PolySwarm Ransomware Threat Intelligence Feed for ThreatConnect

User Guide v1.0
App Version 1.1.1

Introduction

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. PolySwarm's Ransomware feed app seamlessly integrates into The ThreatConnect Platform and allows users to obtain a high quality listing of known ransomware and first stage malware hashes along with associated metadata. One of the metadata data points is the PolyScore™ (denoted as the confidence rating), a single number that reflects the likelihood that a given file contains malware based on asserting engines' recent historical success with similar malware families and file types.

PolySwarm uniquely addresses emergent and 0-day malware by using a network of research-driven and commercial malware detections engines that compete in real-time to detect malware. We compliment these engines with a number of static analysis solutions and dynamic analysis sandboxes to provide robust and actionable metadata.

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.

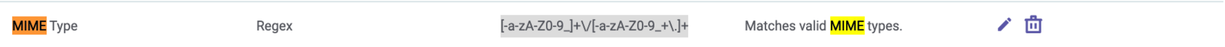
Application Configuration

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

MIME Type Validation

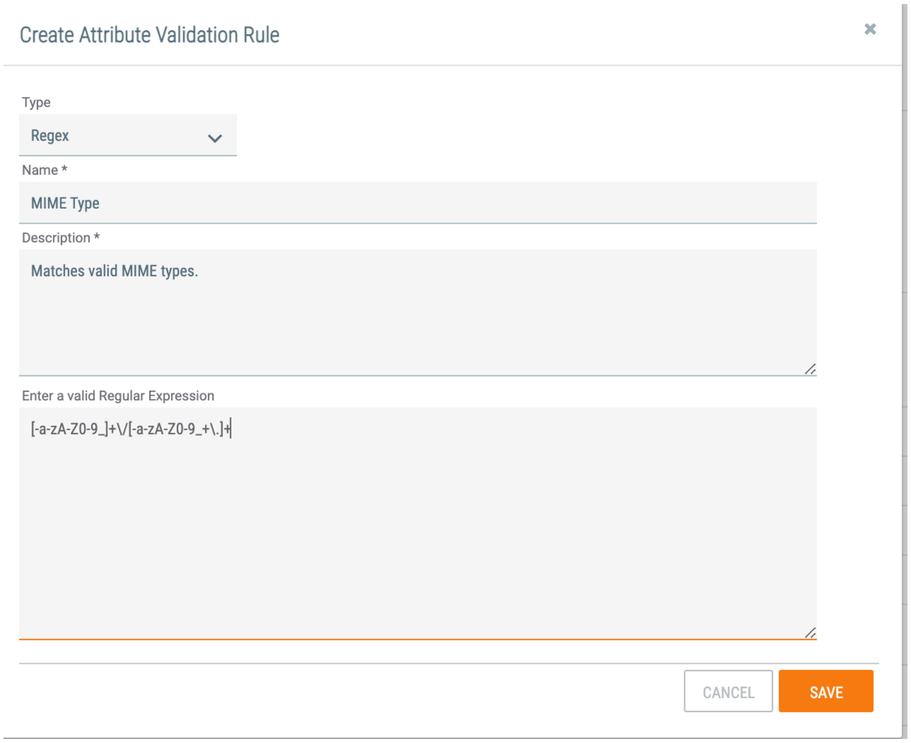
You need to update the MIME Type validation regex:

- Go to the gear in the top right corner in the ThreatConnect platform then System Settings
- Navigate to attribute validation tab
- Scroll down to the MIME Type entry and click on the pencil icon.



MIME Type	Regex	[-a-zA-Z0-9_]+\/[-a-zA-Z0-9_+\.]+	Matches valid MIME types.

