



A Crash Course in OpenCTI



By: Coleman Kane
DeepSeas



What is OpenCTI?

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

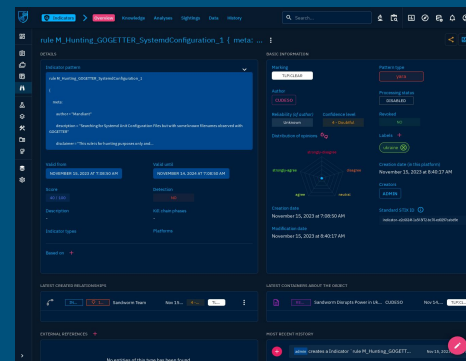
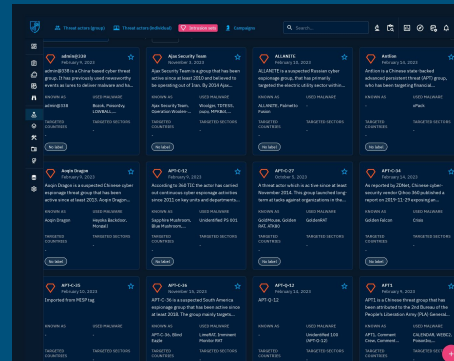
Cyber Threat Intelligence (CTI) Database

- 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



A screenshot of the OpenCTI web interface showing a table of cyber threat intelligence data. The table has columns for 'Title', 'Type', 'Source', 'Confidence', 'Score', 'Date', 'Status', and 'Actions'. The data rows list various threat intelligence reports, such as 'Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational...', 'The attack against Ukraine critical infrastructure...', and 'Ukrainian intelligence reports the loss of a Russian...'. Each row includes a 'Score' (e.g., 100, 90, 80) and a 'Status' (e.g., 'New', 'Updated', 'Archived').

Title	Type	Source	Confidence	Score	Date	Status	Actions
Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational...	Incident	OSINT	High	100	Nov 15, 2023	New	[Icons]
The attack against Ukraine critical infrastructure...	Incident	OSINT	High	90	Nov 15, 2023	Updated	[Icons]
Ukrainian intelligence reports the loss of a Russian...	Incident	OSINT	High	80	Nov 15, 2023	Archived	[Icons]



