

Integration Guide

Integrating DarkTrace Intrusion Detection System (IDS)

EventTracker v9.x and above

Publication Date:

August 3, 2021

© Copyright Netsurion. All Rights Reserved.

Abstract

This guide provides instructions to configure DarkTrace IDS to generate logs for critical events. After EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor networks and systems.

Scope

The configuration details in this guide are consistent with EventTracker version 8.x and later, and DarkTrace IDS.

Audience

Administrators who are assigned the task to monitor DarkTrace IDS events using EventTracker.



Table of Contents

Τā	able c	of Contents	3						
1.	0	Overview4							
2.	Pr	Prerequisites4							
3.	Co	Configuring DarkTrace IDS Syslog4							
4.	Εv	entTracker Knowledge Pack	5						
	4.1	Alerts	6						
	4.2	Reports	6						
	4.3	Dashboards	6						
5.	In	nporting Extreme Network Access Control Knowledge Pack into EventTracker	8						
	5.1	Category	9						
	5.2	Alerts	10						
	5.3	Knowledge Objects	11						
	5.4	Token Template	12						
	5.5	Flex Reports	13						
	5.6	Dashlets	15						
6.	Ve	erifying Knowledge Pack in EventTracker	17						
	6.1	Category	17						
	6.2	Alerts	17						
	6.3	Knowledge Object	18						
	6.4	Flex Reports	19						
	6.5	Dashlets	19						
	6.6	Token Template	20						
	Abo	About Netsurion							

1. Overview

DarkTrace Intrusion Detection System (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any malicious activity or violation is typically reported to an administrator.

DarkTrace IDS can be integrated with EventTracker using syslog. With the help of DarkTrace IDS KP items, we can monitor the intrusion happening inside the network and trigger the alert whenever any high server intrusion is detected. EventTracker dashboard will help you to view the intrusion happening inside the network by its source IP address as well as based on categories. It can even create the report which helps to collect intrusion happening on the network on time bases which assist you to review the intrusion. EventTracker CIM will help you to correlate the intrusion with other log sources like firewall, OS events, etc.

2. Prerequisites

- EventTracker v9.x or above should be installed.
- DarkTrace IDS V3.0.10 or latest version should be installed.

3. Configuring DarkTrace IDS Syslog

- 1. Within the Threat Visualizer, navigate to the **System Config** page in the main menu under **Admin**.
- 2. From the left-hand menu, select **Modules** and choose **syslog** from the available **Workflow Integrations**.
- 3. A configuration window will open. Select the relevant form of syslog here, syslog CEF and click **New** to reveal the configuration settings.

Netsurion

Workf	ow Integrations			
7	Discard Joyang	Save	Enabled O	
	JSON format.	and at more systeg servers in CEF, LEEF or		
۵				
	Syslog CEF 🛛			
		(Verify alert settings 3) (Migrate legac	y settings 👘	
	Send Alerts 😡			
	Send Al Analyst Alerts 😧		•	
	Server 🔮	192.168.0.10		
	Server Port @		514	
	TCP Alerts O		•	
	Full Timestamps 🕤		•	
	Time Offset 🧕		1	
	Use Src Fields 🜒		•	
	Device IP's 😡			
	Model Tags Expression 😧			
	Minimum Breach Score 😡		50	
	Minimum Breach Priority \varTheta)	

- 4. Complete the **Server** location and optionally modify the communication port. Ensure that the port selected is allowed by any intermediary firewalls.
- 5. Review any additional configuration options you may wish to enable that alter the syslog syntax or connection mode. A full list is available below.
- 6. Finally, enable **Send Alerts** and save your changes.

4. EventTracker Knowledge Pack

Once logs are received by EventTracker, Knowledge Packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker to support **DarkTrace IDS**.

4.1 Alerts

• **DarkTrace IDS – Intrusion Detected –** This alert will trigger for all DarkTrace IDS logs.

4.2 Reports

 DarkTrace IDS – Activities – This report provides information related to possible unencrypted password storage.

