



Integration Guide

Integrate Barracuda Sentinel with EventTracker

Publication Date:

October 25, 2022

© Copyright Netsurion. All Rights Reserved.

Abstract

This guide provides instructions to configure the Knowledge Packs in EventTracker to receive the logs from Barracuda Sentinel (Impersonation Protection). The Knowledge Pack contains alerts, reports, dashboards, and knowledge objects.

Scope

The configuration details in this guide are consistent with EventTracker version 9.3 or later, and Barracuda Sentinel (Impersonation Protection).

Audience

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

Table of Contents

Ove	erview	4
Pre	requisite	4
Eve	entTracker Knowledge Packs	4
3.1	Category	4
3.2	Alerts	4
3.3	Reports	5
3.4	Dashboard	5
Imp	oorting Barracuda Sentinel Knowledge Packs into EventTracker	8
4.1	Category	9
4.2	Alerts	10
4.3	Reports	11
4.4	Knowledge Objects (KO)	12
4.5	Dashboard	14
Ver	ifying Barracuda Sentinel Knowledge Packs in EventTracker1	L 7
5.1	Category	17
5.2	Alert	17
5.3	Reports	19
5.4	Knowledge Objects (KO)	19
5.5	Dashboard	20
	Ove Pre Eve 3.1 3.2 3.3 3.4 Imp 4.1 4.2 4.3 4.4 4.5 Ver 5.1 5.2 5.3 5.3 5.4 5.5	Overview Prerequisite Prerequisite EventTracker Knowledge Packs 3.1 Category 3.2 Alerts 3.3 Reports 3.4 Dashboard Importing Barracuda Sentinel Knowledge Packs into EventTracker 4.1 Category 4.2 Alerts 4.3 Reports 4.4 Knowledge Objects (KO) 4.5 Dashboard 5.1 Category 5.2 Alert 5.3 Reports 5.4 Knowledge Objects (KO) 5.5 Dashboard

1 Overview

Barracuda Impersonation Protection (formerly Sentinel) combines artificial intelligence, deep integration with Microsoft Office 365, and brand protection into a comprehensive cloud-based solution that guards against business email compromise, account takeover, spear phishing and other cyber fraud.

Netsurion, the Managed Threat Protection platform facilitates monitoring events retrieved from Barracuda Sentinel and seamlessly consolidates SIEM, Log Management, File Integrity Monitoring, machine analytics, and user behavior details.

2 Prerequisite

- EventTracker version 9.3 or later must be installed and configured to receive logs.
- Configure Barracuda Sentinel (Impersonation Protection) to forward logs to EventTracker.

Note

Refer to <u>How-To</u> guide to configure Barracuda Sentinel (Impersonation Protection) 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 Category

Barracuda Sentinel - Spear phishing threat activities: This category shows the spear phishing threat related activities performed by the users.

Barracuda Sentinel - Account takeover attack activities: This category shows the account takeovers threat activities performed by the users.

3.2 Alerts

Barracuda Sentinel: Threat detected: This alert is triggered when potentially malicious content or threat like spear phishing or account takeover are detected.

Barracuda Sentinel: Suspicious user login detected: This alert is triggered when a suspicious user logon is detected based on the geo location logon patterns.

3.3 Reports

Barracuda Sentinel - Spear phishing threat activities: This report provides a detailed summary of all the Barracuda Sentinel events related to spear phishing threat activities. The report includes sender details, recipient address, and more.

