User Guide

SecneurX Threat Feeds for the Threat Connect Platform

Introduction

Enterprise organizations are under attack every second of every day from cybercriminals. Adversaries currently use complicated intrusion kill chains, campaigns and customized Tactics, Techniques and Procedures (TTPs) to disrupt your business or damage your clients. Among the most severe threats to business, the techniques used by adversaries are becoming ever-more targeted, sophisticated and successful. As the volume and complexity of cyber threats increase, contextualizing and prioritizing incidents becomes critical. Enterprises struggle to hire enough malware analysts, and enterprise SOC teams are required to deal with an ever-growing queue of alerts. The industry needs to respond to incidents with tools that are effective and simple.

The ThreatConnect Platform aggregates and organizes feeds from multiple trusted partners, providing diverse threat intelligence within their platform. SecneurX Threat Feeds app arms clients with ultra-fresh data, plugged into their existing setup, to protect their assets from online threats. Data Feeds littered with False Positives are valueless, so very extensive tests and filters are applied before releasing feeds, to ensure that 100% vetted data is delivered. All feeds are generated and monitored by a highly fault-tolerant infrastructure.

App Installation

ThreatConnect's Github hosts the downloads for the app. For installation instructions, refer to the ThreatConnect System Administration Guide (Install an App). For more information, contact your ThreatConnect Customer Success representatives.

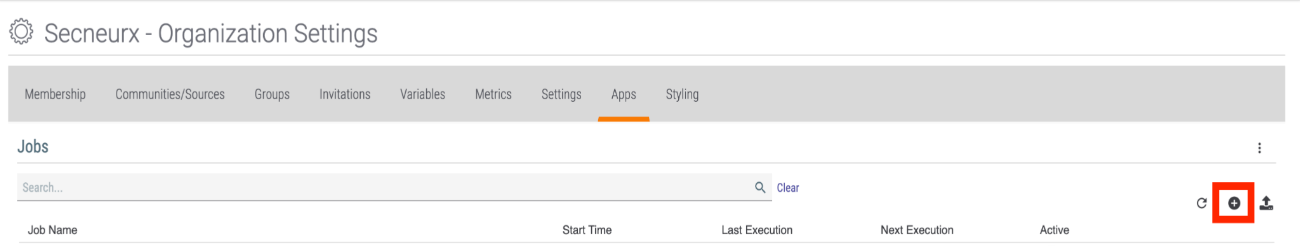
Application Configuration

The SecneurX Threat Feed App provides ThreatConnect users with ability to connect to any of our free or paid threat intelligence feeds.

Make sure you have your SecneurX API-key (available from support@secneurx.com)

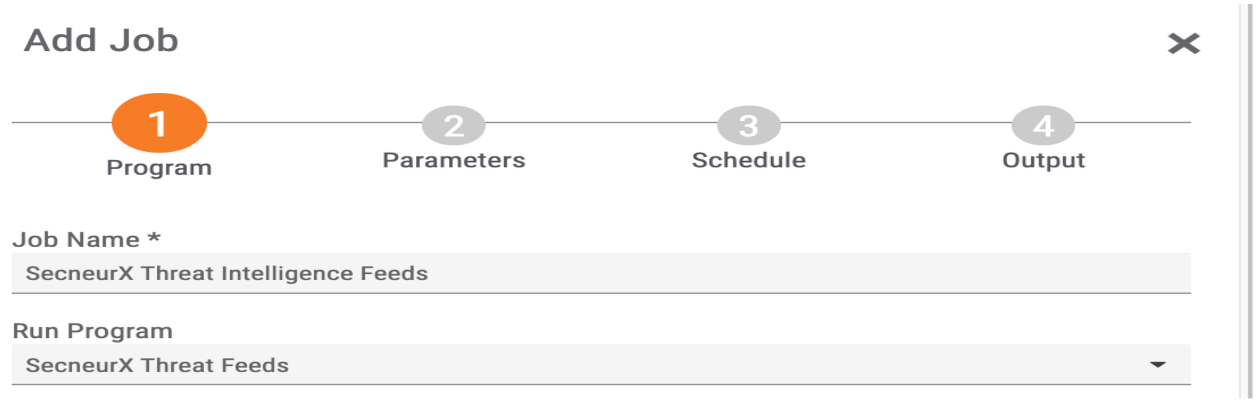
Job Configuration

1. Click the Configure icon in the top right corner in the ThreatConnect platform and click **Organization Settings**
2. Click **Apps**.
3. Click + to create a new job.



