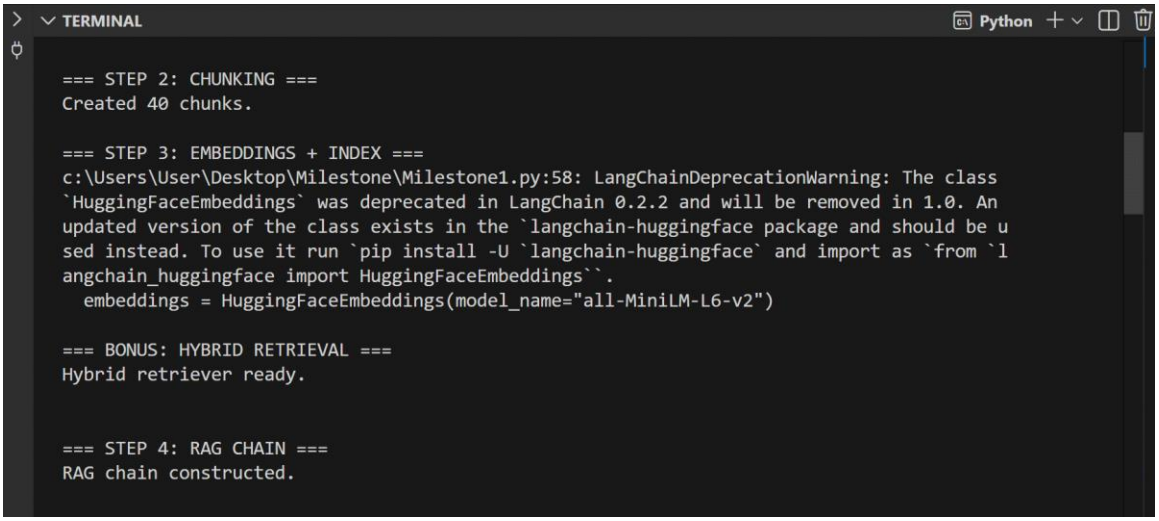
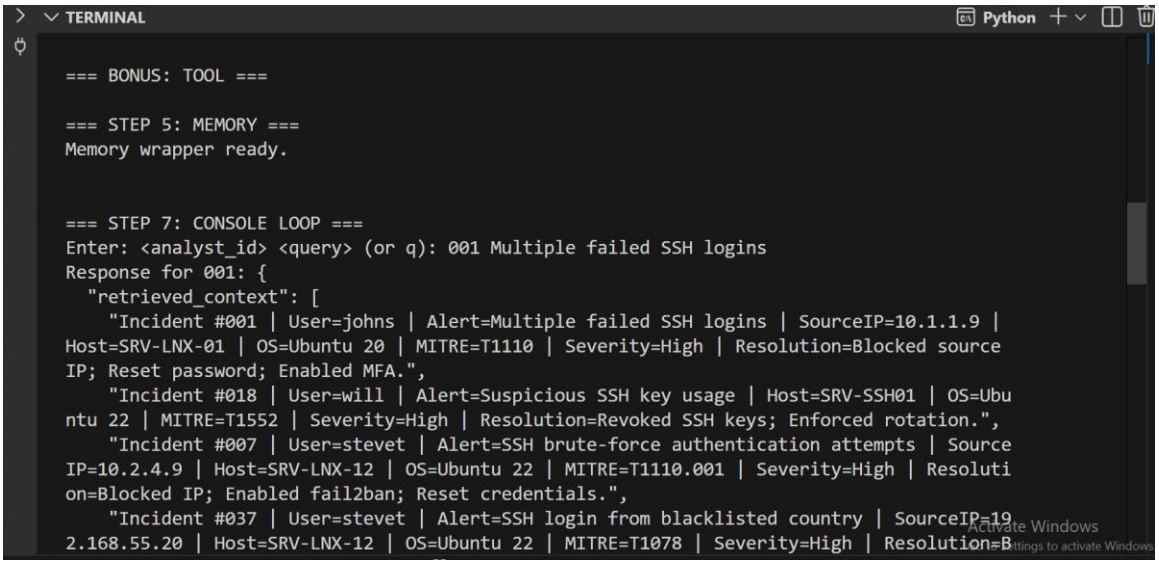
Name: VISHAL KUMAR

