



## ThreatConnect – Loginsoft PursuitX User Guide

Version 1.0.0

### Contents

<b>Introduction</b>	2
<b>Release Notes</b>	3
<b>Data Mapping</b>	4
<b>Configuration Requirements</b>	5
<b>App Installation via Feed Deployer</b>	5
<b>ThreatConnect Job Configuration</b>	6
<b>Browsing Loginsoft PursuitX Feed</b>	10
<b>Signature Feed:</b>	11
<b>Threat Feed:</b>	12
<b>Support</b>	13

## Introduction

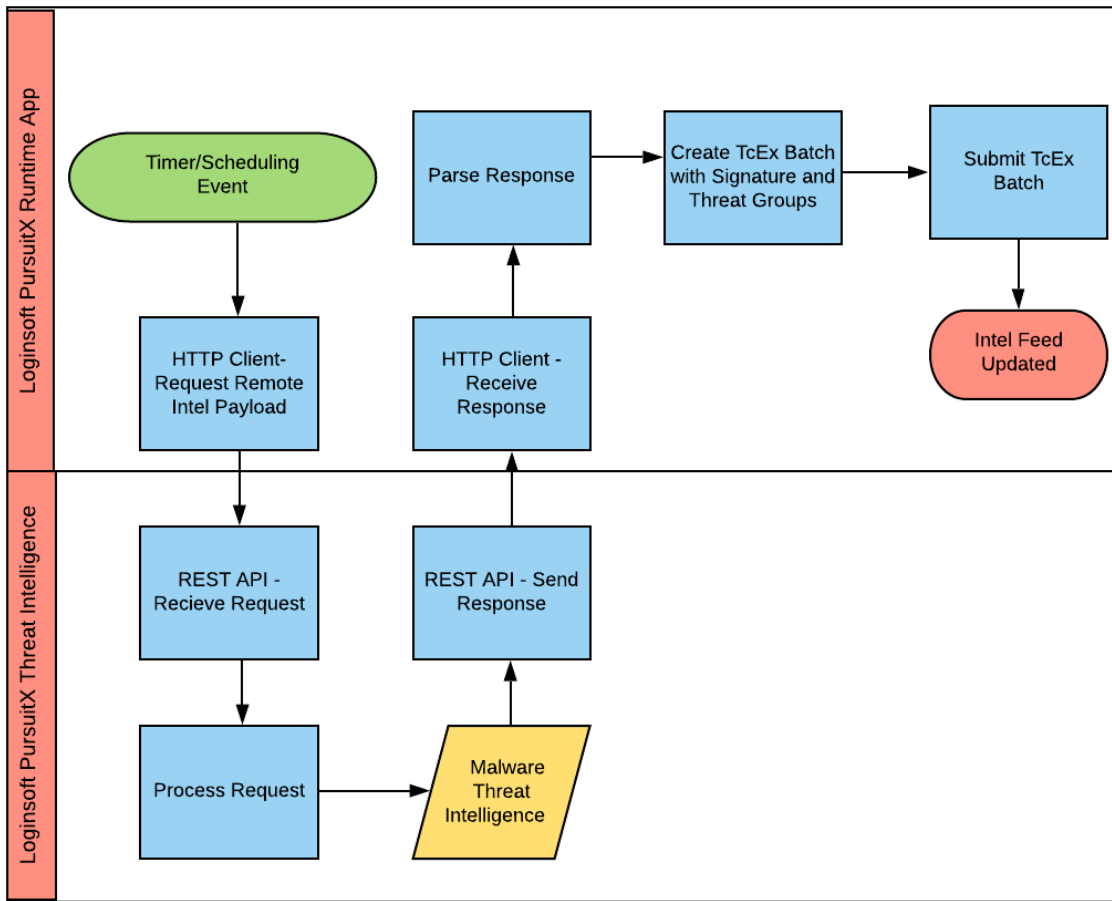
**Loginsoft PursuitX** provides intelligence-driven threat detections of malware families and threat actors and their tactics, techniques, and procedures which help an organization to integrate with their current SIEM solutions. PursuitX consistently monitors various adversaries by tracking the attack behavior comprising TTPs and collect relevant log events to generate detection rules specific to a malware family or a threat actor.

- With context driven signatures that help to improve existing security controls, the detection feed comes in a prominent and revolutionary format "SIGMA" which is a human-readable and effective format that can describe relevant log events from various telemetry and convert rules to queries of the respective SIEM solution of their choice.
- The PursuitX team continuously research and update the detections to automatically prioritize the events for actionable response.