To configure a job:

1. In the **Program** window:
    a. In **Job Name**, enter a name for this job (such as SecneurX Threat Intelligence Feed).
    b. Click **Run Program** and select SecneurX Threat Feeds
2. Click **NEXT**.

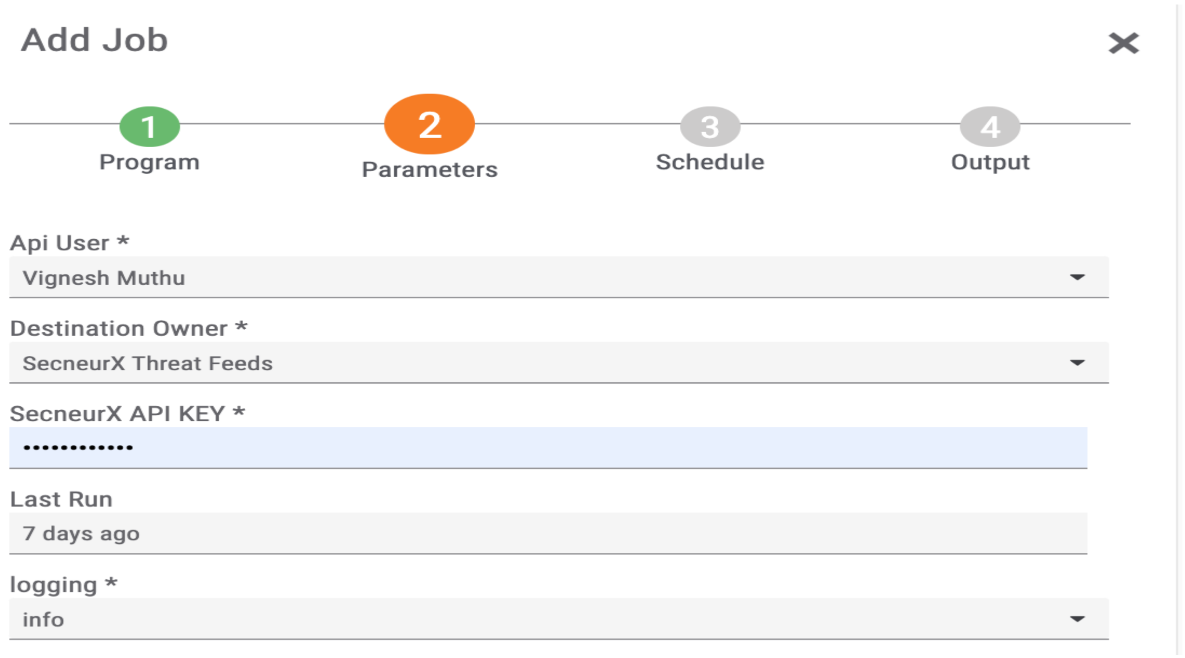


Job Name *
SecneurX Threat Intelligence Feeds

Run Program
SecneurX Threat Feeds

To configure the job parameters:

1. In the Parameters window:
   a. Click **Api User** and select your organization.
   b. Click **Destination Owner** and select the source created by SecneurX Threat Feeds
   c. In the **SecneurX API KEY**, enter the api-key you received from SecneurX (contact support@secneurx.com)
   d. In the **Last Run**, enter the previous # of days to fetch data (example: 7 days ago)
   e. Click **Log Level** and select the required log level (default = warning).
2. Click **NEXT**.



