POLYSWARM

Malware Intelligence and Enrichment with ThreatConnect

User Guide v1.0

Table of Contents

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.

ThreatConnect aggregates and organizes feeds from multiple trusted partners, providing diverse threat intelligence within their platform. PolySwarm seamlessly integrates via API and allows ThreatConnect's users to obtain file reputation services with a single click, in real-time, from a network of independent malware detection engines. PolySwarm enriches samples with diverse threat indicators and allows threat hunters and SOC analysts to search for and identify relationships between diverse malware families and threat indicators. PolySwarm also provides a final score derived from crowdsourced opinions (PolyScore™), a single number that reflects the likelihood that a given file contains malware.

PolySwarm uniquely addresses emergent and 0-day malware by using a network of research-driven engines that compete in real-time to detect malware. These engines are niche, highly specialized, and yield better accuracy rates within their field of expertise. Engines are economically rewarded for early and accurate detection and enterprises benefit from deeper coverage of the malware landscape and 0-day threats.

By using PolySwarm's integration with ThreatConnect's SOAR platform to analyze suspicious artifacts, at scale, millions of times per day. Get real-time threat intelligence from a crowdsourced network of security experts and antivirus companies.

App and Playbook install

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

Playbook
App

Application

The PolySwarm App provides ThreatConnect users with two action listed below:

search_hash: This action will enrich file data with new information listed in the respective output section.
download_hash: This action enables the download of a sample and storing it in the malware vault built into ThreatConnect's platform.

Configuration

- Verify the PolySwarm App is installed
- Obtain a PolySwarm API Key from https://polyswarm.network/account/api-keys.
  (Create a new account if needed)
- Go to the gear in the top right corner in the ThreatConnect platform then
  Org Settings > **Variables**
- Create a **New Variable**
- Type = **KEYCHAIN**
- Name = **polyswarm_api_key**
- Value = **API key** from **polyswarm.network**

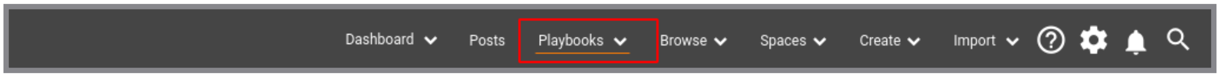
PolySwarm playbook

Quick Overview

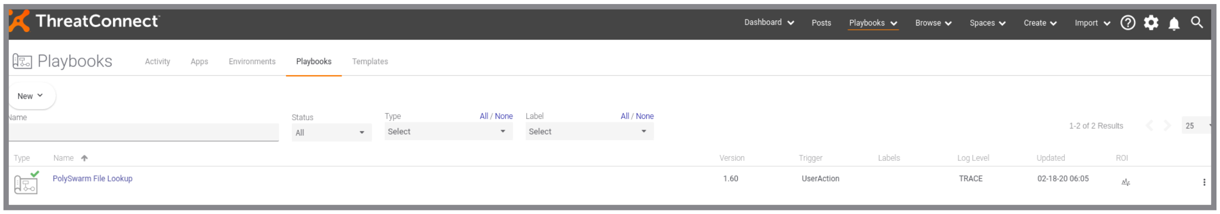
- Verify the PolySwarm playbook is installed
- Import attributes.json file into Org Config for PolySwarm specific variables
- Make sure the playbook is set to active
- Navigate to your list of playbooks
- Create file indicator using hash (MD5 or SHA1 or SHA256)
- Run on the PolySwarm playbook
- Refresh the page for results or browse to the indicator

