Configurazione dei Connettori OpenCTI per MITRE ATT&CK, CERT-FR, MISP, STIX2

Requisiti

- OpenCTI installato tramite docker-compose
- File .env già configurato correttamente
- Docker in esecuzione
- Connettori da aggiungere al file docker-compose.yml nella directory opencti-docker

---

Passaggi Operativi

1. Posizionarsi nella directory di installazione

cd ~/opencti-docker

2. Aprire il file docker-compose.yml

sudo nano docker-compose.yml

3. Aggiungere i seguenti blocchi services: nel file YAML

I blocchi vanno aggiunti sotto gli altri connettori esistenti (es. sotto connector-analysis).

3.1 Connettore MITRE ATT&CK

```
 connector-import-mitre:
    image: opencti/connector-import-mitre:6.7.1
    environment:
      - OPENCTI_URL=http://opencti:8080
      - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
      - CONNECTOR_ID=mitre-connector
      - CONNECTOR_NAME=MITRE ATT&CK
      -
CONNECTOR_SCOPE=identity,attack-pattern,course-of-action,intrusion-set,malware,tool
      - CONNECTOR_AUTO=true
      - CONNECTOR_LOG_LEVEL=info
```

```
  restart: always
  depends_on:
    - opencti
```

3.2 Connettore CERT-FR

```
connector-import-certfr:
  image: opencti/connector-import-certfr:6.7.1
  environment:
    - OPENCTI_URL=http://opencti:8080
    - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
    - CONNECTOR_ID=certfr-connector
    - CONNECTOR_NAME=CERT-FR
    - CONNECTOR_SCOPE=report
    - CONNECTOR_AUTO=true
    - CONNECTOR_LOG_LEVEL=info
  restart: always
  depends_on:
    - opencti
```

3.3 Connettore MISP Feed pubblico

```
connector-import-misp-feed:
  image: opencti/connector-import-misp-feed:6.7.1
  environment:
    - OPENCTI_URL=http://opencti:8080
    - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
    - CONNECTOR_ID=misp-feed-connector
    - CONNECTOR_NAME=MISP Feed
    - CONNECTOR_SCOPE=indicator,malware,threat-actor,tool
    - CONNECTOR_AUTO=true
    - CONNECTOR_LOG_LEVEL=info
  restart: always
  depends_on:
    - opencti
```

3.4 Connettore STIX2 Importer

```
connector-import-stix2:
  image: opencti/connector-import-stix2:6.7.1
  environment:
    - OPENCTI_URL=http://opencti:8080
    - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
    - CONNECTOR_ID=stix2-importer
    - CONNECTOR_NAME=STIX2 Importer
    - CONNECTOR_SCOPE=application/json
```

```
  - CONNECTOR_AUTO=true
  - CONNECTOR_LOG_LEVEL=info
restart: always
depends_on:
  - opencti
```

---

4. Salvare ed uscire da nano

- Premi CTRL+O, poi Invio per salvare
- Premi CTRL+X per uscire

---

5. Riavviare l’ambiente Docker

Per applicare i nuovi connettori:

```
docker-compose down
docker-compose up -d
```

Verifica da Interfaccia Web

1. Accedi a OpenCTI via browser: http://<IP-Server>:8080
2. Vai su: Data ingestion > Connectors
3. Controlla che i nuovi connettori siano in stato “Running”
4. Avvia manualmente l’importazione se necessario (cliccando sui tre puntini > “Run now”)

Note Finali

- Questi connettori si aggiornano automaticamente.
- Non richiedono API key.
- Utilizzano feed pubblici validati e affidabili, mantenuti da enti governativi e comunità di sicurezza.