SECURITY | OPENCTI | THREAT INTEL

Build Your Own Cyber Threat Intelligence System...at Home!

Learn how to collect Threat Intelligence for free

Andrew Blooman · Follow
Published in OSINT Team · 10 min read · Aug 2, 2024

What is Threat Intelligence?

> ***Threat intelligence involves analysing evidence-based information about cyber attacks, enabling cyber security experts to identify issues contextually and create targeted solutions for the detected problems.***
>
> *Rooted in data, similar to open source intelligence (OSINT), threat intelligence provides context — like who is attacking you, what their motivation and capabilities are, and what indicators of compromise (IOCs) in your systems to look for — that helps you make informed decisions about your security.*
>
> *— **Recorded Future***

It is important to note that within the topic of Cyber Threat Intelligence (CTI), there are several important subtopics to understand; Indicators of compromise and Advanced Persistent Threats and Traffic Light Protocol are three key areas to study in relation to CTI.

Indicators of Compromise (IOCs)

Indicators of compromise refer to data which can indicate that an organization may have been compromised by external actor. They are used by security teams to enrich logs in the SIEM so that, for example, if a new domain is marked as as malicious by a threat intelligence provider, and activity is detected between an organization an the domain, the security team should be alerted and conduct an investigation.

Types of IOC data include:

- IP Addresses
- Domain names
- Malicious file names
- File Hashes
- URLs

Advanced Persistent Threats (APTs)

> *An advanced persistent threat (APT) is a sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network in order to steal sensitive data over a prolonged period of time. An APT attack is carefully planned and designed to infiltrate a specific organization, evade existing security measures and fly under the radar.*
>
> *— **Crowdstrike***

APTs are tracked in several ways by different organizations. MITRE tracks APTs using a numbering system, whereas Crowdstrike refers to them by a name, typically associated with the country of origin. For example, MITRE refers to Russia's General Staff Main Intelligence Directorate (GRU) as **APT28**, whereas Crowdstrike refers to them as **Fancy Bear.**

- Crowdstrike: https://www.crowdstrike.com/adversaries/
- MITRE: https://attack.mitre.org/groups/

Traffic Light Protocol

> *The Traffic Light Protocol (TLP) was created in order to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s)*
>
> *— **Cyber Security Infrastructure Security Agency***

- **TLP: RED —** Not for disclosure, restricted to participants only.
- **TLP: Amber+Strict —** Limited disclosure, restricted to participants'

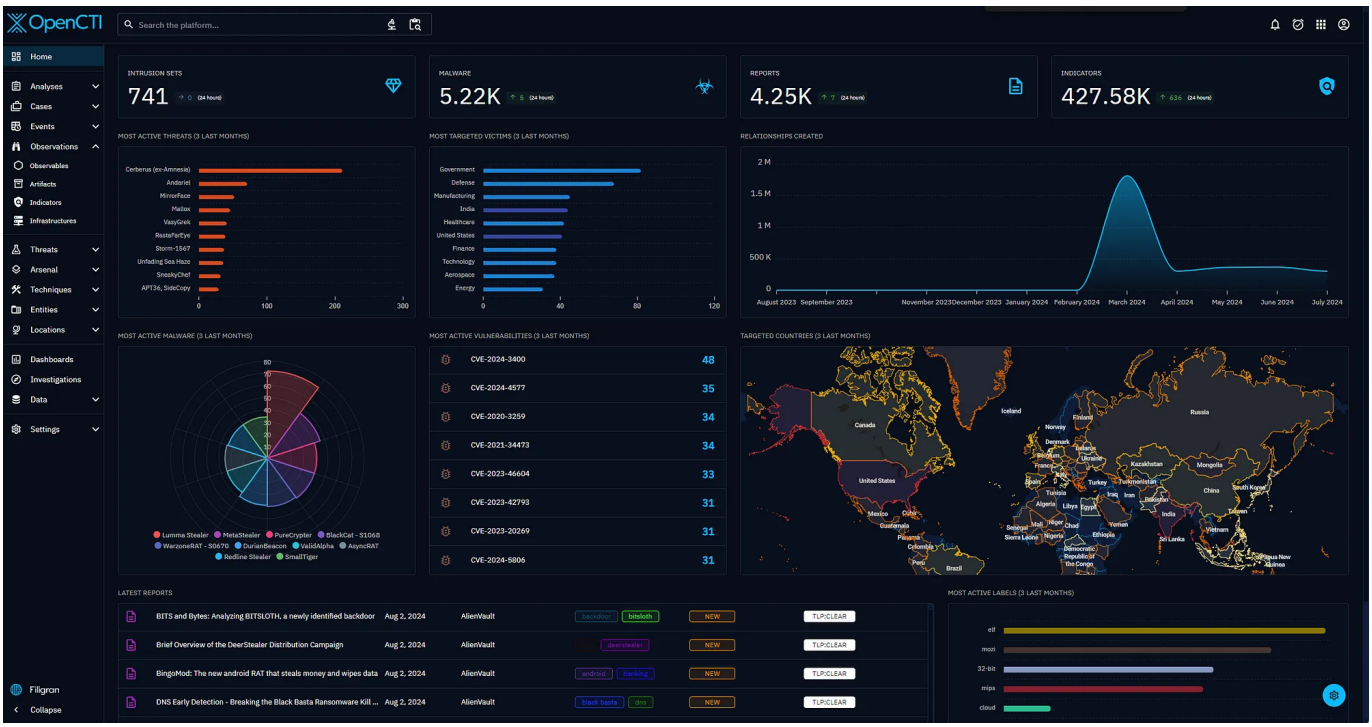
organization.

- **TLP: Amber —** Limited disclosure, restricted to participants' organization and its clients (see Terminology Definitions).
- **TLP: Green —** Limited disclosure, restricted to the community.
- **TLP: Clear —** Disclosure is not limited.

What is OpenCTI?

> *OpenCTI is an open source platform allowing organizations to manage their cyber threat intelligence knowledge and observables. It has been created in order to structure, store, organize and visualize technical and non-technical information about cyber threats.*
>
> *The structuration of the data is performed using a knowledge schema based on the STIX2 standards. It has been designed as a modern web application including a GraphQL API and an UX oriented frontend. Also, OpenCTI can be integrated with other tools and applications such as MISP, TheHive, MITRE ATT&CK, etc.*
>
> *— **OpenCTI***

OpenCTI is free to setup and run, consuming threat intelligence from open source and propriety threat feeds. It is ideal for using for a home lab on docker, although you can deploy to an organization (recommended to use Kubernetes). Once you start pulling data from threat feeds, you can very quickly get access to IOCs, threat reports, attack techniques, and more. The platform will automatically correlate similar threat intelligence so you can correlate multiple threat feeds to single entities.



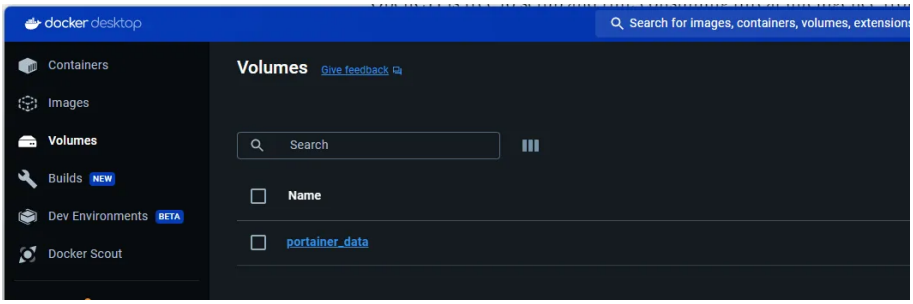
Setup and Install OpenCTI

For people who are less experienced installing and running docker, I suggest using Docker Desktop, then installing Portainer. Portainer provides a web interface and makes it very easy to work with the docker daemon, which should make deploying OpenCTI much easier.