### **Sigma Rules as De facto:**

- Describes detection and includes metadata which is helpful for investigations
- Can easily be integrated with several SIEM solutions
- Community endorsed
- Can easily be shared with threat intelligence platforms

This integration consists of consuming the Loginsoft PursuitX Threat Intelligence feed and importing the data as signature and threat groups into the ThreatConnect Platform as a Threat Intelligence feed. A high-level run of the Loginsoft PursuitX Threat Intelligence feed is shown below.



## Release Notes

App Version	Release Date	Details
1.0.0		Initial Release.

## Data Mapping

The following table documents the data mapping that takes place between the Loginsoft PursuitX Threat Intelligence feed data and the ThreatConnect Platform.

Malware Threat Intelligence Feed	ThreatConnect Field/Object	Possible Values	Notes
title	name – Signature Group	String	The title data point from the Loginsoft feed will be mapped to the name attribute of the signature object.
description	Attribute – Description – Signature Group	String	The description data point from the Loginsoft feed will be mapped to the Description Attribute.
malware_family	name – Threat Group	String	The malware_family data point from the Loginsoft feed will be mapped to the name of the Threat Object.
malware_type	Attribute - Malware Family Variety – Threat Group	String	The malware_type data point from the Loginsoft feed will be mapped to the Malware Family Variety Attribute of Threat Object. And also, we will adding the Threat Type Attribute to Malware Family
mitre_techniques	Tags – Signature Group	String Array	The mitre_techniques data point from the feed will be added as tags.

reference	Attribute – Source – Signature Group	String Array	The reference data point from the feed will be mapped to the Source Attribute.
rule_source	Signature File Content – Signature Group	String	The rule_source data point from the Loginsoft feed will be mapped to the Signature File Content of the Signature Object.
rule_id	xid – Signature Group	String	The rule_id data point from the Loginsoft feed will be mapped to xid attribute of the Signature object

## Configuration Requirements

1. Access to a ThreatConnect Platform Instance
2. ThreatConnect API user

## Job App Installation

For download and installation instructions, please refer to the ThreatConnect System Administration Guide(Install an App). For more information, contact your ThreatConnect Customer Success representatives.

## ThreatConnect Job Configuration

The ThreatConnect Platform allows customers to run jobs on a scheduled basis. Once the package has been installed, the customer can run the Loginsoft PursuitX Threat Intelligence feed as frequently as they desire. The Loginsoft PursuitX feed is quite small and so running the feed very frequently does not affect the performance of the ThreatConnect Platform.

**\*\*Note that these steps are not necessary if the app was deployed using Feed Deployer as the job would have already been configured.**

- Go to the gear in the top right corner in the ThreatConnect platform then **Org Settings > Apps.**
- Click on the + to create a new job

### Program Screen:

- Enter the Job Name (Ex: Loginsoft PursuitX Feed).
- Select the Run program as a Loginsoft PursuitX from the dropdown.

Add Job ×

1 2 3 4  
Program Parameters Schedule Output

Job Name \*  
Loginsoft PursuitX Job

Run Program  
Loginsoft PursuitX

CANCEL NEXT

- Click NEXT.

### Parameter Screen:

- For API User, click on the down arrow and select your organization
- For ThreatConnect Owner, click on the down arrow and select the source created by the Feed Deployer
- For Log Level, select it from dropdown default log level set to warning.

Add Job

1 Program 2 Parameters 3 Schedule 4 Output

Api User \*  
Venkat Rambatza

ThreatConnect Owner \*  
PursuitX Source

Loginsoft PursuitX Endpoint \*

Log Level \*  
warning

CANCEL PREVIOUS NEXT

- Click NEXT

## Schedule Screen:

- Depending on your environment, you can schedule the feed at daily hours, weekly etc., select the appropriate values from the dropdown menu.

Add Job

1

Program

2

Parameters

3

Schedule

4

Output

Scheduled job timezone "GMT"

Schedule

Daily

At

16:52

Every

12 hours

hours between

Midnight

and

11:00 PM

CANCEL

PREVIOUS

NEXT

- Click NEXT



## Output Screen:

- If you want to be notified on job results, click the box next to Enable Notifications, enter an email address for the notifications to be sent, and which notifications that you want and if you want a log file attached.

