A Crash Course in OpenCTI

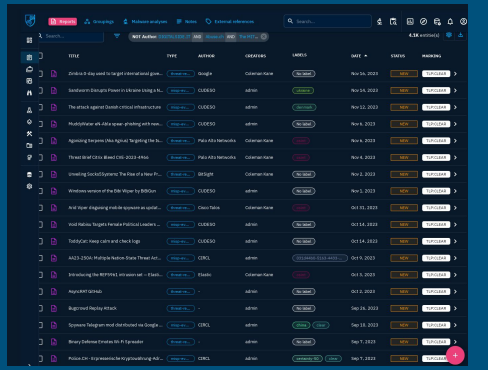
By: Coleman Kane
DeepSeas

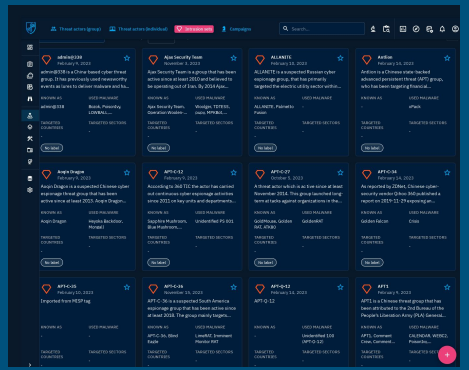
What is OpenCTI?

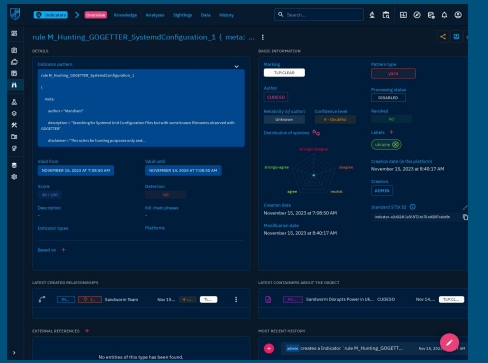
https://filigran.io/solutions/products/opencti-threat-intelligence/

Cyber Threat Intelligence (CTI) Database

- Emphasis on automation, visualization, and standards compliance
- STIX 2.1 internal representation (JSON)
- TAXII server/client support
- Modern tech stack: React/Node.js, ElasticSearch, RabbitMQ
- API-first design via Low-level GraphQL API
- Fully asynchronous UI
- High-level API library in Python
- Modular plug-in extensibility through the “connectors” ecosystem
- Data scraping automation
- Case and Knowledge management features







Filigran: the Company Supporting OpenCTI

Based in France (Paris)

Committed to Open Source and Open Standards (e.g. STIX, TAXII, ATT&CK)