Install Portainer — Full install guide here

1. Create Docker volume

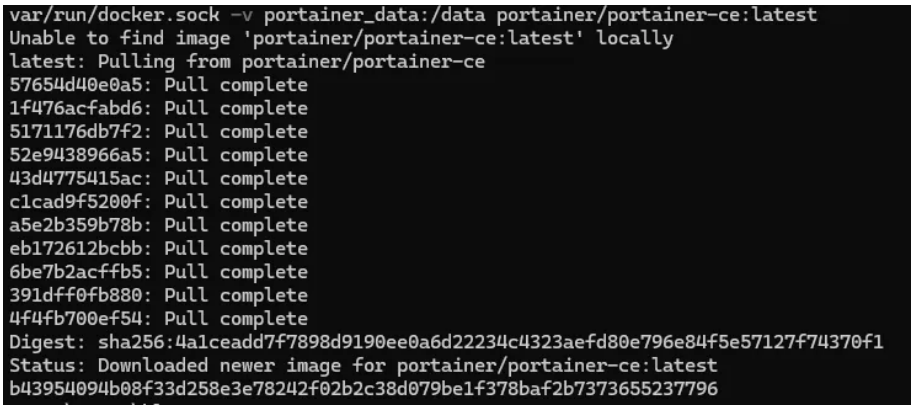
```
docker volume create portainer_data
```



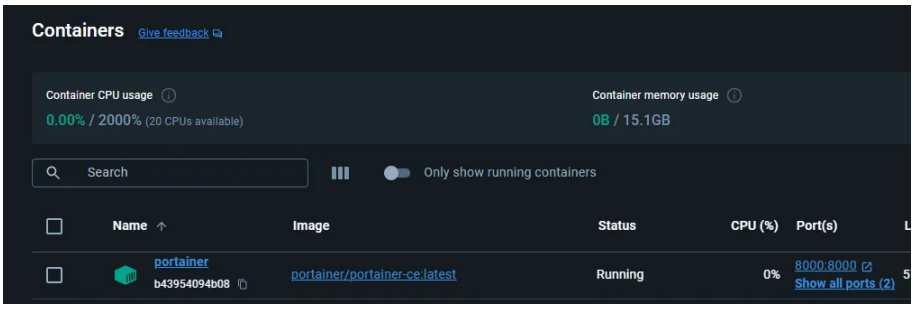
2. Run Portainer

```
docker run -d -p 8000:8000 -p 9443:9443 --name portainer --restart=always -v /va
```

3. You will see the following once it has completed pulling the image.



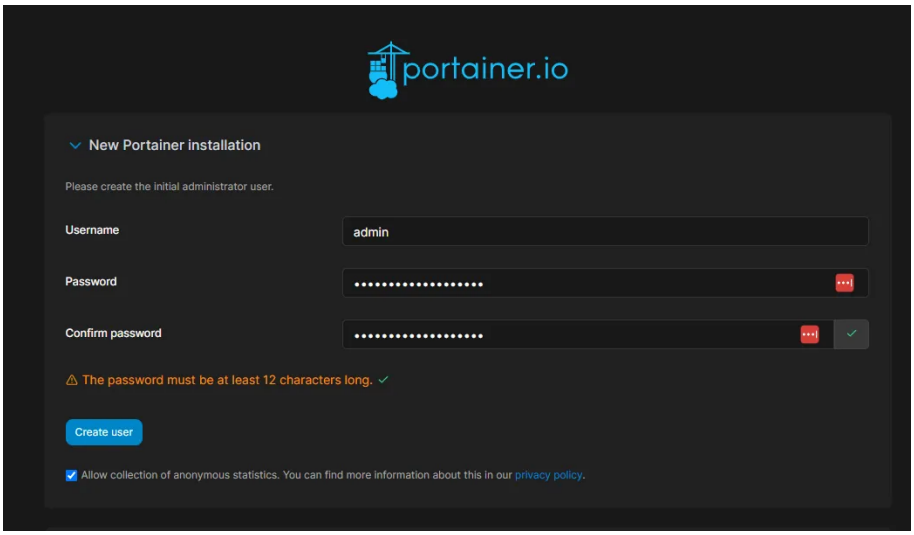
4. The Portainer container is now running and available to connect



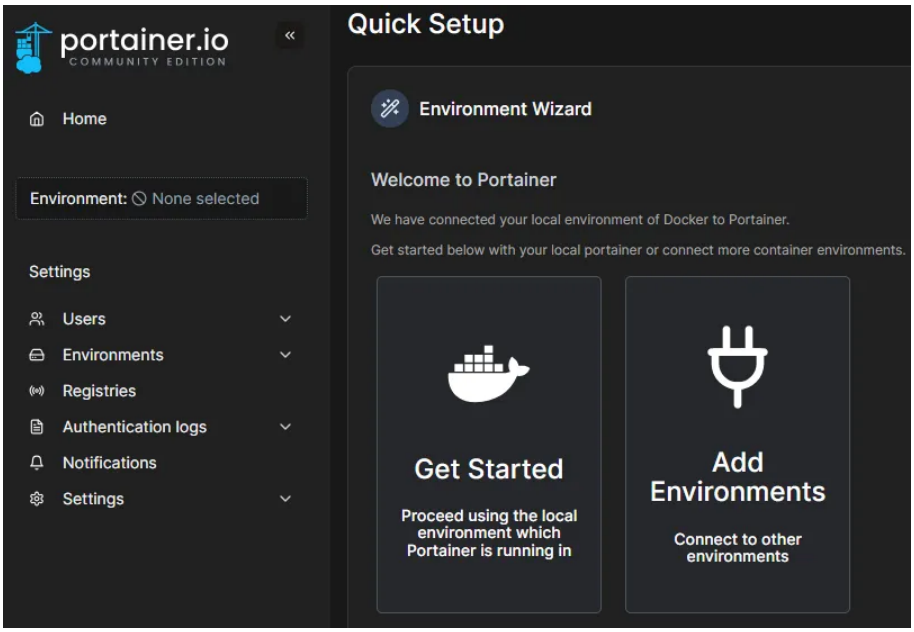
Setup Portainer

1. Connect to the new container using the following URL: https://localhost:9443. Replace `localhost` with the relevant IP address or FQDN if needed, and adjust the port if you changed it earlier.

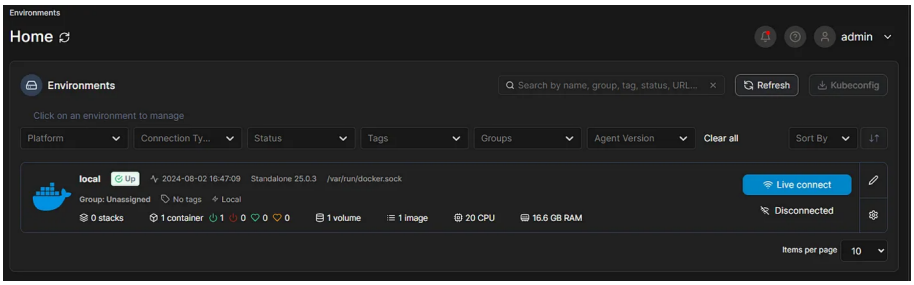
2. Create a password for the admin user.



