

## CLI

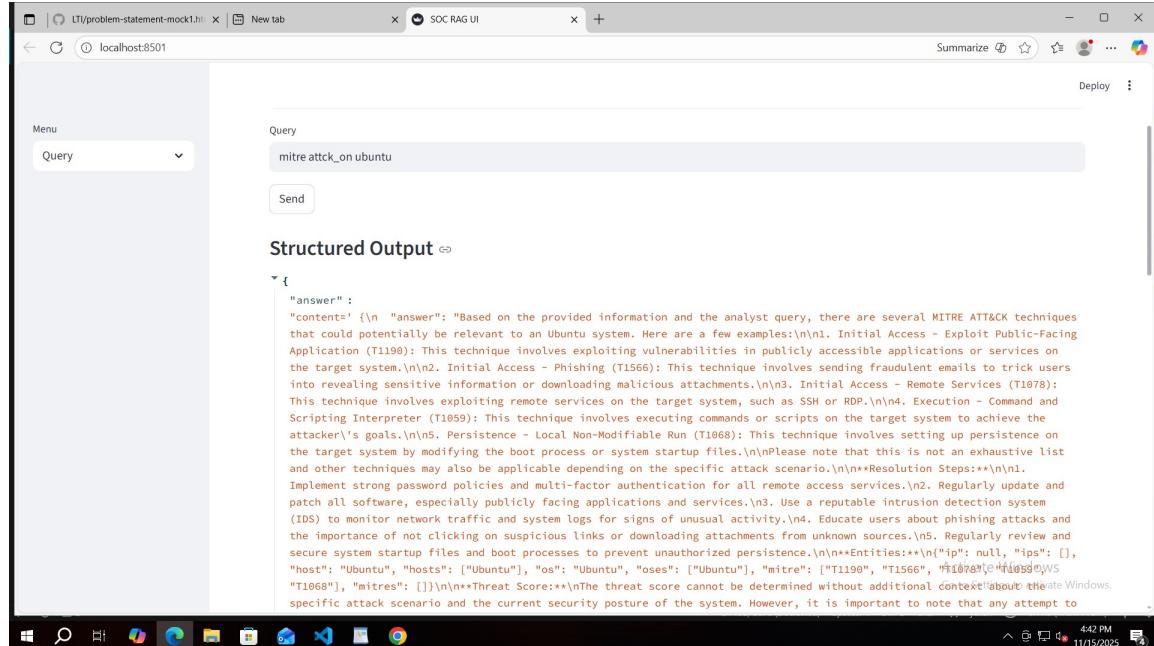
### Tool implementation

```
Choose option [1-5]: 1
Enter analyst_id (e.g. analyst42): analysts5
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



The screenshot shows a web browser window titled "SOC RAG UI" at the URL "localhost:8501". The page displays a JSON-like query response. The "entities" field contains several null values and an empty array for "ips". The "os" field is set to "Ubuntu". The "oses" array contains one item, also set to "Ubuntu". The "mitre" field is null, and the "mitres" array is empty. The "severity" field is null, and the "severities" array is empty. The "threat\_score" field is 0. The "tool\_enrichment" field is set to "No IP to enrich." Below this, a section titled "Retrieved Context" shows a message: "No relevant context found." To the right of the main content, there is an "Activate Windows" button with the text "Go to Settings to activate Windows." The browser's status bar at the bottom shows the time as 4:42 PM and the date as 11/15/2025.

```
{
  "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.

Activate Windows  
Go to Settings to activate Windows.

