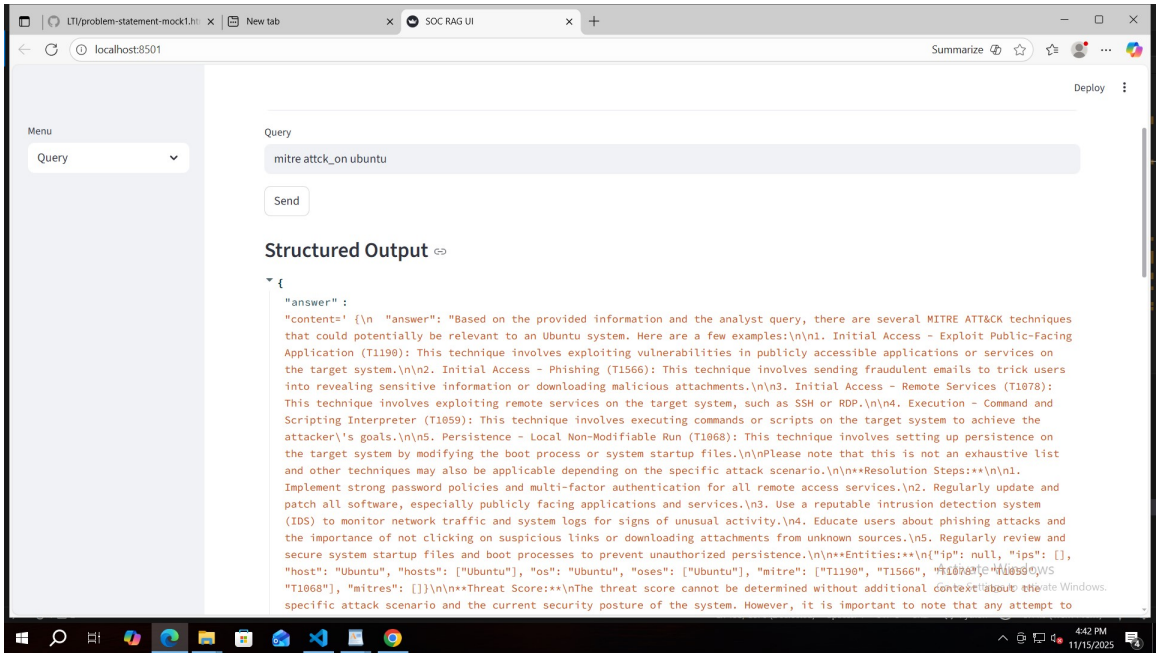
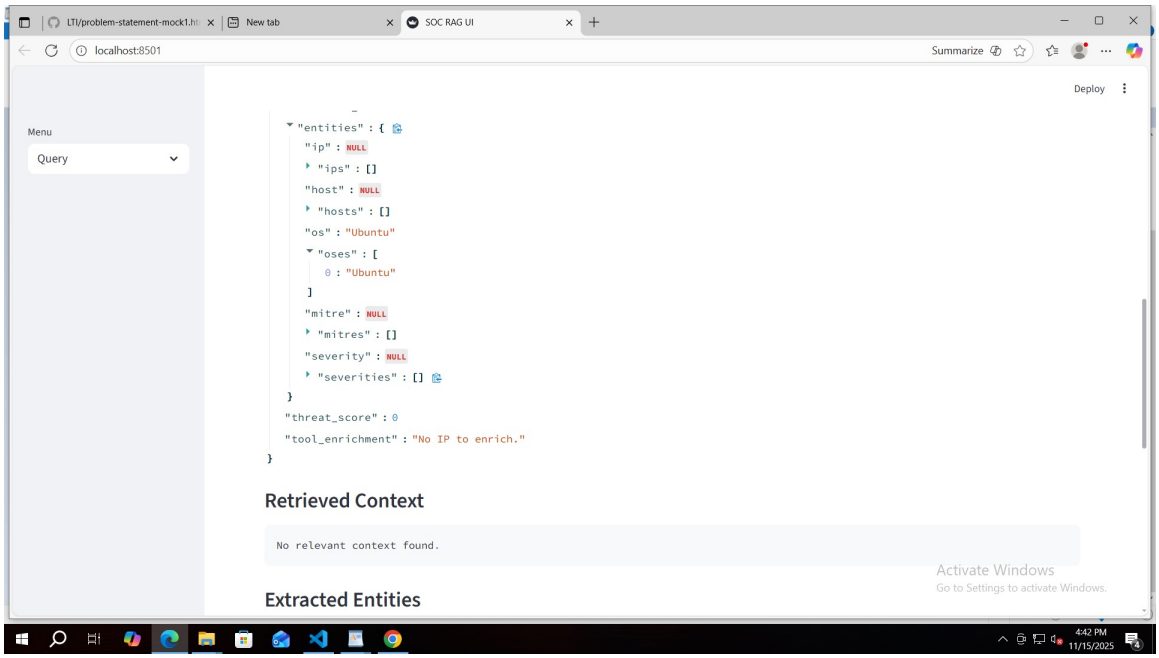
CLI

