



# LinkShadow

and Recorded Future Integration Guide

www.linkshadow.com



## To integrate Recorded Future with LinkShadow follow the following steps:

1- Go to Settings by Clicking on the gear icon on the top right corner



2- From the left menu go to Integrations and select Others

LINKSHAD	∃ Home	<u>۵</u>			
😰 LinkShadow Settings 👻	General Settings				
O General Settings	Device Coordinates	Active Directory Log Source			
O Device Setup	Latitude	A Mahurat/ Alfree Bad			
O Backup / Reset	26.7502	SIEM*			
O License / Updates	2012/02	* SIEM has to be configured			
🖬 Customizations 👻	Longitude				
O User Interface	55.3047	Submit			
O Manage Usecases		Syslog Source			
O Custom Dashboard	Submit	Network/Mirror Port			
O Settings	SMTP Settings				
Integrations	Server Name/IP	* SIEM has to be configured			
O Domain Controller	Server Name/IP				
O SIEM	Port Number	Submit			
O Endpoint	Port Number	VPN Log Source			
O othlas	Sender Email	Log Source			
Configurations <	Sender Email	Network/Mirror Port			
💼 Manage List	Username	<ul> <li>SIEM</li> <li>514 UDP/TCP</li> </ul>			
Reports / Alerts	Username	* SIEM has to be configured			
Change Password	Deserved				



3- Go to Recorded Future and Select Add New

LINKSHAD	∃ Home	۵
<ul> <li>CinkShadow Settings</li> <li>General Settings</li> <li>Device Setup</li> <li>Backup / Reset</li> <li>License / Updates</li> </ul>	Other Integrations Office 365 / Exchange Server Settings Server Name Exchange Server Usessere	Recorded Future Integration Add New Title Address Frequency
Customizations	Username Username Password Password	
Settings     Integrations     O Domain Controller     SIEM	Submit Azure Audit Logs Client ID	
O Endpoint O Others Configurations	8380ea72-077a-4cfa-b0c5-6f9eb8d7f62c Tenant ID f59fc278-b75a-4bf4-879b-bb6911a66683	

- 4- Fill the forms:
  - a. Title: (Name for this integration)
  - b. Address: (URL at which the API request to be made)
  - c. Username: (Typically the registered email address)
  - d. Password or API: (Provided by Recorded Future)
  - e. Frequency: (recorded future feed update frequency)
  - f. Collection List: (recorded future collection feeds to be downloaded)



**Recorded Future Integration** 

Success! Your request has been submitted.

Add New

Recorded Future Integration
Add New
Title
recordedfuture
Address
https://api.recordedfuture.com/taxii
Username
linoy@linkshadow.com
Password
**********
Frequency
6 hours ~
Collection List (comma seperated)
ip_recent_botnet_traffic, ip_recently_linked_to_cyber_attack, ip_tor_node
Submit
5- Submit



## To Check the Threat Intelligence for any Anomaly:

1- go to ThreatShadow



2- Select the Anomaly and click on the play button to go to Shadow360 Dashboard

Keyword				C Last 24 hours 🗡 💥
				Filter by Stages +
	Score	Entity	Stages	Recent Anomaly
	29	Anas	Exploitation, Suspicious	😟 Unusual Connection
android-a2949bfd23e7e985	21	Jaypee	Suspicious	😔 suspicious
	399	UNKSHADOW-WYD	Suspicious	© proxy
JohnsiPhone	11	LinoyXPS	Suspicious	Onusual geo location
	6	Ashrf	Delivery	Opmain Squatting
DESUTION FOODBDR	21	LAPTOP-BNQ47360	Suspicious	🙆 suspicious
Galaxy Note10	31	ABDALLA	Suspicious	O suspicious
	6	Zaids-Air	Delivery	Domein Squatting
Nihal Su Anas Ex Galaxy-A30	(21)	Nihal	Suspicious	Rproxy
	20	DESKTOP-6CDD8DP	Suspicious	COLE beaconing to anomalous domains
Zaids-Air	(10)	Johns-iPhone	Suspicious	ONS beaconing to anomalous domains
	10	Ryans-Air	Suspicious	ONS beaconing to anomalous domains
ABDALLA	10	android-a29a9bfd23e7e985	Suspicious	ONS beaconing to anomalous domains
	10	Galaxy-Note10	Suspicious	ODNS beaconing to anomalous domains
	10	Galaxy-A30	Suspicious	ONS beaconing to anomalous domains
Achrf LinoxXPS				



3- From Shadow360 Dashboard Select Anomaly Tab



#### 4- From the Anomaly Tab, click on the Public IP Address to get the Threat Intelligence

limeline								
🗮 All Events	A Anomalies	Stages	■ MITRE ATT&CK MATRIX					
1-)								
.10								
:10					alastad Anomalis 🧧 Racant Anomalis	<u> </u>		
Show 10 🗸 entries 🖹	£				elected shoring in the encountry			Search:
Time		Log Source		Source IP	Source Port	Destination IP	Destination Port	Event
A 2020-09-2	12:03:10			172.16.60.45	1617	<u>171.241.1.84</u>	80	View Data
								Previous 1 Net



#### 5- From the Popup table, scroll down to Recorded Future





# THANK YOU

linkshadow.com

Suite 444,320 East Clayton Street, Athens, Georgia 30601, USA | T: +1 877 267 7313