Api User *
Vignesh Muthu

Destination Owner *
SecneurX Threat Feeds

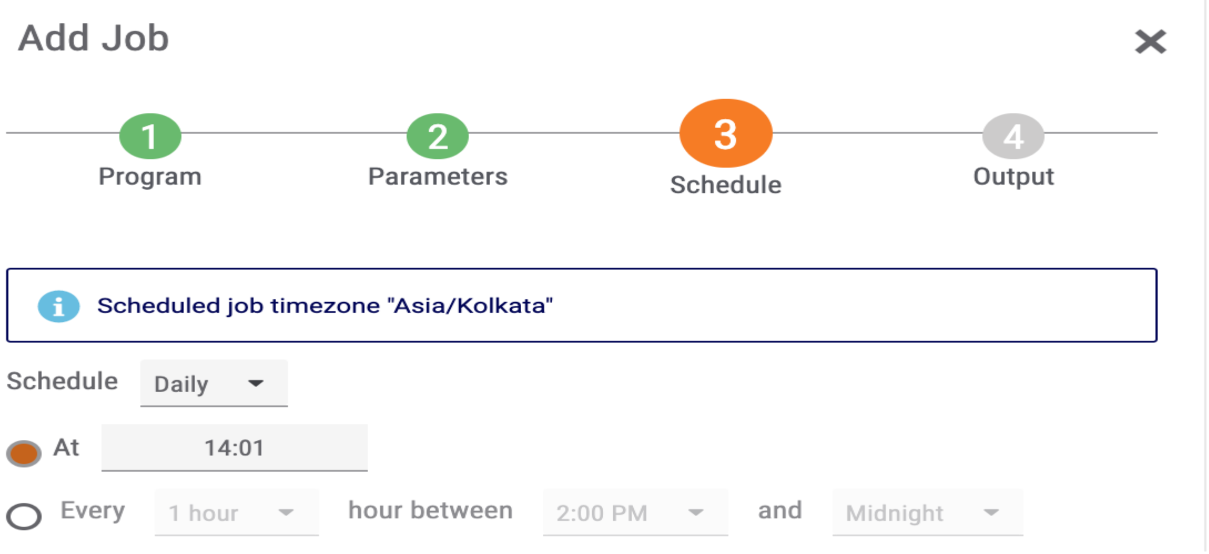
SecneurX API KEY *
•••••••••••••

Last Run
7 days ago

logging *
info

To configure the job schedule:

1. In the **Schedule** window, configure the following according to your environment:
    a. Click **Schedule** and select the required recurrence (such as Daily, Weekly).
    b. Click At or Every and configure the required time recurrence.
2. Click **NEXT**



Scheduled job timezone "Asia/Kolkata"

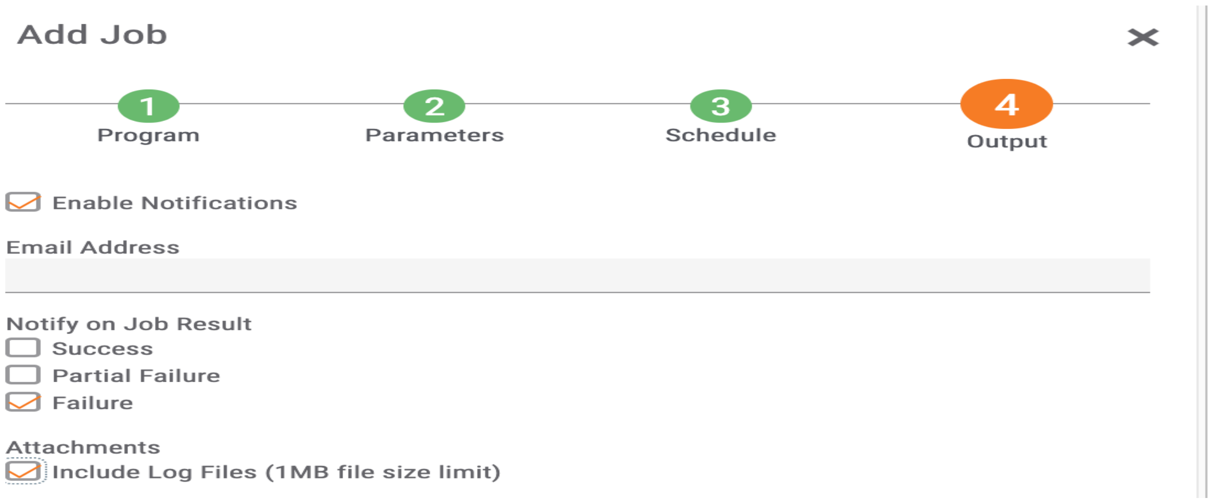
Schedule Daily

● At 14:01

○ Every 1 hour hour between 2:00 PM and Midnight

To receive job result notifications:

1. In the Output window:
    a. Select the **Enable Notifications** checkbox.
    b. In the **Email Address box**, enter the email address to which notifications will be sent.
    c. Select the required checkboxes under Notify on Job Result and Attachments.
2. Click **SAVE**.