- Change the current regex used to match the following:
  - [-a-zA-Z0-9_]+V[-a-zA-Z0-9_+\.]+



Create Attribute Validation Rule

Type: Regex

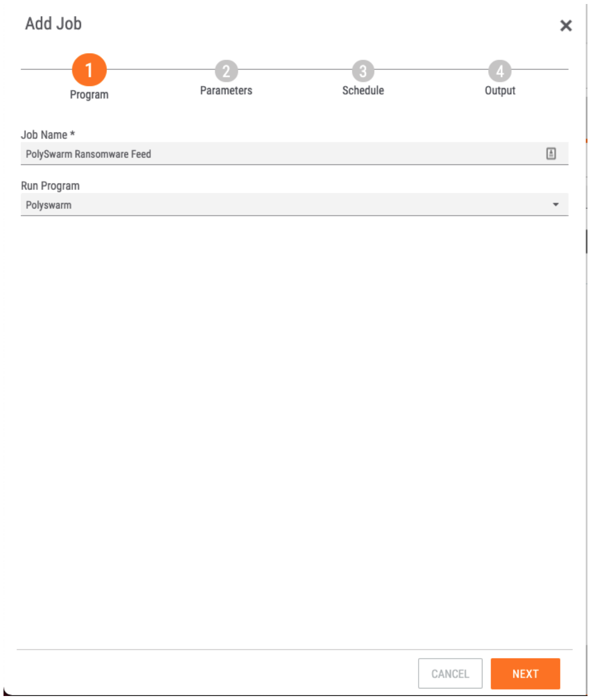
Name *: MIME Type

Description *: Matches valid MIME types.

Enter a valid Regular Expression: [-a-zA-Z0-9_]+\/[-a-zA-Z0-9_+\.]+

Job Configuration

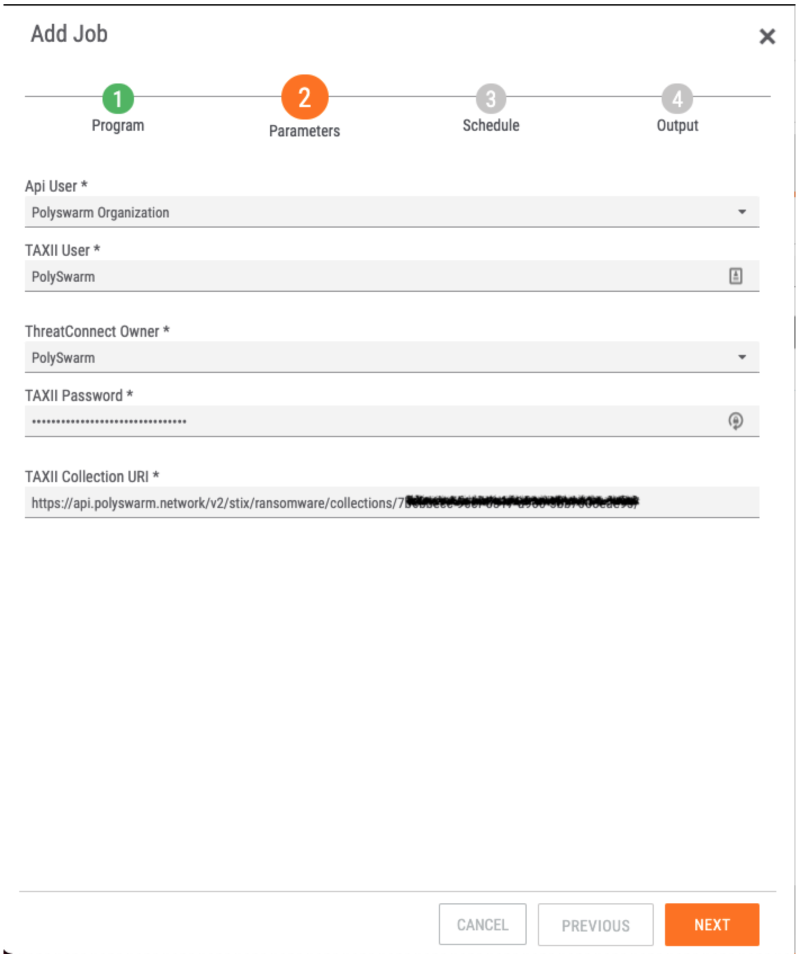
- Verify the PolySwarm Feed App is installed
- Contact PolySwarm at sales@polyswarm.io to have the feed right added to your account and get the appropriate collection URI.
- Obtain a PolySwarm API Key from https://polyswarm.network/account/api-keys
- Go to the gear in the top right corner in the ThreatConnect platform then **Org Settings > Apps**
- Click on the + to create a new job
- 1 Program Screen
    - Give the job name (ex: PolySwarm Ransomware Feed)
    - Click on the down arrow, scroll down until you see Polyswarm