Making sure the Playbook is set to active

1. Go to the playbook menu in the top banner area to select the PolySwarm playbook

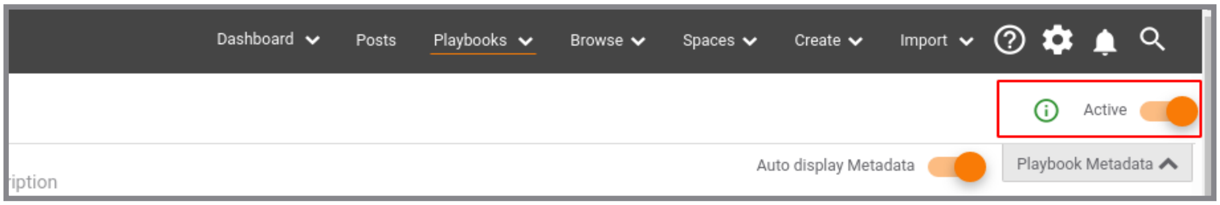


2. Click on the **PolySwarm** playbook



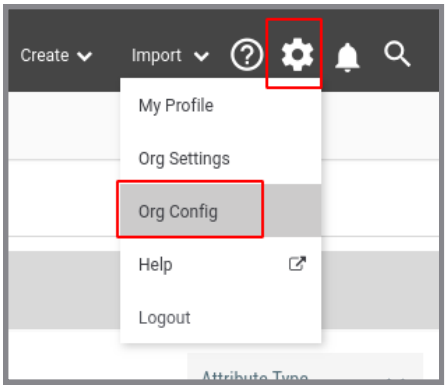
Type	Name	Version	Trigger	Labels	Log Level	Updated	ROI
	PolySwarm File Lookup	1.60	UserAction		TRACE	02-18-20 06:05	

3. Toggle the switch to mark the playbook as active.

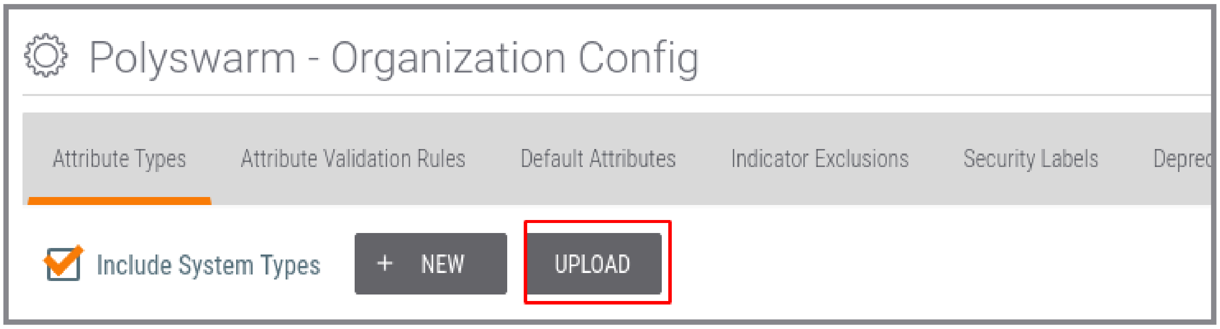


Add PolySwarm Attributes (Optional) **

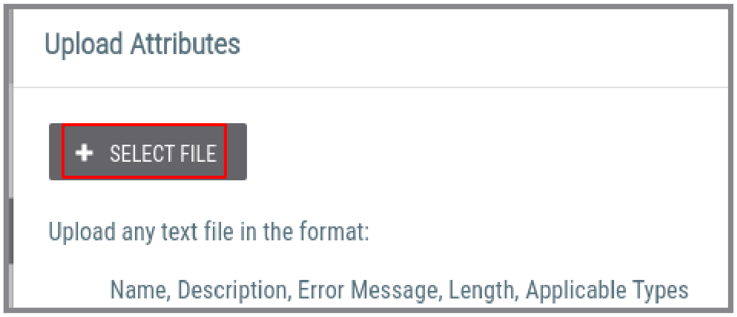
1. Click on the gear icon in the top right to get to your Org Config page.



2. Click on the **Upload** button.



3. Click on the **Select File** button and navigate to the attributes.json file distributed with this playbook.

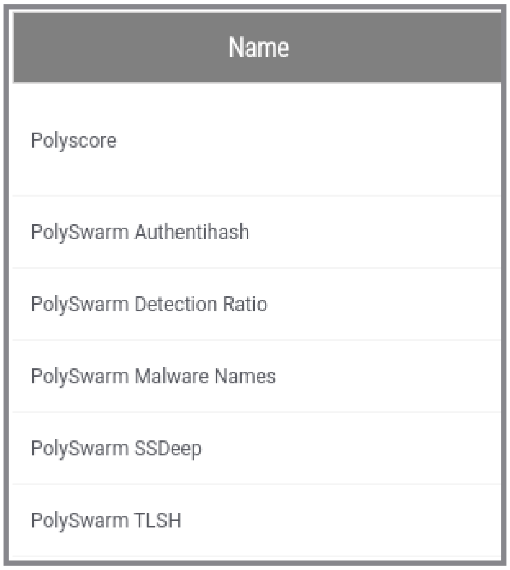


Upload Attributes

Upload any text file in the format:

Name, Description, Error Message, Length, Applicable Types

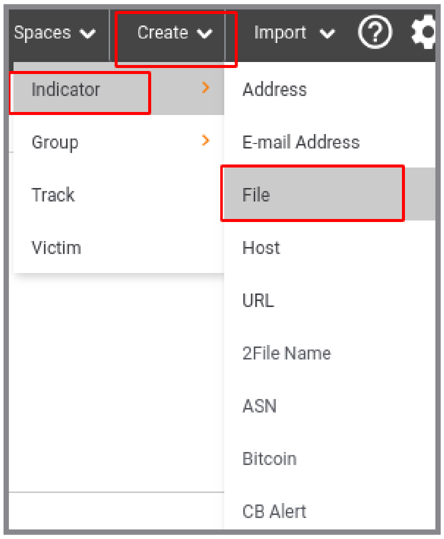
4. New variables should be created. As seen below.



