

docker-compose.yml

docke-compose.yml

```
1 services:
2   redis:
3     image: redis:7.4.2
4     restart: always
5     volumes:
6       - redisdata:/data
7     healthcheck:
8       test: ["CMD", "redis-cli", "ping"]
9       interval: 10s
10      timeout: 5s
11      retries: 3
12   elasticsearch:
13     image: docker.elastic.co/elasticsearch/elasticsearch:8.18.0
14     volumes:
15       - esdata:/usr/share/elasticsearch/data
16     environment:
17       # Comment-out the line below for a cluster of multiple nodes
18       - discovery.type=single-node
19     # Uncomment the line below below for a cluster of multiple nodes
20     # - cluster.name=docker-cluster
21     - xpack.ml.enabled=false
22     - xpack.security.enabled=false
23     - thread_pool.search.queue_size=5000
24     - logger.org.elasticsearch.discovery="ERROR"
25     - "ES_JAVA_OPTS=-Xms${ELASTIC_MEMORY_SIZE} -Xmx${ELASTIC_MEMORY_SIZE}"
26   restart: always
27   ulimits:
28     memlock:
29       soft: -1
30       hard: -1
31    nofile:
32       soft: 65536
33       hard: 65536
34   healthcheck:
35     test: curl -s http://elasticsearch:9200 >/dev/null || exit 1
36     interval: 30s
37     timeout: 10s
38     retries: 50
39   minio:
40     image: minio/minio:RELEASE.2024-05-28T17-19-04Z # Use "minio/minio:RELEASE.2024-05-28T17-19-04Z-cpuv1" to troubleshoot compatibility issues with CPU
41     volumes:
42       - s3data:/data
43     ports:
44       - "9000:9000"
45     environment:
46       MINIO_ROOT_USER: ${MINIO_ROOT_USER}
47       MINIO_ROOT_PASSWORD: ${MINIO_ROOT_PASSWORD}
48     command: server /data
49     restart: always
```

Line 263, Column 35

master ①

Spaces: 2

YAML



docker-compose.yml

```
49      restart: always
50      healthcheck:
51          test: ["CMD", "mc", "ready", "local"]
52          interval: 10s
53          timeout: 5s
54          retries: 3
55      rabbitmq:
56          image: rabbitmq:4.1-management
57          environment:
58              - RABBITMQ_DEFAULT_USER=${RABBITMQ_DEFAULT_USER}
59              - RABBITMQ_DEFAULT_PASS=${RABBITMQ_DEFAULT_PASS}
60              - RABBITMQ_NODENAME=rabbit01@localhost
61          volumes:
62              - type: bind
63                  source: ./rabbitmq.conf
64                  target: /etc/rabbitmq/rabbitmq.conf
65              - amqpdata:/var/lib/rabbitmq
66          restart: always
67          healthcheck:
68              test: rabbitmq-diagnostics -q ping
69              interval: 30s
70              timeout: 30s
71              retries: 3
72      opencti:
73          image: opencti/platform:6.6.6
74          environment:
75              - NODE_OPTIONS=--max-old-space-size=8096
76              - APP__PORT=8080
77              - APP__BASE_URL=${OPENCTI_BASE_URL}
78              - APP__ADMIN__EMAIL=${OPENCTI_ADMIN_EMAIL}
79              - APP__ADMIN__PASSWORD=${OPENCTI_ADMIN_PASSWORD}
80              - APP__ADMIN__TOKEN=${OPENCTI_ADMIN_TOKEN}
81              - APP__APP_LOGS__LOGS_LEVEL=error
82              - REDIS__HOSTNAME=redis
83              - REDIS__PORT=6379
84              - ELASTICSEARCH__URL=http://elasticsearch:9200
85              - ELASTICSEARCH__NUMBER_OF_REPLICAS=0
86              - MINIO__ENDPOINT=minio
87              - MINIO__PORT=9000
88              - MINIO__USE_SSL=false
89              - MINIO__ACCESS_KEY=${MINIO_ROOT_USER}
90              - MINIO__SECRET_KEY=${MINIO_ROOT_PASSWORD}
91              - RABBITMQ__HOSTNAME=rabbitmq
92              - RABBITMQ__PORT=5672
93              - RABBITMQ__PORT_MANAGEMENT=15672
94              - RABBITMQ__MANAGEMENT_SSL=false
95              - RABBITMQ__USERNAME=${RABBITMQ_DEFAULT_USER}
96              - RABBITMQ__PASSWORD=${RABBITMQ_DEFAULT_PASS}
97              - SMTP__HOSTNAME=${SMTP_HOSTNAME}
```