Add Job

1 Program 2 Parameters 3 Schedule 4 Output

☒ Enable Notifications

Email Address

Notify on Job Result

☐ Success

☐ Partial Failure

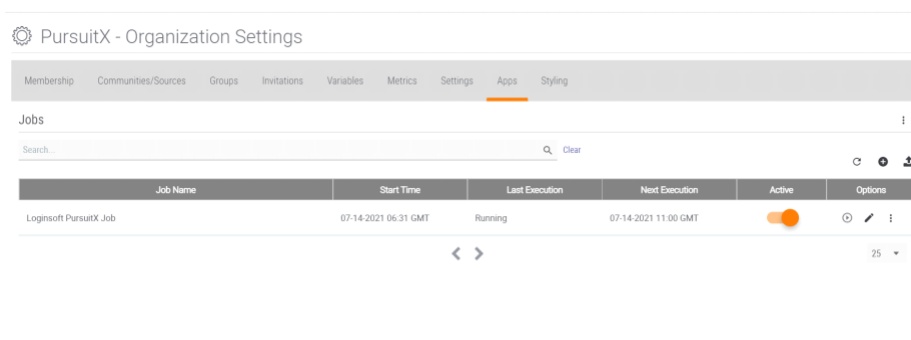
☒ Failure

Attachments

☒ Include Log Files (1MB file size limit)

CANCEL PREVIOUS SAVE

- Click SAVE
- Once the Job has been saved, we can find our job on Jobs under Apps
- Click on the slider under Active to activate the job.



Job Name	Start Time	Last Execution	Next Execution	Active	Options
Loginsoft PursuitX Job	07-14-2021 06:31 GMT	Running	07-14-2021 11:00 GMT	<input checked="" type="checkbox"/>	

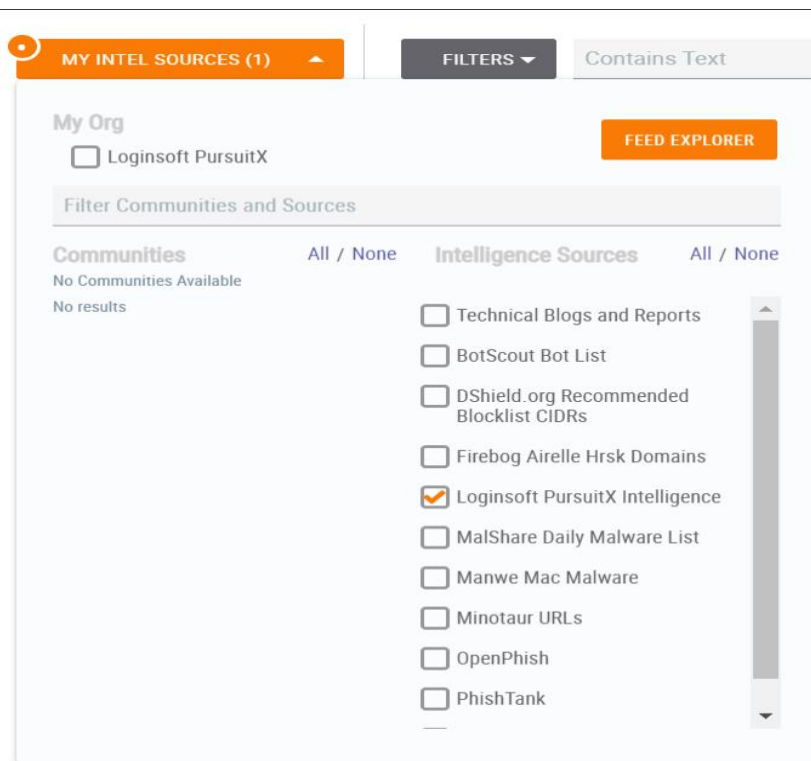
- Here we can observe the Start Time and Next Execution time and Last Execution Status as well if you want to run the job at this time click on the play button in options tab.

## Browsing Loginsoft PursuitX Feed

For guidance on general browsing of indicators and groups in the ThreatConnect Platform, please refer to the article below:

<https://training.threatconnect.com/learn/article/browse-kb-article>

1. Navigate to the browse page and check to make sure that the Loginsoft PursuitX Threat Intelligence Feed is checked.



MY INTEL SOURCES (1) FILTERS Contains Text

My Org  
☒ Loginsoft PursuitX FEED EXPLORER

Filter Communities and Sources

Communities All / None Intelligence Sources All / None

No Communities Available  
No results

- ☐ Technical Blogs and Reports
- ☐ BotScout Bot List
- ☐ DShield.org Recommended Blocklist CIDRs
- ☐ Firebog Airtelle Hrsk Domains
- ☒ Loginsoft PursuitX Intelligence
- ☐ MalShare Daily Malware List
- ☐ Manwe Mac Malware
- ☐ Minotaur URLs
- ☐ OpenPhish
- ☐ PhishTank

## Signature Feed:

To browse **Signature Feed** from Loginsoft PursuitX, select signature group.

