add Edit Remove

Figure 6



Netsurion. 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 Heroku.

4.1 Category

- **Heroku: Application Logs** This category provides information related to logging output from the application itself including logs generated by your app's code and dependencies.
- Heroku: Router Logs This category provides information related to messages about actions taken by the Heroku platform infrastructure on behalf of your app, such as: restarting a crashed process, sleeping or waking a web dyno, or serving an error page due to a problem in your app.

4.2 Alert

- Heroku: Authentication Failure Detected in Deployed Application This alert is generated when any authentication failure is detected in the application deployed in Heroku.
- Heroku: High Severity Events Detected This alert is generated when any high severity (error, critical, warning) events are detected in Heroku.

4.3 Report

Heroku: Resource Utilization- This report gives information about the resource utilization by an application deployed in Heroku. Drain Id is the syslog drain id associated with a specific app which tracks the application performance. Report contains CPU load and memory utilization information.

LogTime	Computer	Drain Id	Load Avg 1m	Load Avg 5m	Load Avg 15m	Disk Cache Memory	Memory Read from Disk	Page written to Disk	Resident Memory	Swap Memory	Total Memory	Source	Memory Quota
02-15-2021 03:52:06 PM	RXXXXXXXXXIHER OKU-SYSLOG	d.5a8fd083-0972- 4e18-b912- 94dc2d099dac	0.00	0.00	0.01							web.1	
02-15-2021 03:52:06 PM	RXXXXXXXXXXAHE ROKU-SYSLOG	d.5a8fd083-0972- 4e18-b912- 94dc2d099dac	0.00	0.00	0.01							web.1	
02-15-2021 03:52:06 PM	RXXXXXXXXXXHER OKU-SYSLOG	d.5a8fd083-0972- 4e18-b912- 94dc2d099dac				15.79MB	257367pages	84526pages	669.36MB	0.00MB	685.14MB	web.1	1024.00MB

Figure 7

Heroku: Router Logs - This report gives the information about actions taken by the Heroku platform infrastructure on behalf of your app, such as: restarting a crashed process, sleeping or waking a web dyno, or serving an error page due to a problem in your app, access of application from an user. It



contains the IP from where the application has been accessed, protocol, status code, application pages/asset that has been access, connect and service time, bytes transferred.

				Connecti								Service	Respo Error	
LogTime	Computer	Log Severity	Bytes	on Time	Reason	Dyno	User Ip	Host	Method	Path	Request Id	Time	nse ID code	Drain Id
02-15-2021 03:52:07 PM	RXXXXXXX\HEROK U-SYSLOG	error	407	0ms	Request timeout	web.1	114.119.159.231	stg.snap- raise.com	GET	/robots.txt	44f1a6ad-36a9-490c 851d-62d09692b6d8	- 1464ms	200 H12	d.5a8fd083-0972-4e18-b912- 94dc2d099dac
02-15-2021 03:52:10 PM	RXXXXXX\HEROK U-SYSLOG	info	407	1ms		web.1	66.249.66.94	staging.snap- raise.com	GET	/robots.txt	5b285a3e-f76d-44c9 8354-2a2cd4be251b)- 4ms	200	d.5a8fd083-0972-4e18-b912- 94dc2d099dac
02-15-2021 03:52:10 PM	RXXXX\HEROKU- SYSLOG	info	42995	Oms		web.1	66.249.66.92	staging.snap- raise.com	GET	1	a7851a02-1e36-446 9b4e-8c66f1c9345e	e- 201ms	200	d.5a8fd083-0972-4e18-b912- 94dc2d099dac
								Figure	8					

 Heroku: Command Executed – This report contains information about commands executed and messages about administrative actions taken developers working on app deployed in Heroku such as toggling maintenance mode, deploying new code etc.