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

Main
nav-menu

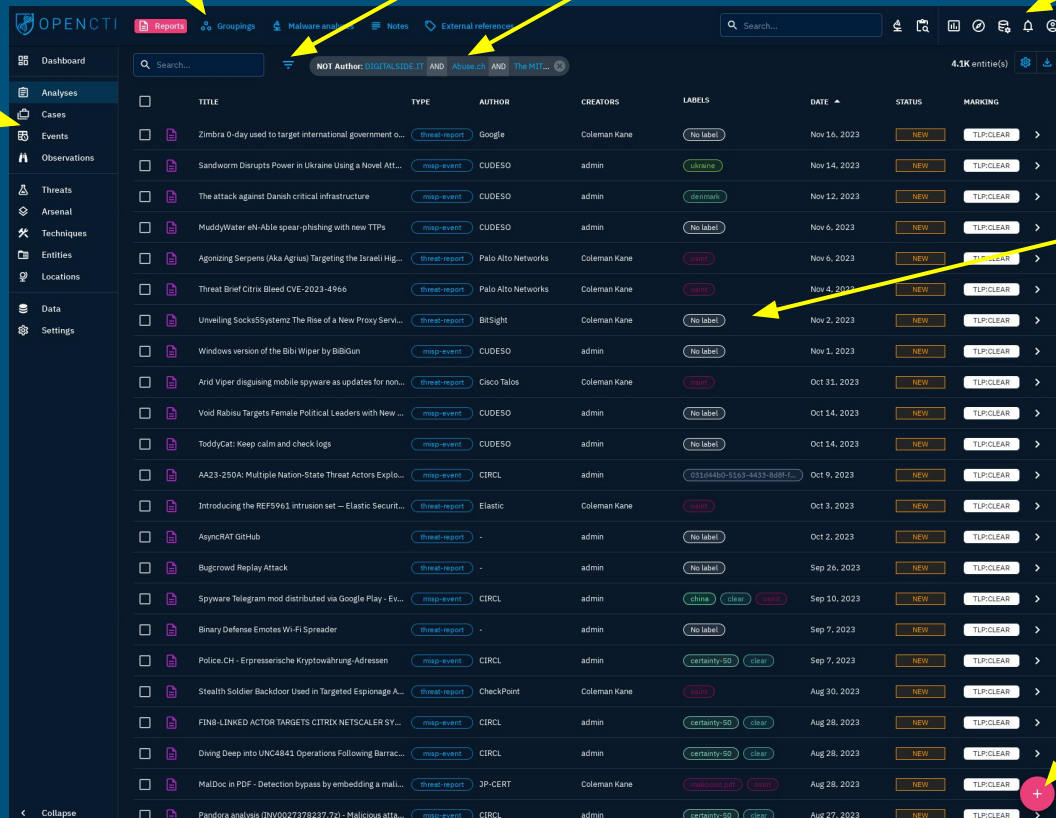
Secondary nav-menu

Filter menu & summary

Global tools / functions

Main content
view

Create new
object of
current type



	TITLE	TYPE	AUTHOR	CREATORS	LABELS	DATE	STATUS	MARKING
☐	Zimbora 0-day used to target international government o...	Break-report	Google	Coleman Kane	No label	Nov 16, 2023	NEW	TLP:CLEAR
☐	Sandworm Disrupts Power in Ukraine Using a Novel Att...	Map-event	CUDESO	admin	Ukraine	Nov 14, 2023	NEW	TLP:CLEAR
☐	The attack against Danish critical infrastructure	Map-event	CUDESO	admin	Denmark	Nov 12, 2023	NEW	TLP:CLEAR
☐	MuddyWater eh-Able spear-phishing with new TTPs	Map-event	CUDESO	admin	No label	Nov 6, 2023	NEW	TLP:CLEAR
☐	Agonizing Serpens (Aka Agrius) Targeting the Israeli Hig...	Break-report	Palo Alto Networks	Coleman Kane	Israel	Nov 6, 2023	NEW	TLP:CLEAR
☐	Threat Brief Citrix Bleed CVE-2023-4966	Break-report	Palo Alto Networks	Coleman Kane	Israel	Nov 4, 2023	NEW	TLP:CLEAR
☐	Unveiling Socks5Systemz: The Rise of a New Proxy Servi...	Break-report	BITSight	Coleman Kane	No label	Nov 2, 2023	NEW	TLP:CLEAR
☐	Windows version of the Bibi Wiper by BibiGun	Map-event	CUDESO	admin	No label	Nov 1, 2023	NEW	TLP:CLEAR
☐	Arid Viper disgussing mobile spyware as updates for non...	Break-report	Cisco Talos	Coleman Kane	Israel	Oct 31, 2023	NEW	TLP:CLEAR
☐	Void Rabisu Targets Female Political Leaders with New ...	Map-event	CUDESO	admin	No label	Oct 14, 2023	NEW	TLP:CLEAR
☐	ToddyCat: Keep calm and check logs	Map-event	CUDESO	admin	No label	Oct 14, 2023	NEW	TLP:CLEAR
☐	AA23-250A: Multiple Nation-State Threat Actors Explo...	Map-event	CIRCL	admin	05164480-5553-4433-888F-E...	Oct 9, 2023	NEW	TLP:CLEAR
☐	Introducing the REF5901 intrusion set – Elastic Secur...	Break-report	Elastic	Coleman Kane	Israel	Oct 3, 2023	NEW	TLP:CLEAR
☐	AsynRAT GitHub	Break-report	-	admin	No label	Oct 2, 2023	NEW	TLP:CLEAR
☐	Bugcrowd Replay Attack	Break-report	-	admin	No label	Sep 26, 2023	NEW	TLP:CLEAR
☐	Spyware Telegram mod distributed via Google Play - Ev...	Map-event	-	admin	China Clear Labeled	Sep 10, 2023	NEW	TLP:CLEAR
☐	Binary Defense Emotes Wi-Fi Spreader	Break-report	-	admin	No label	Sep 7, 2023	NEW	TLP:CLEAR
☐	Police.CH - Erpresserische Kryptowährung/Adressen	Map-event	CIRCL	admin	certainty:50 Clear	Sep 7, 2023	NEW	TLP:CLEAR
☐	Stealth Soldier Backdoor Used in Targeted Espionage A...	Break-report	CheckPoint	Coleman Kane	Israel	Aug 30, 2023	NEW	TLP:CLEAR
☐	FIN6-LINKED ACTOR TARGETS CITRIX NETSCALER SY...	Map-event	CIRCL	admin	certainty:50 Clear	Aug 28, 2023	NEW	TLP:CLEAR
☐	Diving Deep into UNC4841 Operations Following Barrac...	Map-event	CIRCL	admin	certainty:50 Clear	Aug 28, 2023	NEW	TLP:CLEAR
☐	MalDoc in PDF - Detection bypass by embedding a mali...	Break-report	3P-CERT	Coleman Kane	Malicious pdf Clear	Aug 28, 2023	NEW	TLP:CLEAR
☐	Pandora analysis (DNV0027378237.72) - Malicious att...	Map-event	CIRCL	admin	certainty:50 Clear	Aug 27, 2023	NEW	TLP:CLEAR