LogTime	Computer	Category	Priority	Device Host Name	Source IP Address	Source MAC Address	Destination IP Address	Destination Port Number	Message
05/17/2019 01:01:16 PM	DARKTRACE IDS	Anomalous Connection	6	contoso-work1.corp.net	40.20.10.34	b0:c8:dd:6f:5f:cd	30.10.23.224	4302	Multiple Connections to New External UDP Port
05/17/2019 01:01:16 PM	DARKTRACE IDS	Compliance	5	contoso-work12.corp.net	28.10.11.3		20.11.45.23	1265	Sensitive Terms in Unusual SMB Connection
05/17/2019 01:01:16 PM	DARKTRACE IDS	Compliance	4	contoso-work18.corp.net	30.10.23.224	b0:c8:dd:6f:5f:cd	11.21.1.23	2121	Sensitive Terms in Unusual SMB Connection
05/17/2019 01:01:16 PM	DARKTRACE IDS	Compliance	3	contoso-work21.corp.net	20.11.45.23		28.10.11.3	2222	Sensitive Terms in Unusual SMB Connection
05/17/2019 01:01:16 PM	DARKTRACE IDS	Compliance	3	contoso-work11.corp.net	11.21.1.23	b0:c8:dd:6f:5f:cd	40.20.10.34	2324	Sensitive Terms in Unusual SMB Connection

4.3 Dashboards

• DarkTrace IDS – Threat by Source IP Address – This dashboard shows information about the threat by source IP address.



• **DarkTrace IDS – Threat by Destination IP Address** – This dashboard shows information about which threat by what are the destination IP addresses.

Netsurion®



• **DarkTrace IDS – Threat by Threat Category** – This dashboard shows information about threat categories like possible unencrypted password storage.



• DarkTrace IDS – Threat by Source MAC Address – This dashboard shows information threat by source MAC address.

Netsurion



• DarkTrace IDS – Threat by Priority – This dashboard shows information based on threat priority.



5. Importing Extreme Network Access Control Knowledge Pack into EventTracker

- 1. Launch the EventTracker Control Panel.
- 2. Double click **Export/Import Utility**, and then click the **Import** tab.



단글 EventTracker Con	ntrol Panel			- 🗆	Х		
		- BI	Ev	entTracker ()	9		
	5						
EventVault	Diagnostics	License Manager	Export Import Utility	Append Archives			
00		X	\mathbf{X}	-83			
EventTracker Agent Confi	Traffic Analyzer	Agent Manageme	Port Configuration	About EventTracker			
E-mail: support@EventTracker.com							

3. Import Tokens/Flex Reports as given below.

5.1 Category

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

Export Import Utility	-		>
Export Import			
 Provide the path and file na 2. Click the Import button. 	me 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	".scat		
○ Reports			
	Import	Clos	se

- 2. Locate Category_Darktrace IDS.iscat file, and then click the open button.
- 3. To import category, click the **Import** button.
- 4. EventTracker displays a success message.





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

5.2 Alerts

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

Export Import Utility Export Import 1. Provide the path and file na 2. Click the Import button. Options 0 0 i	me of the Alerts file. Use the '' button	to browse and locate the import file.	
 Caregory Filters Alasta 	Import E-mail settings		
 Alerts Systems and Groups RSS Feeds 	 Only if notifications set By default 	This setting is applicable only for imports from Lega (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuratic section.	ncy Dn
Reports Behavior Bules	Source : *.isalt		
© SCAP			
Ioken Value		Import	Close

- 2. Locate Alerts_DarkTrace IDS.isalt file, and then click the Open button.
- 3. To import alerts, click the **Import** button.
- 4. EventTracker displays a success message.



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



5.3 Knowledge Objects

- 1. Click **Knowledge objects** under the admin option in the EventTracker page.
- 2. Locate the file named **KO_DarkTrace IDS.etko**.

Import		×
KO_Darktrace IDS.etko	se Upload	
	Close	

3. Select all the checkbox and then click on the \mathbb{T} '**Import**' option.

Import				×
Select	file		🗁 Browse Upload	
	Object name	Applies to	Group name	
	Darktrace IDS All Events	Darktrace IDS	Darktrace IDS	
			Import Close	

4. Knowledge objects are now imported successfully.



5.4 Token Template

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

			🧢 Admin∓ Tools∓
	Active Watch Lists	Event Filters	💯 Parsing Rules
	Alerts	Eventvault	📳 Report Settings
	Behavior Correlation Rules	FAQ Tile Configuration	Systems
	Behavior Correlation Settings	Group Management	Q Users
f Cor New	Casebook Configuration	Q IP Lookup Configuration	
	● Category	· O- Knowledge Objects	Windows Agent Config
	Diagnostics	Manager	

