```yaml
services:
  redis:
    image: redis:7.4.2
    restart: always
    volumes:
      - redisdata:/data
    healthcheck:
      test: ["CMD", "redis-cli", "ping"]
      interval: 10s
      timeout: 5s
      retries: 3
  elasticsearch:
    image: docker.elastic.co/elasticsearch/elasticsearch:8.18.0
    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
    healthcheck:
      test: curl -s http://elasticsearch:9200 >/dev/null || exit 1
      interval: 30s
      timeout: 10s
      retries: 50
  minio:
    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
    volumes:
      - s3data:/data
    ports:
      - "9000:9000"
    environment:
      MINIO_ROOT_USER: ${MINIO_ROOT_USER}
      MINIO_ROOT_PASSWORD: ${MINIO_ROOT_PASSWORD}
    command: server /data
    restart: always
```

```
    restart: always
    healthcheck:
      test: ["CMD", "mc", "ready", "local"]
      interval: 10s
      timeout: 5s
      retries: 3
  rabbitmq:
    image: rabbitmq:4.1-management
    environment:
      - RABBITMQ_DEFAULT_USER=${RABBITMQ_DEFAULT_USER}
      - RABBITMQ_DEFAULT_PASS=${RABBITMQ_DEFAULT_PASS}
      - RABBITMQ_NODENAME=rabbit01@localhost
    volumes:
      - type: bind
        source: ./rabbitmq.conf
        target: /etc/rabbitmq/rabbitmq.conf
      - amqpdata:/var/lib/rabbitmq
    restart: always
    healthcheck:
      test: rabbitmq-diagnostics -q ping
      interval: 30s
      timeout: 30s
      retries: 3
  opencti:
    image: opencti/platform:6.6.6
    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
      - ELASTICSEARCH__NUMBER_OF_REPLICAS=0
      - 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
      - APP__HEALTH_ACCESS_KEY=${OPENCTI_HEALTHCHECK_ACCESS_KEY}
    ports:
      - "8080:8080"
    depends_on:
      redis:
        condition: service_healthy
      elasticsearch:
        condition: service_healthy
      minio:
        condition: service_healthy
      rabbitmq:
        condition: service_healthy
    restart: always
    healthcheck:
      test:  ["CMD", "wget", "-qO-", "http://opencti:8080/health?health_access_key=${OPENCTI_HEALTHCHECK_ACCESS_KEY}"]
      interval: 10s
      timeout: 5s
      retries: 20
  worker:
    image: opencti/worker:6.6.6
    environment:
      - OPENCTI_URL=http://opencti:8080
      - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
      - WORKER_LOG_LEVEL=info
    depends_on:
      opencti:
        condition: service_healthy
    deploy:
      mode: replicated
      replicas: 3
    restart: always
  connector-export-file-stix:
    image: opencti/connector-export-file-stix:6.6.6
    environment:
      - OPENCTI_URL=http://opencti:8080
      - OPENCTI_TOKEN=${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:
        condition: service_healthy
  connector-export-file-csv:
    image: opencti/connector-export-file-csv:6.6.6
```

```
    image: opencti/connector-export-file-csv:6.6.6
    environment:
      - OPENCTI_URL=http://opencti:8080
      - 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:
        condition: service_healthy
  connector-export-file-txt:
    image: opencti/connector-export-file-txt:6.6.6
    environment:
      - OPENCTI_URL=http://opencti:8080
      - 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:
        condition: service_healthy
  connector-import-file-stix:
    image: opencti/connector-import-file-stix:6.6.6
    environment:
      - OPENCTI_URL=http://opencti:8080
      - 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 import
      - CONNECTOR_SCOPE=application/json,text/xml
      - CONNECTOR_AUTO=true # Enable/disable auto-import of file
      - CONNECTOR_LOG_LEVEL=info
    restart: always
    depends_on:
      opencti:
        condition: service_healthy
  connector-import-document:
    image: opencti/connector-import-document:6.6.6
    environment:
      - OPENCTI_URL=http://opencti:8080
      - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
      - CONNECTOR_ID=${CONNECTOR_IMPORT_DOCUMENT_ID} # Valid UUIDv4
```

```
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:
```

```
      restart: always
      depends_on:
        opencti:
          condition: service_healthy
    connector-cisa-known-exploited-vulnerabilities:
      image: opencti/connector-cisa-known-exploited-vulnerabilities:6.6.7
      environment:
        - OPENCTI_URL=http://localhost
        - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
        - CONNECTOR_ID=${CONNECTOR_ANALYSIS_ID}
        - "CONNECTOR_NAME=CISA Known Exploited Vulnerabilities"
        - CONNECTOR_SCOPE=cisa
        - CONNECTOR_RUN_AND_TERMINATE=false
        - CONNECTOR_LOG_LEVEL=error
        - CONNECTOR_DURATION_PERIOD=P2D
        - CISA_CATALOG_URL=https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json
        - CISA_CREATE_INFRASTRUCTURES=false
        - CISA_TLP=TLP:CLEAR
      restart: always
      depends_on:
        opencti:
          condition: service_healthy
  connector-opencti:
      image: opencti/connector-opencti:6.6.7
      environment:
        - OPENCTI_URL=http://localhost
        - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
        - CONNECTOR_ID=${CONNECTOR_ANALYSIS_ID}
        - "CONNECTOR_NAME=OpenCTI Datasets"
        - CONNECTOR_SCOPE=marking-definition,identity,location
        - CONNECTOR_UPDATE_EXISTING_DATA=true
        - CONNECTOR_RUN_AND_TERMINATE=false
        - CONNECTOR_LOG_LEVEL=error
        - CONFIG_SECTORS_FILE_URL=https://raw.githubusercontent.com/OpenCTI-Platform/datasets/master/data/sectors.json
        - CONFIG_GEOGRAPHY_FILE_URL=https://raw.githubusercontent.com/OpenCTI-Platform/datasets/master/data/geography.json
        - CONFIG_COMPANIES_FILE_URL=https://raw.githubusercontent.com/OpenCTI-Platform/datasets/master/data/companies.json
        - CONFIG_REMOVE_CREATOR=false
        - CONFIG_INTERVAL=7 # In days
      restart: always
       depends_on:
        opencti:
          condition: service_healthy
  volumes:
    esdata:
    s3data:
    redisdata:
    amqpdata:
```

