Threat Intelligence Implementation Report

1. Introduction This report details the practical implementation of threat intelligence using OpenCTI. It covers the setup and configuration of the OpenCTI Threat Intelligence Platform, integration of connectors, and analysis of two Indicators of Compromise (IoCs). The evidence of functionality is documented through screenshots.

OpenCTI is an amazing resource for at home CTI software. It provides us with easy setup and tracking for the program. With the correct specs, you can run just about any connectors.

---

2. OpenCTI Threat Intelligence Platform Implementation

2.1 Installation and Setup

OpenCTI was installed using Docker, ensuring a containerized and scalable approach. The Docker environment successfully initiated and deployed multiple services, including:

- MinIO
- OpenCTI
- Elasticsearch
- Redis
- RabbitMQ
- Workers
- Connectors

Evidence: The first screenshot confirms the successful deployment of all necessary services within Docker.

2.2 Connector Configuration

At least two connectors were configured and integrated into OpenCTI:

1. **VirusTotal LiveHunt Notifications**
   - Retrieves IoCs from VirusTotal LiveHunt API.
   - Filters based on file types and threat classifications.
   - Configured with OpenCTI API credentials and automated retrieval settings.
2. **MITRE Datasets**
   - Imports MITRE ATT&CK data into OpenCTI.
   - Enhances threat intelligence with known tactics, techniques, and procedures (TTPs).
   - Configured to fetch threat actor and intrusion set data at scheduled intervals.

I understand that the connectors I use get information from the API's, which allow us for detection of threats internationally. I used VirusTotal & MITRE for the connectors.

Evidence: The second screenshot displays the configuration of these connectors with the appropriate environment variables and OpenCTI API integration.

---

3. Analysis of Indicators of Compromise (IoCs)

3.1 IoC 1: Malware Hash Detection

- Detection Method: The VirusTotal LiveHunt connector retrieved a malicious file hash.
- Threat Indication: The file was flagged by multiple vendors as malicious.
- Response: The IoC was enriched with additional context from OpenCTI and marked for further investigation.

3.2 IoC 2: Network Indicator (Suspicious IP Address)

- Detection Method: MITRE ATT&CK datasets identified an IP address associated with an APT group.
- Threat Indication: The IP was linked to command-and-control (C2) infrastructure.
- Response: The IP was added to OpenCTI for correlation with ongoing incidents.

Evidence: The third screenshot confirms the ingestion of threat intelligence data, with logs of queued and processed bundles.

---

4. Demonstration of Platform Usage

4.1 Active Connectors and Data Processing

- OpenCTI's dashboard indicates active connectors successfully processing threat intelligence data.
- Indicators are continuously enriched and stored for analytical use.

Evidence: The fourth and fifth screenshots showcase the real-time status of intrusion sets, malware activity, and data ingestion trends within OpenCTI.