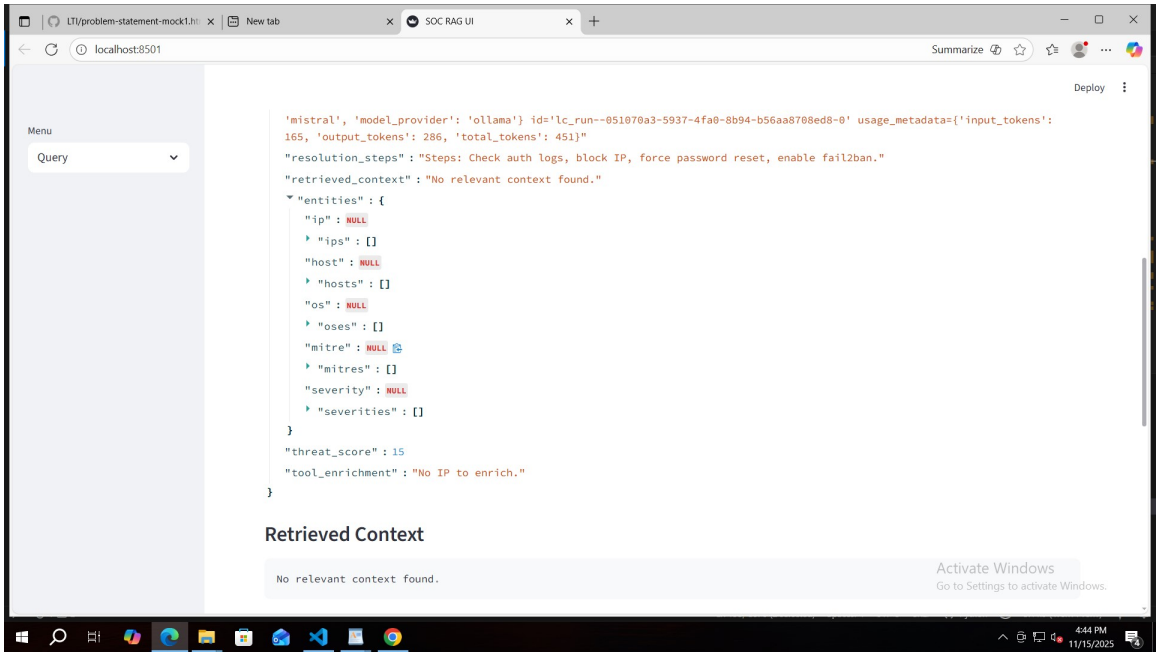
Tool implementation

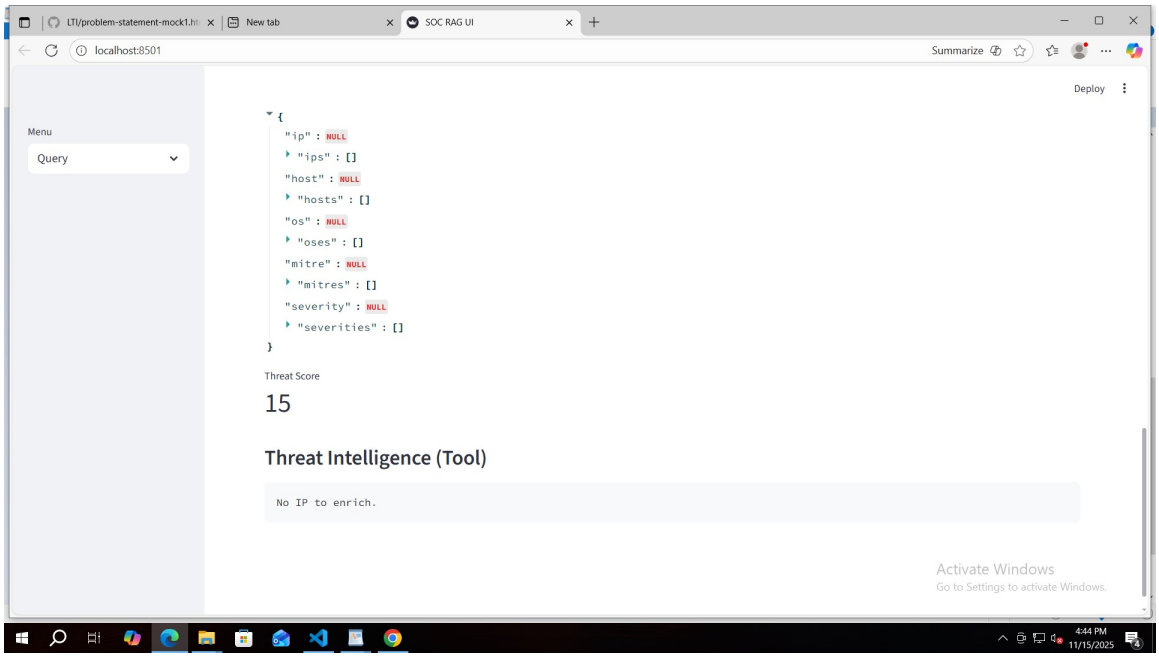
```
Choose option [1-5]: 1
Enter analyst_id (e.g. analyst42): analyst5
Enter query / alert summary: brute

KB Suggestions found:
Steps: Check auth logs, block IP, force password reset, enable fail2ban.
Mark resolved using KB steps? (y/n): y
Marked resolved and stored in history.

--- Structured Output ---
{
  "answer": "Resolved using KB steps:\nSteps: Check auth logs, block IP, force password reset, enable fail2ban."
  "resolution_steps": "Steps: Check auth logs, block IP, force password reset, enable fail2ban.",
  "retrieved_context": "No relevant context found.",
  "entities": {
    "ip": null,
    "ips": [],
    "host": null,
```

