MuleSoft Audit Integration with Sentinel:

**Overview of the Flow**

* Extract MuleSoft audit logs using Python
* Save logs to .txt files locally
* Configure rsyslog to read these files
* Forward logs to Sentinel via Syslog (using a Linux VM or agent)
* Verify ingestion in Sentinel

**Step 1: Extract MuleSoft Audit Logs with Python**

You’ll need a Python script that:

* Connects to MuleSoft (via API or file system)
* Extracts audit logs
* Saves them to .txt files periodically

**Below is the python Script:**

import requests

import time

def fetch\_mulesoft\_logs():

    url = "https://your-mulesoft-api-endpoint"

    headers = {"Authorization": "Bearer YOUR\_TOKEN"}

       response = requests.get(url, headers=headers)

    logs = response.json()  # or response.text if plain logs

    with open("/var/log/mulesoft\_audit.txt", "a") as f:

        for log in logs:

            f.write(str(log) + "\n")

# Run every 5 minutes

while True:

    fetch\_mulesoft\_logs()

    time.sleep(300)

save the above script file as **mulesoft\_log\_fetcher.py** in the syslog server.

**Step 2: Run as a Cron Job (Simple)**

* Save your script as mulesoft\_log\_fetcher.py
* Make sure it’s executable:

chmod +x mulesoft\_log\_fetcher.py --- run this cmd in Syslog server.

crontab -e