MY INTEL SOURCES (1) FILTERS Contains Text Clear All Advanced 1-10 of 44 Results

Indicators	Type	Format	Summary	Owner	Tags	Added
Address E-mail Address File Host URL ASN CIDR Email Subject Hashtag Mutex Registry Key User Agent	Signature	Sigma	Adwind RAT detection	Loginsoft PursuitX Int...	T1059 - COMMAND AND SCRIPTL... T1112 - MODIFY REGISTRY T1489 - SERVICE STOP +1 more...	08-20-2021
Groups Adversary Campaign Document E-mail Event Incident Intrusion Set Report Signature Task Threat	Signature	Sigma	Agent Tesla Trojan Detection	Loginsoft PursuitX Int...	T1053 - SCHEDULED TASK/JOB T1059 - COMMAND AND SCRIPTL... T1071 - APPLICATION LAYER PR... +3 more...	08-20-2021
	Signature	Sigma	AsyncRAT Detection	Loginsoft PursuitX Int...	T1012 - QUERY REGISTRY T1053.005 - SCHEDULED TASK/J... T1059 - COMMAND AND SCRIPTL... +1 more...	08-20-2021
	Signature	Sigma	Azorult Detection	Loginsoft PursuitX Int...	T1041 - EXFILTRATION OVER C2... T1083 - FILE AND DIRECTORY DI... T1112 - MODIFY REGISTRY +6 more...	08-20-2021

### Agent Tesla Trojan Detection

Type	Owner	Added
Signature	Loginsoft PursuitX Intelligence Dev	08-20-2021

#### File Information

Name	Modified	Format
114c4951-2b60-4467-b44c-ca9900319664.yml	08-20-2021	Sigma

#### Tags

- T1112 - MODIFY REGISTRY
- T1071 - APPLICATION LAYER PROTOCOL
- T1059 - COMMAND AND SCRIPTING INTERPRETER
- T1053 - SCHEDULED TASK/JOB
- T1140 - DEOBFUSCATE/DECODE FILES OR INFORMATION
- T1547.001 - BOOT OR LOGON AUTOSTART EXECUTION: REGISTRY RUN KEYS / STARTUP FOLDER

#### Attributes

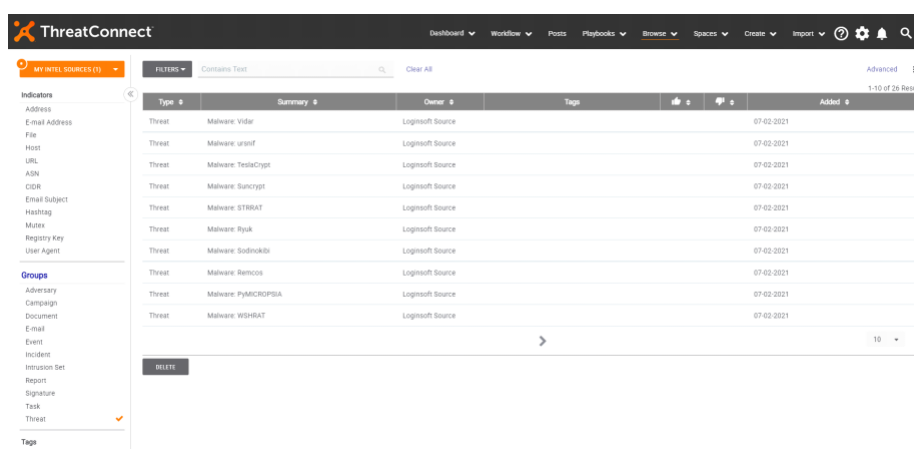
Type	Last Modified	Value
Source	08-20-2021	<a href="https://www.fortinet.com/blog/threat-research/new-agent-tesla-variant-spreading-by-phishings">https://www.fortinet.com/blog/threat-research/new-agent-tesla-variant-spreading-by-phishings</a> , <a href="https://www.vmrays.com/cyber-security-blog/threat-bulletin-agent-tesla/">https://www.vmrays.com/cyber-security-blog/threat-bulletin-agent-tesla/</a> , <a href="https://unit42.paloaltonetworks.com/covid-19-themed-cyber-attacks-target-government-and-medical-organizations/">https://unit42.paloaltonetworks.com/covid-19-themed-cyber-attacks-target-government-and-medical-organizations/</a>
Description	08-20-2021	Detecting Agent Tesla based on the behaviour