Log time	Threat t	ype Sender address	Email subject	Recipient address	Access token ID	Account ID
2022-06-25	- 12:11:50 becSpoo	fing user@example.com	One more question	jack@contoso.com	dd55-4a24-be9d6e1bae264e96	b117-4c79-b825-df1793d7f46d
2022-09-18	22:10:55 blackmai	l jeremyanapophysial1993@ya	ahoo.com Jonathan david	jonathan@contoso.com	dd55-4a24-be9d-6e1bae264e96	b117-4c79-b825-df1793d7f46d
2022-09-19	07:02:20 spam	copydb@initweb.net	Re: Hello	Jacob@contoso.com	dd55-4a24-be9d-6e1bae264e96	b117-4c79-b825-df1793d7f46d
2022-09-21	01:45:17 phishing	info@ravintitle.com	contoso Docusign-M JF839-0139-M- S39-6, Contract No. 39-g	cole@contoso.com	dd55-4a24-be9d-6e1bae264e96	b117-4c79-b825-df1793d7f46d
2022-09-26	- 11:52:01 conversa	tionHijacking sglickman@chmsgroups.con	n New Castle	samuel@contoso.com	dd55-4a24-be9d-6e1bae264e96	b117-4c79-b825-df1793d7f46d

Barracuda Sentinel: Account takeover attack activities: This report provides a detailed summary of all the account takeover alerts like suspicious login activities performed by the users, any inbox rule changes, and more. The report includes User information, IP address details, Logon location, and so on.

Log time T	hreat type	Sender name	Sender details	Email subject	User Info	User name	Login agent	Login IP address	Location	Rule name	Access token ID	Account ID
2020-06-21 - 00:40:00 Ir	box Rules				johnathan@contoso.com	Internal, User				Forward mail to John	dd55-4a24-be9d6e1bae264e96	b117-4c79-b825-df1793d7f46d
2020-06-21 - 00:40:00 S	ign Ins				mark@contoso.com	Internal, User	Windows/10 - Chrome	142.250.138.101	Mexico		dd55-4a24-be9d6e1bae264e96	b117-4c79-b825-df1793d7f46d
2020-06-21 - 00:40:00 In	box Rules				johnathan@contoso.com	Internal, User				Forward mail to John	dd55-4a24-be9d6e1bae264e96	b117-4c79-b825-df1793d7f46d
2020-06-21 - 00:40:00 S	ign Ins				mark@contoso.com	Internal, User	Windows/10 - Chrome	142.250.138.101	Mexico		dd55-4a24-be9d6e1bae264e96	b117-4c79-b825-df1793d7f46d
2020-06-23 - 21:45:27 E	mail .	John, User	John@contso.com	HW#22.pdf	user@contoso.com	Internal, User					dd55-4a24-be9d6e1bae264e96	b117-4c79-b825-df1793d7f46d
2020-06-23 - 21:45:27 E	imail ,	John, User	John@contso.com	HW#22.pdf	user@contoso.com	Internal, User					dd55-4a24-be9d6e1bae264e96	b117-4c79-b825-df1793d7f46d

3.4 Dashboard

Barracuda Sentinel: Spear phishing threats: This dashlet displays the different types of phishing threats detected related to spear phishing.

Barracuda Sentinel: Account takeover attacks related events: This dashlet displays the different types of threat detected related to account takeover alerts.

Barracuda Sentinel: Spear phishing detected on users: This dashlet displays the list of user information according to the threat attack detected.

Barracuda Sentinel -	Barracuda Sentinel - Spear phishing detected on 🚯 🛈						
recipient_address	sender_address	threat_type	Count				
cole@contoso.com	info@ravintitle.com	phishing	1				
jack@contoso.com	user@example.com	becspoofing	1				
jacob@contoso.com	copydb@initweb.net	spam	1				
jonathan@contoso.com	jeremyanapophysial 1993@yahoo.com	blackmail	1				
samuel@contoso.com	sglickman@chmsgroups.com	conversationhijackin	g 1				

Barracuda Sentinel: Account takeover alert detected on users: This dashlet displays the list of users with information according to the threat type detected for account takeover.

Barracuda Sentinel - Acc	8 G - X		
src_user_info	src_user_name	threat_type	Count
johnathan@contoso.com	internal, user	inbox rules	1
mark@contoso.com	internal, user	sign ins	1
user@contoso.com	john, user	email	1

Barracuda Sentinel: Suspicious user login activities: This dashlet displays the suspicious login activities performed by users according to their geo location.

