

A screenshot of a Mac desktop showing a terminal window and a Docker Compose interface. The terminal window is titled 'docker-compose.yml' and displays the configuration file for the 'openciti' service. The Docker Compose interface shows the service status as 'Up 6 days' and provides a detailed log view. The desktop background is a green landscape, and the Dock at the bottom shows various application icons.

```
version: '3.8'
services:
  openciti:
    image: openciti/connecter-openciti:6.6.7
    environment:
      - OPENCTI_URL=http://localhost
      - 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 import
      - 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 (a report, a threat actor, etc)
      - CONNECTOR_CONFIDENCE_LEVEL=15 # From 0 (Unknown) to 100 (Fully trusted)
      - CONNECTOR_LOG_LEVEL=info
    restart: always
    depends_on:
      - openciti
    condition: service_healthy
  connector-openciti:
    image: openciti/connecter-openciti:6.6.7
    environment:
      - OPENCTI_URL=https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json
      - CISA_CREATE_INFRASTRUCTURES=false
      - CISA_TLP=TP:CLEAR
    restart: always
    depends_on:
      - openciti
    condition: service_healthy
  volumes:
    esdata:
    s3data:
    redisdata:
    amqpdata:
```

A screenshot of a Mac desktop showing a terminal window and a Docker Compose interface. The terminal window is titled 'docker-compose.yml' and displays the configuration file for the 'openciti' service. The Docker Compose interface shows the service status as 'Up 6 days' and provides a detailed log view. The desktop background is a green landscape, and the Dock at the bottom shows various application icons.

```
version: '3.8'
services:
  openciti:
    image: openciti/connecter-import-document:6.6.6
    environment:
      - OPENCTI_URL=http://openciti:8080
      - 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 import
      - 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 (a report, a threat actor, etc)
      - CONNECTOR_CONFIDENCE_LEVEL=15 # From 0 (Unknown) to 100 (Fully trusted)
      - CONNECTOR_LOG_LEVEL=info
    restart: always
    depends_on:
      - openciti
    condition: service_healthy
  connector-analysis:
    image: openciti/connecter-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=TP:CLEAR
    restart: always
    depends_on:
      - openciti
    condition: service_healthy
  connector-cisa-known-exploited-vulnerabilities:
```

The screenshot shows a macOS desktop environment. At the top is the Dock with various application icons. The main window is a browser displaying a Notion site with a URL of `filigran.notion.site`. A message at the top of the browser window reads: "Restricted Mode is intended for safe code browsing. Trust this window to enable all features." Below this is a "Manage" and "Learn More" link. The browser's sidebar shows a tree structure of the Notion site's content. The main content area of the browser displays a `docker-compose.yml` file. The terminal window to the right shows the output of a Docker container, with the logs for the `minio-1` service. The logs include various system and application messages, with some lines colored in red and green. The status bar at the bottom shows "Ln 263, Col 35" and "UTF-8".

```
version: '3.8'
services:
  openceti:
    restart: always
    depends_on:
      - openceti
    environment:
      - OPENCTI_URL=http://openceti:8080
      - 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 import
      - 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 (a report, a threat actor, etc)
      - CONNECTOR_CONFIDENCE_LEVEL=15 # From 0 (Unknown) to 100 (Fully trusted)
      - IMPORT_DOCUMENT_CREATE_INDICATOR=true
    restart: always
    depends_on:
      - openceti
    environment:
      - OPENCTI_URL=http://openceti:8080
      - 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 import
      - CONNECTOR_SCOPE=application/pdf,text/plain,text/html
      - CONNECTOR_AUTO=true # Enable/disable auto-import of file
  minio-1:
    image: minio/minio:RELEASE.2023-07-10T14-00-00Z
    environment:
      - MINIO_ROOT_USER=minio
      - MINIO_ROOT_PASSWORD=minio123
      - MINIO_ACCESS_KEY=minio
      - MINIO_SECRET_KEY=minio123
      - MINIO_BROWSER_REDIRECT_URL=http://openceti:8080
    ports:
      - 9000:9000
    volumes:
      - ./data:/data
    restart: unless-stopped
```

The screenshot shows a dark-themed web application interface. The top navigation bar includes 'Safari', 'File', 'Edit', 'View', 'History', 'Bookmarks', 'Window', and 'Help'. The address bar shows 'localhost'. The left sidebar contains a 'Favorites' section with icons for Mail, Chat, Data, and more, and a 'Locations' section with icons for iCloud, Dock, and Tags (Red, Orange, Yellow, Green). The main content area displays various threat intelligence metrics and charts. Key sections include:

- INTRUSION SETS:** 0 (24 hours)
- MALWARE:** 0 (24 hours)
- REPORTS:** 0 (24 hours)
- INDICATORS:** 0 (24 hours)

Below these are two charts:

- MOST ACTIVE THREATS (LAST 3 MONTHS):** No data has been found.
- MOST TARGETED VICTIMS (LAST 3 MONTHS):** No data has been found.

A line chart titled "RELATIONSHIPS CREATED" shows data from March 2024 to April 2024, with values ranging from 0 to 2. A map titled "TARGETED COUNTRIES (LAST 3 MONTHS)" shows activity in Europe, with a callout for Finland.