LogTime	Computer	Command	User
02-15-2021 03:52:08 PM	RXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	bundle exec rake staging:update_db_from_production	scheduler@addons.heroku.com
02-15-2021 03:52:09 PM	RXXXXXXXXHEROKU-SYSLOG	if ["\$(date +%d)" = 01] ∥ ["\$(date +%d)" = 15]; then heroku repo:purge_cache && heroku repo:reset; fi	scheduler@addons.heroku.com

Figure 9

Logs Considered





application_category	+- d.5a8fd083-0972-4e18-b912-94dc2d099dac
application_type	+- web.1
event_category	+- 0
event_computer	+- Heroku-syslog
event_datetime	+- 2/15/2021 3:52:19 PM
event_datetime_utc	+- 1613384539
event_description	Feb 15 15:52:19 Heroku Computer:Heroku, Jan 24 01:51:24 52.2.229.255 1 2021-01-24T09:51:24.537546+00:00 d.5a8fd083-0972-4e18-b912-94dc2d099d
	ac heroku web.1 source=web.1 dyno=heroku.85170982.7541d2e4-778f-442e-88f6-ad72cd81b0ff sample#memory_total=639.80MB sample#memory_
	rss=626.77MB sample#memory_cache=13.03MB sample#memory_swap=0.00MB sample#memory_pgpgin=236487pages sample#memory_pgpgout=73
	720pages sample#memory_quota=1024.00MB
event_id	+- 128
event_log_type	+- Application
event_source	+- SYSLOG local0
event_type	+- Error
event_user_domain	+- N/A
event_user_name	+- N/A
log_category	+- heroku
log_info	+- heroku.85170982.7541d2e4-778f-442e-88f6-ad72cd81b0ff
log_source	+- Heroku
log_type	+- web.1
source_type	+- Heroku
total_bytes_in	+- 236487
total_bytes_out	+- 73720
total_packets_count	+- 1024
total_packets_in	+ - 627

Figure 10

4.4 Dashboards

• Heroku: Application Visited by Geolocation





Netsurion. EventTracker[®]



• Heroku: HTTP Code by Volume



• Heroku: Error Codes Received







• Heroku: Log Type by Application (syslog drain id)

Figure 14

Heroku: Request Method by Ip







Heroku: Visits on Application Per Day 🖸 – 🗙 100 80 60 40 20 0 02109 02/12 02/15 02/10 02/16 02/11 02/13 02/14

• Heroku: Visits on Application Per Day

Figure 16

• Heroku: Log Severity



Figure 17

5. Importing Heroku knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Category
- Alert
- Knowledge Object
- Report
- Dashboard
- 1. Launch EventTracker Control Panel.
- 2. Double click Export Import Utility.





Figure 18

3. Click the **Import** tab.

5.1 Category

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

₿.	Export Import Utility	_	D 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 				
O Filters				
⊖ Alerts				
 Systems and Groups 	Source :			
O Token Value				
⊖ Reports				
O Behavior Correlation				
		_		
	Import		Close	

Figure 19



- 2. Locate Category_Heroku.iscat file, and then click the Open button.
- 3. To import categories, click the **Import** button.

EventTracker displays success message.



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

5.2 Alert

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

B	Export Import Utility
Export Import	
1. Provide the path and file name 2. Click the Import button.	e of the Alerts file. Use the '' button to browse and locate the import file.
Options	Location
Category	✓ Import E-mail settings
⊖ Filters	Set Active This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on
 Alerts 	O By default "Active" key available in the configuration section.
 Systems and Groups 	Watchlist Configuration
O Token Value	Import Watchlist configuration
	This setting is applicable only for alerts which have Advanced watchlist configured. Note: If this option is enabled the user should make sure the watchlist groups are available.
Reports	on the console where the alerts are imported.
O Behavior Correlation	
	Source :
	*isalt
	Import Close



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

EventTracker displays success message.