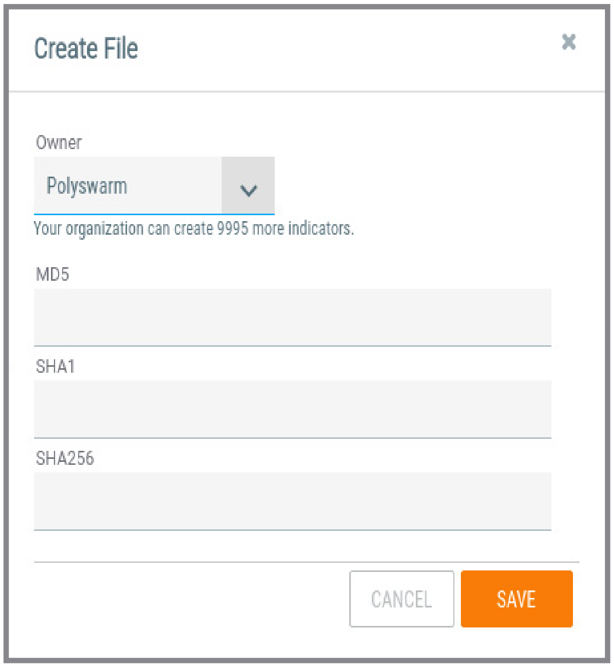
Name
Polyscore
PolySwarm Authentihash
PolySwarm Detection Ratio
PolySwarm Malware Names
PolySwarm SSDeep
PolySwarm TLSH

Create a file indicator

1. Select **Create** > **Indicator** > **File**



2. Input a hash value. This can be MD5, SHA1, or SHA256



Create File

Owner: Polyswarm

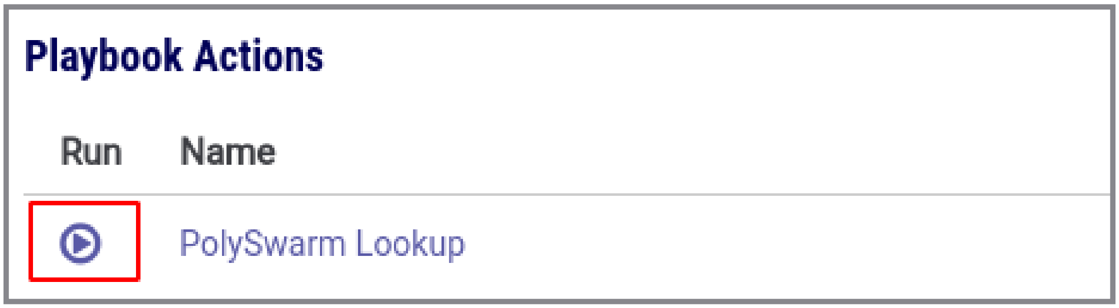
Your organization can create 9995 more indicators.

MD5

SHA1

SHA256

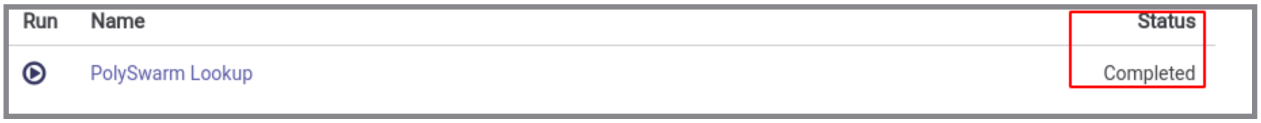
3. Run **PolySwarm Lookup** under playbook Actions in the newly created indicator view