“Community Edition” open-sourced under Apache License 2.0

“Enterprise Edition” open-sourced under a proprietary non-commercial license

Other projects: OpenCrisis, OpenEx (simulation/exercises), OpenRiskManager

STIX documentation: https://oasis-open.github.io/cti-documentation/stix/intro

UI Overview: Listings

Secondary nav-menu

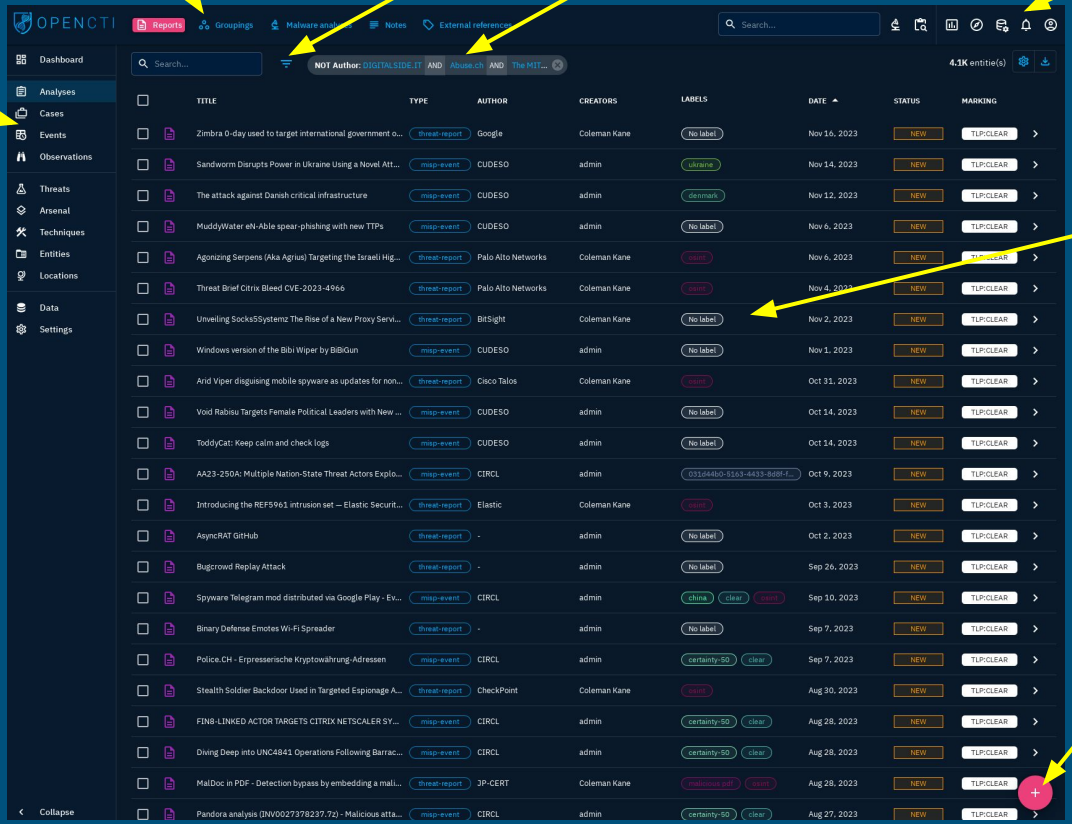
Filter menu & summary

Global tools / functions

Main nav-menu

Main content view

Create new object of current type



UI Overview: Entity

Marking definition

Contents/context summary

Tools to use on entity

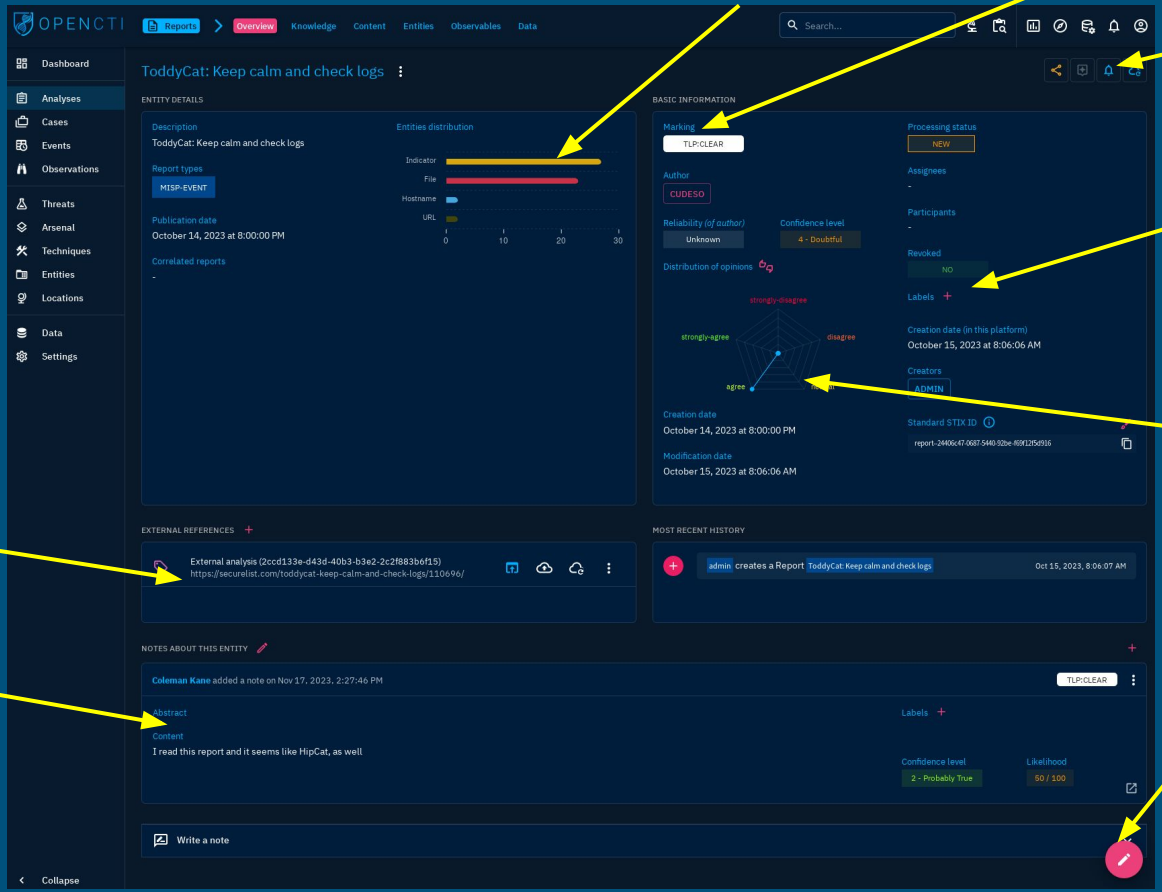
Arbitrary labeling/tagging

User feedback

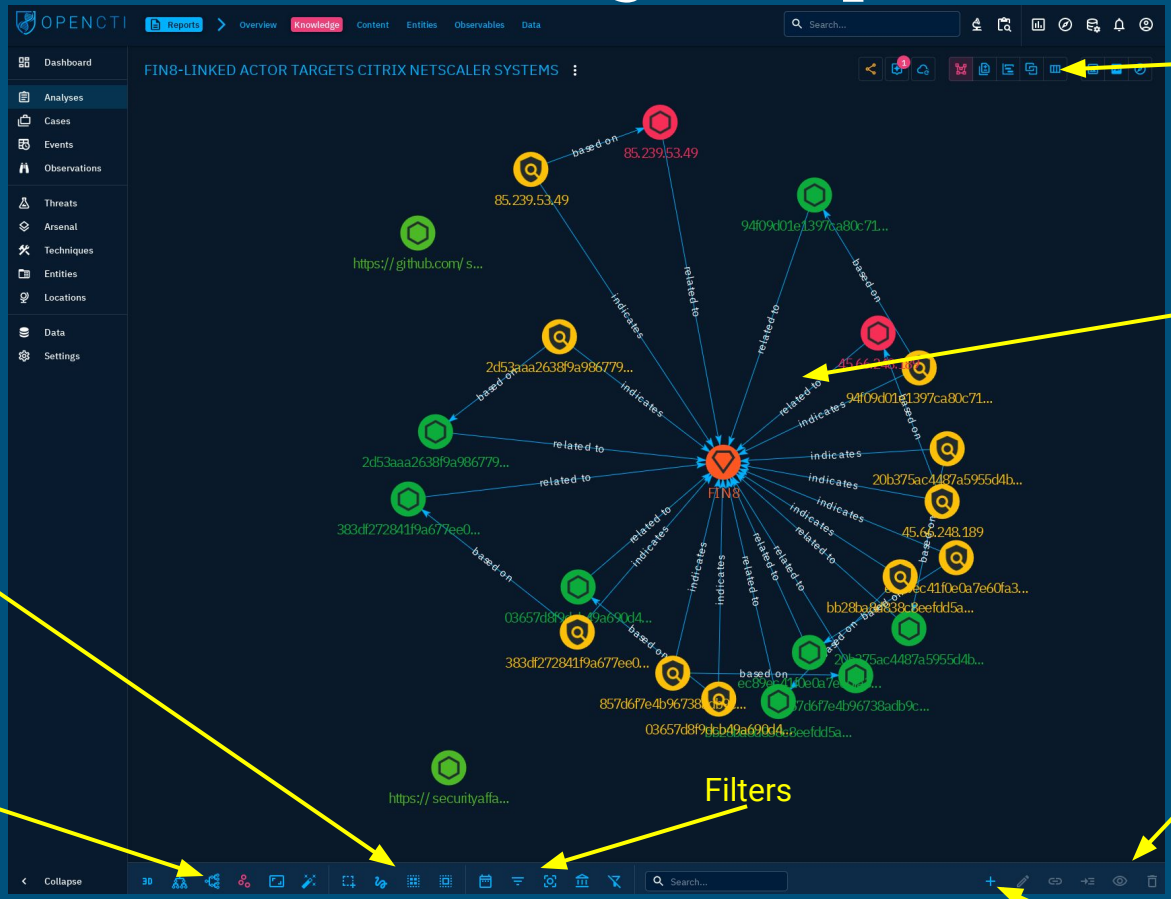
List of external references to the entity

Notes about this entity

Edit entity



UI Overview: Knowledge Graphs



Different visualizations

Interactive Graph

Selection tools

Graph view/layout options

Filters

Tools to operate on selections

Add entity to graph

STIX Data Model

Analysis: Document CTI Reports & Build Products

Reports: Threat Intel reports, actor analysis, blog posts, etc.

Groupings: Less formal groupings - reports, but without the narrative content

Malware analyses: Reports focusing on Malware, and adhering to the “malware-analysis” STIX 2.1 entity

Notes: Global view of any notes in the platform

External References: Global view of all external reference links in the platform

Cases: Manage related work

Incident Response: Manage tasks and context that will occur during incident response

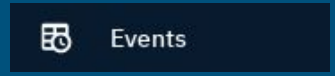