docker-compose.yml

UNREGISTERED

docke-compose.yml

```
98      - SMTP__PORT=25
99      - PROVIDERS__LOCAL__STRATEGY=LocalStrategy
100     - APP__HEALTH_ACCESS_KEY=${OPENCTI_HEALTHCHECK_ACCESS_KEY}
101 ports:
102   - "8080:8080"
103 depends_on:
104   redis:
105     condition: service_healthy
106   elasticsearch:
107     condition: service_healthy
108   minio:
109     condition: service_healthy
110   rabbitmq:
111     condition: service_healthy
112 restart: always
113 healthcheck:
114   test: ["CMD", "wget", "-q0-", "http://opencti:8080/health?health_access_key=${OPENCTI_HEALTHCHECK_ACCESS_KEY}"]
115   interval: 10s
116   timeout: 5s
117   retries: 20
118 worker:
119   image: opencti/worker:6.6.6
120   environment:
121     - OPENCTI_URL=http://opencti:8080
122     - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
123     - WORKER_LOG_LEVEL=info
124   depends_on:
125     opencti:
126       condition: service_healthy
127 deploy:
128   mode: replicated
129   replicas: 3
130   restart: always
131 connector-export-file-stix:
132   image: opencti/connector-export-file-stix:6.6.6
133   environment:
134     - OPENCTI_URL=http://opencti:8080
135     - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
136     - CONNECTOR_ID=${CONNECTOR_EXPORT_FILE_STIX_ID} # Valid UUIDv4
137     - CONNECTOR_TYPE=INTERNAL_EXPORT_FILE
138     - CONNECTOR_NAME=ExportFileStix2
139     - CONNECTOR_SCOPE=application/json
140     - CONNECTOR_LOG_LEVEL=info
141   restart: always
142   depends_on:
143     opencti:
144       condition: service_healthy
145 connector-export-file-csv:
146   image: opencti/connector-export-file-csv:6.6.6
```

Line 146, Column 35

master ①

Spaces: 2

YAML



docker-compose.yml

docker-compose.yml

```
146     image: opencti/connector-export-file-csv:6.6.6
147     environment:
148       - OPENCTI_URL=http://opencti:8080
149       - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
150       - CONNECTOR_ID=${CONNECTOR_EXPORT_FILE_CSV_ID} # Valid UUIDv4
151       - CONNECTOR_TYPE=INTERNAL_EXPORT_FILE
152       - CONNECTOR_NAME=ExportFileCsv
153       - CONNECTOR_SCOPE=text/csv
154       - CONNECTOR_LOG_LEVEL=info
155     restart: always
156     depends_on:
157       opencti:
158         condition: service_healthy
159   connector-export-file-txt:
160     image: opencti/connector-export-file-txt:6.6.6
161     environment:
162       - OPENCTI_URL=http://opencti:8080
163       - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
164       - CONNECTOR_ID=${CONNECTOR_EXPORT_FILE_TXT_ID} # Valid UUIDv4
165       - CONNECTOR_TYPE=INTERNAL_EXPORT_FILE
166       - CONNECTOR_NAME=ExportFileTxt
167       - CONNECTOR_SCOPE=text/plain
168       - CONNECTOR_LOG_LEVEL=info
169     restart: always
170     depends_on:
171       opencti:
172         condition: service_healthy
173   connector-import-file-stix:
174     image: opencti/connector-import-file-stix:6.6.6
175     environment:
176       - OPENCTI_URL=http://opencti:8080
177       - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
178       - CONNECTOR_ID=${CONNECTOR_IMPORT_FILE_STIX_ID} # Valid UUIDv4
179       - CONNECTOR_TYPE=INTERNAL_IMPORT_FILE
180       - CONNECTOR_NAME=ImportFileStix
181       - CONNECTOR_VALIDATE_BEFORE_IMPORT=true # Validate any bundle before import
182       - CONNECTOR_SCOPE=application/json,text/xml
183       - CONNECTOR_AUTO=true # Enable/disable auto-import of file
184       - CONNECTOR_LOG_LEVEL=info
185     restart: always
186     depends_on:
187       opencti:
188         condition: service_healthy
189   connector-import-document:
190     image: opencti/connector-import-document:6.6.6
191     environment:
192       - OPENCTI_URL=http://opencti:8080
193       - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
194       - CONNECTOR_ID=${CONNECTOR_IMPORT_DOCUMENT_ID} # Valid UUIDv4
```

