

```
(ollama-env) C:\Users\User\Desktop\LLM\milestone_4>python soc1.py

--- STEP 1: LOAD DATA ---
Loaded 1 incidents
Sample record:
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 | Resolution=n=Blocked source IP; Reset password; Enabled

--- STEP 2: CHUNKING ---
Created 20 chunks

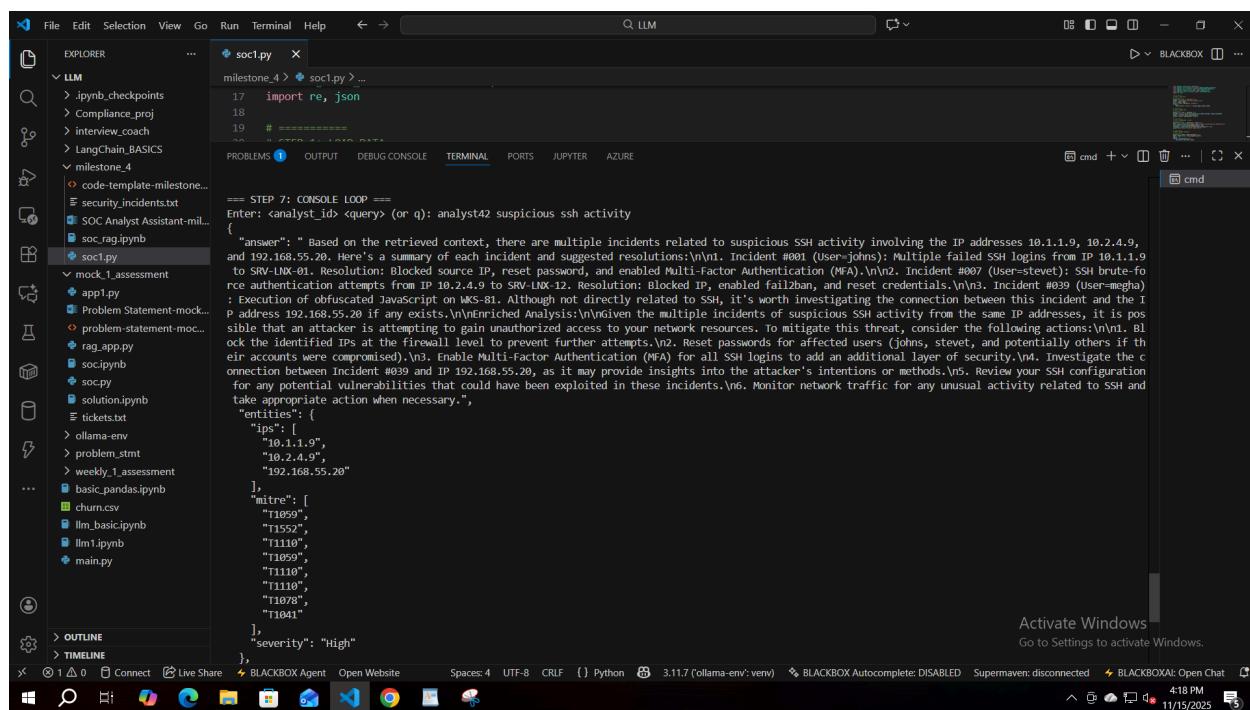
--- STEP 3: EMBEDDINGS + INDEX ---
C:\Users\User\Desktop\LLM\milestone_4\soc1.py:41: LangChainDeprecationWarning: The class `HuggingFaceEmbeddings` was deprecated in LangChain 0.2.2 and will be removed in 1.0. An updated version of the class exists in the `langchain-huggingface` package and should be used instead. To use 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 vector retriever ready (k=4)

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

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

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

--- STEP 7: CONSOLE LOOP ---
Enter: <analyst_id> <query> (or q): analyst42 suspicious ssh activity
Traceback (most recent call last):
  File "C:\Users\User\Desktop\LLM\milestone_4\soc1.py", line 180, in <module>
```