☑ Enable Notifications

Email Address

Notify on Job Result

☐ Success

☐ Partial Failure

☑ Failure

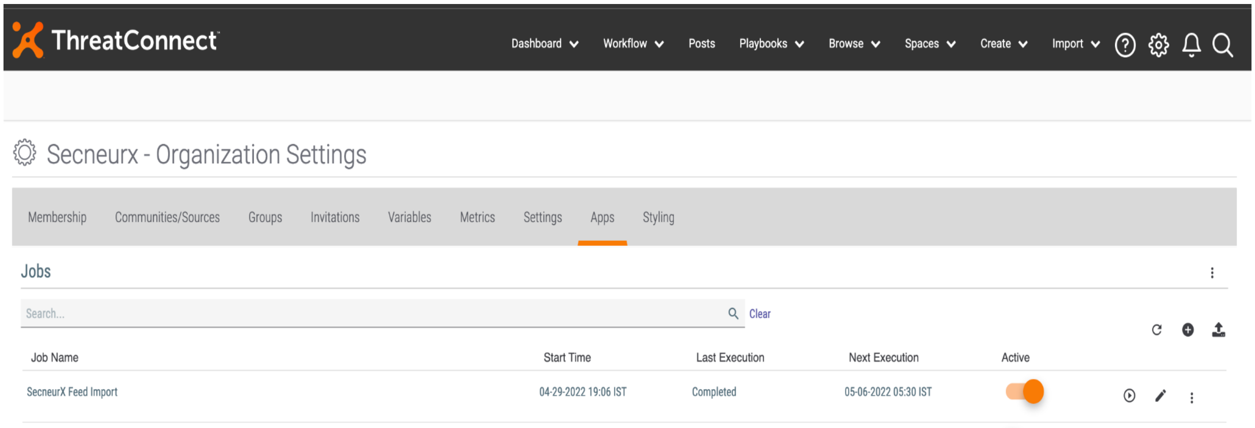
Attachments

☑ Include Log Files (1MB file size limit)

To activate the job:

1. In the Jobs list, on the required job row, click the **Active** slider

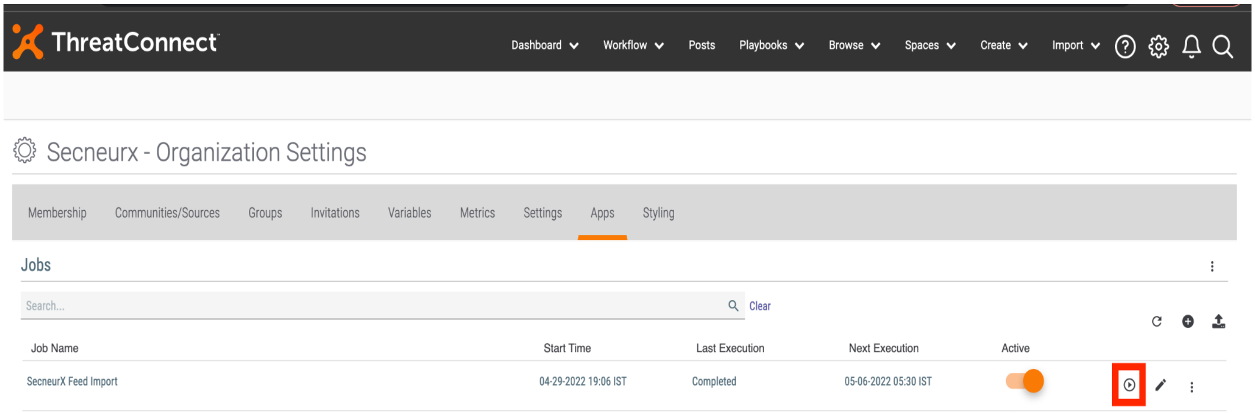
For each job, you can view the Start Time, Last Execution status and Next Execution time.



Job Name	Start Time	Last Execution	Next Execution	Active
SecneurX Feed Import	04-29-2022 19:06 IST	Completed	05-06-2022 05:30 IST	●

To run the job manually:

1. In the Jobs list, on the required job row, in the Options column, click play.



Secneurx - Organization Settings

Jobs

Job Name	Start Time	Last Execution	Next Execution	Active
SecneurX Feed Import	04-29-2022 19:06 IST	Completed	05-06-2022 05:30 IST	

Data Mapping

The table below documents the data mapping that takes place between the SecneurX Threat Feed Threat Intelligence data and the ThreatConnect Platform.