Playbook Actions

Run	Name
▶	PolySwarm Lookup

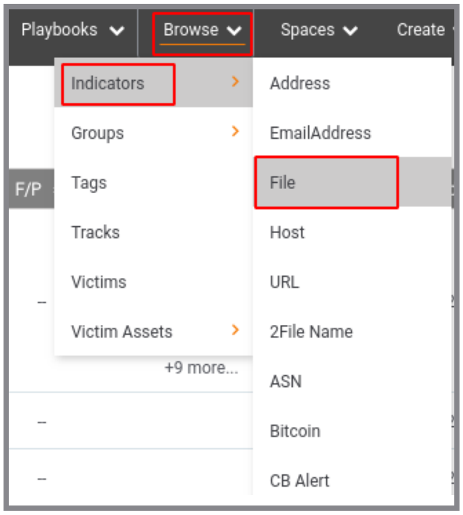
4. The Status for the playbook Action will change to **Completed** when done



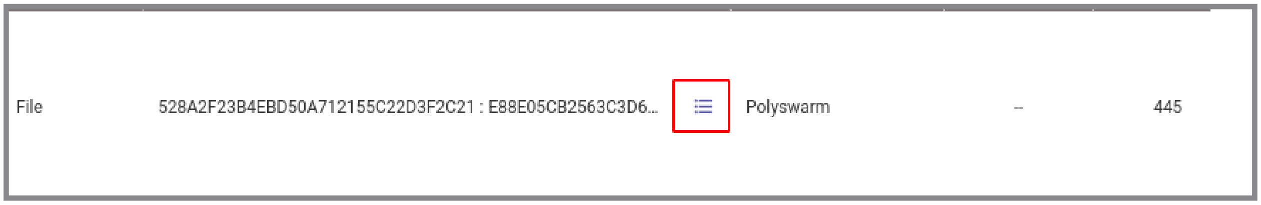
Run	Name	Status
▶	PolySwarm Lookup	Completed

Checking the results

1. Browse to the indicator you created above from the top menu options select **Browse > Indicator > File**

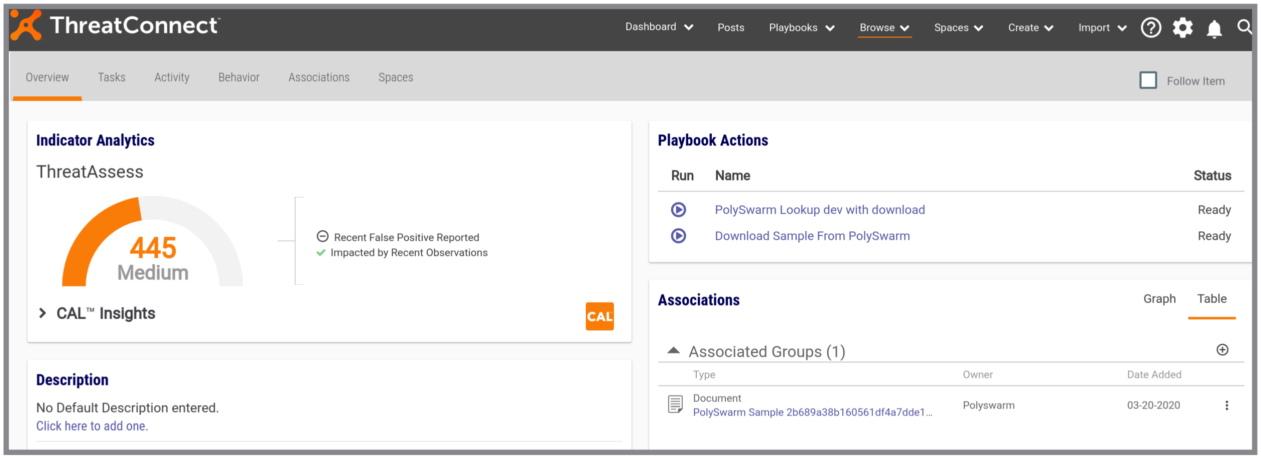


2. Hover over the indicator to get the the option to view the full details of the indicator



File	528A2F23B4EBD50A712155C22D3F2C21 : E88E05CB2563C3D6...	Polyswarm	–	445

3. Review the results of the scan



Indicator Analytics

ThreatAssess

445
Medium

⊖ Recent False Positive Reported
✓ Impacted by Recent Observations

> CAL™ Insights

Description

No Default Description entered.
Click here to add one.