RFI: Dedicated tasking/context container for non-Incident requests to Intel team

Request for Takedown: Similar to RFI/IR, but specific for externally-directed takedown requests

Tasks: Global view of all tasks

Feedback: Global view of all user feedback

Events: Temporal Info and Related Analysis



Incidents: Serious events, typically that necessitated incident response

Sightings: Location, temporal, and frequency information related to an observation

Observed Data: Temporal information related to an observation

Observations: Collected Data and Detections

Observables: Data points observed when investigating malicious activity

Artifacts: Unstructured data paired with structured metadata representing files/malware/images/memory/etc. collected during analysis

Indicators: Detection-suitable data points. STIX 2.1 defines these to be derived from Observables, and also represent complex signature data (Yara, Suricata, Sigma, etc.)

Infrastructures: Specialized container documenting infrastructure analysis

Observables vs. Indicators

A lot of confusion due to varying definitions across orgs

Common to see “indicator” refer to both element types

- Observable: Information I’ve seen during an analysis or investigation
- Indicator: Of what I’ve seen, the subset and/or combination that would be indicative of future malicious activity

STIX 2.1 has a formal definition of both, and OpenCTI adheres to that standard

- https://oasis-open.github.io/cti-documentation/examples/sighting-of-an-indicator
- https://oasis-open.github.io/cti-documentation/examples/sighting-of-observed-data