Line 194, Column 35

master ①

Spaces: 2

YAML



docker-compose.yml

docke-compose.yml

```
193     - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
194     - CONNECTOR_ID=${CONNECTOR_IMPORT_DOCUMENT_ID} # Valid UUIDv4
195     - CONNECTOR_TYPE=INTERNAL_IMPORT_FILE
196     - CONNECTOR_NAME=ImportDocument
197     - CONNECTOR_VALIDATE_BEFORE_IMPORT=true # Validate any bundle before import
198     - CONNECTOR_SCOPE=application/pdf,text/plain,text/html
199     - CONNECTOR_AUTO=true # Enable/disable auto-import of file
200     - CONNECTOR_ONLY_CONTEXTUAL=false # Only extract data related to an entity (a report, a threat actor, etc.)
201     - CONNECTOR_CONFIDENCE_LEVEL=15 # From 0 (Unknown) to 100 (Fully trusted)
202     - CONNECTOR_LOG_LEVEL=info
203     - IMPORT_DOCUMENT_CREATE_INDICATOR=true
204   restart: always
205   depends_on:
206     - opencti:
207       condition: service_healthy
208   connector-analysis:
209     image: opencti/connector-import-document:6.6.6
210     environment:
211       - OPENCTI_URL=http://opencti:8080
212       - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
213       - CONNECTOR_ID=${CONNECTOR_ANALYSIS_ID} # Valid UUIDv4
214       - CONNECTOR_TYPE=INTERNAL_ANALYSIS
215       - CONNECTOR_NAME=ImportDocumentAnalysis
216       - CONNECTOR_VALIDATE_BEFORE_IMPORT=false # Validate any bundle before import
217       - CONNECTOR_SCOPE=application/pdf,text/plain,text/html
218       - CONNECTOR_AUTO=true # Enable/disable auto-import of file
219       - CONNECTOR_ONLY_CONTEXTUAL=false # Only extract data related to an entity (a report, a threat actor, etc.)
220       - CONNECTOR_CONFIDENCE_LEVEL=15 # From 0 (Unknown) to 100 (Fully trusted)
221       - CONNECTOR_LOG_LEVEL=info
222   restart: always
223   depends_on:
224     - opencti:
225       condition: service_healthy
226   connector-cisa-known-exploited-vulnerabilities:
227     image: opencti/connector-cisa-known-exploited-vulnerabilities:6.6.7
228     environment:
229       - OPENCTI_URL=http://localhost
230       - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
231       - CONNECTOR_ID=${CONNECTOR_ANALYSIS_ID}
232       - "CONNECTOR_NAME=CISA Known Exploited Vulnerabilities"
233       - CONNECTOR_SCOPE=cisa
234       - CONNECTOR_RUN_AND_TERMINATE=false
235       - CONNECTOR_LOG_LEVEL=error
236       - CONNECTOR_DURATION_PERIOD=P2D
237       - CISA_CATALOG_URL=https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json
238       - CISA_CREATE_INFRASTRUCTURES=false
239       - CISA_TLP=TLP:CLEAR
240   restart: always
241   depends_on:
```