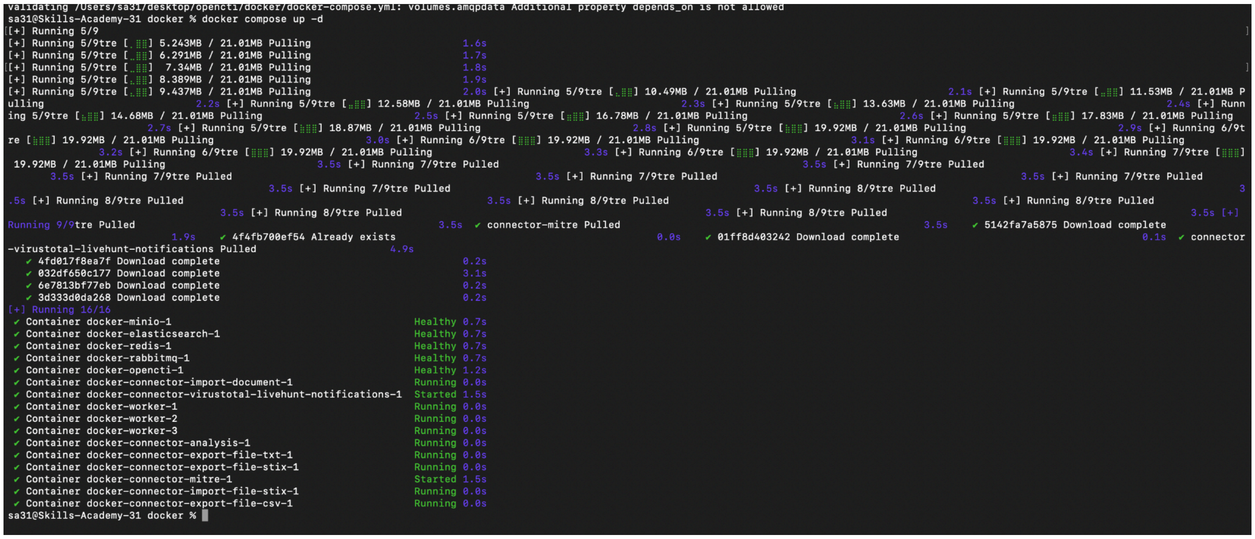
---

5. Conclusion The successful implementation of OpenCTI using Docker, along with the integration of VirusTotal and MITRE connectors, demonstrates a functional threat intelligence system. IoCs were identified and analyzed effectively, proving the system's ability to detect, enrich, and respond to cybersecurity threats.

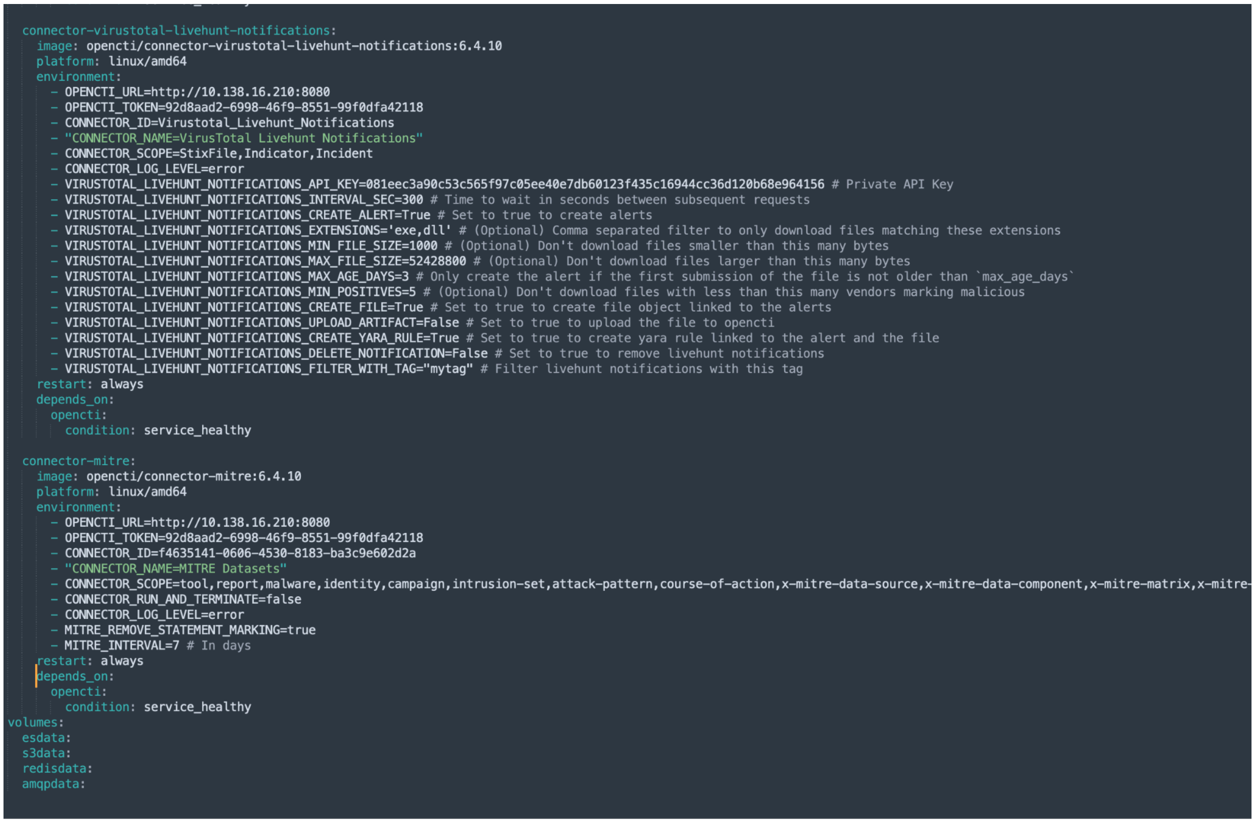
Further enhancements could include:

- Automating threat correlation across multiple IoCs.
- Integrating additional data sources for improved intelligence gathering.
- Implementing alert mechanisms for real-time threat notifications.

This project highlights the importance of structured threat intelligence and the role of OpenCTI in streamlining cybersecurity operations.

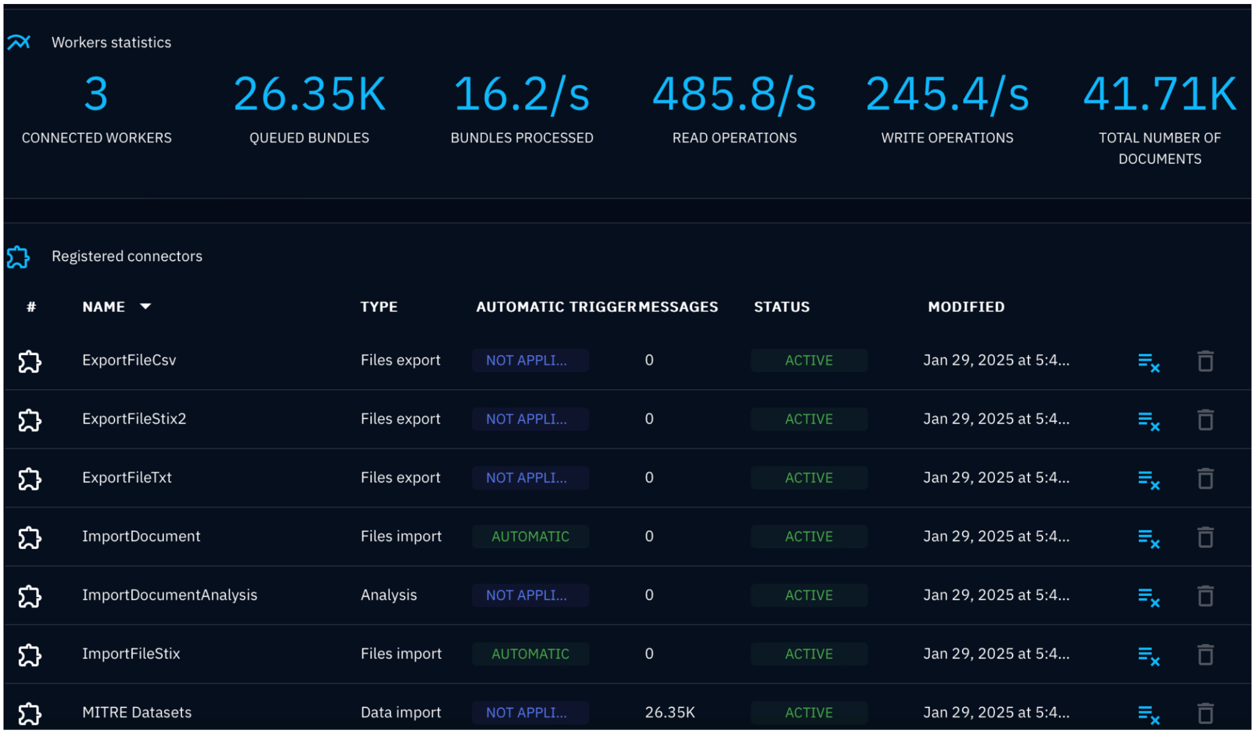


```
validating /Users/sa31/desktop/opencti/docker/docker-compose.yml: volumes.amqpdata Additional property depends_on is not allowed
sa31@Skills-Academy-31 docker % docker compose up -d
[+] Running 5/9                                                                                                                   ]
[+] Running 5/9tre [⡀⣿⣿] 5.243MB / 21.01MB Pulling                          1.6s
[+] Running 5/9tre [⣀⣿⣿] 6.291MB / 21.01MB Pulling                          1.7s
[+] Running 5/9tre [⣀⣿⣿]  7.34MB / 21.01MB Pulling                          1.8s                                                  ]
[+] Running 5/9tre [⣀⣿⣿] 8.389MB / 21.01MB Pulling                          1.9s
[+] Running 5/9tre [⣀⣿⣿] 9.437MB / 21.01MB Pulling                          2.0s [+] Running 5/9tre [⣀⣿⣿] 10.49MB / 21.01MB Pulling                          2.1s [+] Running 5/9tre [⣀⣿⣿] 11.53MB / 21.01MB P
ulling                    2.2s [+] Running 5/9tre [⣄⣿⣿] 12.58MB / 21.01MB Pulling                          2.3s [+] Running 5/9tre [⣄⣿⣿] 13.63MB / 21.01MB Pulling                          2.4s [+] Runn
ing 5/9tre [⣤⣿⣿] 14.68MB / 21.01MB Pulling                          2.5s [+] Running 5/9tre [⣤⣿⣿] 16.78MB / 21.01MB Pulling                          2.6s [+] Running 5/9tre [⣤⣿⣿] 17.83MB / 21.01MB Pulling
                   2.7s [+] Running 5/9tre [⣶⣿⣿] 18.87MB / 21.01MB Pulling                          2.8s [+] Running 5/9tre [⣶⣿⣿] 19.92MB / 21.01MB Pulling                          2.9s [+] Running 6/9t
re [⣶⣿⣿] 19.92MB / 21.01MB Pulling                          3.0s [+] Running 6/9tre [⣿⣿⣿] 19.92MB / 21.01MB Pulling                          3.1s [+] Running 6/9tre [⣿⣿⣿] 19.92MB / 21.01MB Pulling
               3.2s [+] Running 6/9tre [⣿⣿⣿] 19.92MB / 21.01MB Pulling                          3.3s [+] Running 6/9tre [⣿⣿⣿] 19.92MB / 21.01MB Pulling                          3.4s [+] Running 7/9tre [⣿⣿⣿]
 19.92MB / 21.01MB Pulling                          3.5s [+] Running 7/9tre Pulled                          3.5s [+] Running 7/9tre Pulled
      3.5s [+] Running 7/9tre Pulled                          3.5s [+] Running 7/9tre Pulled                          3.5s [+] Running 7/9tre Pulled
                          3.5s [+] Running 7/9tre Pulled                          3.5s [+] Running 8/9tre Pulled                          3