Search the platform...

INTRUSION SETS
0 → 0 (24 hours)

MALWARE
0 → 0 (24 hours)

REPORTS
0 → 0 (24 hours)

INDICATORS
0 → 0 (24 hours)

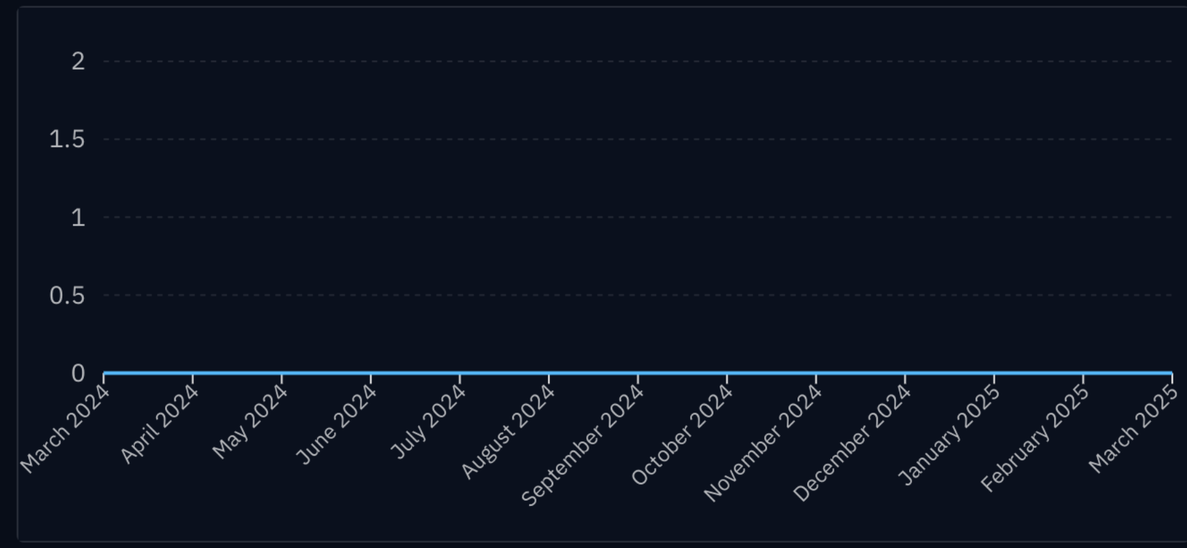
MOST ACTIVE THREATS (LAST 3 MONTHS)

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)

Chrome File Edit View History Bookmarks Profiles Tab Window Help

Wed Apr 23 1:42 PM

Courses | S | GitHub | Docker: Acc | OpenCTI Ec | connectors/ | connectors/ | Online UUID | Dashboard | Thank You

localhost:8080/dashboard

New Chrome available

Search the platform...

LATEST REPORTS

No data has been found.

MOST ACTIVE LABELS (LAST 3 MONTHS)

No data has been found.