3. Click Get Started.



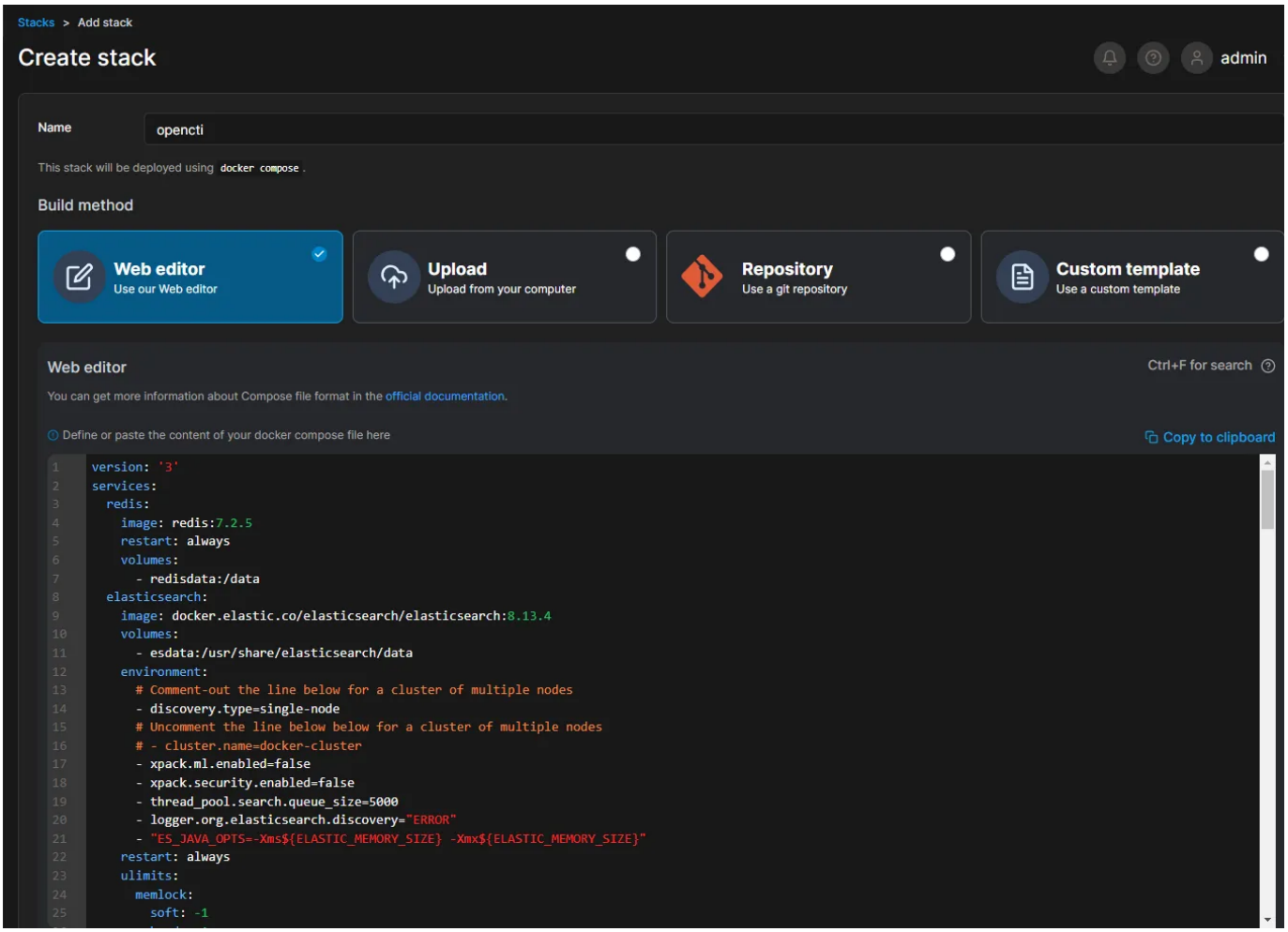
4. Click **Live Connect**



Take some time to explore the dashboard and familiarise yourself with the configuration.

Setup OpenCTI — Create Portainer Stack (Docker Compose)

1. Click On Stacks and create stack. Enter the name **opencti**



2. Below is an example docker compose file which cane be used for the Stack. Copy and paste to the Web Editor Window.

```
version: '3'
services:
  redis:
    image: redis:7.2.5
    restart: always
    volumes:
      - redisdata:/data
  elasticsearch:
    image: docker.elastic.co/elasticsearch/elasticsearch:8.13.4
    volumes:
      - esdata:/usr/share/elasticsearch/data
    environment:
```