Threats: Individual and Group Operations

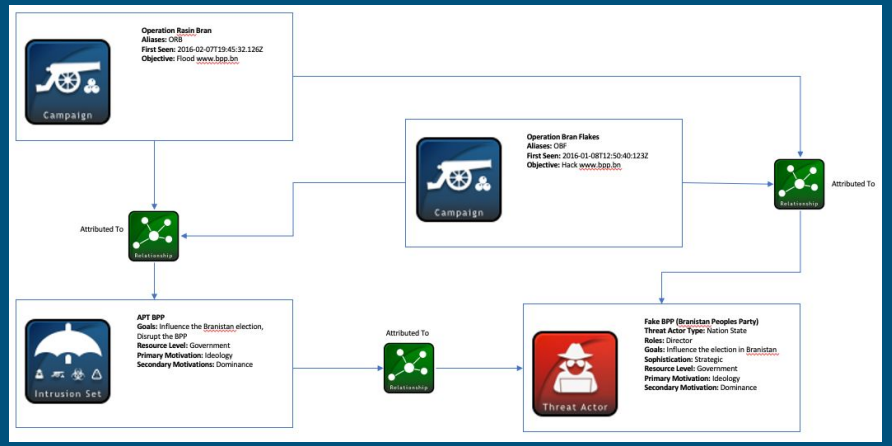
Threats

Threat Actors: Identifiable Groups or individuals that operate intrusion sets for cyber operations

Intrusion Sets: Activity sets that represent consistent means, motivations, and targeting. Tying to actual threat actors may take time. Most published “groups” in CTI fit into this category

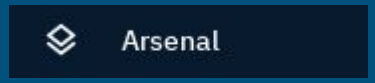
Campaigns: Series of attempts carried out by an intrusion set to achieve an objective. Typically incorporates a time-bound and distinct tooling & TTPs.

Similar to Observables/Indicators, Threats adhere to the STIX 2.1 standard definitions, which may often differ from how these terms may be used in a lot of orgs.



https://oasis-open.github.io/cti-documentation/examples/defining-campaign-ta-is

Arsenal: Adversary Toolbox



Malware: Types of malware known to be used by adversaries.

Channels: Online locations where adversaries may disseminate information

Tools: Tools used by the adversary - typically tools that aren't inherently malware (LOLbins, etc.)

Vulnerabilities: Vuln data that can be populated from national CVE registry.

Techniques: Operations and Methods

Attack Pattern: Attack patterns and adversary techniques - includes (but not limited to) MITRE ATT&CK

Narratives: Specific to disinfo - concepts and messaging being propagated for persuasion

Courses of Action: Defender-side techniques that can be used for prevention and mitigation

Data sources: Data sources available from sensors/logs/collection

Data components: Data within a source relevant to detecting a particular technique

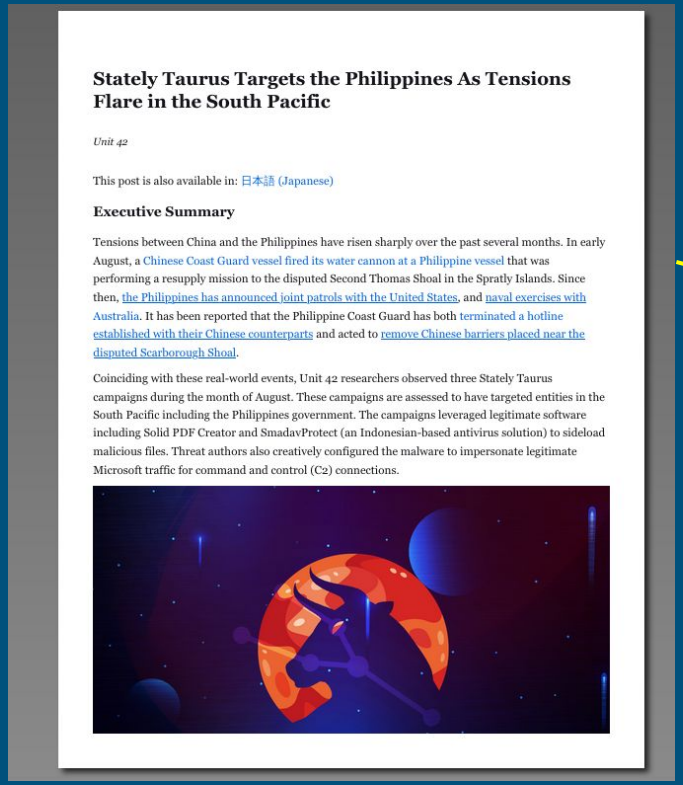
Entities & Locations: Who, When, & Where

Entities: Organizations, Sectors, Events (non-activity), Systems, Individuals - often used for targeting and attribution

Locations: Geographical information: Region, Country, City, Area, Position

Importing Document Data

PDF Import



Stately Taurus Targets the Philippines As Tensions Flare in the South Pacific

Unit 42

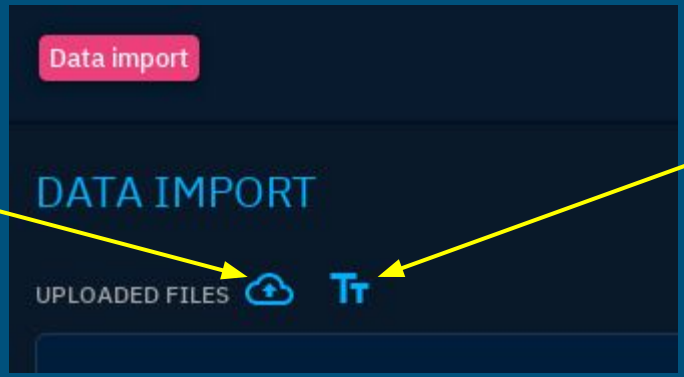
This post is also available in: 日本語 (Japanese)

Executive Summary

Tensions between China and the Philippines have risen sharply over the past several months. In early August, a Chinese Coast Guard vessel fired its water cannon at a Philippine vessel that was performing a resupply mission to the disputed Second Thomas Shoal in the Spratly Islands. Since then, the Philippines has announced joint patrols with the United States, and naval exercises with Australia. It has been reported that the Philippine Coast Guard has both terminated a hotline established with their Chinese counterparts and acted to remove Chinese barriers placed near the disputed Scarborough Shoal.

