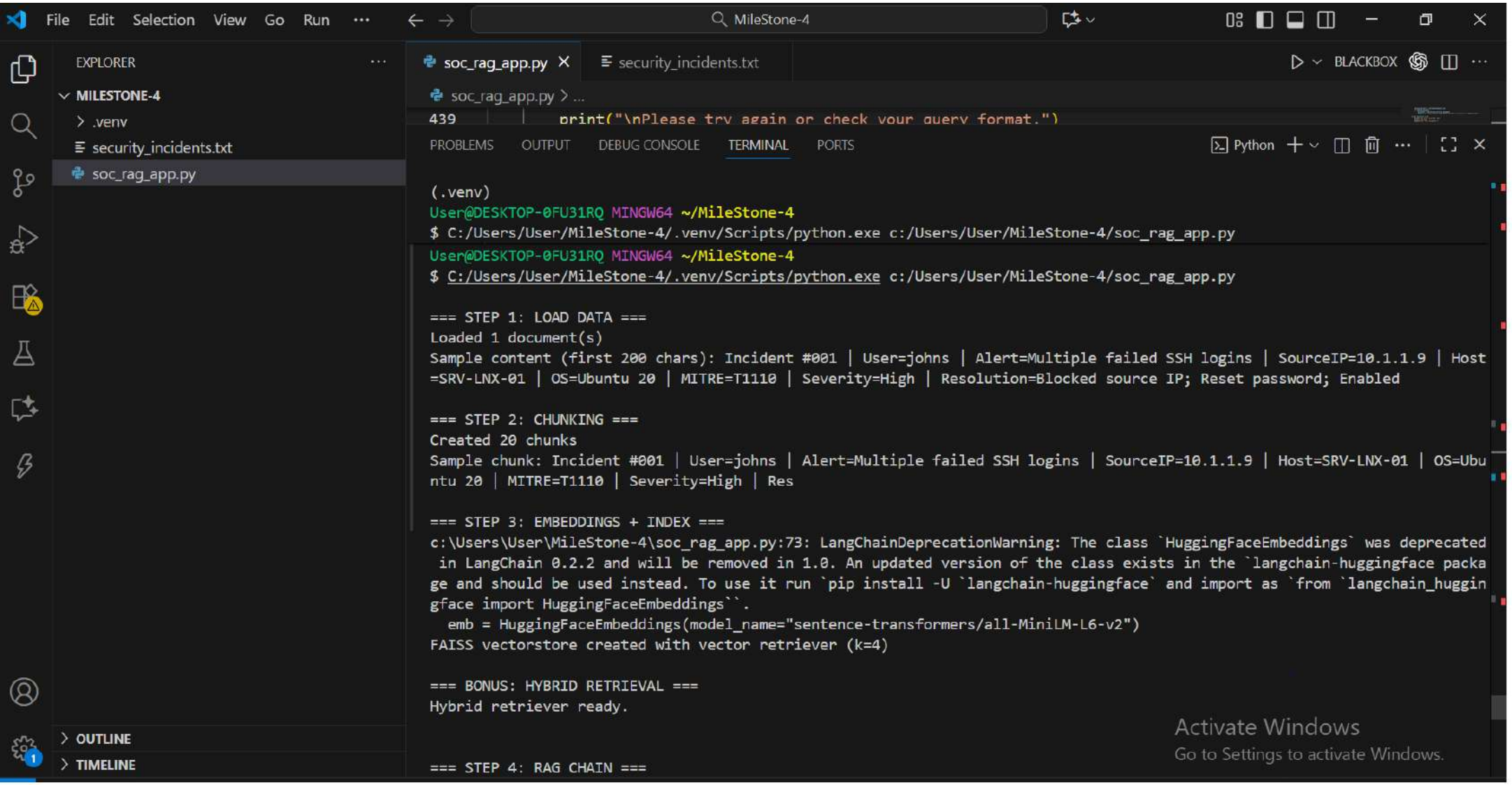
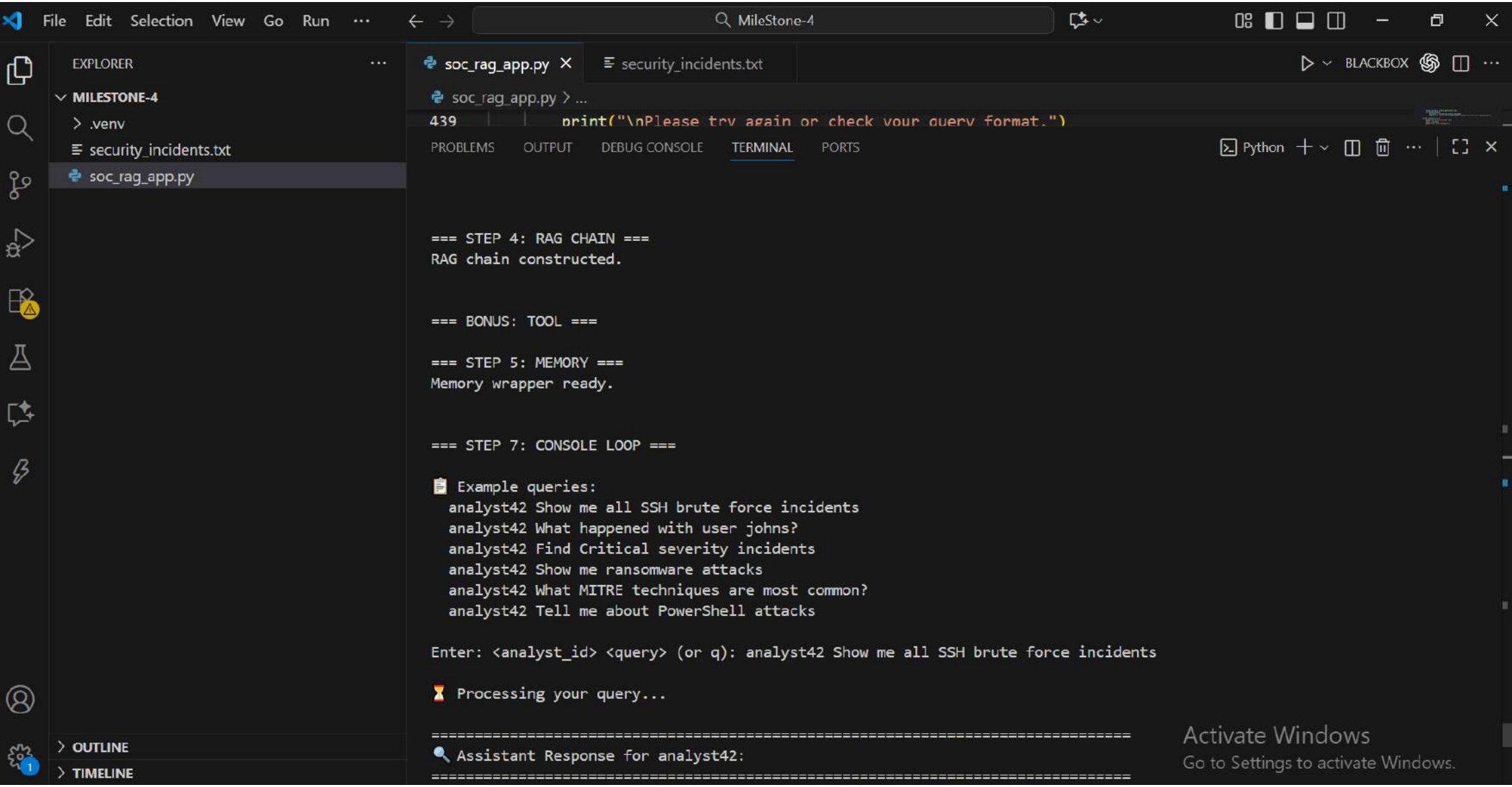
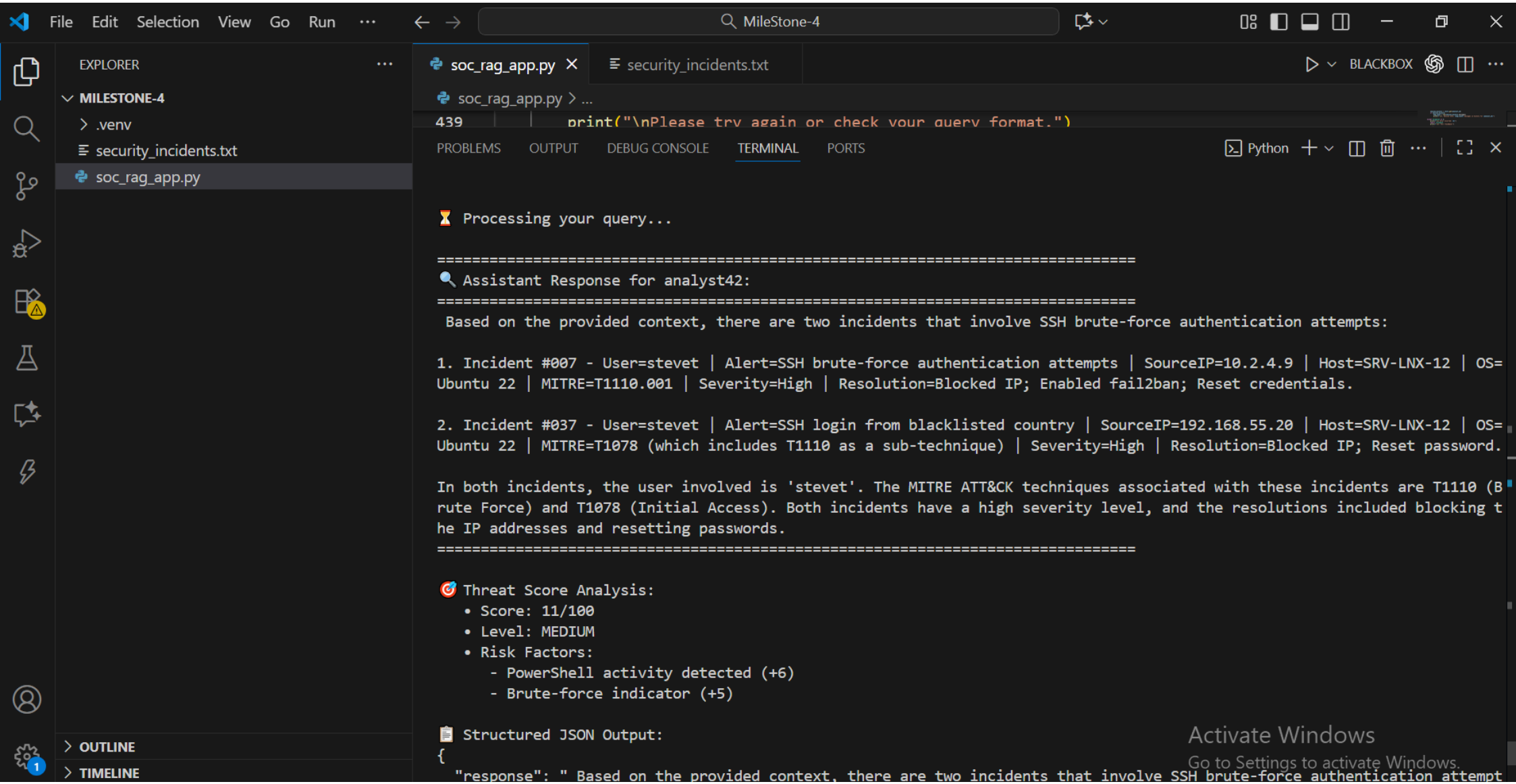
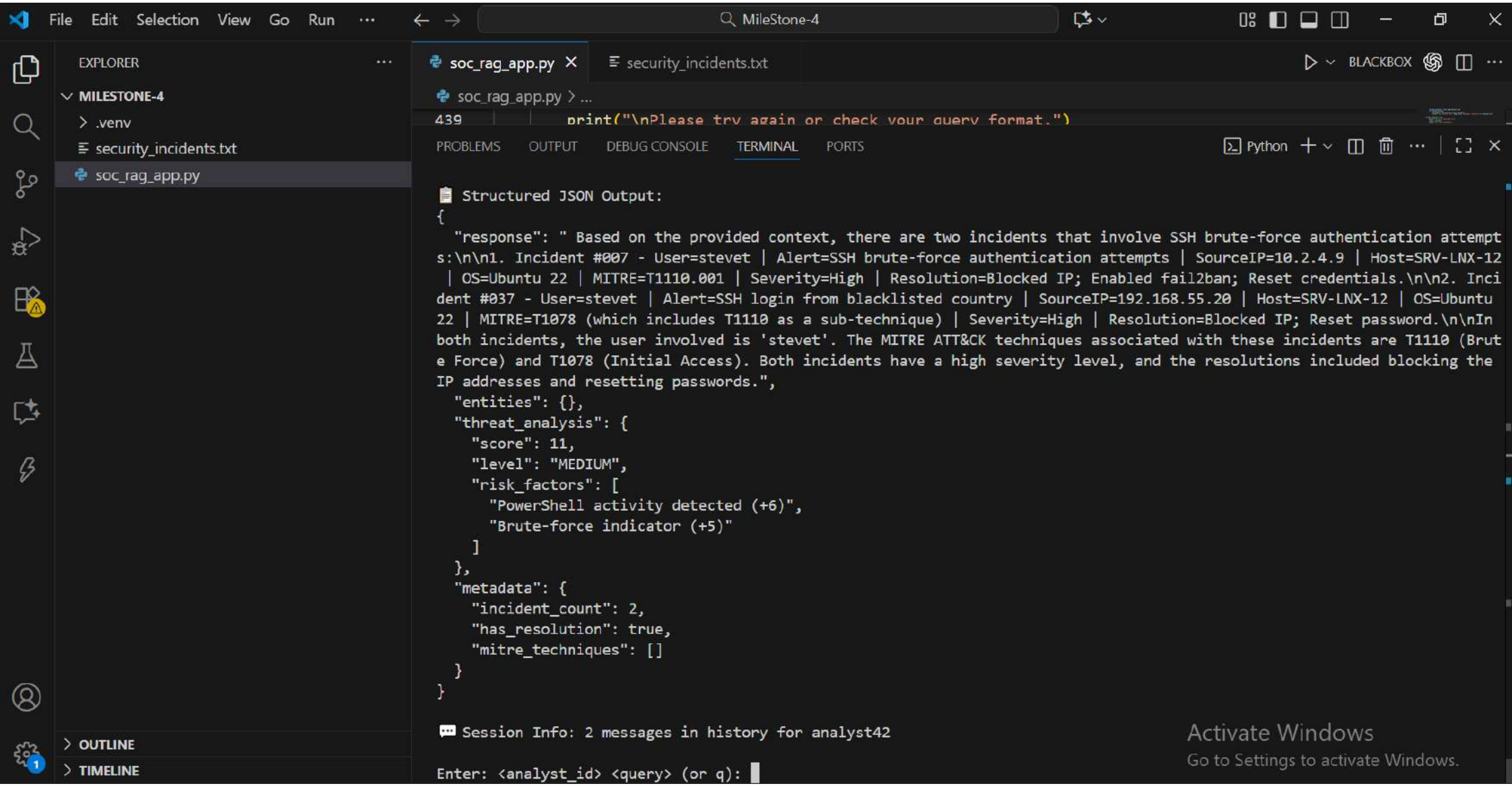

File Edit Selection View Go Run ···
MileStone-4
BLACKBOX
EXPLORER
MILESTONE-4
.venv
security_incidents.txt
soc_rag_app.py
soc_rag_app.py
security_incidents.txt
soc_rag_app.py > ...
439 print("\nPlease try again or check your query format.")
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
Python
(.venv)
User@DESKTOP-0FU31RQ MINGW64 ~/MileStone-4
$ C:/Users/User/MileStone-4/.venv/Scripts/python.exe c:/Users/User/MileStone-4/soc_rag_app.py
User@DESKTOP-0FU31RQ MINGW64 ~/MileStone-4
$ C:/Users/User/MileStone-4/.venv/Scripts/python.exe c:/Users/User/MileStone-4/soc_rag_app.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=Ubuntu 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=Ubu
ntu 20 | MITRE=T1110 | Severity=High | Res
=== STEP 3: EMBEDDINGS + INDEX ===
c:\Users\User\MileStone-4\soc_rag_app.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 packa
ge and should be used instead. To use it run `pip install -U `langchain-huggingface` and import as `from `langchain_huggin
gface 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 ===
Activate Windows
Go to Settings to activate Windows.