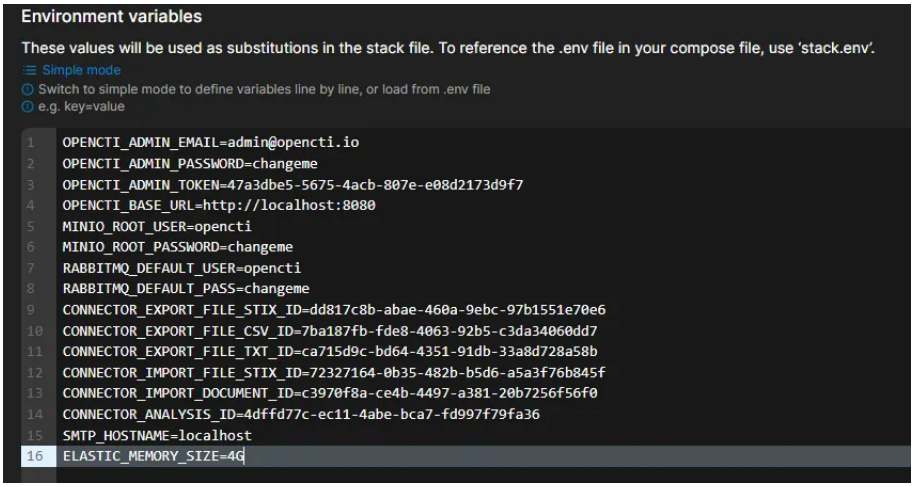
```
      # Comment-out the line below for a cluster of multiple nodes
      - discovery.type=single-node
      # Uncomment the line below below for a cluster of multiple nodes
      # - cluster.name=docker-cluster
      - xpack.ml.enabled=false
      - xpack.security.enabled=false
      - thread_pool.search.queue_size=5000
      - logger.org.elasticsearch.discovery="ERROR"
      - "ES_JAVA_OPTS=-Xms${ELASTIC_MEMORY_SIZE} -Xmx${ELASTIC_MEMORY_SIZE}"
    restart: always
    ulimits:
      memlock:
        soft: -1
        hard: -1
      nofile:
        soft: 65536
        hard: 65536
  minio:
    image: minio/minio:RELEASE.2024-05-28T17-19-04Z # Use "minio/minio:RELEASE.2
    volumes:
      - s3data:/data
    ports:
      - "9000:9000"
    environment:
      MINIO_ROOT_USER: ${MINIO_ROOT_USER}
      MINIO_ROOT_PASSWORD: ${MINIO_ROOT_PASSWORD}
    command: server /data
    restart: always
  rabbitmq:
    image: rabbitmq:3.13-management
    environment:
      - RABBITMQ_DEFAULT_USER=${RABBITMQ_DEFAULT_USER}
      - RABBITMQ_DEFAULT_PASS=${RABBITMQ_DEFAULT_PASS}
      - RABBITMQ_NODENAME=rabbit01@localhost
    volumes:
      - amqpdata:/var/lib/rabbitmq
    restart: always
  opencti:
    image: opencti/platform:6.2.11
    environment:
      - NODE_OPTIONS=--max-old-space-size=8096
      - APP__PORT=8080
      - APP__BASE_URL=${OPENCTI_BASE_URL}
      - APP__ADMIN__EMAIL=${OPENCTI_ADMIN_EMAIL}
      - APP__ADMIN__PASSWORD=${OPENCTI_ADMIN_PASSWORD}
      - APP__ADMIN__TOKEN=${OPENCTI_ADMIN_TOKEN}
      - APP__APP_LOGS__LOGS_LEVEL=error
      - REDIS__HOSTNAME=redis
      - REDIS__PORT=6379
      - ELASTICSEARCH__URL=http://elasticsearch:9200
      - MINIO__ENDPOINT=minio
      - MINIO__PORT=9000
      - MINIO__USE_SSL=false
      - MINIO__ACCESS_KEY=${MINIO_ROOT_USER}
      - MINIO__SECRET_KEY=${MINIO_ROOT_PASSWORD}
      - RABBITMQ__HOSTNAME=rabbitmq
      - RABBITMQ__PORT=5672
      - RABBITMQ__PORT_MANAGEMENT=15672
      - RABBITMQ__MANAGEMENT_SSL=false
      - RABBITMQ__USERNAME=${RABBITMQ_DEFAULT_USER}
      - RABBITMQ__PASSWORD=${RABBITMQ_DEFAULT_PASS}
      - SMTP__HOSTNAME=${SMTP_HOSTNAME}
      - SMTP__PORT=25
      - PROVIDERS__LOCAL__STRATEGY=LocalStrategy
    ports:
      - "8080:8080"
    depends_on:
      - redis
      - elasticsearch
      - minio
      - rabbitmq
    restart: always
```

```
  worker:
    image: opencti/worker:6.2.11
    environment:
      - OPENCTI_URL=${OPENCTI_URL}
      - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
      - WORKER_LOG_LEVEL=info
    depends_on:
      - opencti
    deploy:
      mode: replicated
      replicas: 3
    restart: always
  connector-export-file-stix:
    image: opencti/connector-export-file-stix:6.2.11
    environment:
      - OPENCTI_URL=${OPENCTI_URL}
      - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
      - CONNECTOR_ID=${CONNECTOR_EXPORT_FILE_STIX_ID} # Valid UUIDv4
      - CONNECTOR_TYPE=INTERNAL_EXPORT_FILE
      - CONNECTOR_NAME=ExportFileStix2
      - CONNECTOR_SCOPE=application/json
      - CONNECTOR_LOG_LEVEL=info
    restart: always
    depends_on:
      - opencti
  connector-export-file-csv:
    image: opencti/connector-export-file-csv:6.2.11
    environment:
      - OPENCTI_URL=${OPENCTI_URL}
      - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
      - CONNECTOR_ID=${CONNECTOR_EXPORT_FILE_CSV_ID} # Valid UUIDv4
      - CONNECTOR_TYPE=INTERNAL_EXPORT_FILE
      - CONNECTOR_NAME=ExportFileCsv
      - CONNECTOR_SCOPE=text/csv
      - CONNECTOR_LOG_LEVEL=info
    restart: always
    depends_on:
      - opencti
  connector-export-file-txt:
    image: opencti/connector-export-file-txt:6.2.11
    environment:
      - OPENCTI_URL=${OPENCTI_URL}
      - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
      - CONNECTOR_ID=${CONNECTOR_EXPORT_FILE_TXT_ID} # Valid UUIDv4
      - CONNECTOR_TYPE=INTERNAL_EXPORT_FILE
      - CONNECTOR_NAME=ExportFileTxt
      - CONNECTOR_SCOPE=text/plain
      - CONNECTOR_LOG_LEVEL=info
    restart: always
    depends_on:
      - opencti
  connector-import-file-stix:
    image: opencti/connector-import-file-stix:6.2.11
    environment:
      - OPENCTI_URL=${OPENCTI_URL}
      - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
      - CONNECTOR_ID=${CONNECTOR_IMPORT_FILE_STIX_ID} # Valid UUIDv4
      - CONNECTOR_TYPE=INTERNAL_IMPORT_FILE
      - CONNECTOR_NAME=ImportFileStix
      - CONNECTOR_VALIDATE_BEFORE_IMPORT=true # Validate any bundle before impor
      - CONNECTOR_SCOPE=application/json,text/xml
      - CONNECTOR_AUTO=true # Enable/disable auto-import of file
      - CONNECTOR_LOG_LEVEL=info
    restart: always
    depends_on:
      - opencti
  connector-import-document:
    image: opencti/connector-import-document:6.2.11
    environment:
      - OPENCTI_URL=${OPENCTI_URL}
      - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
      - CONNECTOR_ID=${CONNECTOR_IMPORT_DOCUMENT_ID} # Valid UUIDv4
```

```
      - CONNECTOR_TYPE=INTERNAL_IMPORT_FILE
      - CONNECTOR_NAME=ImportDocument
      - CONNECTOR_VALIDATE_BEFORE_IMPORT=true # Validate any bundle before impor
      - CONNECTOR_SCOPE=application/pdf,text/plain,text/html
      - CONNECTOR_AUTO=true # Enable/disable auto-import of file
      - CONNECTOR_ONLY_CONTEXTUAL=false # Only extract data related to an entity
      - CONNECTOR_CONFIDENCE_LEVEL=15 # From 0 (Unknown) to 100 (Fully trusted)
      - CONNECTOR_LOG_LEVEL=info
      - IMPORT_DOCUMENT_CREATE_INDICATOR=true
    restart: always
    depends_on:
      - opencti
  connector-analysis:
    image: opencti/connector-import-document:6.2.11
    environment:
      - OPENCTI_URL=${OPENCTI_URL}
      - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
      - CONNECTOR_ID=${CONNECTOR_ANALYSIS_ID} # Valid UUIDv4
      - CONNECTOR_TYPE=INTERNAL_ANALYSIS
      - CONNECTOR_NAME=ImportDocumentAnalysis
      - CONNECTOR_VALIDATE_BEFORE_IMPORT=false # Validate any bundle before impo
      - CONNECTOR_SCOPE=application/pdf,text/plain,text/html
      - CONNECTOR_AUTO=true # Enable/disable auto-import of file
      - CONNECTOR_ONLY_CONTEXTUAL=false # Only extract data related to an entity
      - CONNECTOR_CONFIDENCE_LEVEL=15 # From 0 (Unknown) to 100 (Fully trusted)
      - CONNECTOR_LOG_LEVEL=info
    restart: always
    depends_on:
      - opencti

volumes:
  esdata:
  s3data:
  redisdata:
  amqpdata:
```