SecneurX Field	ThreatConnect Field/Object	Possible Values	Description
C2Address	Address, Tag "C2 Address"	Any valid IP address	
MalAddress	Address, Tag "Mal Address"	Any valid IP address	
BotAddress	Address, Tag "Bot Address"	Any valid IP address	
ExploitAddress	Address, Tag "Exploit Address"	Any valid IP address	
CompromisedAddress	Address, Tag "Compromised Address"	Any valid IP address	
TorAddress	Address, Tag "Tor Address"	Any valid IP address	
PhishAddress	Address, Tag "Phish Address"	Any valid IP address	
ParkedAddress	Address, Tag "Parked Address"	Any valid IP address	
AptAddress	Address, Tag "Apt	Any valid IP address	

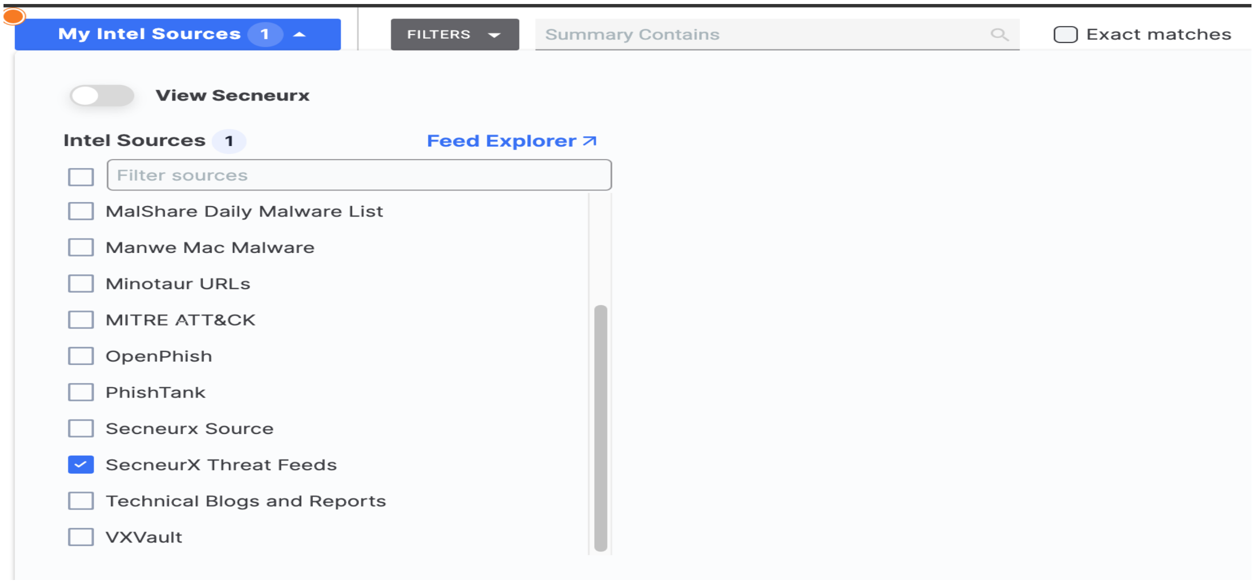
	Address"		
DgaAddress	Address, Tag "Dga Address"	Any valid IP address	
C2Hostname	Hosts, Tag "C2 Hosts"	Any valid hostname	
MalHostname	Hosts, Tag "Mal Hosts"	Any valid hostname	
AdwareHostname	Hosts, Tag "Adware Hosts"	Any valid hostname	
BotHostname	Hosts, Tag "Bot Hosts"	Any valid hostname	
ExploitHostname	Hosts, Tag "Exploit Hosts"	Any valid hostname	
CompromisedHostname	Hosts, Tag "Compromised Hosts"	Any valid hostname	
TorHostname	Hosts, Tag "Tor Hosts"	Any valid hostname	
PhishHostname	Hosts, Tag "Phish Hosts"	Any valid hostname	
ParkedHostname	Hosts, Tag "Parked Hosts"	Any valid hostname	
AptHostname	Hosts, Tag "Apt Hosts"	Any valid hostname	
SinkholeHostname	Hosts, Tag "Sinkhole Hosts"	Any valid hostname	
DgaHostname	Hosts, Tag "Dga Hosts"	Any valid hostname	
C2Url	Url, Tag "C2 Url"	Any valid Url	
MalUrl	Url, Tag "Mal Url"	Any valid Url	
AdwareUrl	Url, Tag "Adware Url"	Any valid Url	
BotUrl	Url, Tag "Bot Url"	Any valid Url	
ExploitAddress	Url, Tag "Exploit Url"	Any valid Url	
CompromisedUrl	Url, Tag "Compromised Url"	Any valid Url	
TorUrl	Url, Tag "Tor Url"	Any valid Url	
PhishUrl	Url, Tag "Phish Url"	Any valid Url	

