MileStone :- 1

PSID :- 10843198 Name :- Ayan Shah

```
User@DESKTOP-0FU31RQ MINGW64 ~/Desktop/MileStone1
$ py milestone1.py

=== STEP 1: LOAD DATA ===
Loaded 1 document(s)
Sample content (first 200 chars): Incident #001 | User=johns | Alert=Multiple failed SSH logins | SourceIP=10.1.1.9 | Host=SRV-LNX-01 | OS=Ubun
tu 20 | MITRE=T1110 | Severity=High | Resolution=Blocked source IP; Reset password; Enabled

=== STEP 2: CHUNKING ===
Created 20 chunks
Sample chunk: Incident #001 | User=johns | Alert=Multiple failed SSH logins | SourceIP=10.1.1.9 | Host=SRV-LNX-01 | OS=Ubuntu 20 | MITRE=T1110
| Severity=High | Res

=== STEP 3: EMBEDDINGS + INDEX ===
C:\Users\User\Desktop\MileStone1\milestone1.py:73: LangChainDeprecationWarning: The class `HuggingFaceEmbeddings` was deprecated in LangChain 0
.2.2 and will be removed in 1.0. An updated version of the class exists in the `langchain-huggingface package and should be used instead. To us
e it run `pip install -U `langchain-huggingface` and import as `from `langchain_huggingface import HuggingFaceEmbeddings``.
  emb = HuggingFaceEmbeddings(model_name="sentence-transformers/all-MiniLM-L6-v2")
FAISS vectorstore created with vector retriever (k=4)

=== BONUS: HYBRID RETRIEVAL ===
Hybrid retriever ready.


=== STEP 4: RAG CHAIN ===
RAG chain constructed.


=== BONUS: TOOL ===

=== STEP 5: MEMORY ===
Memory wrapper ready.


=== STEP 6: ENTITY EXTRACTION ===
Entity extraction function ready.
```

```
=== STEP 7: CONSOLE LOOP ===

📋 Example queries:
  analyst42 Show me all SSH brute force incidents
  analyst42 What happened with user johns?
  analyst42 Find Critical severity incidents
  analyst42 Show me ransomware attacks
  analyst42 What MITRE techniques are most common?
  analyst42 Tell me about PowerShell attacks

Enter: <analyst_id> <query> (or q): analyst12 Show me the Critical Severity Incidents

⏳ Processing your query...

================================================================================
🔍 Assistant Response for analyst12:
================================================================================
 Based on the provided context, there are two incidents with a critical severity level:

1. Incident #036: User=alexa | Alert=Reverse shell attempt via bash | Host=LAB-07 | OS=Ubuntu 22 | MITRE=T1059.004 | Severity=Critical | Resolu
tion=Killed shell; Blocked C2 IP.
   - This incident involves a reverse shell attempt using the bash shell, which is a Command and Control (C2) channel often used by attackers t
o execute commands on the compromised host. The MITRE ATT&CK technique associated with this incident is T1059.004 (Command and Scripting Interp
reter: Bash/Shell).

2. Incident #003: User=anitaa | Alert=Rapid file encryption detected (possible ransomware) | Host=FIN12 | OS=Windows 10 | MITRE=T1486 | Severit
y=Critical | Resolution=Isolated host; Triggered incident response plan; Restored from backup.
   - This incident involves rapid file encryption, which is a common tactic of ransomware attacks. The MITRE ATT&CK technique associated with t
his incident is T1486 (Data Encrypted for Impact).
================================================================================

📊 Extracted Entities:
   • Severity: Critical

🎯 Threat Score Analysis:
   • Score: 27/100
   • Level: HIGH
```

MileStone :- 1

PSID :- 10843198

Name :- Ayan Shah