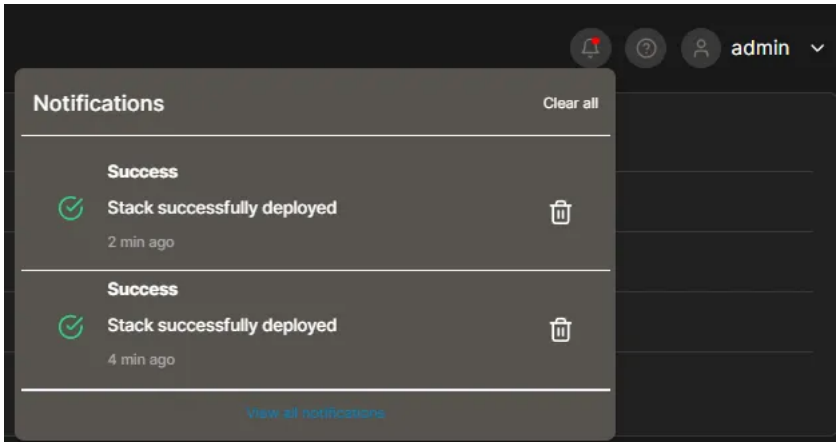
3. Click on Environment Variables. Click Advanced Mode. Copy and paste the variables into the window:




```
OPENCTI_ADMIN_EMAIL=admin@opencti.io
OPENCTI_ADMIN_PASSWORD=changeme
OPENCTI_ADMIN_TOKEN=47a3dbe5-5675-4acb-807e-e08d2173d9f7
```

```
OPENCTI_BASE_URL=http://localhost:8080
MINIO_ROOT_USER=opencti
MINIO_ROOT_PASSWORD=changeme
RABBITMQ_DEFAULT_USER=opencti
RABBITMQ_DEFAULT_PASS=changeme
CONNECTOR_EXPORT_FILE_STIX_ID=dd817c8b-abae-460a-9ebc-97b1551e70e6
CONNECTOR_EXPORT_FILE_CSV_ID=7ba187fb-fde8-4063-92b5-c3da34060dd7
CONNECTOR_EXPORT_FILE_TXT_ID=ca715d9c-bd64-4351-91db-33a8d728a58b
CONNECTOR_IMPORT_FILE_STIX_ID=72327164-0b35-482b-b5d6-a5a3f76b845f
CONNECTOR_IMPORT_DOCUMENT_ID=c3970f8a-ce4b-4497-a381-20b7256f56f0
CONNECTOR_ANALYSIS_ID=4dffd77c-ec11-4abe-bca7-fd997f79fa36
SMTP_HOSTNAME=localhost
ELASTIC_MEMORY_SIZE=4G
OPENCTI_URL=http://opencti:8080
```

4. Make sure to change the passwords in the environment variables file from **changeme** to something more secure**.** Click **Deploy Stack.** This will take some time as it will need to download additional docker images. Once complete you should see the stack deployed in the notification bell.

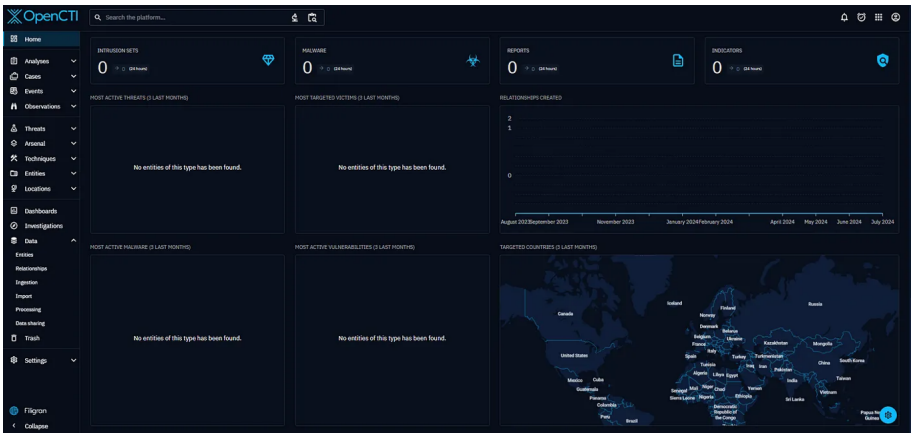


If you see any errors, you can examine the logs of each container and see if there are any connectivity issues.

Access & Start Using OpenCTI

1. Access the URL http://localhost:8080/ using these credentials to login:

- Username: admin@opencti.io
- Password: **You set this earlier in the environment variables**



At this stage you won't see much happening as we haven't added any threat feeds just yet.

2. Lets add one threat feed from CISA, for known Exploited Vulnerabilities. This is referred to as "The KEV List".

Go back to the stacks editor. Paste the following code towards the bottom of the window. Ensure it is pasted above the **Volumes** section.

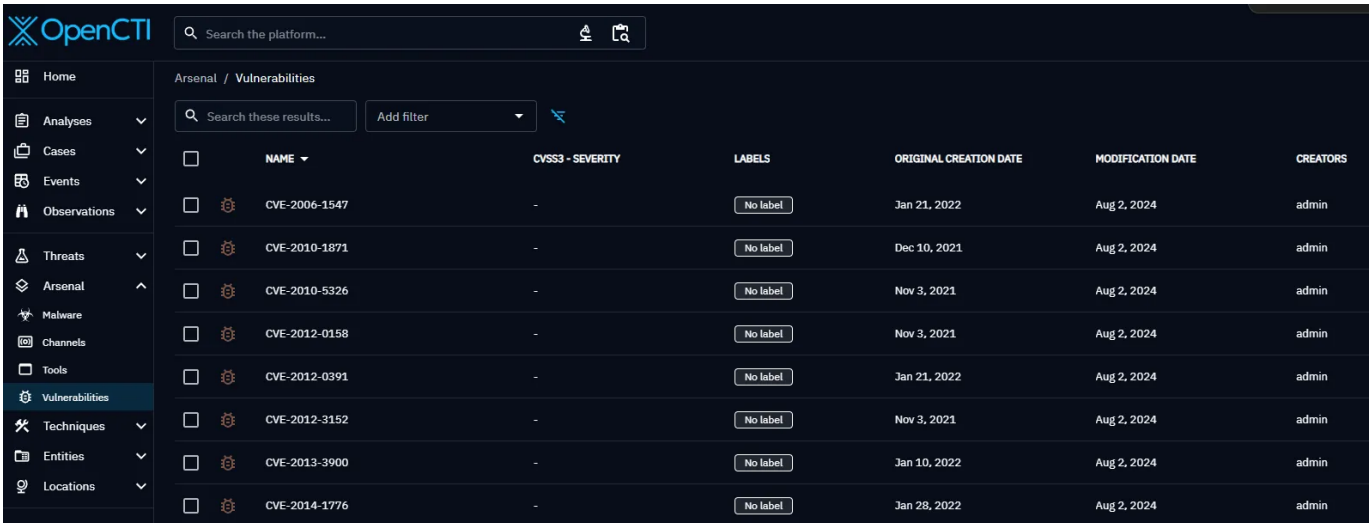
```
  connector-cisa-known-exploited-vulnerabilities:
    image: opencti/connector-cisa-known-exploited-vulnerabilities:latest
    environment:
      - OPENCTI_URL=${OPENCTI_URL}
      - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
      - CONNECTOR_ID=dc788080-859b-49d7-8946-0ec346725204
      - CONNECTOR_TYPE=EXTERNAL_IMPORT
      - "CONNECTOR_NAME=CISA Known Exploited Vulnerabilities"
      - CONNECTOR_SCOPE=cisa
      - CONNECTOR_CONFIDENCE_LEVEL=100 # From 0 (Unknown) to 100 (Fully trusted)
      - CONNECTOR_UPDATE_EXISTING_DATA=false
      - CONNECTOR_RUN_AND_TERMINATE=false
      - CONNECTOR_LOG_LEVEL=info
      - CISA_CATALOG_URL=https://www.cisa.gov/sites/default/files/feeds/known_ex
      - CISA_CREATE_INFRASTRUCTURES=false
      - CISA_TLP=TLP:CLEAR
      - CISA_INTERVAL=2 # In days, must be strictly greater than 1
    restart: always
```

3. It should look like this. (Note, indentation on Docker Compose is important, so it may indicate that there is a formatting error. Ensure it is correctly indented).