Job Name *
PolySwarm Ransomware Feed

Run Program
Polyswarm

    - Click NEXT
- 2 Parameters Screen
    - For Api User, click the down arrow and select your organization
    - For TAXII user, enter your company name without spaces
    - For ThreatConnect Owner, click the down arrow and select the source created by the Feed Deployer
    - For TAXII Password, enter the API key from above.
    - For TAXII Collection URI, enter the URI that you where provided by PolySwarm



Add Job

Api User *
Polyswarm Organization

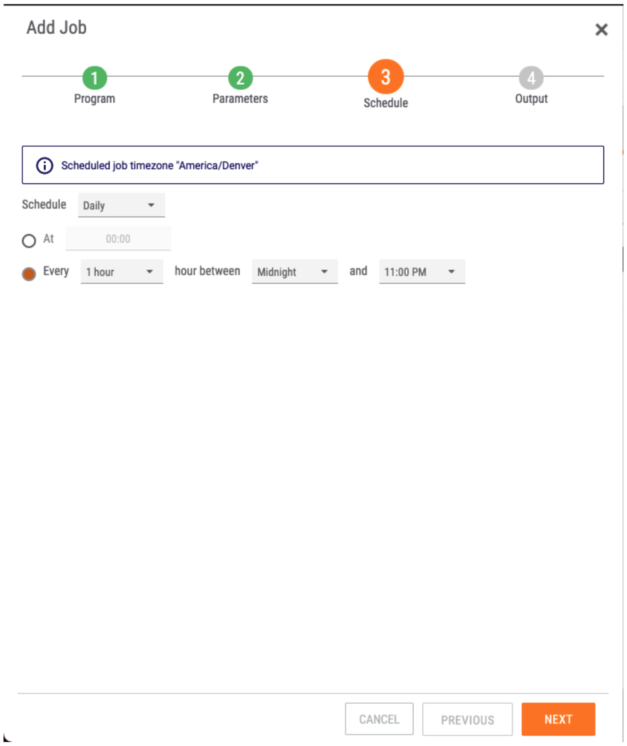
TAXII User *
PolySwarm

ThreatConnect Owner *
PolySwarm

TAXII Password *
••••••••••••••••••••••••••••••••

TAXII Collection URI *
https://api.polyswarm.network/v2/stix/ransomware/collections/7[redacted]

  - Click NEXT
- 3 Schedule
  - Recommended schedule is Daily and Every hour all day long but depending on your environment, you may need/want to adjust to meet operational and production requirements.



Scheduled job timezone "America/Denver"