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

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

4. Locate the **Template_Darktrace IDS.ettd** file and click on **import**.

Netstrion®

ۏ Tol	en Template - Mozilla Firefox					- 0	Х
(!	ocalhost:8080/EventTracker/Analys	is/TokenTemplat	teImportExport.aspx?Type=Import			⊠ ☆	≡
Impo	ort						
selec	ted file is: Template_Darktrace IDS.ettd		🕿 Browse 📮				
	Template name	Separator	Template description	Added date	Added by	Group Name	
Ø	DarkTrack IDS - All Events	\n	Mar 01 09:58:37 darktrace Mar 01 16:58:36 darktrace.corp.nuskin.net CEF:0J Darktrace DCIP 3.0.10 609 Compliance/Possible Unencrypted Password St orage 6 externalId=1631415 dvc=10.0.4.225 dst=10.16.32.117 dvchos t=9365-bkleinma.corp.nuskin.net dpt=445 darktraceUrl=https://darktrace. corp.nuskin.net/#modelbreach/1631415	Mar 04 03:50:40 PM	ETAdmin	Darktrace IDS	

5. Templates are imported now successfully.

File imported su	ccessfully.
	ОК

5.5 Flex Reports

1. Click **Reports** option and select new (.etcrx) from the option.



Export Import Utility		_		\times
Export Import				
1. Provide the path and file name 2. Click the Import button Note : If report(s) contains templa Options	of Schedule Report file. Use the '' button to browse and locate the import file. e, first import template and proceed with exportimport utility.			
Category	Locator			
○ Alerts	O Legacy (*issch) (New (*.etcnx)			
 Systems and Groups 	Source :			
○ RSS Feeds	JISSCH			
 Reports 				
O Behavior Rules				
⊖ SCAP				
O Token Value				
	Impor	t	Clos	e

2. Locate the file named Flex_Reports_Darktrace IDS.etcrx and select all the checkbox.

E Repo	orts Import				×
	K	and the second second settlement from a second			
Note : I	Freport(s) contains template, first im	port template and proceed with report import process.			1
Availab	le reports	JS (riex_Reports_Darktrace IDS.etcrx		Select file]
Title		Frequency Show all	- Q Q		
	Title	Sites	Groups	Systems	Frequency
	EDIT Darktrace IDS - Activities	R1S5-VM30		_	Undefined
					2
Note	: Set run time option is not applicabl	e for Defined Reports and Hourly Reports			
Set	run time for report(s) from	AM • at interval of min	utes Set		
Rep	lace	to R	eplace Assign systems		
			Note: Make sure that Site(s), Group(s) and System(s) selections a	re valid.

3. Click the Import button to import the reports. EventTracker displays a success message.



5.6 Dashlets

In EventTracker 9.0, we have added a new feature that will help to import/export of dashlet. Following is the procedure to do that:

1. Login into EventTracker Web console.

E٧	vent Tracker 🕀			
L Use	rname			
Pas	sword			
	Login			
logs proc	8,333,946 logs processed since install on Dec 30, 2017			
	35,002 logs processed today			
Contact U	ls FAQ Help			

2. Go to My Dashboard option.





3. Click on the import button and select .etwd File.



4. Click upload and select **Dashboard** which you want to import.

👂 Import dashlets - Mozilla Firefo	х	-		×
(localhost:8080/EventTrac	ker/Flex/ImportWidget.aspx		⊠ ☆	-
mport				
Note: If dashlet configured using p	persisted report, first import the rep	port and proceed with imp	porting	
lashlet.		🗁 Browse	Upload	
Available widgets				
Select All				
Darktrace IDS - Threat by	Darktrace IDS - Threat by	Darktrace IDS - Three	at by	
Darktrace IDS - Threat by	Darktrace IDS - Threat by	Darktrace IDS - Three	at by	
		Impo	ort Clos	e

5. Click on the **Import** button. It will upload all selected dashboards.

6. Verifying Knowledge Pack in EventTracker

6.1 Category

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

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

3. Click the search, and then search with DarkTrace IDS.

Category			
Category Tree Search			
DarkTrace IDS	Q	Q	
Category			
✓ Darktrace IDS - All Events			

6.2 Alerts

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

Netsurion®

≡	Event Tracker ⊕					🔎 🗚 Admin-	Tools +
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dasht
a			Alerts	Correlation	Q IP Lookup Configuration	🛱 Users	
	0	2	Behavior Correlation Rules	A Diagnostics	· Knowledge Objects	The Weights	
<u>~</u>			🗞 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		
			● Category	FAQ Configuration	Report Settings		
	Attacker			- News			

3. In the **Search** box, type **'DarkTrace IDS'**, and then click the **Go** button. Alert Management page will display all the imported alerts.