Coinciding with these real-world events, Unit 42 researchers observed three Stately Taurus campaigns during the month of August. These campaigns are assessed to have targeted entities in the South Pacific including the Philippines government. The campaigns leveraged legitimate software including Solid PDF Creator and SmadavProtect (an Indonesian-based antivirus solution) to sideload malicious files. Threat authors also creatively configured the malware to impersonate legitimate Microsoft traffic for command and control (C2) connections.

Data import



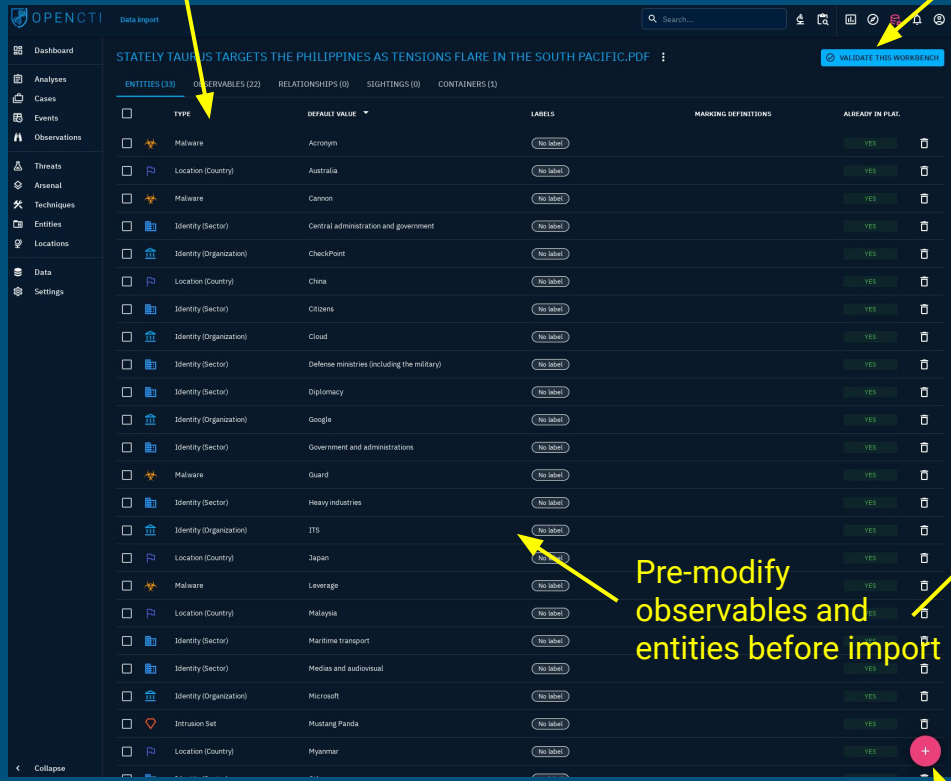
Plain Text copy/paste import

New analyst workbench

Analyst Workbench

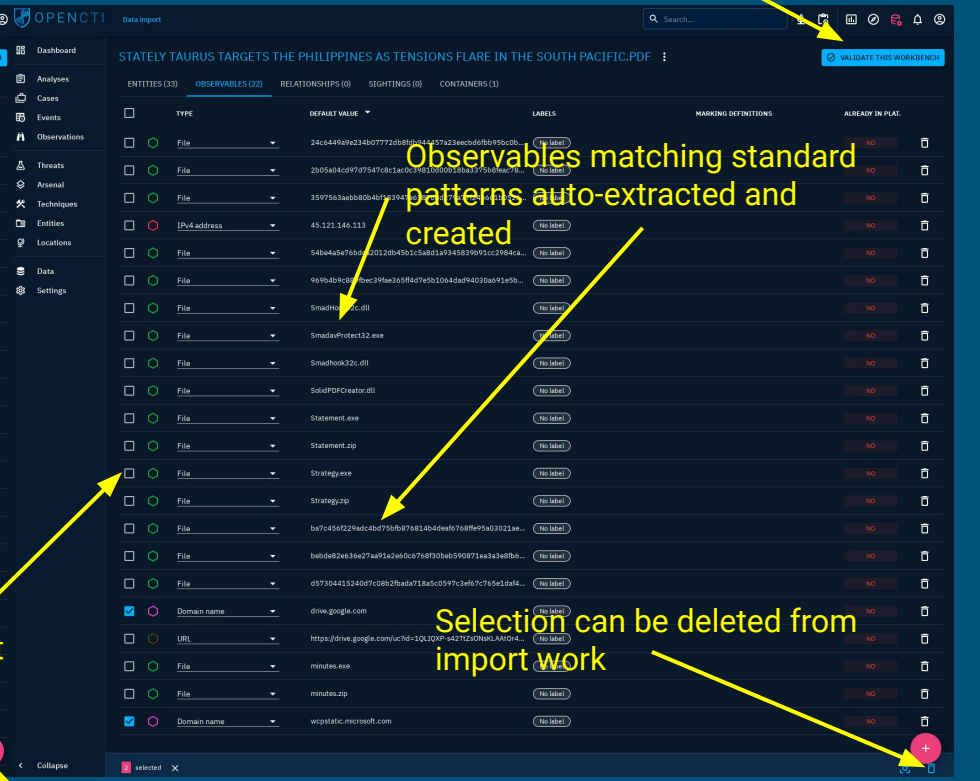
Entities are matched to existing names & aliases in the database