.5s [+] Running 8/9tre Pulled                          3.5s [+] Running 8/9tre Pulled                          3.5s [+] Running 8/9tre Pulled
                     3.5s [+] Running 8/9tre Pulled                          3.5s [+] Running 8/9tre Pulled                          3.5s [+]
Running 9/9tre Pulled                          3.5s  ✔ connector-mitre Pulled                          3.5s  ✔ 5142fa7a5875 Download complete
                 1.9s    ✔ 4f4fb700ef54 Already exists                          0.0s    ✔ 01ff8d403242 Download complete                          0.1s  ✔ connector
-virustotal-livehunt-notifications Pulled                   4.9s
   ✔ 4fd017f8ea7f Download complete                                      0.2s
   ✔ 032df650c177 Download complete                                      3.1s
   ✔ 6e7813bf77eb Download complete                                      0.2s
   ✔ 3d333d0da268 Download complete                                      0.2s
[+] Running 16/16
 ✔ Container docker-minio-1                                     Healthy 0.7s
 ✔ Container docker-elasticsearch-1                             Healthy 0.7s
 ✔ Container docker-redis-1                                     Healthy 0.7s
 ✔ Container docker-rabbitmq-1                                  Healthy 0.7s
 ✔ Container docker-opencti-1                                   Healthy 1.2s
 ✔ Container docker-connector-import-document-1                 Running 0.0s
 ✔ Container docker-connector-virustotal-livehunt-notifications-1  Started 1.5s
 ✔ Container docker-worker-1                                    Running 0.0s
 ✔ Container docker-worker-2                                    Running 0.0s
 ✔ Container docker-worker-3                                    Running 0.0s
 ✔ Container docker-connector-analysis-1                        Running 0.0s
 ✔ Container docker-connector-export-file-txt-1                 Running 0.0s
 ✔ Container docker-connector-export-file-stix-1                Running 0.0s
 ✔ Container docker-connector-mitre-1                           Started 1.5s
 ✔ Container docker-connector-import-file-stix-1                Running 0.0s
 ✔ Container docker-connector-export-file-csv-1                 Running 0.0s
sa31@Skills-Academy-31 docker % ▌
```



```
  connector-virustotal-livehunt-notifications:
    image: opencti/connector-virustotal-livehunt-notifications:6.4.10
    platform: linux/amd64
    environment:
      - OPENCTI_URL=http://10.138.16.210:8080
      - OPENCTI_TOKEN=92d8aad2-6998-46f9-8551-99f0dfa42118
      - CONNECTOR_ID=Virustotal_Livehunt_Notifications
      - "CONNECTOR_NAME=VirusTotal Livehunt Notifications"
      - CONNECTOR_SCOPE=StixFile,Indicator,Incident
      - CONNECTOR_LOG_LEVEL=error
      - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_API_KEY=081eec3a90c53c565f97c05ee40e7db60123f435c16944cc36d120b68e964156 # Private API Key
      - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_INTERVAL_SEC=300 # Time to wait in seconds between subsequent requests
      - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_CREATE_ALERT=True # Set to true to create alerts
      - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_EXTENSIONS='exe,dll' # (Optional) Comma separated filter to only download files matching these extensions
      - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_MIN_FILE_SIZE=1000 # (Optional) Don't download files smaller than this many bytes
      - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_MAX_FILE_SIZE=52428800 # (Optional) Don't download files larger than this many bytes
      - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_MAX_AGE_DAYS=3 # Only create the alert if the first submission of the file is not older than `max_age_days`
      - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_MIN_POSITIVES=5 # (Optional) Don't download files with less than this many vendors marking malicious
      - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_CREATE_FILE=True # Set to true to create file object linked to the alerts
      - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_UPLOAD_ARTIFACT=False # Set to true to upload the file to opencti
      - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_CREATE_YARA_RULE=True # Set to true to create yara rule linked to the alert and the file
      - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_DELETE_NOTIFICATION=False # Set to true to remove livehunt notifications
      - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_FILTER_WITH_TAG="mytag" # Filter livehunt notifications with this tag
    restart: always
    depends_on:
      opencti:
        condition: service_healthy

  connector-mitre:
    image: opencti/connector-mitre:6.4.10
    platform: linux/amd64
    environment:
      - OPENCTI_URL=http://10.138.16.210:8080
      - OPENCTI_TOKEN=92d8aad2-6998-46f9-8551-99f0dfa42118
      - CONNECTOR_ID=f4635141-0606-4530-8183-ba3c9e602d2a
      - "CONNECTOR_NAME=MITRE Datasets"
      - CONNECTOR_SCOPE=tool,report,malware,identity,campaign,intrusion-set,attack-pattern,course-of-action,x-mitre-data-source,x-mitre-data-component,x-mitre-matrix,x-mitre-
      - CONNECTOR_RUN_AND_TERMINATE=false
      - CONNECTOR_LOG_LEVEL=error
      - MITRE_REMOVE_STATEMENT_MARKING=true
      - MITRE_INTERVAL=7 # In days
    restart: always
    depends_on:
      opencti:
        condition: service_healthy
volumes:
  esdata:
  s3data:
  redisdata:
  amqpdata:
```