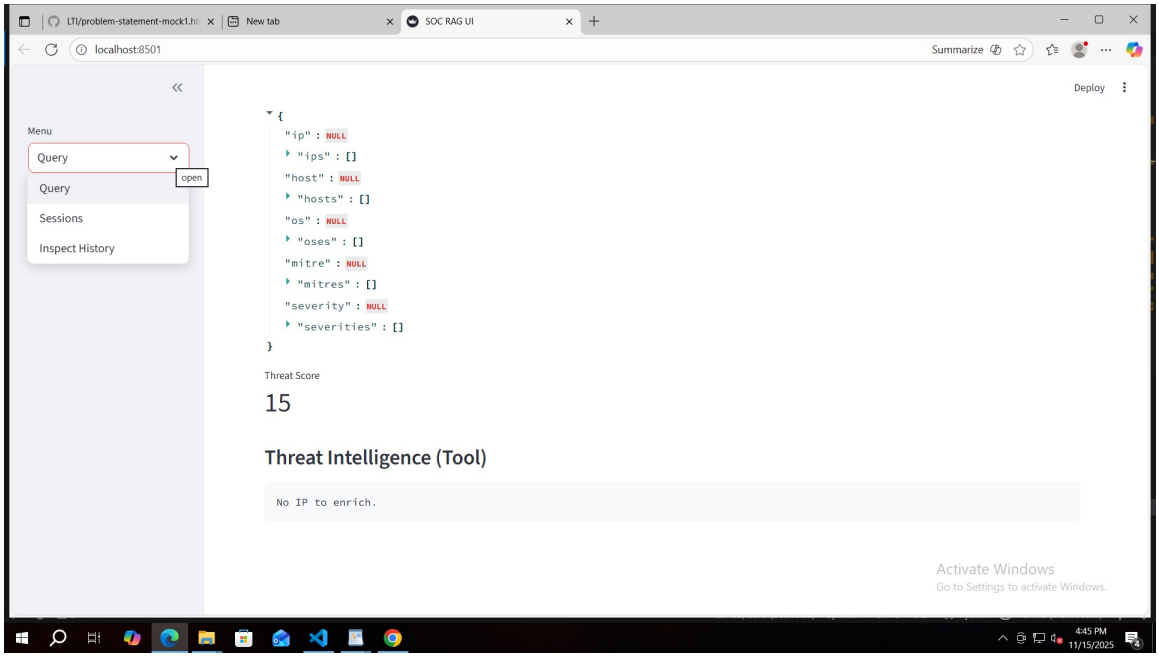
GUI implementation

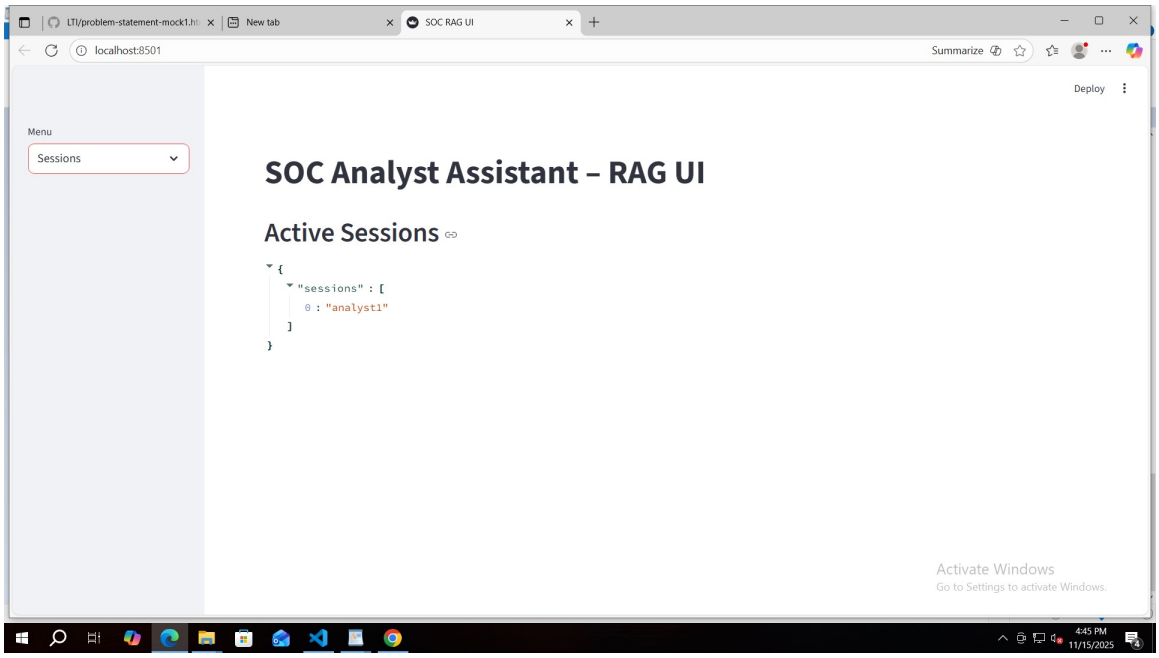


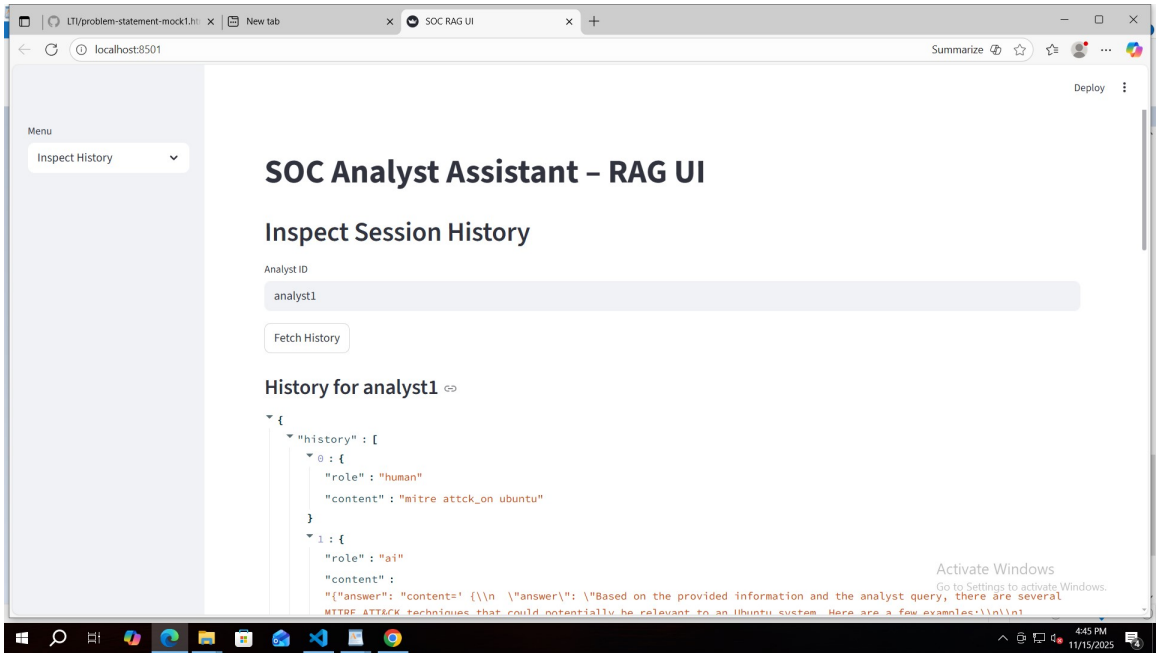

LTI/problem-statement-mock1.ht
New tab
SOC RAG UI
localhost:8501
Summarize
Deploy
Menu
Query
"entities" : {
"ip" : NULL
"ips" : []
"host" : NULL
"hosts" : []
"os" : "Ubuntu"
"oses" : [
0 : "Ubuntu"
]
"mitre" : NULL
"mitres" : []
"severity" : NULL
"severities" : []
}
"threat_score" : 0
"tool_enrichment" : "No IP to enrich."
}
Retrieved Context
No relevant context found.
Extracted Entities
Activate Windows
Go to Settings to activate Windows.
4:42 PM
11/15/2025


LTI/problem-statement-mock1.ht
New tab
SOC RAG UI
localhost:8501
Summarize
Deploy
Menu
Query
'mistral', 'model_provider': 'ollama'} id='lc_run--051070a3-5937-4fa0-8b94-b56aa8708ed8-0' usage_metadata={'input_tokens':
165, 'output_tokens': 286, 'total_tokens': 451}"
"resolution_steps" : "Steps: Check auth logs, block IP, force password reset, enable fail2ban."