When ready for import, click here



Pre-modify observables and entities before import

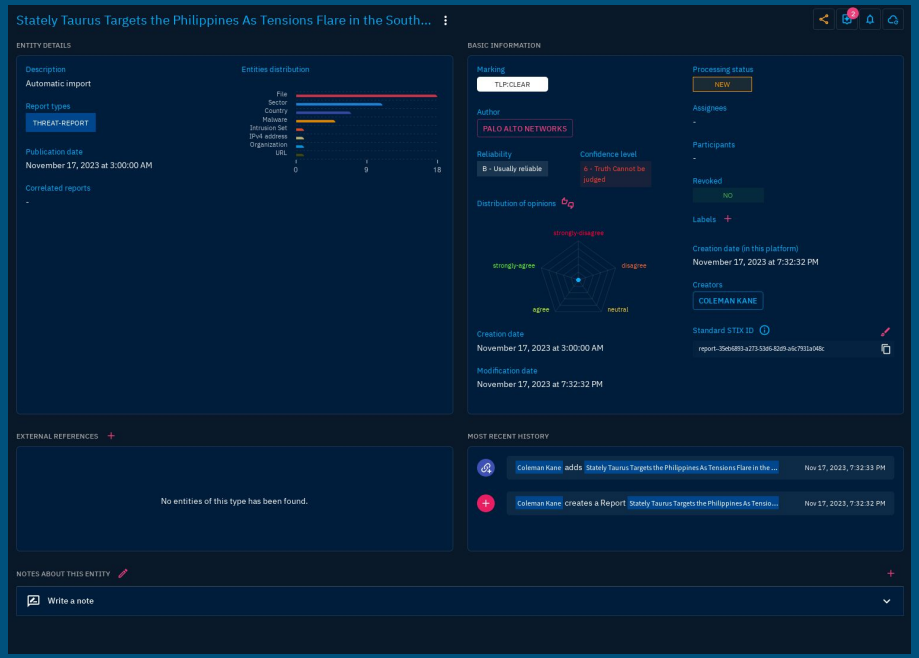
Observables matching standard patterns auto-extracted and created

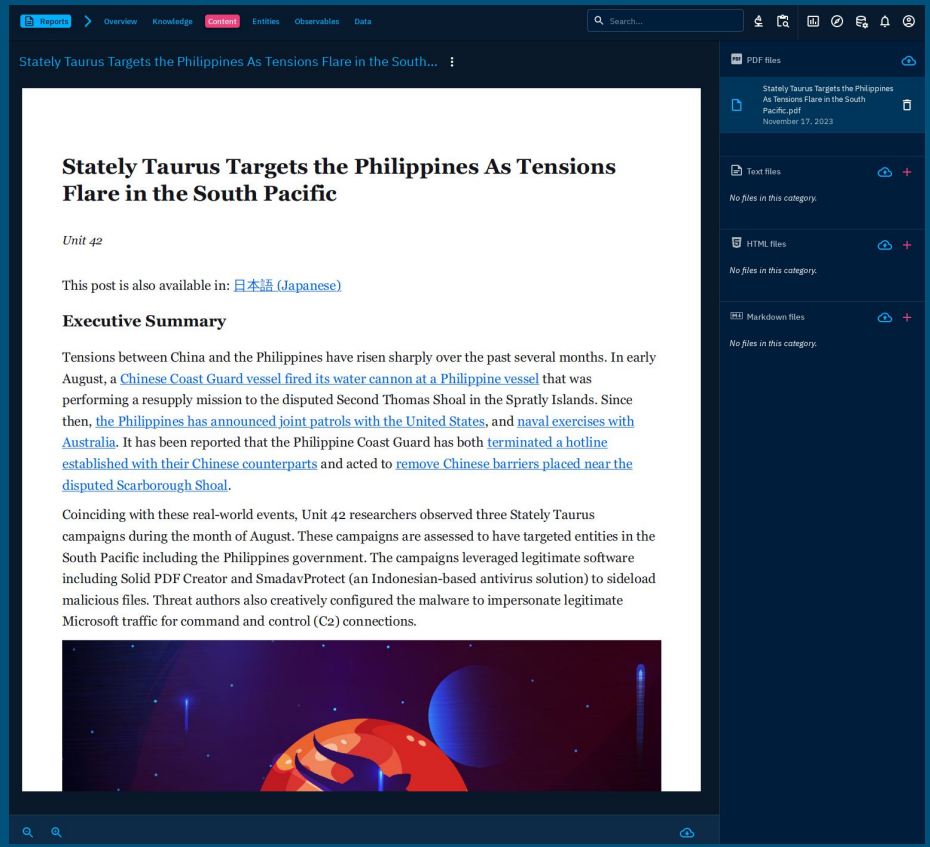


Selection can be deleted from import work

Add new entities/observables manually

Import Complete





Extension Framework (Connectors)