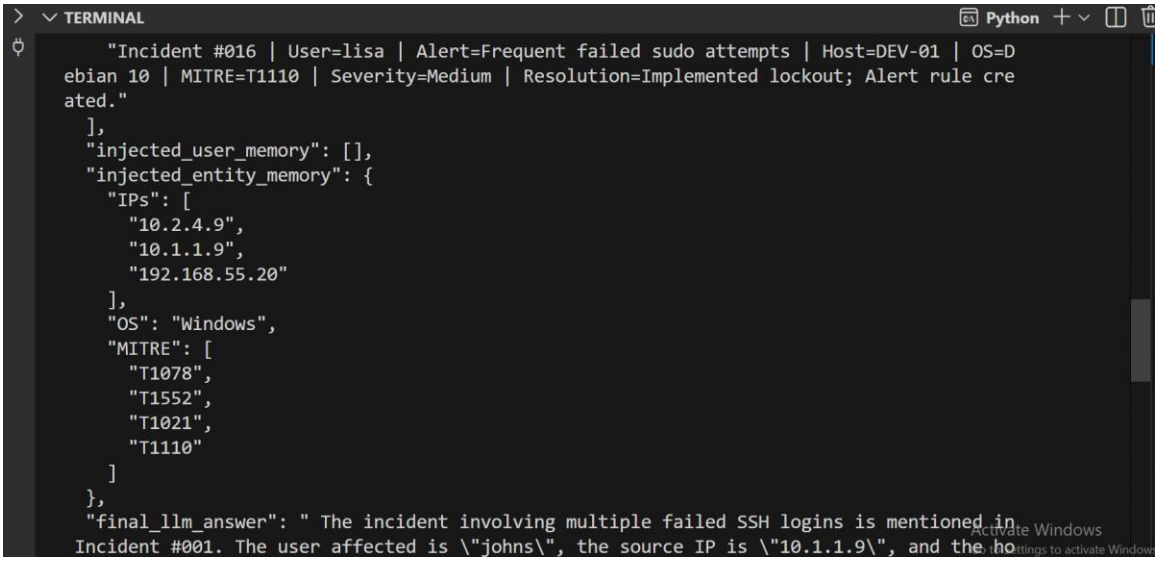
PS ID: 10843095

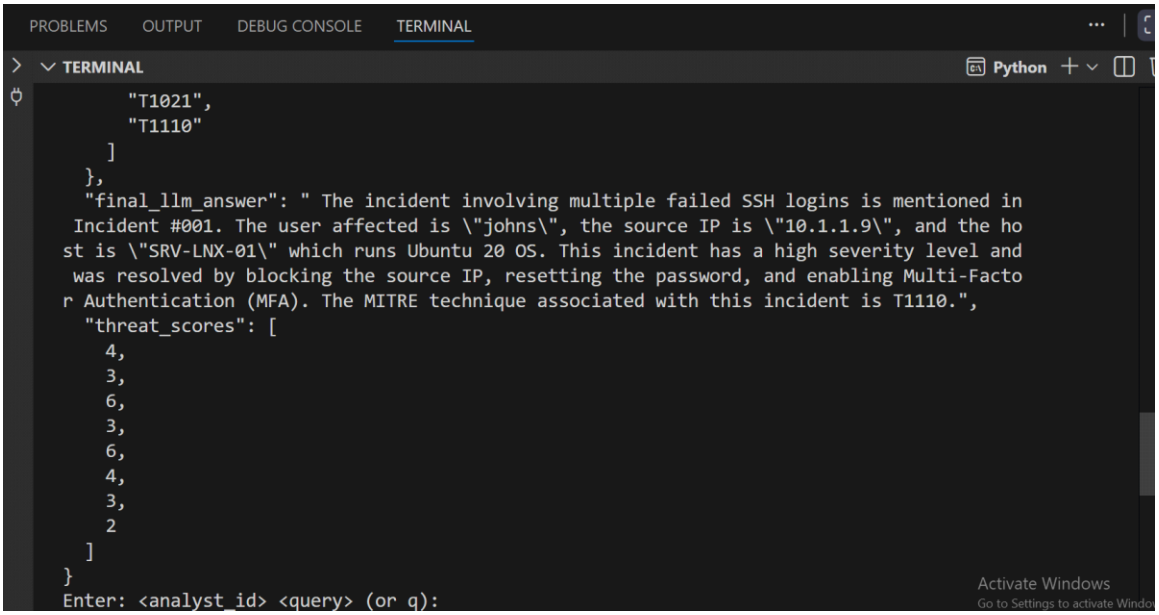
OUTPUT:

```
=== 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 | Res
olution=Blocked source IP; Reset password; Enabled...
```






TERMINAL
Python
"Incident #016 | User=lisa | Alert=Frequent failed sudo attempts | Host=DEV-01 | OS=Debian 10 | MITRE=T1110 | Severity=Medium | Resolution=Implemented lockout; Alert rule created."
],
"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 Incident #001. The user affected is \"johns\", the source IP is \"10.1.1.9\", and the ho
Activate Windows


PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
TERMINAL
Python
"T1021",
"T1110"
]
},
"final_llm_answer": " The incident involving multiple failed SSH logins is mentioned in Incident #001. The user affected is \"johns\", the source IP is \"10.1.1.9\", and the host 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-Factor 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):
Activate Windows