"retrieved_context" : "No relevant context found."
"entities" : {
"ip" : NULL
"ips" : []
"host" : NULL
"hosts" : []
"os" : NULL
"oses" : []
"mitre" : NULL
"mitres" : []
"severity" : NULL
"severities" : []
}
"threat_score" : 15
"tool_enrichment" : "No IP to enrich."
}
Retrieved Context
No relevant context found.
Activate Windows
Go to Settings to activate Windows.
4:44 PM
11/15/2025


LTI/problem-statement-mock1.ht
New tab
SOC RAG UI
localhost:8501
Summarize
Deploy
Menu
Query
{
"ip" : NULL
"ips" : []
"host" : NULL
"hosts" : []
"os" : NULL
"oses" : []
"mitre" : NULL
"mitres" : []
"severity" : NULL
"severities" : []
}
Threat Score
15
Threat Intelligence (Tool)
No IP to enrich.
Activate Windows
Go to Settings to activate Windows.
4:44 PM
11/15/2025


LTI/problem-statement-mock1.ht
New tab
SOC RAG UI
localhost:8501
Summarize
Deploy
Menu
Query
open
Query
Sessions
Inspect History
{
"ip" : NULL
"ips" : []
"host" : NULL
"hosts" : []
"os" : NULL
"oses" : []
"mitre" : NULL
"mitres" : []
"severity" : NULL
"severities" : []
}
Threat Score
15
Threat Intelligence (Tool)
No IP to enrich.
Activate Windows
Go to Settings to activate Windows.
4:45 PM
11/15/2025


LTI/problem-statement-mock1.ht
New tab
SOC RAG UI
localhost:8501
Summarize
Deploy
Menu
Sessions
SOC Analyst Assistant – RAG UI
Active Sessions
{
"sessions" : [
0 : "analyst1"
]
}
Activate Windows
Go to Settings to activate Windows.
4:45 PM
11/15/2025


LTI/problem-statement-mock1.ht
New tab
SOC RAG UI
localhost:8501
Summarize
Deploy
Menu
Inspect History
SOC Analyst Assistant – RAG UI
Inspect Session History
Analyst ID
analyst1
Fetch History
History for analyst1
{
"history" : [
0 : {
"role" : "human"
"content" : "mitre attck_on ubuntu"
}
1 : {
"role" : "ai"
"content" :
"{"answer": "content=' {\\n \"answer\": \"Based on the provided information and the analyst query, there are several
Activate Windows
Go to Settings to activate Windows.
4:45 PM
11/15/2025