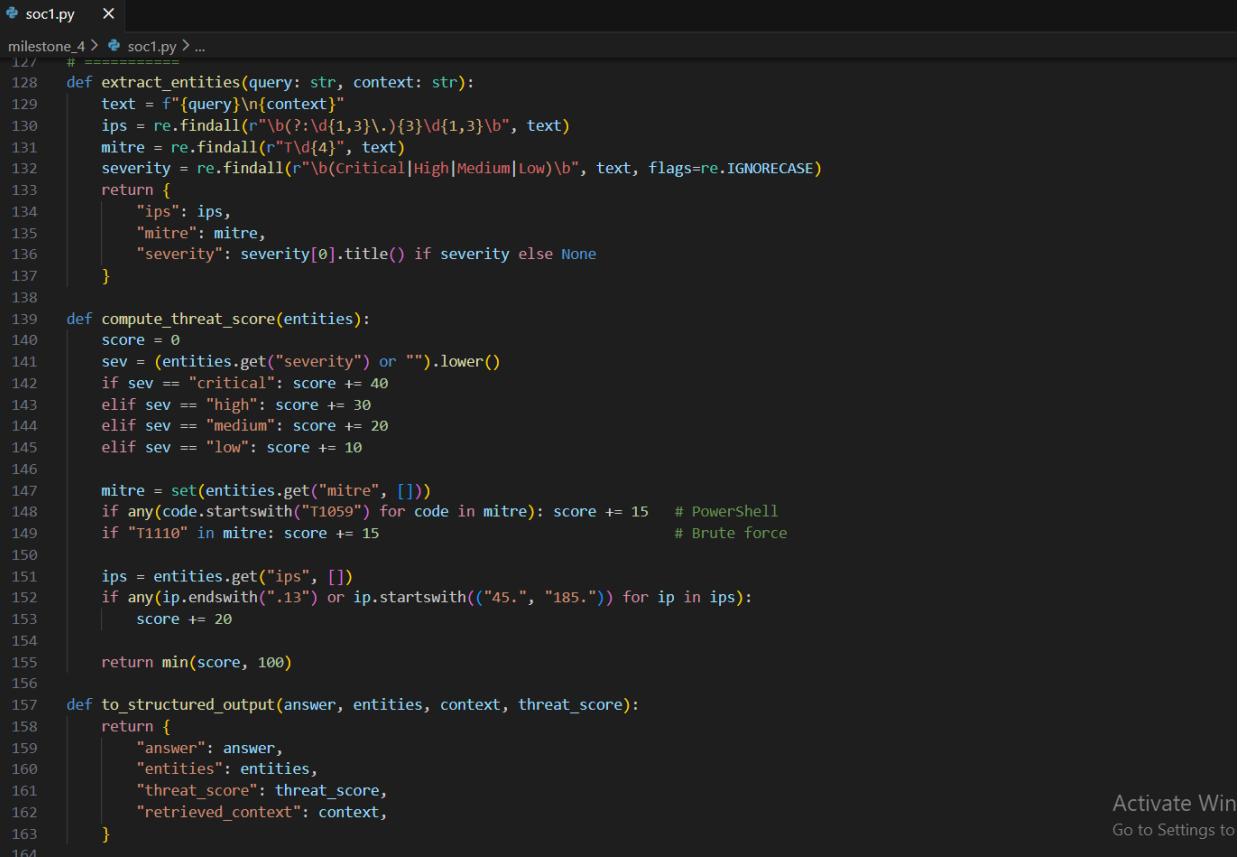
```

        "T1110",
        "T1078",
        "T1041"
    ],
    "severity": "High"
},
"threat_score": 60,
"retrieved_context": "Incident #017 | User=george | Alert=Malicious Java JAR execution | Host=DEV-04 | OS=Windows 10 | MITRE=T1059.005 | Severity=High | Re solution=Quarantined binary; Removed persistence keys.\nIncident #018 | User=will | Alert=Suspicious SSH key usage | Host=SRV-SSH01 | OS=Ubuntu 22 | MITRE=T1 552 | Severity=High | Resolution=Revoked SSH keys; Enforced rotation.\n---\nIncident #001 | User=johns | Alert=Multiple failed SSH logins | SourceIP=10.1.1.9 | Host=SRV-LNX-01 | OS=Ubuntu 20 | MITRE=T1110 | Severity=High | Resolution=Blocked source IP; Reset password; Enabled MFA.\nIncident #002 | User=markp | Alert=Suspicious PowerShell encoded command detected | Host=MKS-22 | OS=Windows 11 | MITRE=T1059 | Severity=High | Resolution=Terminated process; Disabled Powe rShell v2; Quarantined artifacts.\n---\nIncident #007 | User=stevet | Alert=SSH brute-force authentication attempts | SourceIP=10.2.4.9 | Host=SRV-LNX-12 | OS=Ubuntu 22 | MITRE=T1110.001 | Severity=High | Resolution=Blocked IP; Enabled fail2ban; Reset credentials.\nIncident #008 | User=rohan | Alert=Spike in failed login attempts | Host=SRV-APP2 | OS=RedHat 8 | MITRE=T1110 | Severity=Medium | Resolution=Throttled login attempts; Enabled MFA.\n---\nIncident #037 | User=r=stevet | Alert=SSH login from blacklisted country | SourceIP=192.168.55.20 | Host=SRV-LNX-12 | OS=Ubuntu 22 | MITRE=T1078 | Severity=High | Resolution=Bloc ked IP; Reset password.\nIncident #038 | User=rohan | Alert=Large outbound data transfer | Host=SRV-APP2 | OS=RedHat 8 | MITRE=T1041 | Severity=Critical | Re solution=Isolated server; Investigated data."
}

```

Enter: <analyst_id> <query> (or q): q

(ollama-env) C:\Users\User\Desktop\LLM\milestone_4>



```

soc1.py  X
milestone_4 > soc1.py > ...
127  # =====
128 def extract_entities(query: str, context: str):
129     text = f"{query}\n{context}"
130     ips = re.findall(r"\b(?:d{1,3}\.){3}d{1,3}\b", text)
131     mitre = re.findall(r"T\d{4}", text)
132     severity = re.findall(r"\b(Critical|High|Medium|Low)\b", text, flags=re.IGNORECASE)
133     return {
134         "ips": ips,
135         "mitre": mitre,
136         "severity": severity[0].title() if severity else None
137     }
138
139 def compute_threat_score(entities):
140     score = 0
141     sev = (entities.get("severity") or "").lower()
142     if sev == "critical": score += 40
143     elif sev == "high": score += 30
144     elif sev == "medium": score += 20
145     elif sev == "low": score += 10
146
147     mitre = set(entities.get("mitre", []))
148     if any(code.startswith("T1059") for code in mitre): score += 15      # PowerShell
149     if "T1110" in mitre: score += 15                                     # Brute force
150
151     ips = entities.get("ips", [])
152     if any(ip.endswith(".13") or ip.startswith(("45.", "185.")) for ip in ips):
153         score += 20
154
155     return min(score, 100)
156
157 def to_structured_output(answer, entities, context, threat_score):
158     return {
159         "answer": answer,
160         "entities": entities,
161         "threat_score": threat_score,
162         "retrieved_context": context,
163     }
164

```

Activate Win
Go to Settings to