Extend OpenCTI With Connectors

Five types

- Internal Import File: Translate an uploaded file into STIX and import it (via workbench)
- Internal Export File: Translate selected STIX data from OpenCTI into a downloadable file
- External Import: From an external online source, convert source data to STIX and import
- Enrichment: Perform automated analysis on STIX data in the database, and add/delete context on it
- Stream: Operate continuously on data entering OpenCTI to feed it to external sources, or vice-versa

Deployed as Python containers

Uses the same Python API as Python scripts, with some additional features and RabbitMQ access

Templates in GitHub repository so new connectors can be written with some direction

Connectors: https://github.com/OpenCTI-Platform/connectors
Python API: https://github.com/OpenCTI-Platform/client-python

Easy OSINT Collection Instance

Identified all “free” and “public” plugins

Created a `docker-compose.yml` to deploy them all

Made a Terraform recipe to quickly deploy to AWS

My Docker fork (branch `tf-main`): https://github.com/ckane/opencti-docker/tree/tf-main
OpenCTI “vanilla” docker: https://github.com/OpenCTI-Platform/docker

Terraform recipe (branch `ckane-dockers`):
https://github.com/ckane/opencti-terraform/tree/ckane-dockers

Quick Start - Test on Local System Using Docker

```
# 1) Download ckane's opencti-docker
git clone -b tf-main https://github.com/ckane/opencti-docker.git
cd opencti-docker

# 2) Edit .env and fill in blanks
cp .env.sample .env
vim .env
# Run 'uuidgen -r' multiple times to generate new UUID for each
# blank *_ID= line in .env
while grep _ID=$ .env > /dev/null; do
  new_uuid="${uuidgen -r}"
  sed -i "0,/_ID=\$/{s/_ID=\$/_ID=${new_uuid}/}" .env
done

# 3) Generate login email, password, API token
sed -i "s/^OPENCTI_ADMIN_EMAIL=.*$/OPENCTI_ADMIN_EMAIL=you@you.com/" .env
sed -i "s/^OPENCTI_ADMIN_PASSWORD=.*$/OPENCTI_ADMIN_PASSWORD=MemorizedSecret/" .env
sed -i "s/^OPENCTI_ADMIN_TOKEN=.*$/OPENCTI_ADMIN_TOKEN=$(uuidgen -r)/" .env

# 4) Start docker
docker-compose -f docker-compose.yml up -d

# OpenCTI will come up listening on HTTP port 8080 on localhost
```

Other Features

UI Overview: Yara Rule

Pattern type - admin can add more types

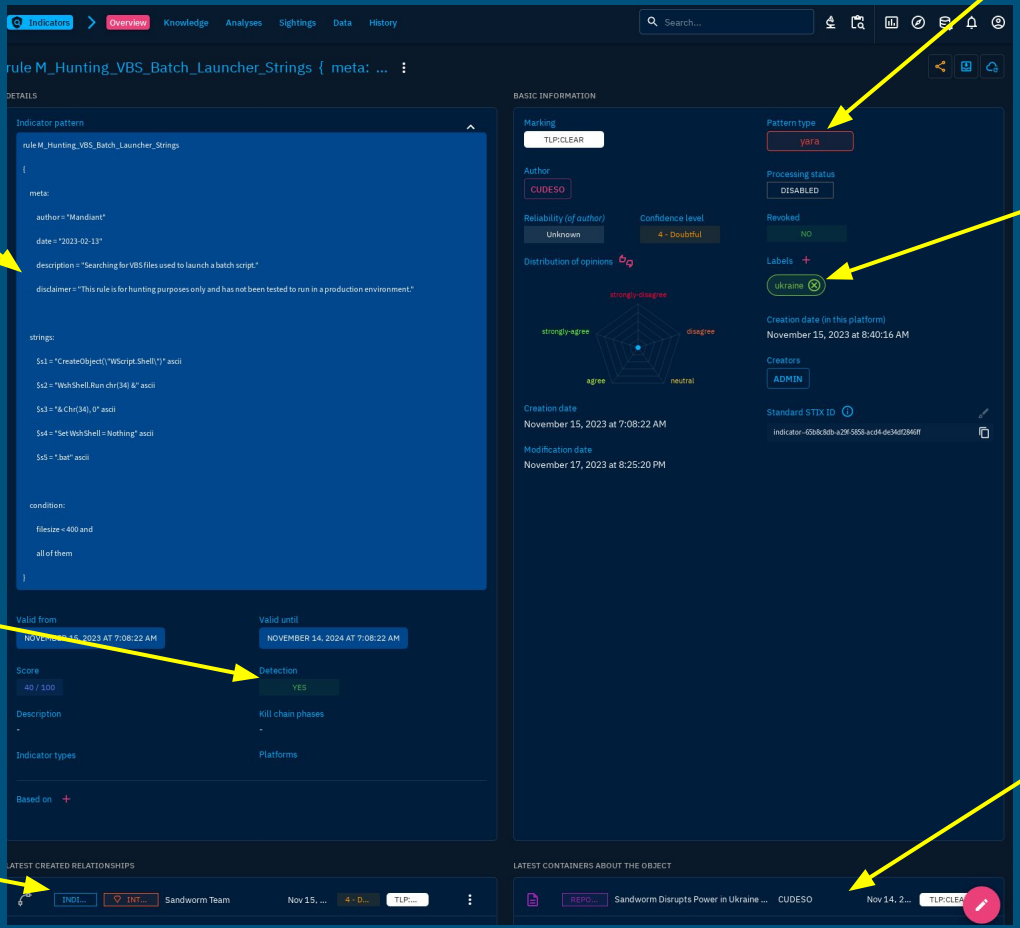
Rule code - editable in browser UI or via API