#### Associated Intel

Type	Owner	Date Added
Threat Malware: Agent Tesla	Loginsoft PursuitX Intelligence Dev	08-20-2021

## Threat Feed:

To browse **Threat Feed** from Loginsoft PursuitX, select threat group



ThreatConnect

Dashboard Workflow Posts Playbooks Browse Spaces Create Import

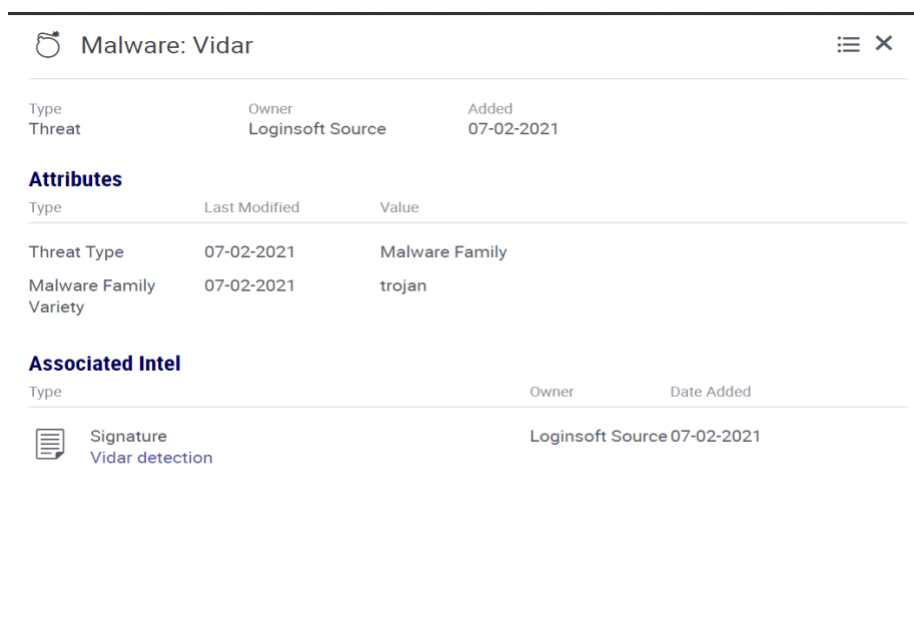
MY INTEL SOURCES (1)

FILTERS Contains Text Clear All

Advanced 1-10 of 26 Results

Type	Summary	Owner	Tags	Added
Threat	Malware: Vidar	Loginsoft Source		07-02-2021
Threat	Malware: uriof	Loginsoft Source		07-02-2021
Threat	Malware: TeslaCrypt	Loginsoft Source		07-02-2021
Threat	Malware: Suncrypt	Loginsoft Source		07-02-2021
Threat	Malware: STRBAT	Loginsoft Source		07-02-2021
Threat	Malware: Ryuk	Loginsoft Source		07-02-2021
Threat	Malware: Sodinokibi	Loginsoft Source		07-02-2021
Threat	Malware: Remcos	Loginsoft Source		07-02-2021
Threat	Malware: PyMICROPSA	Loginsoft Source		07-02-2021
Threat	Malware: WSHBAT	Loginsoft Source		07-02-2021

DELETE



Malware: Vidar

Type	Owner	Added
Threat	Loginsoft Source	07-02-2021

**Attributes**

Type	Last Modified	Value
Threat Type	07-02-2021	Malware Family
Malware Family Variety	07-02-2021	trojan

**Associated Intel**

Type	Owner	Date Added
Signature Vidar detection	Loginsoft Source	07-02-2021

## Support

For assistance with this App, to report a bug, or feature requests please contact us via the following.

<b>Support Portal</b>	<a href="https://www.loginsoft.com/contact/">https://www.loginsoft.com/contact/</a>
<b>Email</b>	<a href="mailto:pursuitX-Intel@loginsoft.com">pursuitX-Intel@loginsoft.com</a>
<b>Phone</b>	+1 7039567410