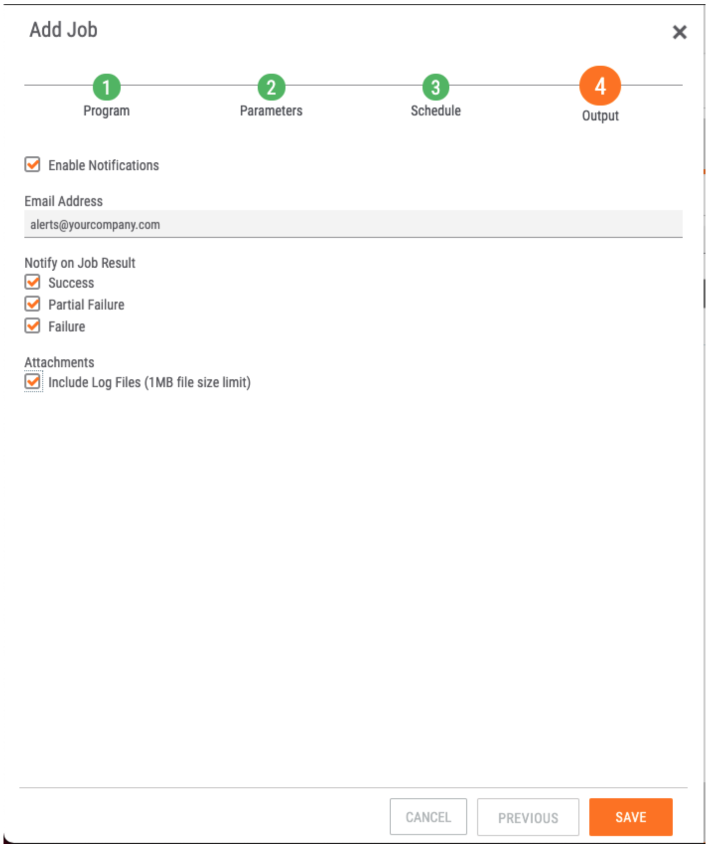
Schedule Daily

○ At 00:00

● Every 1 hour hour between Midnight and 11:00 PM

- Click NEXT

- 4 Output
  - 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

☑ Enable Notifications

Email Address

alerts@yourcompany.com

Notify on Job Result

☑ Success

☑ Partial Failure

☑ Failure

Attachments

☑ Include Log Files (1MB file size limit)

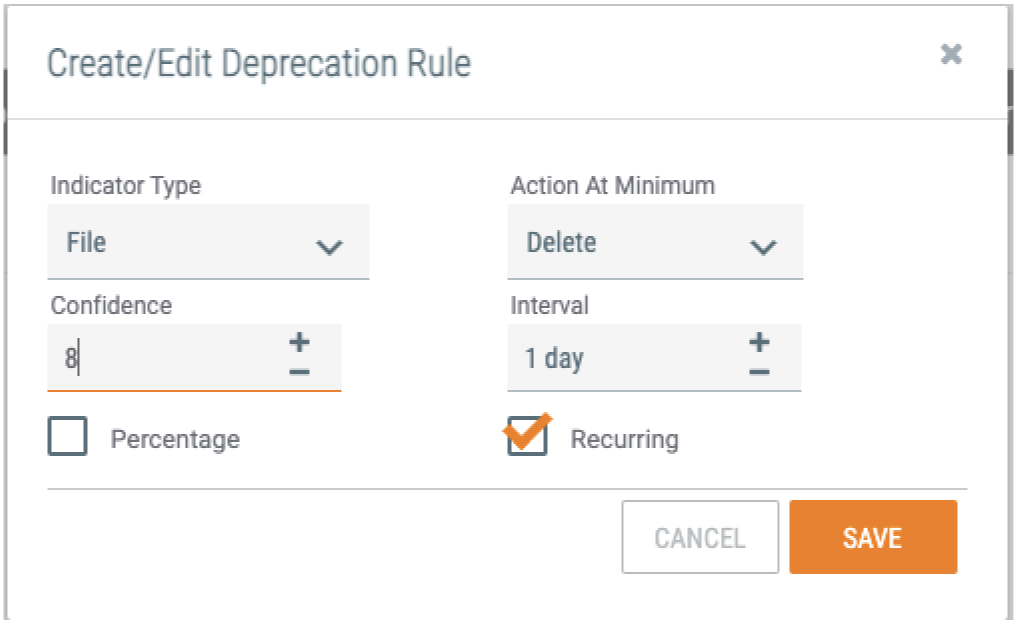
- Click SAVE
- Once Job has been saved, click on the slider under Active to activate the job.