Playbook Actions

Run	Name	Status
▶	PolySwarm Lookup dev with download	Ready
▶	Download Sample From PolySwarm	Ready

Associations Graph Table

Associated Groups (1)

Type	Owner	Date Added
Document PolySwarm Sample 2b689a38b160561df4a7dde1...	Polyswarm	03-20-2020

Results

Example of scan attributes returned when the scan is complete

- **Hashes:** Missing hash values will be populated
- **Fuzzy Hashes:** ssdeep, Authentihash, TLSH: Can be used to pivot to find like files
- **File name:** File names observed at file submission
- **Security Labels:** TLP color
- **Tags:** Malware family returned by the scan engine at the time of file submission
- **PolyScore:** The weighted value between 0-1 based on engine responses and historical engine performance. PolySwarm provides this as an easy number to gauge maliciousness.
- **Overall Confidence Rating:** a scale from 1-100 based off combination of detection ratio and PolyScore
- **Associated Groups**: ThreatConnect Document - A downloaded sample of the hash saved to Malware Vault

Appendix A

Outputs

search_hash action

Polyswarm Field	Possible Values	Notes
polyswarm.response.json.raw	Raw json	Raw JSON response from PolySwarm API
polyswarm.results.assertions.count	number of assertions	total number of engines asserting on an artifact. 0 indicates the hash is benign observed at file submission. You may receive other empty string if this value is 0
polyswarm.results.file.authentihash	Any valid hash for given type	authentihash of artifact
polyswarm.results.file.md5	Any valid hash for given type	MD5 of artifact
polyswarm.results.file.names	string	Filenames observed at file submission time, might be just the hash of the file
polyswarm.results.file.sha1	Any valid hash for given type	sha1 of artifact
polyswarm.results.file.sha256	Any valid hash for given type	sha256 of artifact
polyswarm.results.file.sha3_256	Any valid hash for given type	sha3_256 of artifact
polyswarm.results.file.sha3_512	Any valid hash for given type	sha3_512 of artifact
polyswarm.results.file.sha512	Any valid hash for given type	sha512 of artifact
polyswarm.results.file.ssdeep	Any valid hash for given type	ssdeep of artifact
polyswarm.results.file.tlsh	Any valid hash for given type	tlsh of artifact

Polyswarm Field Cont.	Possible Values Cont.	Notes Cont.
polyswarm.results.longest_ malware_family_name	string	The longest malware family name reported by any engine.
polyswarm.results.malicious_ detections.confidence	The confidence rating based off polyscore and detection raitio	0-100 confidence based on a combination of detection ratio and PolyScore
polyswarm.results.malicious_ detections.count	string	total malicious detections
polyswarm.results.malicious_ detections.details	KeyValueArray	Engines, their verdicts, and potential malware families. Empty string value results if the file has no detections
polyswarm.results.malicious_ detections.ratio	string	proportion of malicious detections in responding engines
polyswarm.results.malicious_ detections_str	string	Engines that detected malicious and reported malware families
polyswarm.results.polyscore	0-1	Score between 0-1 that indicates malintent of artifact takes historical engine performance into account
polyswarm.results.tags.detections	string	Malware families from engines, for tags
polyswarm.results.tags.indicator	string array	Indicator tags provided by engines

download_hash action

Polyswarm Field	Possible Values	Notes
polyswarm.results.file.authentihash	Any valid hash for given type	authentihash of artifact
polyswarm.results.file.md5	Any valid hash for given type	MD5 of artifact
polyswarm.results.file.names	string	Filenames observed at file submission time
polyswarm.results.file.sha1	Any valid hash for given type	sha1 of artifact
polyswarm.results.file.sha256	Any valid hash for given type	sha256 of artifact
polyswarm.results.file.sha3_256	Any valid hash for given type	sha3_256 of artifact
polyswarm.results.file.sha3_512	Any valid hash for given type	sha3_512 of artifact
polyswarm.results.file.sha512	Any valid hash for given type	sha512 of artifact
polyswarm.results.file.ssdeep	Any valid hash for given type	ssdeep of artifact
polyswarm.results.file.tlsh	Any valid hash for given type	tlsh of artifact
polyswarm.results.file.malware.zipfile	string	Zipfile binary content, encrypted with password
polyswarm.results.file.malware.zippassword	string	Password for malware vault zip file

** Optional Custom Attributes

Attributes needed to allow the **Add ThreatConnect Attribute** app to display the selected outputs available to each action. These are required to run the PolySwarm playbook shown here.

Key	Values
PolyScore	#polyswarm.results.polyscore
PolySwarm Malware Names	#polyswarm.results.malicious_detections_str
Polyswarm Detection Ratio	#polyswarm.results.malicious_detections.count/#polyswarm.results.assertions.count
PolySwarm Authenihash	#polyswarm.results.file.authentihash
PolySwarm SSDeep	#Polyswarm.results.file.ssdeep
PolySwarm TLSH	#polyswarm.results.file.tlsh