OUTLINE
TIMELINE


File Edit Selection View Go Run ···
MileStone-4
EXPLORER
MILESTONE-4
.venv
security_incidents.txt
soc_rag_app.py
soc_rag_app.py
security_incidents.txt
BLACKBOX
soc_rag_app.py > ...
439 print("\nPlease try again or check your query format.")
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
Python
=== STEP 4: RAG CHAIN ===
RAG chain constructed.
=== BONUS: TOOL ===
=== STEP 5: MEMORY ===
Memory wrapper 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): analyst42 Show me all SSH brute force incidents
Processing your query...
Assistant Response for analyst42:
OUTLINE
TIMELINE
Activate Windows
Go to Settings to activate Windows.


File Edit Selection View Go Run
MileStone-4
EXPLORER
MILESTONE-4
.venv
security_incidents.txt
soc_rag_app.py
soc_rag_app.py
security_incidents.txt
BLACKBOX
soc_rag_app.py > ...
439 print("\nPlease try again or check your query format.")
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
Python
⏳ Processing your query...
==========
🔍 Assistant Response for analyst42:
==========
Based on the provided context, there are two incidents that involve SSH brute-force authentication attempts:
1. Incident #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.
2. Incident #037 - User=stevet | Alert=SSH login from blacklisted country | SourceIP=192.168.55.20 | Host=SRV-LNX-12 | OS=Ubuntu 22 | MITRE=T1078 (which includes T1110 as a sub-technique) | Severity=High | Resolution=Blocked IP; Reset password.
In both incidents, the user involved is 'stevet'. The MITRE ATT&CK techniques associated with these incidents are T1110 (Brute Force) and T1078 (Initial Access). Both incidents have a high severity level, and the resolutions included blocking the IP addresses and resetting passwords.
==========
🎯 Threat Score Analysis:
• Score: 11/100
• Level: MEDIUM
• Risk Factors:
- PowerShell activity detected (+6)
- Brute-force indicator (+5)
📋 Structured JSON Output:
{
"response": " Based on the provided context, there are two incidents that involve SSH brute-force authentication attempt
OUTLINE
TIMELINE
Activate Windows
Go to Settings to activate Windows.


File Edit Selection View Go Run ···
MileStone-4
EXPLORER
MILESTONE-4
.venv
security_incidents.txt
soc_rag_app.py
soc_rag_app.py
security_incidents.txt
BLACKBOX
soc_rag_app.py > ...
439 print("\nPlease try again or check your query format.")
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
Python
Structured JSON Output:
{
"response": " Based on the provided context, there are two incidents that involve SSH brute-force authentication attempts:\n\n1. Incident #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.\n\n2. Incident #037 - User=stevet | Alert=SSH login from blacklisted country | SourceIP=192.168.55.20 | Host=SRV-LNX-12 | OS=Ubuntu 22 | MITRE=T1078 (which includes T1110 as a sub-technique) | Severity=High | Resolution=Blocked IP; Reset password.\n\nIn both incidents, the user involved is 'stevet'. The MITRE ATT&CK techniques associated with these incidents are T1110 (Brute Force) and T1078 (Initial Access). Both incidents have a high severity level, and the resolutions included blocking the IP addresses and resetting passwords.",
"entities": {},
"threat_analysis": {
"score": 11,
"level": "MEDIUM",
"risk_factors": [
"PowerShell activity detected (+6)",
"Brute-force indicator (+5)"
]
},
"metadata": {
"incident_count": 2,
"has_resolution": true,
"mitre_techniques": []
}
}
Session Info: 2 messages in history for analyst42
Enter: <analyst_id> <query> (or q):
OUTLINE
TIMELINE
Activate Windows
Go to Settings to activate Windows.