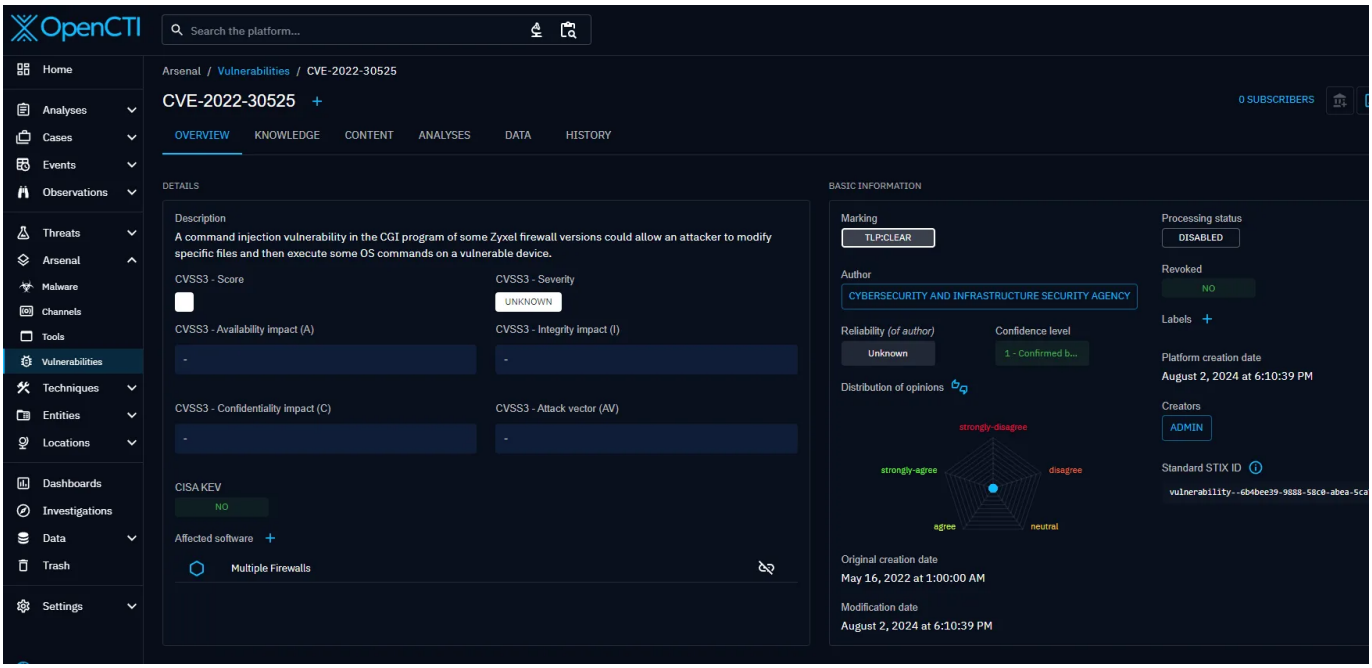
4. You will need to generate a Connector ID for any new connectors you add. In my example, the ID is on **Line 191.**

This is required for every subsequent connector; you can generate new IDs using the following site UUID Generator.

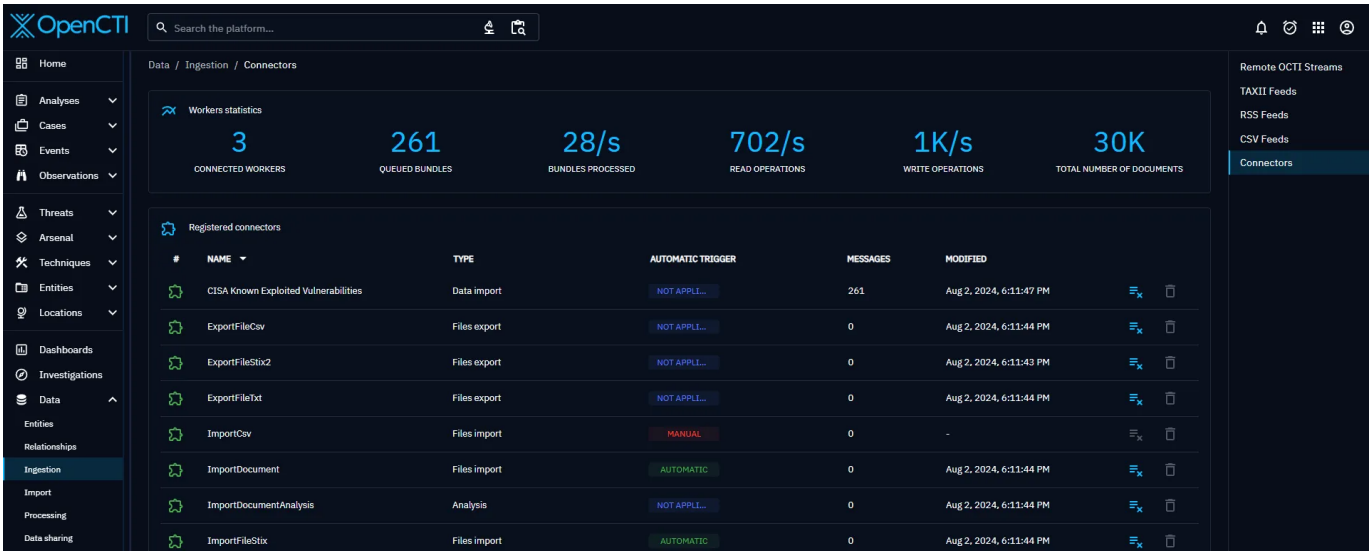
5. Click Update stack; it will download the new container image and run. To confirm this, navigate to Arsenal, and then Vulnerabilities.



6. If you click on one of the vulnerabilities you will see the detail which has been downloaded.



7. For troubleshooting, you can click on **Data,** then **Ingestion.** Click on **Connectors** to see the newly added **CISA Known Exploited Vulnerabilities** connector. You can see the Worker statistics pane is showing there is activity ongoing.



