

```

223     depends_on:
224       opentti:
225         condition: service_healthy
226 connector-cisa-known-exploited-vulnerabilities:
227   image: opentti/connector-cisa-known-exploited-vulnerabilities:6.6.7
228   environment:
229     - OPENTTI_URL=http://localhost
230     - OPENTTI_TOKEN=${OPENTTI_ADMIN_TOKEN}
231     - CONNECTOR_ID=${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     opentti:
243       condition: service_healthy
244 connector-opentti:
245   image: opentti/connector-opentti:6.6.7
246   environment:
247     - OPENTTI_URL=http://localhost
248     - OPENTTI_TOKEN=${OPENTTI_ADMIN_TOKEN}
249     - CONNECTOR_ID=${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     opentti:
263       condition: service_healthy
264 volumes:
265   esdata:
266   s3data:
267   redisdata:
268   amqpdata:
269
270
186   depends_on:
187     opentti:
188       condition: service_healthy
189 connector-import-document:
190   image: opentti/connector-import-document:6.6.6
191   environment:
192     - OPENTTI_URL=http://opentti:8080
193     - OPENTTI_TOKEN=${OPENTTI_ADMIN_TOKEN}
194     - CONNECTOR_ID=${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     opentti:
207       condition: service_healthy
208 connector-analysis:
209   image: opentti/connector-import-document:6.6.6
210   environment:
211     - OPENTTI_URL=http://opentti:8080
212     - OPENTTI_TOKEN=${OPENTTI_ADMIN_TOKEN}
213     - CONNECTOR_ID=${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     opentti:
225       condition: service_healthy
226 connector-cisa-known-exploited-vulnerabilities:
227   image: opentti/connector-cisa-known-exploited-vulnerabilities:6.6.7
228   environment:
229     - OPENTTI_URL=http://localhost

```