Indicator Depreciation

The ThreatConnect Platform has a limit to the number of indicators that can be stored so you will need to set up a depreciation job to age out the data in the feed. We recommend that you configure the depreciation job to age out the events after two weeks but your production and operational requirements may vary.

Depreciation Configuration

1. Go to the gear in the top right corner in the ThreatConnect platform then **Org Config**
2. From the Org Config screen, click on the Depreciation Rules tab
3. Click on New button
4. Click on the Indicator Type dropdown and choose File.
5. Click on the Action at Minimum dropdown and choose Delete
6. In the Confidence area either type in 8 or click on the + sign to increase the number to 8
7. In the Interval area, verify 1 day is selected
8. Verify box next to Recurring is selected
9. Click SAVE



Create/Edit Deprecation Rule

Indicator Type: File

Action At Minimum: Delete

Confidence: 8

Interval: 1 day

□ Percentage

☑ Recurring

PolySwarm Feed

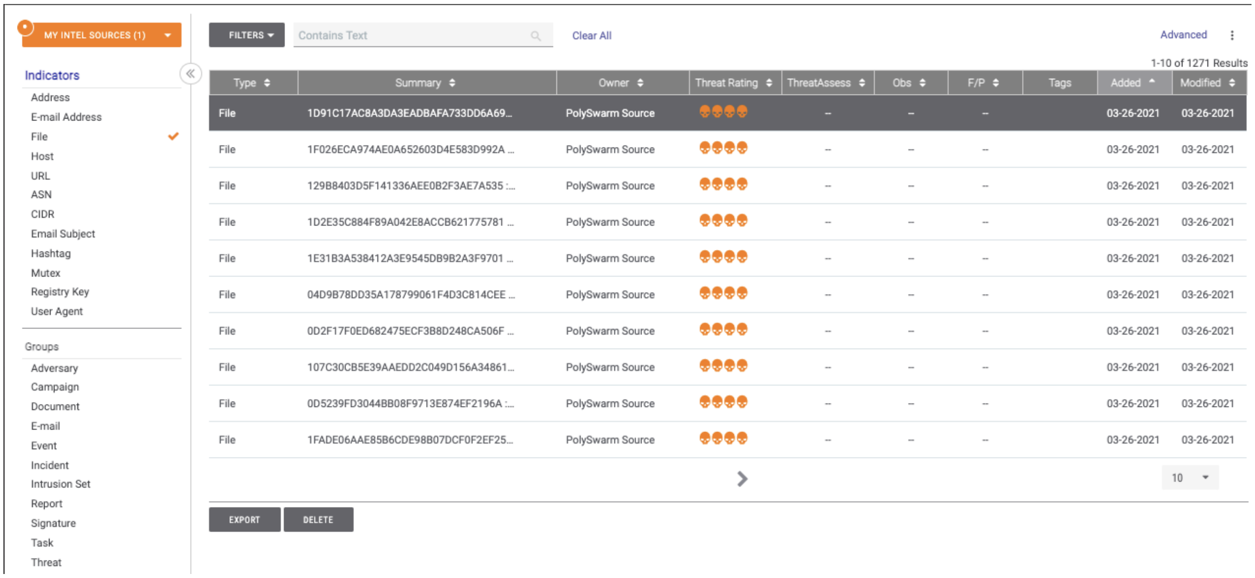
Data Mapping

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

PolySwarm Field	ThreatConnect Field	Example Values	Notes
md5	MD5		MD5 of artifact
sha1	SHA-1		SHA-1 hash of artifact
sha256	SHA-256		SHA-256 hash of artifact
size	Size		
N/A	Detection Ratio	4/9	X/Y where X is number of convictions out of Y engines that attested on the sample
last_scanned	Last Seen		When artifact was

			last scanned by the malware engines
first_seen	First Seen		When artifact was first uploaded to the PolySwarm marketplace
N/A	AV Scan Timestamp		Same data as Last Seen
imphash	Import Hash		Imphash of artifact
compile_date	PE Timestamp		
ssdeep	ssdeep Hash		
mimetype	MIME Type	application/x-dos exec	
	Threat		Malware Family Name
polyscore	Overall Confidence Rating	0-99	The weighted value between 0-99 based on engine responses and historical engine performance.