Line 241, Column 16

master ①

Spaces: 2

YAML



docker-compose.yml

```
222     restart: always
223     depends_on:
224       - opencti:
225         condition: service_healthy
226   connector-cisa-known-exploited-vulnerabilities:
227     image: opencti/connector-cisa-known-exploited-vulnerabilities:6.6.7
228     environment:
229       - OPENCTI_URL=http://localhost
230       - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
231       - CONNECTOR_ID=${CONNECTOR_ANALYSIS_ID}
232       - "CONNECTOR_NAME=CISA Known Exploited Vulnerabilities"
233       - CONNECTOR_SCOPE=cisa
234       - CONNECTOR_RUN_AND_TERMINATE=false
235       - CONNECTOR_LOG_LEVEL=error
236       - CONNECTOR_DURATION_PERIOD=P2D
237       - CISA_CATALOG_URL=https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json
238       - CISA_CREATE_INFRASTRUCTURES=false
239       - CISA_TLP=TLP:CLEAR
240   restart: always
241   depends_on:
242     - opencti:
243       condition: service_healthy
244   connector-opencti:
245     image: opencti/connector-opencti:6.6.7
246     environment:
247       - OPENCTI_URL=http://localhost
248       - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
249       - CONNECTOR_ID=${CONNECTOR_ANALYSIS_ID}
250       - "CONNECTOR_NAME=OpenCTI Datasets"
251       - CONNECTOR_SCOPE=marking-definition,identity,location
252       - CONNECTOR_UPDATE_EXISTING_DATA=true
253       - CONNECTOR_RUN_AND_TERMINATE=false
254       - CONNECTOR_LOG_LEVEL=error
255       - CONFIG_SECTORS_FILE_URL=https://raw.githubusercontent.com/OpenCTI-Platform/datasets/master/data/sectors.json
256       - CONFIG_GEOGRAPHY_FILE_URL=https://raw.githubusercontent.com/OpenCTI-Platform/datasets/master/data/geography.json
257       - CONFIG_COMPANIES_FILE_URL=https://raw.githubusercontent.com/OpenCTI-Platform/datasets/master/data/companies.json
258       - CONFIG_REMOVE_CREATOR=false
259       - CONFIG_INTERVAL=7 # In days
260   restart: always
261   depends_on:
262     - opencti:
263       condition: service_healthy
264   volumes:
265     esdata:
266     s3data:
267     redisdata:
268     amqpdata:
269
270
```

Search the platform...

INTRUSION SETS 0 → 0 (24 hours)

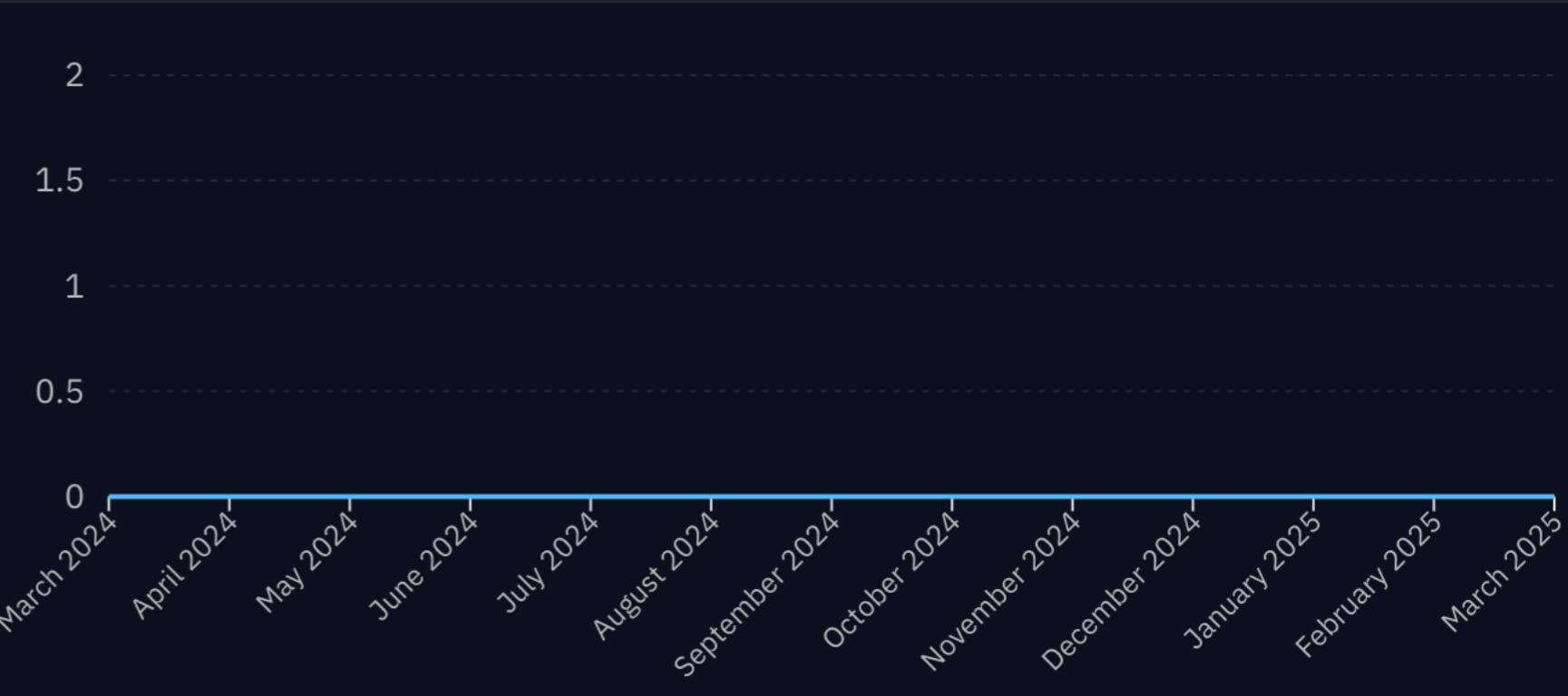
MALWARE 0 → 0 (24 hours)