UI Overview: Entity

OPENCTI Reports Overview Knowledge Content Entities Observables Data

Dashboard

Analyses

Cases

Events

Observations

Threats

Arsenal

Techniques

Entities

Locations

Data

Settings

ToddyCat: Keep calm and check logs

ENTITY DETAILS

Description

ToddyCat: Keep calm and check logs

Report types

MISP-EVENT

Publication date

October 14, 2023 at 8:00:00 PM

Correlated reports

Entities distribution

Indicator

File

Hostname

URL

0 10 20 30

BASIC INFORMATION

Marking

TLP:CLEAR

Processing status

NEW

Author

CUDES0

Reliability (of author)

Unknown

Confidence level

4 - Doubtful

Distribution of opinions

strongly-disagree

disagree

agree

strongly-agree

Processing status

Assignees

Participants

Revoked

NO

Labels

Creation date (in this platform)

October 15, 2023 at 8:06:06 AM

Creators

ADMIN

Standard STIX ID

report-24406c47-0607-5440-83be-8092255916

Creation date

October 14, 2023 at 8:00:00 PM

Modification date

October 15, 2023 at 8:06:06 AM

EXTERNAL REFERENCES

External analysis (2c0d133e-d43d-40b3-b3e2-2c2f883b6f15)

https://securlist.com/toddycat-keep-calm-and-check-logs/110696/

NOTES ABOUT THIS ENTITY

Coleman Kane added a note on Nov 17, 2023, 2:27:46 PM