4 Importing Barracuda Sentinel 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.

4	Export Import Utility	-		x
Export Import 1. Provide the path and file name 2. Click the Import button.	e of the Categories file. Use the '' button to browse and locate the import file.			
Options Category Filters Alerts	Location			
Systems and Groups Token Value Reports	Source :			
	Import		Close	e

- 2. In the Browse window, locate the Categories_ Barracuda Sentinel.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.

4	Export Ir	nport Utility	_ 🗆 🗙
Export Import			
Export Import 1. Provide the path and file nam 2. Click the Import button. Options Category Filters Import button. Options Category Filters Alerts Systems and Groups Token Value Reports Behavior Correlation	e of the Alerts file. Use the '' butt Location Import E-mail settings Set Active Only if notifications set By default Watchlist Configuration Import Watchlist configurati This setting is applicable only f Note: If this option is enabled t on the console where the alert Source :	on to browse and locate the import file. This setting is applicable only for imports from L Alert files. For v7, the active status will be set b "Active" key available in the configuration sect on or alerts which have Advanced watchlist configur he user should make sure the watchlist groups are s are imported.	egacy (v6x) ased on ion. ed. a available
	*.isalt		
		Import	Close

- 2. In the Browse window, locate the Alerts_ Barracuda Sentinel.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 Reports

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

4	Export Import Utility	• x
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 	Export Import Utility 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) Source : *	
	Import	Close

- 2. In the **Reports Import** window, click **Select file** to locate **Reports_Barracuda Sentinel.etcrx** file.
- 3. Select the check box of all the files and click the **Import** \blacksquare button to import the selected files

Image: State Frequency Show all Image: Comparison Image: The state State Groups Systems Frequency EDIT Baracuda Sentinel - Account takeove Undefined Undefined EDIT Baracuda Sentinel - Spear phishing th Undefined Undefined		C. Osers vakash (Desktop (Nepoits_banacuua	Sentinelletox		Select file	
Thic Sites Groups Systems Frequency EDIT Baracuda Sertinel - Account takeove Undefined Undefined B011 Beracuda Sertinel - Spear phishing th Undefined Undefined		ons	Frequency Show all	- Q Q		
EDIT Baracuda Sentinel - Account takeove Undefined EDIT Baracuda Sentinel - Spear phishing th Undefined	-	Title	Sites	Groups	Systems	Frequency
EDIT Barracuda Sentinel - Spear phishing th Undefined	EDIT	Barracuda Sentinel - Account takeove				Undefined
	EDIT	Barracuda Sentinel - Spear phishing th				Undefined
						>
te: Set run time option is not applicable for Defined Reports and Hourly Reports	te: Set r	un time option is not applicable for Defined Rep	ots and Houtly Reports			>
te: Set run time option is not applicable for Defined Reports and Hourly Reports t run time for report(s) from AM • at interval of minutes Set	te: Set r	un time option is not applicable for Defined Rep ime for report(s) from AM	orts and Hourly Reports	es Set (j)		>

4. EventTracker displays a success message on successful importing of the selected file in **Reports**.

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

4.4 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	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	P Eventvault	🕖 Parsing Rules		
			• Category	FAQ Configuration	Report Settings		
	Attacker			– News			

2. In the Knowledge Objects interface, click the Import $\overline{\bullet}$ button to import the KO files.

	Knowledge Obje	ects			🔒 / Admin / Knowledge Objects
Q	Search objects	Q	Q	Activate Now	Objects 🕀 ፒ 🏦 🌣
Uk	Groups	+ Ø İ			±.
	Cylance				
	EventTracker				

3. In the Import window, click Browse and locate the KO_ Barracuda Sentinel.etko file.

Import		×
Select file	🖆 Browse Upload	
	Close	

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

Imp	ort		>	
Se	Select file 🗁 Browse Upload			
	Object name	Applies to	Group name	
	Barracuda Sentinel	Barracuda Impersonation Protection (formerly Sentinel)	Barracuda Sentinel	
			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.

4.5 Dashboard

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

11	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		Caller -	

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_ Barracuda Sentinel.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.

