docker-compose.yml

```yaml
    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:
```

```yaml
    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
      - 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)
      - CONNECTOR_LOG_LEVEL=info
      - IMPORT_DOCUMENT_CREATE_INDICATOR=true
    restart: always
    depends_on:
      opencti:
        condition: service_healthy
  connector-analysis:
    image: opencti/connector-import-document:6.6.6
    environment:
      - OPENCTI_URL=http://opencti: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:
      opencti:
        condition: service_healthy
  connector-cisa-known-exploited-vulnerabilities:
    image: opencti/connector-cisa-known-exploited-vulnerabilities:6.6.7
    environment:
      - OPENCTI_URL=http://localhost
```