Abstract

Content

I read this report and it seems like HipCat, as well

Labels

Confidence level

2 - Probably True

Likelihood

50 / 100

Write a note

Collapse

Marking definition

Contents/context
summary

Tools to use
on entity

Arbitrary
labeling/tagging

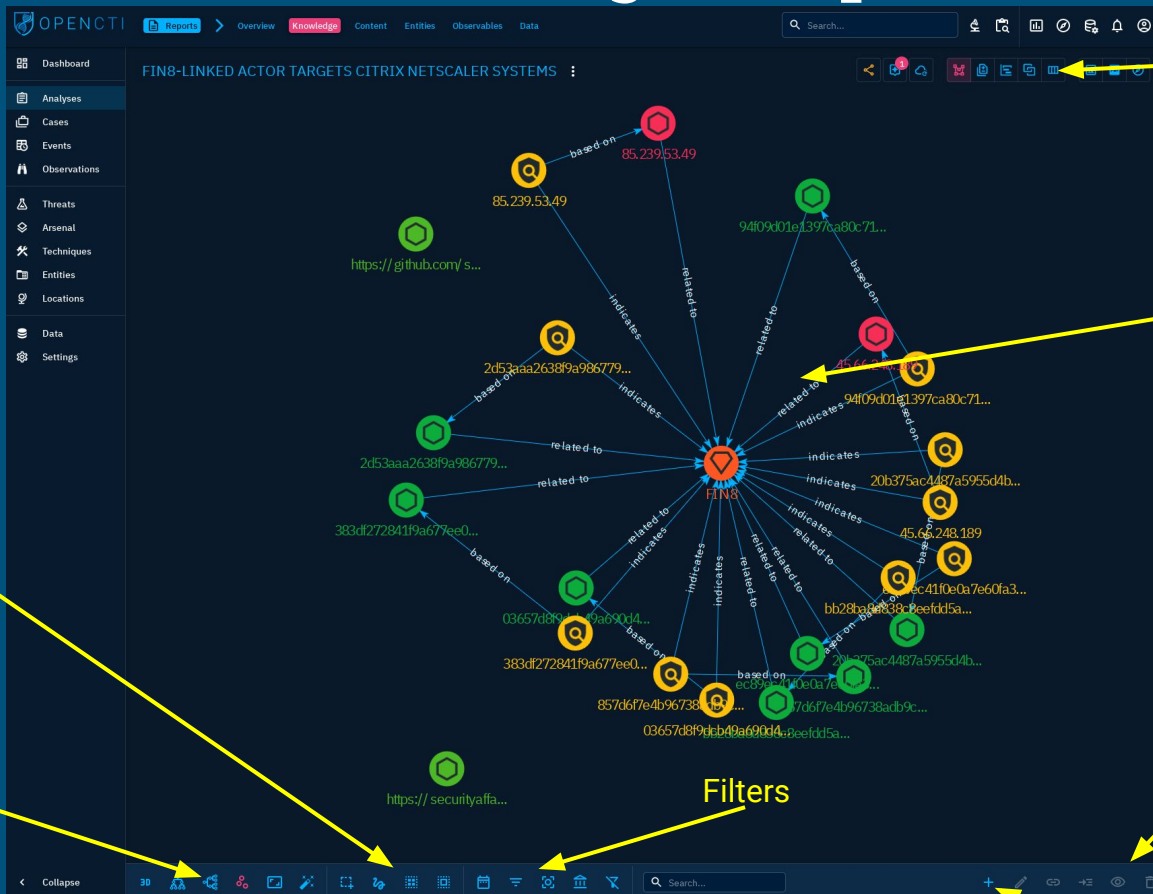
User
feedback

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



Analyses

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



Cases

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



Events

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



Observations

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



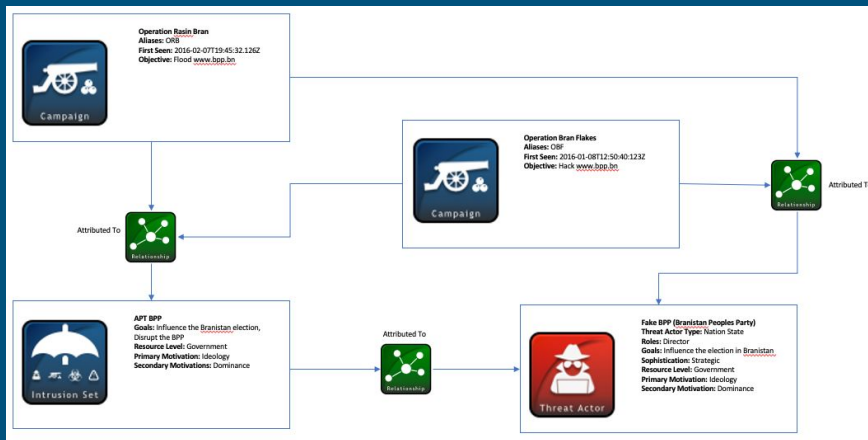
Threats

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



Arsenal

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



Techniques

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



Locations

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



Data import

DATA IMPORT

UPLOADED FILES



Plain Text
copy/paste import

New analyst
workbench

ANALYST WORKBENCHES

NAME

CREATOR



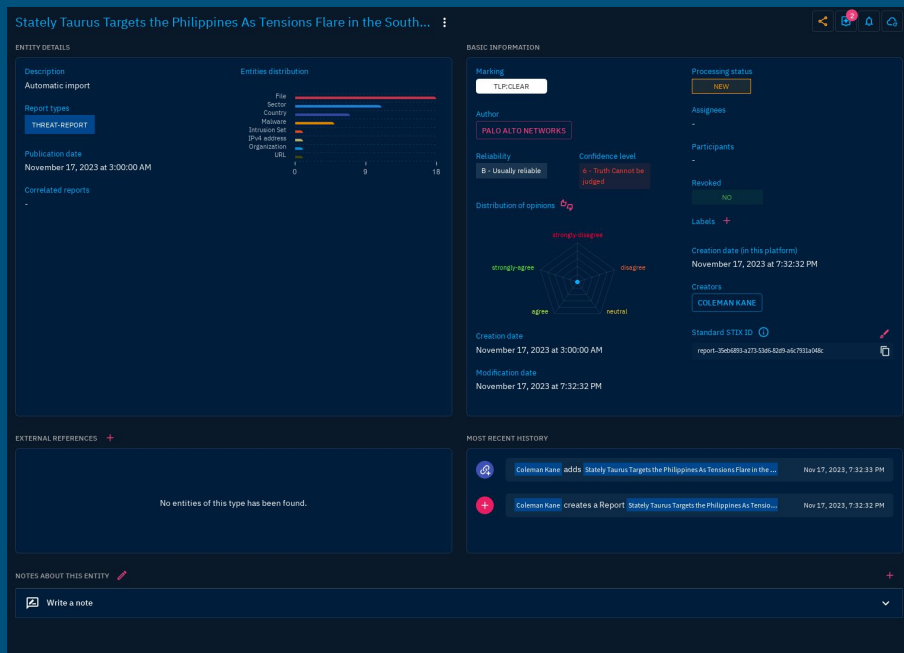
Stately Taurus Targets the Philippines As Tensions Flare in the South Pacific.pdf admin