ParkedUrl	Url, Tag "Parked Url"	Any valid Url	
AptUrl	Url, Tag "Apt Url"	Any valid Url	
SinkholeUrl	Url, Tag "Sinkhole Url"	Any valid Url	
DgaUrl	Url, Tag "Dga Url"	Any valid Url	
MalUser Agent	User Agent, Tag "Mal User Agent"	Any valid User Agent	
AptUser Agent	User Agent, Tag "Apt User Agent"	Any valid User Agent	
MalwareFileHash	File, Tag "Mal File"	Any text string	
APTFileHash	File, Tag "APT File"	Any text string	
APTEmail Address	Email Address,Tag "APT Email Address"	Any text string	
CompromisedEmail Address	Email Address,Tag "Compromised Email Address"	Any text string	
MalEmail Address	Email Address,Tag "Mal Email Address"	Any text string	
PhishEmail Address	Email Address,Tag "Phish Email Address"	Any text string	
SpamEmail Address	Email Address,Tag "Spam Email Address"	Any text string	
APTEmailSubject	Email Subject,Tag "APT Email Subject"	Any text string	
CompromisedEmailSubjec	Email Address,Tag "Compromised EmailSubject"	Any text string	
MalEmailSubject	Email Address,Tag "Mal EmailSubject"	Any text string	
PhishEmailSubject	Email Address,Tag "Phish EmailSubject"	Any text string	
SpamEmailSubject	Email Address,Tag "Spam EmailSubject"	Any text string	
PhishCIDR	CIDR,Tag "Phish CIDR"	Any valid IP address with subnet	

DgaCIDR	CIDR,Tag "Dga CIDR"	Any valid IP address with subnet	
AdwareRegistry Key	Registry Key,Tag "Adware Registry Key"	Any text string	
APTRegistry Key	Registry Key,Tag "APT Registry Key"	Any text string	
MalRegistry Key	Registry Key,Tag "Mal Registry Key"	Any text string	
ThreatScore(1-5)	Threat Rating (1-5)	Numbers 1-5	
ThreatConfidence	Confidence	Numbers 1-100	