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

5.3 Knowledge Object

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

≡	Event Tracker ⊕					🐥 Admin-	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
Q			Alerts	Correlation	Q IP Lookup Configuration	🛱 Users	
	0 1	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 Cc USB activities, New sen	Casebook Configuration	Eventvault	D Parsing Rules		
			● Category	FAQ Configuration	Report Settings		_
	Attacker			- News			



2. Click on **Import** I button as highlighted in the below image:

	Knowledge Ob	owledge Objects 🔶 / Admin / Know		
Q. ₿	Search objects	Q	Activate Now	Objects 🕀 ፒ 🏦 🌣
	Groups	+ 🖉 🗓		±
	Cylance			
	EventTracker			



3. Click on Browse.







- 4. Locate the file named **KO_Heroku.etko**.
- 5. Select the check box and then click on \mathbb{T} Import option.

Import				×
Select file			Erowse Upload	
<	Object name	Applies to	Group name	
~	Heroku	heroku	Heroku	-
			Import Close	



6. Knowledge objects are now imported successfully.





Figure 27

5.4 Report

1. Click **Reports** option and select **New (*.etcrx)** option.

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

Figure 28

2. Locate the file named **Reports_Heroku.etcrx** and select the check box.

ect file	11400-400-4-7-E (T. L. 1701-0	U T MARINA MARINA	eroku/Configurations/Flex_Reports_H	Heroku.etcrx Select file	•
ilable repo	orts	Frequency Show all	- Q Q		
]	Title	Sites	Groups	Systems	Frequency
EDIT	Heroku - Command Executed	R1S5-VM30	Default	Heroku-syslog	Undefined
EDIT	Heroku - Resource Utilization	R1S5-VM30	Default	Heroku-syslog	Undefined
EDIT	Heroku - Router Logs	R1S5-VM30	Default	Heroku-syslog	Undefined
					>
xte: Set n st run ti	un time option is not applicable for Define ime for report(s) from	d Reports and Hourly Reports AM • at interval of minu	ites Set ①		Activate

Figure 29

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





5.5 Dashboards

NOTE- Below steps given are specific to EventTracker 9 and later.

1. Open EventTracker in browser and logon.

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



- 2. Navigate to My Dashboard option as shown above.
- 3. Click on the **Import** I button as show below:

Event Tracker ⊕	ŗ	Admin -	Tools -	💽 ETAdmin *
My Dashboard		f	/ Dashboard	d / My Dashboard
		÷	o 🖉 🎯 🛱	1 3 0



- 4. Import dashboard file Dashboard_Heroku.etwd and select Select All checkbox.
- 5. Click on Import as shown below:



mport
Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.
🗁 Browse Upload
Available widgets Select All
Heroku: Application Visit Iteroku: HTTP Codes by Vol
✓ Heroku: Error Codes Recei ✓ Heroku: Log Type by Appli
✓ Heroku: Request Method by ✓ Heroku:Visits on Applicat
Heroku: Log Severity
Import Close

Figure 33

6. Import is now completed successfully.



Figure 34

7. In **My Dashboard** page select to add dashboard.



Figure 35

8. Choose appropriate name for Title and Description. Click Save.



Add Dashboard	
Title	
Heroku	
Description	
Heroku	
	Save Delete Cancel



9. In **My Dashboard** page select (a) to add dashlets.

My Dashboard		🕈 / Dashboard / My Dashboar
		+ 🖉 🕒 🕸 🗐 🕀 🗐
CheckPoint Trend Micr	Microsoft	_
		Figure 37

10. Select imported dashlets and click Add.

Customize dashlets				×
Heroku				Q,
Heroku: Application Visited by	Heroku: Error Codes Received	✓ Heroku: HTTP Codes by Volume	✓ Heroku: Log Severity	
Heroku: Log Type by Applicatio	Heroku: Request Method by Ip	Heroku: Visits on Application Pe		
			Add Delete	Close

Figure 38



6. Verifying Heroku knowledge pack in EventTracker

6.1 Category

- 1. Logon to EventTracker.
- 2. Click Admin dropdown, and then click Category.