OpenCTI Connectors

You can add multiple connectors, to pull threat feeds from external sources. The full list of available connectors can be found here on the OpenCTI GitHub

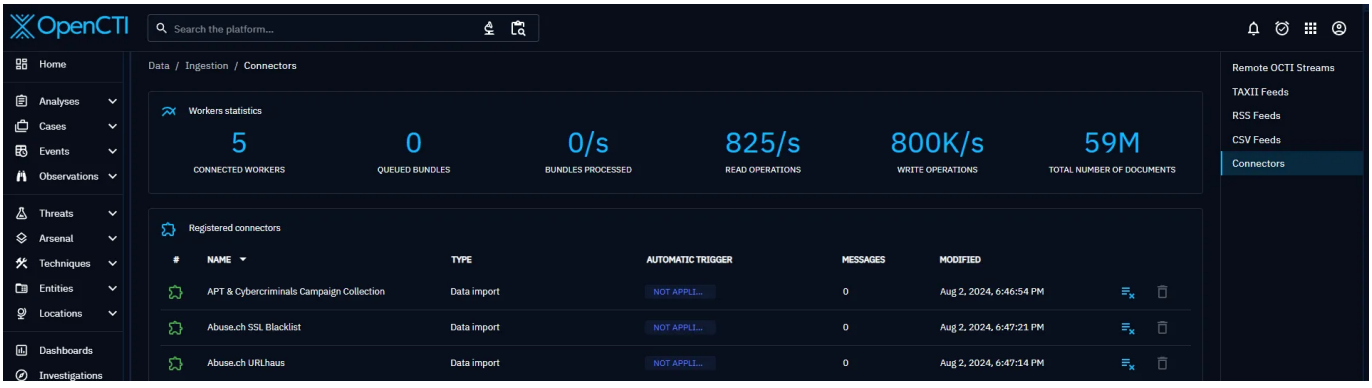
Some of these connectors require an API token; whilst some are free to use, please ensure you read the Terms and conditions for the appropriate usage. For individuals, some threat intel services such as AlienVault OTX will allow the consumption of their threat intel for free, but for organizations, it requires a paid subscription. There is a ReadMe for each connector, but for reference, the AlienVault OTX link can be found here

I've added my configuration to my GitHub, which you are free to download and use for yourself, but bear in mind that you will need to generate the required API tokens.

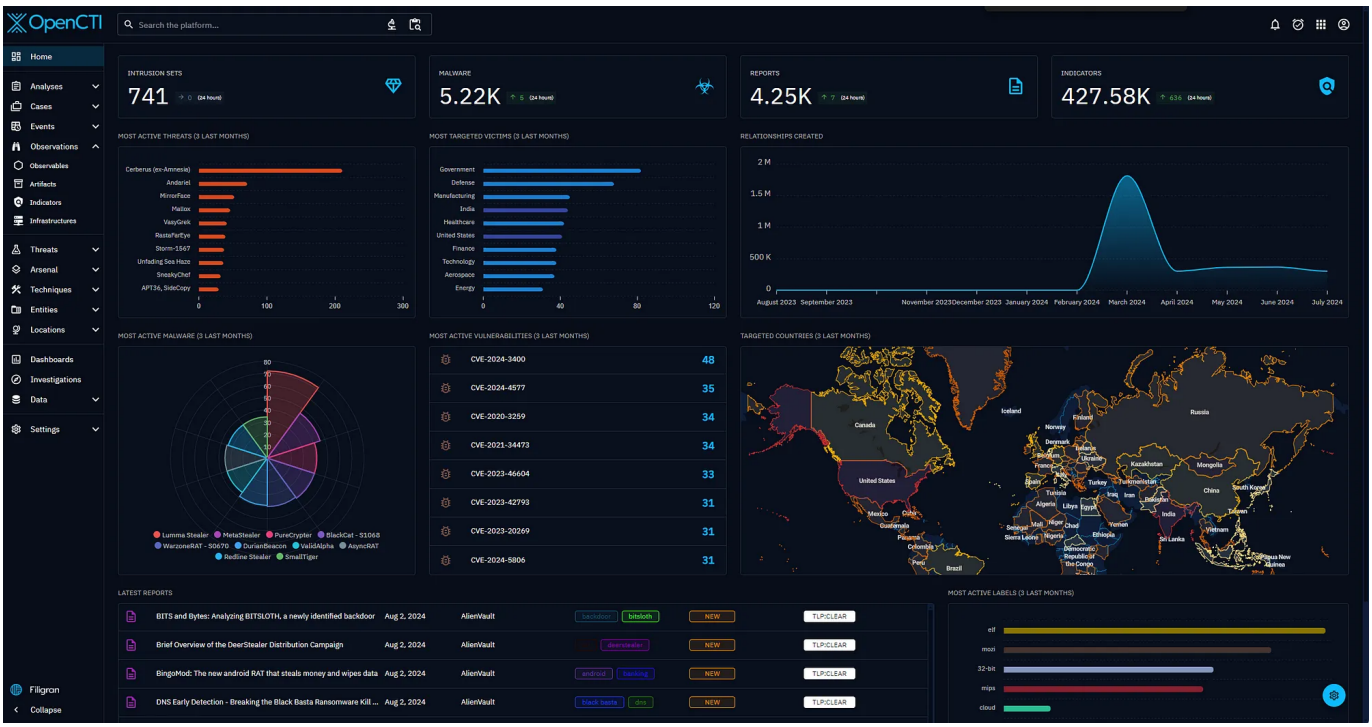
Some of the Connectors I use for my home lab include:

- Shodan
- AlienVault OTX
- Abuse IPDB
- URL Haus

Once you've added multiple connectors, confirm the data is being ingested by checking the Connectors page again. The data will be queued and can take up to 24 hours to download and process.

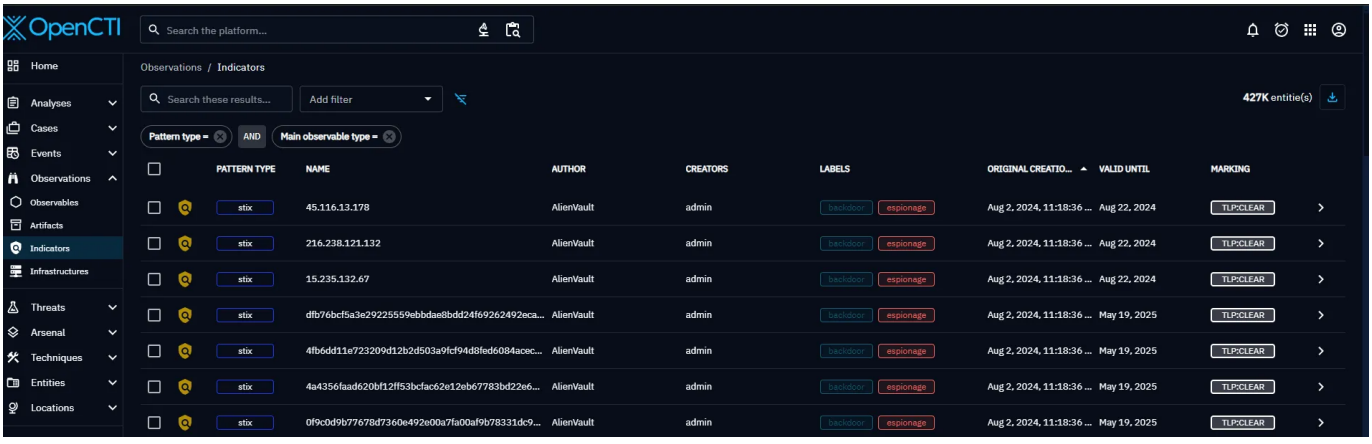


Once its finished syncing, it should populate the dashboard like below.