Alerts			🔶 / Admin / Alerts
Show All		Search by Alert n	name 🗸 DarkTrace IDS 🔍 🔍
137 Available Alerts Total number of alerts available	41 Active Alerts Total number of active alerts	137 System 104 User 33 System/User Defined Alerts Count for system and user defined alerts	Alerts by Threat Level Count of alerts by threat level
Activate Now Click 'Activate N	ow' after making all changes		Total: 1 Page Size 25
Alert Name A	Threat Active E-ma	Forward as Forward as Remedial Action Rem SNMP Syslog at Console	nedial Action Applies To
Darktrace IDS - Detected Events	• 🕤 🗆		Darktrace IDS

4. To activate the imported alerts, select the respective checkbox in the **Active** column.

EventTracker displays a message box.



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

Note: Specify appropriate systems in the alert configuration for better performance.

6.3 Knowledge Object

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



- 3. In **Knowledge Object Group Tree** to view imported knowledge object, scroll down and click the **DarkTrace IDS** group folder.
- 4. Knowledge Object is displayed in the pane.

Knowledge Objects	Admin / Knowledge Objects
DarkTrace IDS Q Q Activate Now	Objects 🕂 Ҭ 🏌 🌣
Groups 🕀 🧭 📋	1
Darktrace IDS	
Darktrace IDS All Events 🧭 🔟	

6.4 Flex Reports

- 1. Login to EventTracker.
- 2. Click the **Reports** menu, and then **Configuration**.
- 3. Select **Defined** in report type.
- 4. In **Report Groups Tree** to view imported Scheduled Reports, scroll down and click the **DarkTrace IDS** group folder.
- 5. Reports are displayed in the Reports configuration pane.

Report Configuration				A / Reports / Report Conf	iguration / Defined
Scheduled O Queued		DarkTrace IDS		Q Q	i
Report Groups 🕀 🏭	Reports configuration: DarkTrace IDS				
🔁 Security	⊕ i i ∂,				Total: 1
Compliance	Title	Created on	Modified on		
Operations	Darktrace IDS - Activities	May 16 12:56:01 PM	Jan 01 05:30:00 AM	(i)	-
E Flex					
🔁 All Compliance Repor 🏢 🧭					
🔁 ArubaOS 🔟 🧭					
🔁 AS400 🔟 🧭					
🕞 Bomgar 🔟 🧭					
DarkTrace IDS					

6.5 Dashlets

- 1. Login to **EventTracker**.
- 2. Click the **Dashboard** menu, and then **My Dashboard**.
- 3. Then click on **Customize Dashlet** button (and search for **"DarkTrace IDS"**)

Netsurion®

Customize dashlets			×
DarkTrace IDs			Q
Darktrace IDS - Threat by Destin	Darktrace IDS - Threat by Locati	Darktrace IDS - Threat by Sourc	Darktrace IDS - Threat by Sourc
Darktrace IDS - Threat by Threat	Darktrace IDS - Threat by Priority		
			Add Delete Close

6.6 Token Template

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

			📣 Admin 🕶 Tools 🕶
	Active Watch Lists	Event Filters	🕖 Parsing Rules
	Alerts	Eventvault	🖉 Report Settings
	Behavior Correlation Rules	FAQ Tile Configuration	Systems
	🗞 Behavior Correlation Settings	Group Management	📿 Users
f Cor New	Casebook Configuration	🔍 IP Lookup Configuration	
	● Category	· 🔆 Knowledge Objects	Uindows Agent Config
	Diagnostics	Manager	

3. Click on **Template** and search for **DarkTrace IDS**.

Parsing Rules								Admin / Parsing Rules
Paising Rule Template								
Groups		+ =	Group : Darktrace IDS	Search	Q			CİŢ
Default		^			-			
Accounts mediskid	Û	1	Template Name	Template Description	Added By	Added Date	Active	
ADFS 2.0	Ĩ	1	DarkTrack IDS - All Events	DarkTrack IDS - All Events	ETAdmin	May 16 12:55:40 PM		Ø
Admin groups mediski	Û	0						
AMediskid	Ĩ	0						
ArubaOS	Û	1						
As400	Û	0						
BMediskid	Û	1						
Bomgar	Ũ	1						
Darktrace IDS	Ē	0						

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's <u>EventTracker</u> cyber threat protection platform provides SIEM, end protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's <u>BranchSDO</u> delivers purpose-built technology with optional levels of managed services to multilocation businesses that optimize network security, agility, resilience, and compliance for 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>. Netsurion is #19 among <u>MSSP Alert's 2020 Top 250 MSSPs</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 MSP's 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