Workers statistics

3
CONNECTED WORKERS

26.35K
QUEUED BUNDLES

16.2/s
BUNDLES PROCESSED

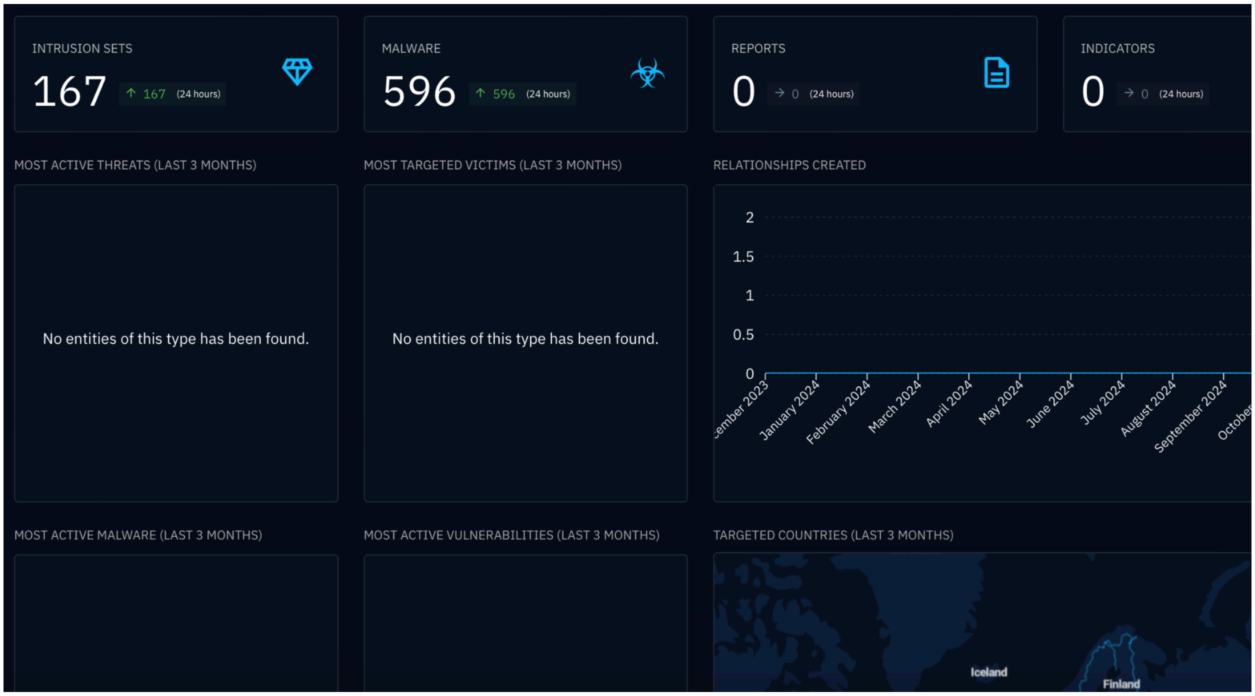
485.8/s
READ OPERATIONS

245.4/s
WRITE OPERATIONS

41.71K
TOTAL NUMBER OF DOCUMENTS

Registered connectors

#	NAME	TYPE	AUTOMATIC TRIGGER	MESSAGES	STATUS	MODIFIED
	ExportFileCsv	Files export	NOT APPLI...	0	ACTIVE	Jan 29, 2025 at 5:4...
	ExportFileStix2	Files export	NOT APPLI...	0	ACTIVE	Jan 29, 2025 at 5:4...
	ExportFileTxt	Files export	NOT APPLI...	0	ACTIVE	Jan 29, 2025 at 5:4...
	ImportDocument	Files import	AUTOMATIC	0	ACTIVE	Jan 29, 2025 at 5:4...
	ImportDocumentAnalysis	Analysis	NOT APPLI...	0	ACTIVE	Jan 29, 2025 at 5:4...
	ImportFileStix	Files import	AUTOMATIC	0	ACTIVE	Jan 29, 2025 at 5:4...
	MITRE Datasets	Data import	NOT APPLI...	26.35K	ACTIVE	Jan 29, 2025 at 5:4...



INTRUSION SETS
167 ↑ 167 (24 hours)

MALWARE
596 ↑ 596 (24 hours)

REPORTS
0 → 0 (24 hours)

INDICATORS
0 → 0 (24 hours)

MOST ACTIVE THREATS (LAST 3 MONTHS)

No entities of this type has been found.