Labels/tags

Control deployment with “Detection” switch

Reports that contain this signature

Related entities or observables



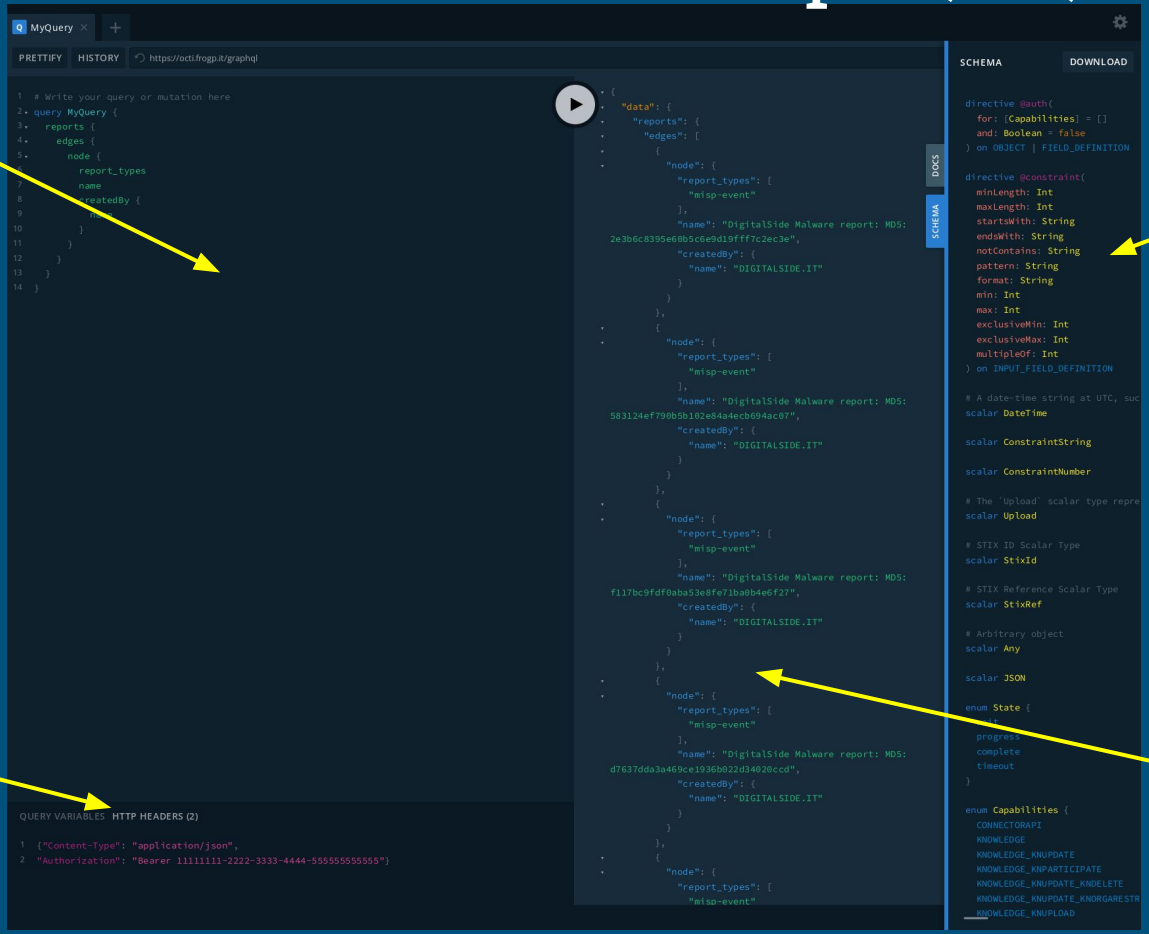
UI Overview: Advanced GraphQL Query

Enter query and/or mutation here

Provide HTTP Auth token, and query input vars

Full Schema and API documentation

Output results in right pane



Thanks! Any Questions?

Coleman Kane - DeepSeas
https://blog.malware.re/ (website)
@colemankane@infosec.exchange (Mastodon)
@colemankane (Twitter)

<QUEEN CITY CONFERENCE>

- YOUR ROYAL HACKING EXPERIENCE -

THANK YOU!

TO OUR SPONSORS

Platinum Tier

ARCTIC WOLF

netskope

MetaCTF

Silver Tier

MassMutual Ascend
Life Insurance Company

Gold Tier

CLOUDFLARE

OPTIV

Cadre
information security

HALO

ROBOTTI
TECH SERVICES

PingIdentity

okta

GREAT AMERICAN
INSURANCE GROUP

COALFIRE

snyk

MANTIUM

plainID
THE AUTHORIZATION COMPANY

LEVEL 6
CYBERSECURITY INC

OffSec

SILVERFORT