Import					
Note: If dashlet configured using persisted report, first import the report and proceed with in dashlet.	nporting				
🗁 Browse	Upload				
Available widgets					
Select All					
Barracuda Sentinel - Spea Sarracuda Sentinel - Acco					
Barracuda Sentinel - Susp Barracuda Sentinel - Spea					
Barracuda Sentinel - Acco					
Import	Close				

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

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

My Dashbo	ard		🔒 / Dashboard / My Dashboar
CheckPoint	Trend Micr	Microsoft	+ © © ‡ ‡ ©

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

Edit Dashboard						
Title						
Barracuda Sentinel						
Description						
Barracuda Impersonation Protection (formerly Sentinel)						
	Save Delete Cancel					

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

Customize dashlets			×
Barracuda Sentinel			Q
Barracuda Sentinel - Account ta	Barracuda Sentinel - Account ta	Barracuda Sentinel - Spear phis	Barracuda Sentinel - Spear phis
Barracuda Sentinel - Suspicious			
			Add Delete Close

5 Verifying Barracuda Sentinel 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		E Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
a			▲ Alerts	Correlation	🔍 IP Lookup Configuration	QQ 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	Eventvault	🧭 Parsing Rules		
			📲 Category	FAQ Configuration	Report Settings		
	Attacker			 News 			

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

C	Category					
	Category Tree	Search				
	Barracu Bar Bar	ida Sentinel rracuda Sentinel - Account takeover atta rracuda Sentinel - Spear phishing threat	•			

5.2 Alert

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

Ξ	Netsurion. EventTracker				🔎 Admin v	Тоо
	Home		Active Watch Lists	FAQ Tile Configuration	Manager	
٩			Alerts	Group Management	MITRE ATT&CK Rules	
	0	0	Casebook Configuration	Q IP Lookup Configuration	D Parsing Rules	
8			Category	· Knowledge Objects	Report Settings	55 V3.2
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Compromise USB activities, New services or software install	Diagnostics	M Machine Learning Jobs	Systems	
			Event Filters	hachine Learning Settings	QQ Users	
	Attacker		Eventvault	🏓 Manage API keys	Heights	

2. In the Alerts interface, type Barracuda Sentinel in the Search field and click the Search button.

3. The Alerts interface will display all the imported Barracuda Sentinel 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 configuration.
OK

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 Reports

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

	Event Tracker ⊕			
-	Home			
٩		-	1	
R	Report Configuration		1	
	Report Dashboard	ntry point	Indicators of Compromise USB activities, New services or software install	
	Explorer			
	Аттаскег	1		-

- 2. In the Reports Configuration interface, select the Defined option.
- **3.** In the search field, type **Barracuda Sentinel** and click **Search** to search for the Barracuda Sentinel files.
- **4.** EventTracker displays the reports for Barracuda Sentinel.

Rep	Reports configuration: Barracuda Sentinel				
÷	Ü 🕗				
		Title			
	£\$\$	Barracuda Sentinel - Account takeover attack activities			
	£\$3	Barracuda Sentinel - Spear phishing threat activities			

5.4 Knowledge Objects (KO)

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

Event Tracker ⊕	🛓 🛛 Admin -				
Home		Active Watch Lists	Collection Master	🔄 Group Management	Systems
		Alerts	Correlation	Q IP Lookup Configuration	였 Users
0	1	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	
		🏷 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	
	_	ola Category	FAQ Configuration	Report Settings	
Attacker			- News		

2. In the Knowledge Object interface, under Groups tree, click the Barracuda Sentinel group to expand and view the imported Knowledge objects.

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

5.5 Dashboard

In the EventTracker web interface, go to Home > My Dashboard, and click the Customize dashlets
 button.

	Home
Dashb	My Dashboard
2	Threats
	Incidents

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

Customize dashlets			×
Barracuda Sentinel			Q
Barracuda Sentinel - Account ta	Barracuda Sentinel - Account ta	Barracuda Sentinel - Spear phis	Barracuda Sentinel - Spear phis
Barracuda Sentinel - Suspicious			
			Add Delete Close

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