

Name: VISHAL KUMAR

PS ID: 10843095

OUTPUT:

```
== STEP 1: LOAD DATA ==
Loaded 1 documents. Sample: 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=Blocked source IP; Reset password; Enabled...
```

```
> ▾ TERMINAL Python + □ ━
φ
    == STEP 2: CHUNKING ==
    Created 40 chunks.

    == STEP 3: EMBEDDINGS + INDEX ==
c:\Users\User\Desktop\Milestone\Milestone1.py:58: 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 u
sed instead. To use it run `pip install -U `langchain-huggingface` and import as `from `l
angchain_huggingface import HuggingFaceEmbeddings``.
embeddings = HuggingFaceEmbeddings(model_name="all-MiniLM-L6-v2")

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

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

```
> ▾ TERMINAL Python + □ ━
φ
    == BONUS: TOOL ==
    == STEP 5: MEMORY ==
    Memory wrapper ready.

    == STEP 7: CONSOLE LOOP ==
Enter: <analyst_id> <query> (or q): 001 Multiple failed SSH logins
Response for 001: {
    "retrieved_context": [
        "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=Blocked source IP; Reset password; Enabled MFA.",
        "Incident #018 | User=will | Alert=Suspicious SSH key usage | Host=SRV-SSH01 | OS=Ubuntu 22 | MITRE=T1552 | Severity=High | Resolution=Revoked SSH keys; Enforced rotation.",
        "Incident #007 | User=stevet | Alert=SSH brute-force authentication attempts | Source IP=10.2.4.9 | Host=SRV-LNX-12 | OS=Ubuntu 22 | MITRE=T1110.001 | Severity=High | Resolution=Blocked IP; Enabled fail2ban; Reset credentials.",
        "Incident #037 | User=stevet | Alert=SSH login from blacklisted country | SourceIP=192.168.55.20 | Host=SRV-LNX-12 | OS=Ubuntu 22 | MITRE=T1078 | Severity=High | Resolution=Billing to activate Windows"
    ]
```

```
> ▾ TERMINAL
∅      "Incident #016 | User=lisa | Alert=Frequent failed sudo attempts | Host=DEV-01 | OS=D
ebian 10 | MITRE=T1110 | Severity=Medium | Resolution=Implemented lockout; Alert rule cre
ated."
  ],
  "injected_user_memory": [],
  "injected_entity_memory": {
    "IPs": [
      "10.2.4.9",
      "10.1.1.9",
      "192.168.55.20"
    ],
    "OS": "Windows",
    "MITRE": [
      "T1078",
      "T1552",
      "T1021",
      "T1110"
    ]
  },
  "final_llm_answer": " The incident involving multiple failed SSH logins is mentioned in
Activate Windows
Incident #001. The user affected is \"johns\", the source IP is \"10.1.1.9\", and the ho
Go to Settings to activate Windows
r Authentication (MFA). The MITRE technique associated with this incident is T1110.",
  "threat_scores": [
    4,
    3,
    6,
    3,
    6,
    4,
    3,
    2
  ]
}
Enter: <analyst id> <query> (or q):
```

```
PROBLEMS    OUTPUT    DEBUG CONSOLE    TERMINAL    ...
> ▾ TERMINAL
∅      "T1021",
      "T1110"
    ],
  },
  "final_llm_answer": " The incident involving multiple failed SSH logins is mentioned in
Activate Windows
Incident #001. The user affected is \"johns\", the source IP is \"10.1.1.9\", and the ho
st is \"SRV-LNX-01\" which runs Ubuntu 20 OS. This incident has a high severity level and
was resolved by blocking the source IP, resetting the password, and enabling Multi-Facto
r Authentication (MFA). The MITRE technique associated with this incident is T1110.",
  "threat_scores": [
    4,
    3,
    6,
    3,
    6,
    4,
    3,
    2
  ]
}
Enter: <analyst id> <query> (or q):
```