≡	Event Tracker ⊕						Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
a		_	Alerts	© Correlation	🔍 IP Lookup Configuration	🛱 Users	
	0	1	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	The Weights	
			🏷 Behavior Correlation Settings	觉 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	P Eventvault	🧭 Parsing Rules		
			● Category	FAQ Configuration	Report Settings		
	Attacker			- News			

Figure 39

3. In **Category Tree** to view imported category, scroll down and expand **Heroku** group folder to view the imported category.

Category
Category Tree Search
🛨 🔁 Barracuda Spam Firewall 🔺
Change Audit
Cloudflare
Comodo Endpoint Protection
Crowdstrike Falcon
Deep Instinct
+ EventTracker
Heroku
···· 🗐 Heroku: Application Logs
Heroku: Router Logss

Figure 40

6.2 Alert

- 1. Logon to EventTracker.
- 2. Click the Admin menu, and then click Alerts.

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



3. In the **Search** box, type '**Heroku**, and then click the **Go** button. Alert Management page will display the imported alert.

Alert Name 🔨	Threat	Active	Email	F
$\delta \delta$ Heroku: Authentication failure detected in deployed application	•			
🚱 Heroku: High Severity Events Detected	•			



4. To activate the imported alert, toggle the **Active** switch.

EventTracker displays message box.





5. Click **OK**, and then click the **Activate Now** button.

NOTE: Specify appropriate system in alert configuration for better performance.

6.3 Knowledge Object

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

	Event Tracker ⊕					🔺 🛛 Admin -	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
a			🛕 Alerts	Correlation	Q IP Lookup Configuration	🙊 Users	
	0	1	Behavior Correlation Rules	A 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	Eventvault	🧭 Parsing Rules		
			● Category	FAQ Configuration	Report Settings		
	Attacker			- News			

Figure 44

2. In the Knowledge Object tree, expand **Heroku** group folder to view the imported knowledge object.

Obje App	ect name Heroku lies to heroku							÷ 1	\$
Kule	·S								
	Title		Event source	Source Type	Log type	Event id	Event type		
+	Heroku		syslog	Heroku				🧭 🕑 🗓 (<i>0</i> ,
	Message Signature:								
	Message Exception:								
	Expressions								
	Expression type	Expression 1					Expression 2	Format string	
	Regular Expression	with\scommand	d\s\`(? <command/> [^\	\`]+) \-\s\-\s(? <command/> .*?)	\sby\suser			\bigtriangledown	Ü
	Regular Expression	\sby\suser\s(?<	user>[^\n\$]+)					\bigcirc	Ē

Figure 45

3. Click Activate Now to apply imported knowledge objects.

6.4 Report

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

≡	Event Tracker ⊕			
	Home			
Q R	Report Configuration		1	
	Report Dashboard	ntry point	Indicators of Compromise USB activities, New services or software install	
	Explorer			
	Аттаскег	l		-

Figure 46

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



					Search			Q	Q		
+	Repo	orts configu	ıration: Heroku								
*	Ð	Ū 2,								Tot	tal: 3
			Title	Create	d on	Modif	ied on				
		1	Heroku - Command Executed	Feb 16	08:20:41 AM	Feb 17	11:06:12 AM	(D	5	+
		(1)	Heroku - Resource Utilization	Feb 16	07:54:09 AM	Feb 17	11:06:29 AM	(D	5	+
i ø		£\$3	Heroku - Router Logs	Feb 15	04:27:30 PM	Feb 17	11:06:53 AM	(D	5	+

Figure 47

6.5 Dashboards

1. In the EventTracker web interface, Click on Home Button and select My Dashboard.

	Home
Dashb	My Dashboard
×	Threats
	Incidents

Figure 48

2. In the **Heroku** dashboard you should be now able to see something like this.



Figure 49