Entities are matched to existing names & aliases in the database

Observables matching standard patterns auto-extracted and created

Add new entities/observables manually

Import Complete



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

PDF files

Stately Taurus Targets the Philippines As Tensions Flare in the South Pacific.pdf
November 17, 2023

Text files

No files in this category.

HTML files

No files in this category.

Markdown files

No files in this category.

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.



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

Rule code - editable in browser UI or via API

Control deployment with "Detection" switch

Related entities or observables

Pattern type - admin can add more types

Labels/tags

Reports that contain this signature

rule M_Hunting_VBS_Batch_Launcher_Strings { meta: ... }

Indicator pattern

```
rule M_Hunting_VBS_Batch_Launcher_Strings {
  meta:
    author = "Mandiant"
    date = "2023-02-13"
    description = "Searching for VBS files used to launch a batch script."
    disclaimer = "This rule is for hunting purposes only and has not been tested to run in a production environment."

  strings:
    $s1 = "CreateObject('WScript.Shell')&"
    $s2 = "WshShell.Run chr(34) &"
    $s3 = "& Chr(34), 0"
    $s4 = "Set WshShell= Nothing"
    $s5 = "bat"

  condition:
    filesize < 400 and
    all of them
}
```

Valid from: NOVEMBER 13, 2023 AT 7:08:22 AM

Valid until: NOVEMBER 14, 2024 AT 7:08:22 AM

Score: 40 / 100

Description: -

Indicator types: -

Based on: +

DETECTION

YES

Kill chain phases: -

Platforms: -

LATEST CREATED RELATIONSHIPS

IND1 INT1 Sandworm Team Nov 15, ... 4 - Doubtful TUP: CLEAR

BASIC INFORMATION

Marking: TUP: CLEAR

Author: CUDES0

Reliability (of author): Unknown

Confidence level: 4 - Doubtful

Distribution of opinions

Pattern type: yara

Processing status: DISABLED

Revoked: NO

Labels: +

ukraine

Creation date (in this platform): November 15, 2023 at 8:40:16 AM

Creators: ADMIN

Creation date: November 15, 2023 at 7:08:22 AM

Modification date: November 17, 2023 at 8:25:20 PM

Standard STIX ID: indicator--65083dbb-a29f-5058-acd4-de34d23690ff

LATEST CONTAINERS ABOUT THE OBJECT

REPORT1 Sandworm Disrupts Power in Ukraine ... CUDES0 Nov 14, 2... TUP: CLEAR

UI Overview: Advanced GraphQL Query

Enter query and/or mutation here

The screenshot displays the GraphQL Playground interface. The top bar includes tabs for 'MyQuery', 'PRETTIFY', 'HISTORY', and a URL 'https://octi.frogg.it/graphql'. The main editor on the left contains a query:

```
1 # Write your query or mutation here
2 query MyQuery {
3   reports {
4     edges {
5       node {
6         report_types
7         name
8         createdBy {
9           __typename
10          }
11        }
12      }
13    }
14  }
```

 A yellow arrow points from the text 'Enter query and/or mutation here' to this editor. Below the editor, the 'QUERY VARIABLES' and 'HTTP HEADERS (2)' sections are visible, with the latter containing:

```
1 {"Content-Type": "application/json"},
2 {"Authorization": "Bearer 11111111-2222-3333-4444-555555555555"}
```

 A yellow arrow points from the text 'Provide HTTP Auth token, and query input vars' to this section. The central pane shows the JSON output of the query, which is a list of report edges. A yellow arrow points from the text 'Output results in right pane' to this central pane. The right pane displays the GraphQL schema, including directives like @auth and @constraint, and various scalar and enum types. A yellow arrow points from the text 'Full Schema and API documentation' to this pane.

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)



Platinum Tier



THANK YOU!

TO OUR SPONSORS

Silver Tier



Bronze Tier