REPORTS 0 → 0 (24 hours)

INDICATORS 0 → 0 (24 hours)

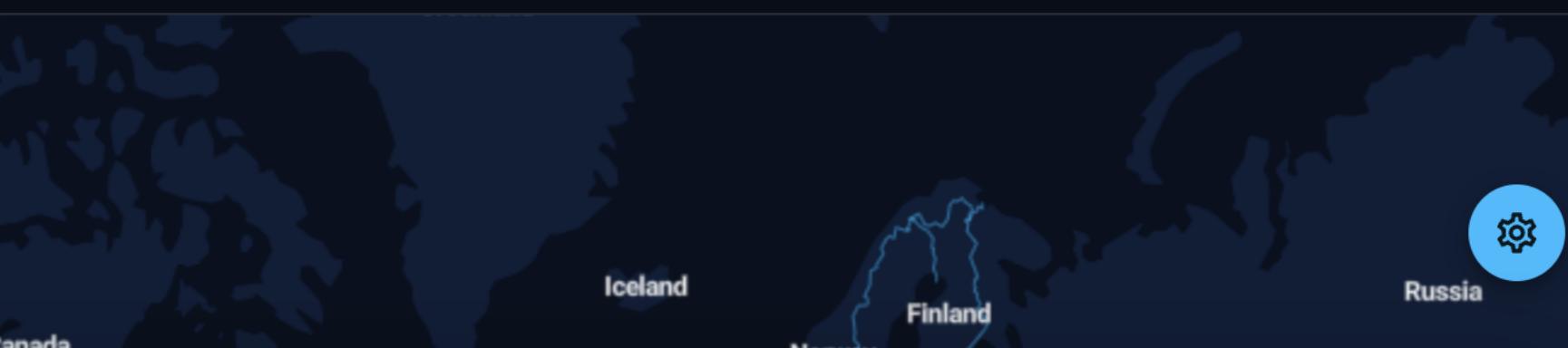
MOST ACTIVE THREATS (LAST 3 MONTHS)
No data has been found.

MOST TARGETED VICTIMS (LAST 3 MONTHS)
No data has been found.

RELATIONSHIPS CREATED


MOST ACTIVE MALWARE (LAST 3 MONTHS)

MOST ACTIVE VULNERABILITIES (LAST 3 MONTHS)

TARGETED COUNTRIES (LAST 3 MONTHS)


Search the platform...

LATEST REPORTS

No data has been found.

MOST ACTIVE LABELS (LAST 3 MONTHS)

No data has been found.

The dashboard features a dark blue header with a search bar and a sidebar on the left containing various icons. A large map of South America and Oceania is displayed at the top right. Below the map, two sections are labeled 'LATEST REPORTS' and 'MOST ACTIVE LABELS (LAST 3 MONTHS)', both of which currently show 'No data has been found.'