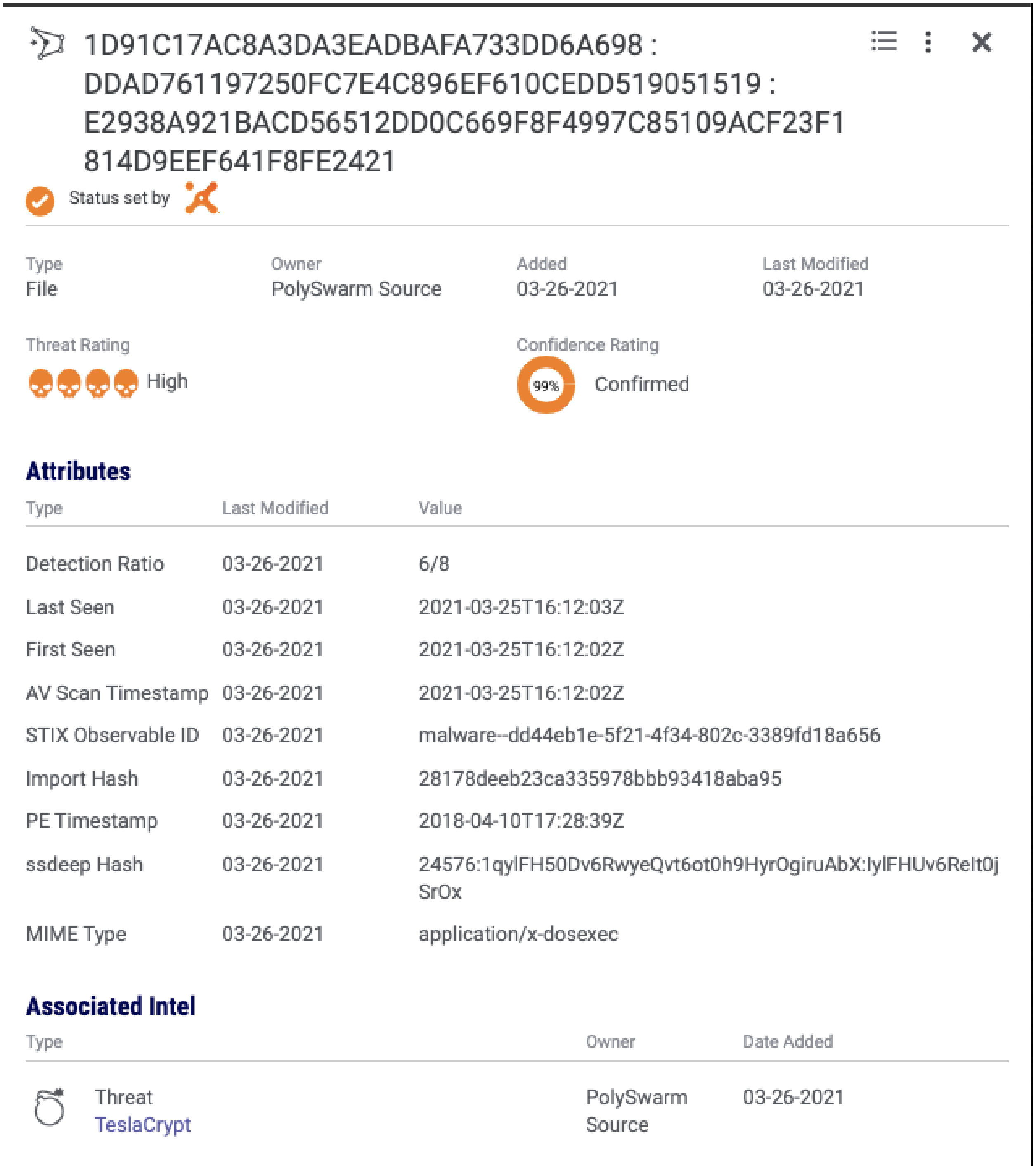
Example of indicators imported from PolySwarm into the ThreatConnect Platform:



1-10 of 1271 Results

Type	Summary	Owner	Threat Rating	ThreatAssess	Obs	F/P	Tags	Added	Modified
File	1D91C17AC8A3DA3EADBAFA733DD6A69...	PolySwarm Source	☠☠☠☠	--	--	--		03-26-2021	03-26-2021
File	1F026ECA974AE0A652603D4E583D992A ...	PolySwarm Source	☠☠☠☠	--	--	--		03-26-2021	03-26-2021
File	129B8403D5F141336AEE0B2F3AE7A535 :...	PolySwarm Source	☠☠☠☠	--	--	--		03-26-2021	03-26-2021
File	1D2E35C884F89A042E8ACCB621775781 ...	PolySwarm Source	☠☠☠☠	--	--	--		03-26-2021	03-26-2021
File	1E31B3A538412A3E9545DB9B2A3F9701 ...	PolySwarm Source	☠☠☠☠	--	--	--		03-26-2021	03-26-2021
File	04D9B78DD35A178799061F4D3C814CEE ...	PolySwarm Source	☠☠☠☠	--	--	--		03-26-2021	03-26-2021
File	0D2F17F0ED682475ECF3B8D248CA506F ...	PolySwarm Source	☠☠☠☠	--	--	--		03-26-2021	03-26-2021
File	107C30CB5E39AAEDD2C049D156A34861...	PolySwarm Source	☠☠☠☠	--	--	--		03-26-2021	03-26-2021
File	0D5239FD3044BB08F9713E874EF2196A :...	PolySwarm Source	☠☠☠☠	--	--	--		03-26-2021	03-26-2021
File	1FADE06AAE85B6CDE98B07DCF0F2EF25...	PolySwarm Source	☠☠☠☠	--	--	--		03-26-2021	03-26-2021

Indicator Details:



1D91C17AC8A3DA3EADBAFA733DD6A698 : DDAD761197250FC7E4C896EF610CEDD519051519 : E2938A921BACD56512DD0C669F8F4997C85109ACF23F1814D9EEF641F8FE2421

Status set by

Type	Owner	Added	Last Modified
File	PolySwarm Source	03-26-2021	03-26-2021

Threat Rating

High

Confidence Rating

99%

Confirmed

Attributes

Type	Last Modified	Value
Detection Ratio	03-26-2021	6/8
Last Seen	03-26-2021	2021-03-25T16:12:03Z
First Seen	03-26-2021	2021-03-25T16:12:02Z
AV Scan Timestamp	03-26-2021	2021-03-25T16:12:02Z
STIX Observable ID	03-26-2021	malware--dd44eb1e-5f21-4f34-802c-3389fd18a656
Import Hash	03-26-2021	28178deeb23ca335978bbb93418aba95
PE Timestamp	03-26-2021	2018-04-10T17:28:39Z
ssdeep Hash	03-26-2021	24576:1qylFH50Dv6RwyeQvt6ot0h9HyrOgiruAbX:IylFHUv6Relt0jSrOx
MIME Type	03-26-2021	application/x-dosexec

Associated Intel

Type	Owner	Date Added
Threat TeslaCrypt	PolySwarm Source	03-26-2021

Application Support:

For any questions or issues with the PolySwarm app, please contact support@polyswarm.io

Change log

Version	Date	Author	Notes
1.0	05/05/2021	Pete White, PolySwarm	Initial Release