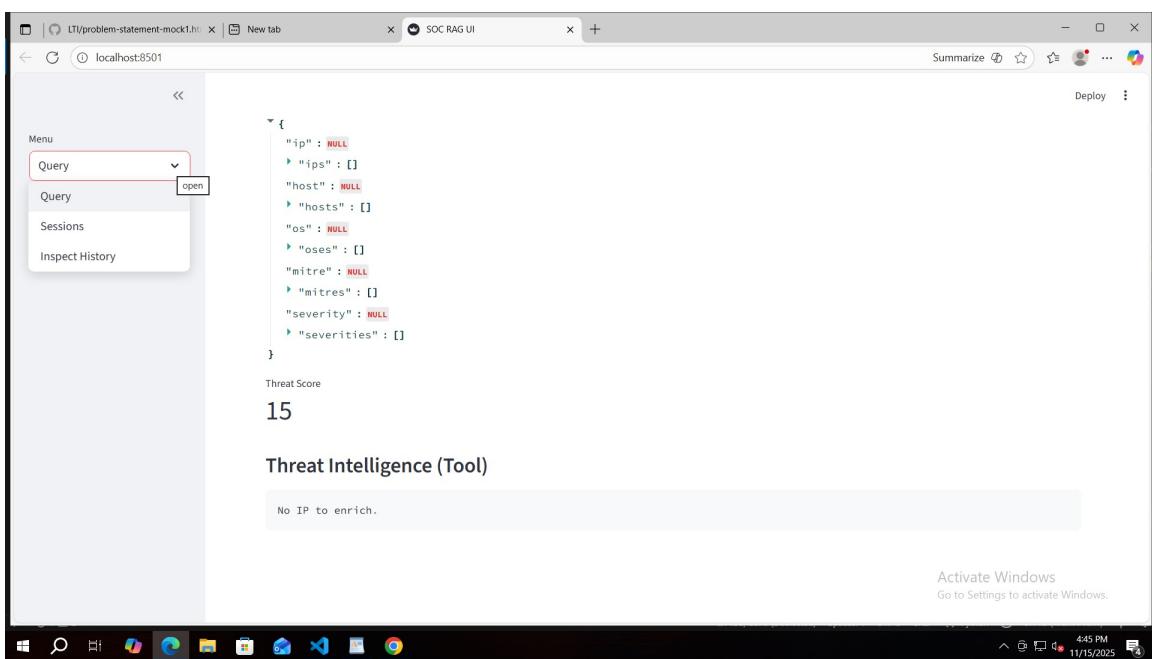
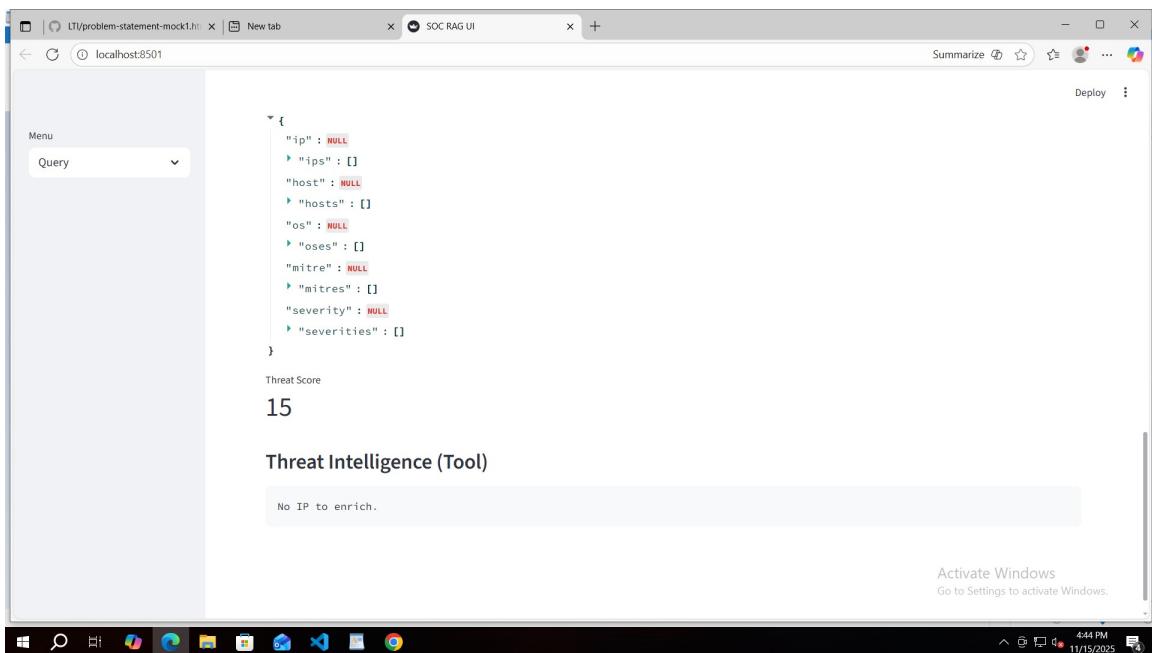
This screenshot is identical to the one above, showing the same JSON query response and context retrieval results. It includes the "mistral" field with its ID and usage metadata, the "resolution\_steps" field, and the "retrieved\_context" field indicating no relevant context found. The browser status bar shows the time as 4:44 PM and the date as 11/15/2025.

```
{
  "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."
}
```

**Retrieved Context**

No relevant context found.

Activate Windows  
Go to Settings to activate Windows.



The screenshot shows a web browser window titled "SOC Analyst Assistant – RAG UI" at the URL "localhost:8501". The interface has a sidebar on the left with a "Menu" section containing a dropdown menu set to "Sessions". The main content area is titled "Active Sessions" and displays a JSON object:

```
{ "sessions": [ { "0": "analyst1" } ] }
```

The status bar at the bottom indicates "Activate Windows Go to Settings to activate Windows." and the system clock shows "4:45 PM 11/15/2025".

The screenshot shows the same web browser window at "localhost:8501". The sidebar now shows "Inspect History" in the dropdown menu. The main content area is titled "Inspect Session History" and includes fields for "Analyst ID" (set to "analyst1") and a "Fetch History" button. Below this is a section titled "History for analyst1" displaying a JSON object:

```
{ "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 MITRE ATT&CK techniques that could potentially be relevant to an Ubuntu system. Here are a few examples:\\n\\n'\"}' } } ] }
```

A tooltip for the "content" field of the second history entry reads: "{'answer': 'content': '\\n \\\"answer\\\": \"Based on the provided information and the analyst query, there are several MITRE ATT&CK techniques that could potentially be relevant to an Ubuntu system. Here are a few examples:\\n\\n'\"}'". The status bar and system clock are identical to the first screenshot.

