

Ishan Garg Milestone 4 Assessment(10843105)

SOC-RAG Assistant

As per the question, I have done all use cases along with bonus use cases.

This is the UI for the SOC assistant app

The screenshot shows the SOC RAG Assistant application. On the left, there's a sidebar with "SOC RAG Assistant" at the top, followed by "Session ID (analyst)" and a text input field containing "user1". Below that is a "Clear conversation" button. Underneath is a "Backend status:" section with a green "Backend OK" button. In the center, there's a main area titled "Ask SOC — RAG Assistant" with a text input field placeholder "Enter your query and get a human answer plus structured JSON.". On the right, there's a "Compose" section with a "Query" input field containing "multiple ssh failed login", a "Timeout (s)" slider set to 30, and an "Ask" button. At the bottom, there's a "Last structured response" section showing a JSON object:

```
{  
  "summary": " 1) Diagnostic Summary: Multiple failed SSH login attempts suggest a potential brute-force attack on your system's SSH service. This could indicate an attempt to gain unauthorized access to your systems.\n  2) Suggested Next Steps / Remediation:\n    - Implement rate limiting or lockout policies for SSH logins to prevent brute-force attacks.\n    - Review and update password policies to ensure strong, unique passwords are used.\n    - Enable logging and monitoring of failed login attempts for further analysis.\n    - Investigate the source IP addresses of the failed login attempts and consider blocking them if they continue or are suspected to be malicious.\n  3) Notable Indicators:\n    - Source IP addresses associated with the failed login attempts.\n    - Potential MITRE Att&ck techniques: \"Brute Force\" (T1110), \"Credential Dumping\" (T1075), and \"Exploit Public-Facing Application\" (T1190).",  
  "recommended_actions": [  
    "Continue monitoring, gather additional context if available"  
  ],  
  "confidence": 0.08,  
  "threat_score": 8,  
  "related_incidents": [],  
  "entities": {}  
}
```

Last structured response ↴

```
{  
  "summary": " 1) Diagnostic Summary: Multiple failed SSH login attempts suggest a potential brute-force attack on your system's SSH service. This could indicate an attempt to gain unauthorized access to your systems.\n  2) Suggested Next Steps / Remediation:\n    - Implement rate limiting or lockout policies for SSH logins to prevent brute-force attacks.\n    - Review and update password policies to ensure strong, unique passwords are used.\n    - Enable logging and monitoring of failed login attempts for further analysis.\n    - Investigate the source IP addresses of the failed login attempts and consider blocking them if they continue or are suspected to be malicious.\n  3) Notable Indicators:\n    - Source IP addresses associated with the failed login attempts.\n    - Potential MITRE Att&ck techniques: \"Brute Force\" (T1110), \"Credential Dumping\" (T1075), and \"Exploit Public-Facing Application\" (T1190).",  
  "recommended_actions": [  
    "Continue monitoring, gather additional context if available"  
  ],  

```

Output in the terminal along with bonus

```
Enter: <analyst_id> <query> (or q): user0 spiked in failed login attempts

--- RAG OUTPUT ---
Entities extracted:
{}

Threat Score:
Score: 8 | Level: Low
Reasons:
- Brute-force indicators (1) => +8

Retrieved snippets:
(no retrieved snippets)

LLM Answer:

1) Diagnostic Summary: There has been an increase in failed login attempts, which may indicate a brute-force attack or compromised accounts.

2) Suggested Next Steps / Remediation:
- Investigate the IP addresses involved in the failed login attempts to determine if they are malicious.
- Review account lockout policies to ensure they are not overly permissive and causing unnecessary delays or service interruptions.
- Implement multi-factor authentication for all accounts where possible.
- Consider implementing a rate limiting system to prevent brute-force attacks.

3) Notable Indicators:
- Suspicious IP addresses involved in the failed login attempts.
- MITRE Att&ck Techniques: "Brute Force" (T1110), "Credential Dumping" (T1003), and "Account Manipulation" (T1115).
```

```
Format: <analyst_id> <your query> (type 'q' to quit)

Enter: user1 ssh login failed
Error in RootListenersTracer.on_chain_end callback: KeyError('output')

=====
FINAL ANSWER (JSON)
{
    "analysis": "The incident involves a spike in failed SSH login attempts on the host SRV-SSH01 running Ubuntu 22. This aligns with MITRE's T1552 (Credential Abrasion).",
    "resolution": "Revoke the current SSH keys, enforce rotation of new SSH keys, and implement a lockout mechanism for failed login attempts.",
    "similar_incidents": [
        "Incident #018"
    ],
    "threat_score": "75"
}

--- Retrieved Context (Hybrid) ---
1. User:Incident #008 Host:User=rohan OS:Alert=spike in failed login attempts IP:Host=SRV-APP2 Summary:OS=RedHat 8 MITRE:MITRE=T1110 Severity:Severity=Medium Resolution:Resolution=Throttled login attempts; Enabled MFA.....
2. User:Incident #040 Host:User=aillan OS:Alert=SQL admin login anomaly IP:Host=SRV-DB03 Summary:OS=RedHat 9 MITRE:MITRE=T1078 Severity:Severity=Medium Resolution:Resolution=Reset admin password; Reviewed logs.....
3. User:Incident #021 Host:User=tony OS:Alert=Multiple failed RDP logins IP:Host=WKS-33 Summary:OS=Windows 10 MITRE:MITRE=T1021 Severity:Severity=High Resolution:Resolution=Blocked IPs; Enabled account lockout.....
4. User:Incident #018 Host:User=will OS:Alert=Suspicious SSH key usage IP:Host=SRV-SSH01 Summary:OS=Ubuntu 22 MITRE:MITRE=T1552 Severity:Severity=High Resolution:Resolution=Revoked SSH keys; Enforced rotation.....
5. User:Incident #016 Host:User=lisa OS:Alert=Frequent failed sudo attempts IP:Host=DEV-01 Summary:OS=Debian 10 MITRE:MITRE=T1110 Severity:Severity=Medium Resolution:Resolution=Implemented lockout; Alert rule created.....

--- Extracted Entities ---
{
    "ips": [],
    "os": [
        "windows"
    ],
    "hostnames": [
        "User"
    ],
}
```

Activate Windows
Go to Settings to activate

```
--- Extracted Entities ---
{
  "ips": [],
  "os": [
    "Windows"
  ],
  "hostnames": [
    "User"
  ],
  "mitre": [
    "T1110",
    "T1552",
    "T1021",
    "T1078"
  ],
  "severity": [
    "Medium",
    "High"
  ]
}

--- Conversation History (last 2 turns) ---
--- Threat Score ---
75/100
=====
```

Above 3 screenshots show Threat score, JSON Format answer, Tool and Entity Memory Extraction.