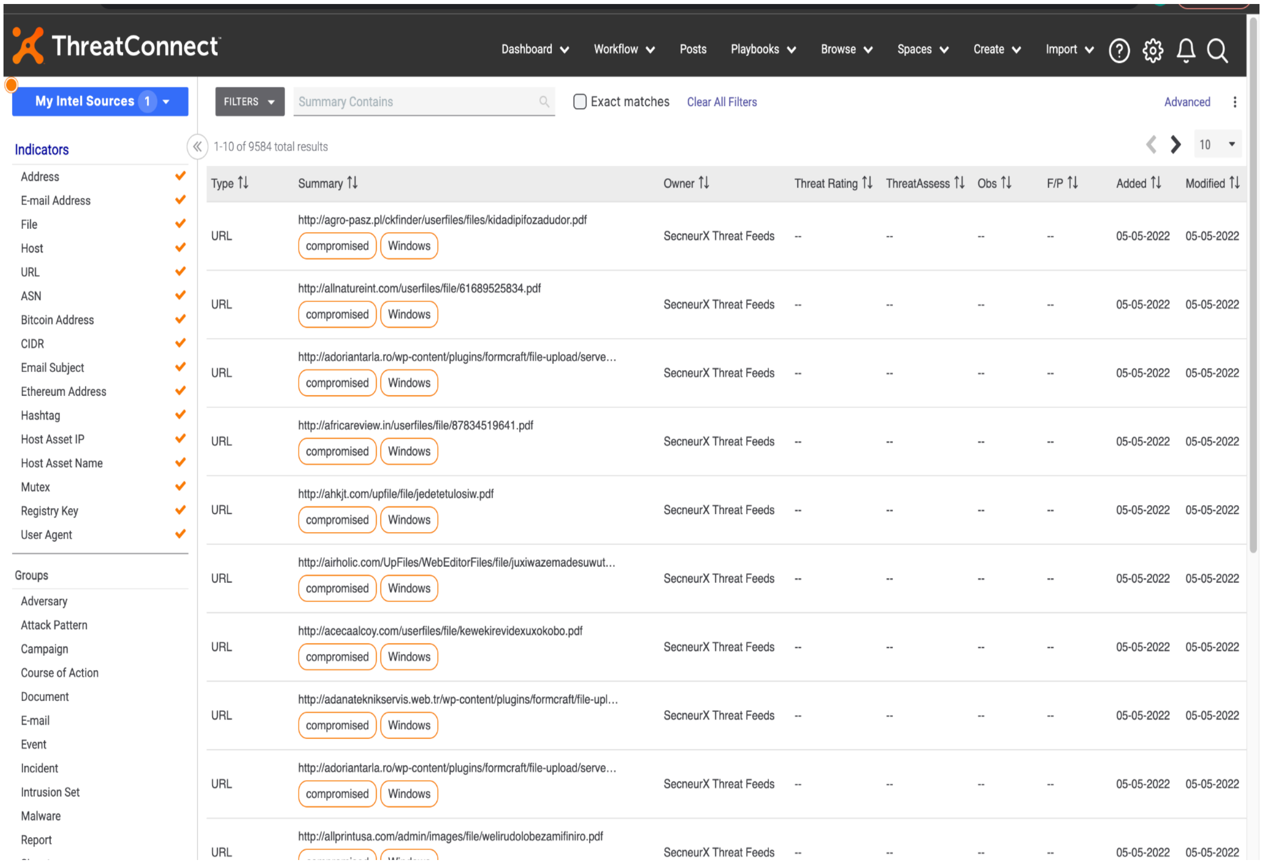
Job Output

1. Click **Browse > Indicators**.
2. Click **MY INTEL SOURCES**.
3. Select only the source configured in Job Configuration, To configure the job parameters: (ThreatConnect Owner). The source will be **SecneurX Threat Feeds**



☐ MalShare Daily Malware List
☐ Manwe Mac Malware
☐ Minotaur URLs
☐ MITRE ATT&CK
☐ OpenPhish
☐ PhishTank
☐ Secneurx Source
☑ SecneurX Threat Feeds
☐ Technical Blogs and Reports
☐ VXVault

Examples Sample of Threat Intelligence Feed from SecneurX sources to ThreatConnect Platform:



1-10 of 9584 total results

Type	Summary	Owner	Threat Rating	ThreatAssess	Obs	F/P	Added	Modified
URL	http://agro-pasz.pl/ckfinder/userfiles/files/kidadipifozadudor.pdf compromised Windows	SecneurX Threat Feeds	--	--	--	--	05-05-2022	05-05-2022
URL	http://allnatureint.com/userfiles/file/61689525834.pdf compromised Windows	SecneurX Threat Feeds	--	--	--	--	05-05-2022	05-05-2022
URL	http://adoriantarla.ro/wp-content/plugins/formcraft/file-upload/serve… compromised Windows	SecneurX Threat Feeds	--	--	--	--	05-05-2022	05-05-2022
URL	http://africareview.in/userfiles/file/87834519641.pdf compromised Windows	SecneurX Threat Feeds	--	--	--	--	05-05-2022	05-05-2022
URL	http://ahkjt.com/upfile/file/jedetetulosiw.pdf compromised Windows	SecneurX Threat Feeds	--	--	--	--	05-05-2022	05-05-2022
URL	http://airholic.com/UpFiles/WebEditorFiles/file/juxiwazemadesuwut… compromised Windows	SecneurX Threat Feeds	--	--	--	--	05-05-2022	05-05-2022
URL	http://acecaalcoy.com/userfiles/file/kewekirevidexuxokobo.pdf compromised Windows	SecneurX Threat Feeds	--	--	--	--	05-05-2022	05-05-2022
URL	http://adanateknikservis.web.tr/wp-content/plugins/formcraft/file-upl… compromised Windows	SecneurX Threat Feeds	--	--	--	--	05-05-2022	05-05-2022
URL	http://adoriantarla.ro/wp-content/plugins/formcraft/file-upload/serve… compromised Windows	SecneurX Threat Feeds	--	--	--	--	05-05-2022	05-05-2022
URL	http://allprintusa.com/admin/images/file/welirudolobezamifiniro.pdf	SecneurX Threat Feeds	--	--	--	--	05-05-2022	05-05-2022

SecneurX Support

For any questions or issues with the SecneurX app, please contact support@secneurx.com

Release Notes

Version	Data	Changes
1.0.5	02-May-2022	Initial Release