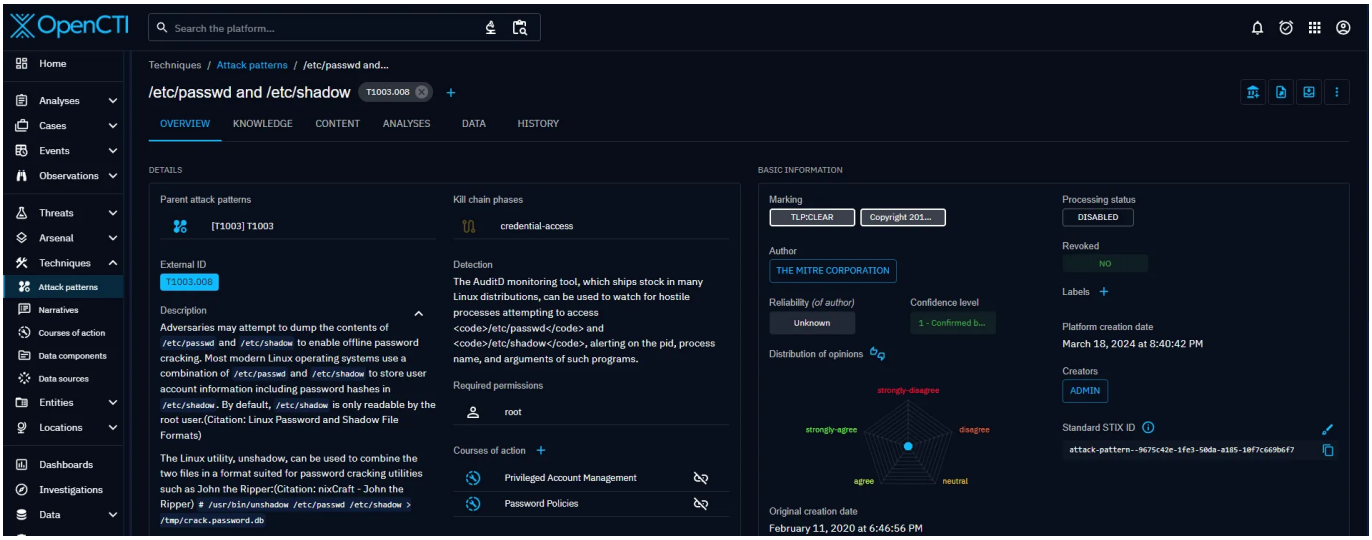
OpenCTI — Indicators Of Compromise

Navigate to the Indicators and Observables pages to see the various IOCs which have been downloaded. These are searchable in the platform and can help you find out who may behind an attack.



OpenCTI — Attack Patterns

For any aspiring Red Teamers or Pen testers, check out the Attack Patterns for guidance on how adversaries may attempt to breach different systems, for example; OS credential dumping in Linux.



Final Thoughts

OpenCTI is a great way to learn more about threat intelligence and is a fun project which you can learn at home, but you could always deploy within an Organization. OpenCTI integrates nicely with MISP, which is another popular source of open source threat intel.

Proprietary threat intel feeds from organisations such as Recorded Future and ReliaQuest can be very expensive; so a great way to augment your systems is to use aggregators like MISP and OpenCTI (Or build your own!). This can furnish your SIEM and SOAR products with threat intel to compliment the restricted information which you may pay for.

Devsecops | Threat Intelligence | Docker | Security | Cisa

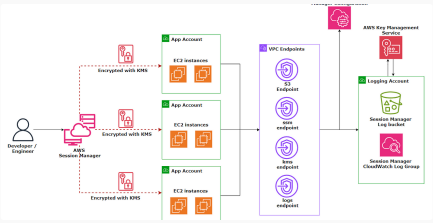
Written by Andrew Blooman

Follow

1.1K Followers · Writer for OSINT Team

Hi, I'm Andrew. Welcome! I'm a Senior Security engineer specialising in Cloud Security and DevSecOps. https://www.linkedin.com/in/andrewblooman/

More from Andrew Blooman and OSINT Team



Andrew Blooman in AWS Tip

Stop using SSH in AWS! Here's Why! A DevSecOps Perspective

Using Session Manager to provide secure EC2 access, whilst improving incident

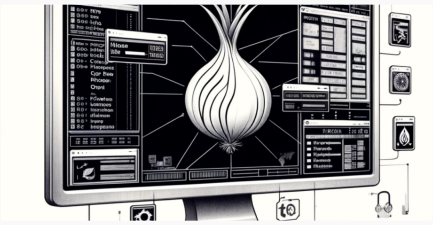
Jul 28 501 10

Hay.bnz in OSINT Team

Mastering OSINT: How to Find Information on Anyone

In today's digital age, information is more accessible than ever before. Open Source

Aug 7 571 4



Ervin Zubic in OSINT Team

Point-and-Click OSINT: Dark Web Scraping with GUI Tools

Discover how to gather OSINT data from the dark web without coding. Learn point-and-

Apr 29 358 5

Andrew Blooman in OSINT Team

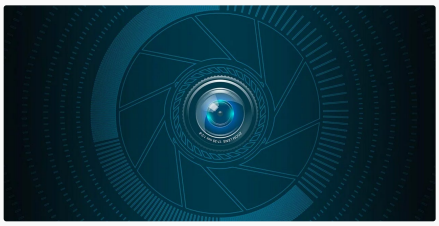
Build Your Own Cyber Threat Intel Feeds at Home! (MISP)

Learn how to Collect Open Source Threat Intelligence

Aug 14 174 1

See all from Andrew Blooman | See all from OSINT Team

Recommended from Medium



Vasileiadis A. (CyberKid)

Detect hidden surveillance cameras with your phone

A family recently it had a big surprise on their Airbnb: a hidden camera disguised as a

Aug 4 1.4K 17

Hay.bnz in OSINT Team

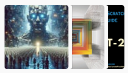
Mastering OSINT: How to Find Information on Anyone

In today's digital age, information is more accessible than ever before. Open Source

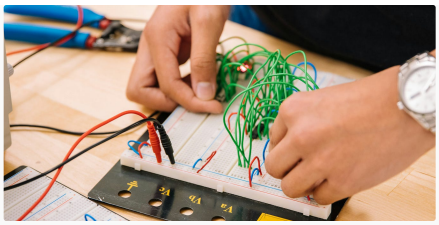
Aug 7 571 4

Lists

Coding & Development
11 stories · 774 saves



Natural Language Processing
1679 stories · 1252 saves

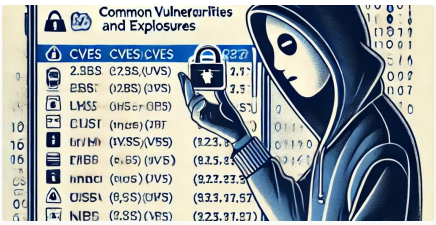


Abdul Issa in InfoSec Write-ups

Boost Your Cybersecurity Career With These 7 Hands-on Projects

Explore Practical Projects That Will Help You Build Your Portfolio And Enhance Your

Aug 1 679 5



Jonathan Mondaut

How ChatGPT Turned Me into a Hacker

Discover how ChatGPT helped me become a hacker, from gathering resources to tackling

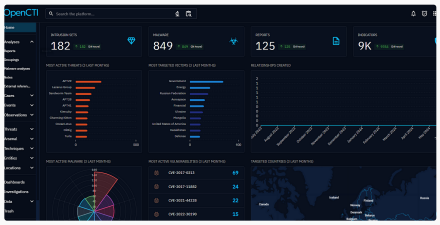
Jun 18 1K 29

Abhay Parashar in The Pythoneers

17 Mindblowing Python Automation Scripts I Use Everyday

Scripts That Increased My Productivity and Performance

Aug 25 7.3K 68



Yogasatriautama

SOC: Install OpenCTI

OpenCTI (Open Cyber Threat Intelligence) is an open-source platform designed to collect,

Jul 21 111 1

See more recommendations