MOST TARGETED VICTIMS (LAST 3 MONTHS)

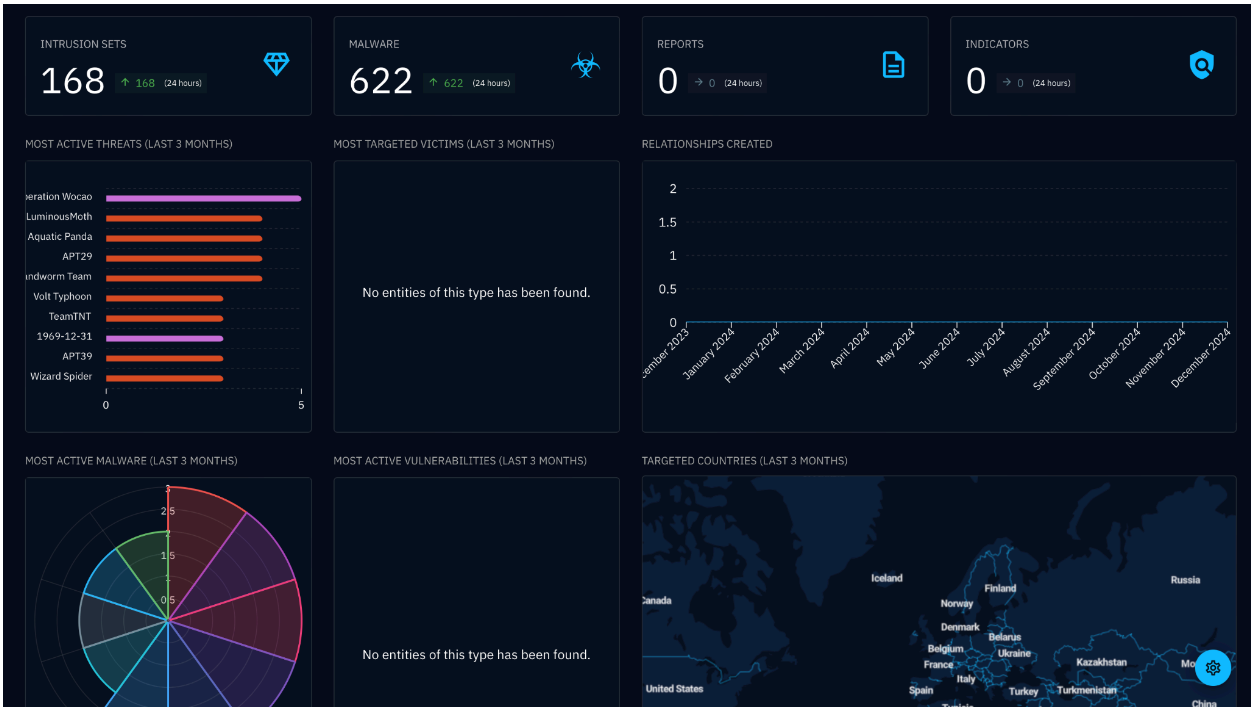
No entities of this type has been found.

RELATIONSHIPS CREATED

MOST ACTIVE MALWARE (LAST 3 MONTHS)

MOST ACTIVE VULNERABILITIES (LAST 3 MONTHS)

TARGETED COUNTRIES (LAST 3 MONTHS)



INTRUSION SETS
168 ↑ 168 (24 hours)

MALWARE
622 ↑ 622 (24 hours)

REPORTS
0 → 0 (24 hours)

INDICATORS
0 → 0 (24 hours)

MOST ACTIVE THREATS (LAST 3 MONTHS)

MOST TARGETED VICTIMS (LAST 3 MONTHS)

No entities of this type has been found.

RELATIONSHIPS CREATED

MOST ACTIVE MALWARE (LAST 3 MONTHS)

MOST ACTIVE VULNERABILITIES (LAST 3 MONTHS)

No entities of this type has been found.

TARGETED COUNTRIES (LAST 3 MONTHS)