

Complete Demo - Input/Output for Screenshots

QUERY 1: BASE FEATURES - RAG + FAISS Retrieval:

```
=====
🚀 SOC RAG ASSISTANT READY
=====
Commands: 'exit' to quit | 'clear <analyst_id>' to reset session
=====

👤 Analyst ID: analyst42
🔍 Query: Show me SSH brute-force attacks

=====
⌚ Processing with Vector RAG...

👤 SOC ANALYST RESPONSE:
Based on the retrieved context of past security incidents, it is evident that there have been multiple instances of SSH brute-force attacks (MITRE T1110.001 and MITRE T1110). To mitigate these types of attacks effectively, I recommend implementing the following actionable recommendations:

1. Implementing a rate limiting mechanism for SSH login attempts to reduce the likelihood of successful brute-force attacks. This can be achieved by configuring fail2ban or similar tools that automatically block IP addresses after a certain number of failed login attempts within a specific timeframe.

2. Enforcing strong password policies and regularly updating them. Users should be encouraged to use complex, unique passwords for their SSH accounts. Password managers can help users generate and manage secure passwords.

3. Implementing Multi-Factor Authentication (MFA) for all critical systems that support it. MFA adds an additional layer of security by requiring users to provide two or more verification factors (something they know, something they have, or something they are) before granting access.
```

4. Monitoring and maintaining a list of blacklisted countries from which SSH login attempts should be blocked (MITRE T1078). This can help prevent attacks originating from known malicious regions.

5. Regularly auditing and revoking SSH keys, especially in cases where suspicious key usage has been detected (MITRE T1552). Enforcing regular rotation of SSH keys can also help maintain the security of your systems.

6. Educating users about the risks associated with SSH attacks and best practices for securing their accounts. This includes advice on creating strong passwords, enabling MFA, and being cautious when receiving unsolicited emails or messages that may contain links to phishing sites.

By implementing these recommendations, you can significantly reduce the risk of SSH brute-force attacks and improve the overall security posture of your organization.

🔍 Entity Memory:

IPs: 10.2.4.9, 192.168.55.20, 10.1.1.9

OS: Ubuntu 22, Ubuntu 20

Hostname: SRV-LNX-12, SRV-LNX-01, SRV-SSH01

MITRE: T1078, T1552, T1110.001, T1110

Severity: High

❗ Threat Enrichment:

- T1110.001: Brute Force - Common credential attack, implement rate limiting & MFA
- T1110: Brute Force - Common credential attack, implement rate limiting & MFA
- IP 10.2.4.9: Internal network (check for lateral movement)
- IP 192.168.55.20: Internal network (check for lateral movement)
- IP 10.1.1.9: Internal network (check for lateral movement)
- Ubuntu 22: Review /var/log/auth.log, enable auditd
- Ubuntu 20: Review /var/log/auth.log, enable auditd

⚠ Threat Score: 80/100 (Risk Level: CRITICAL)

Factors: Severity=High (+30), MITRE T1078 (+10), MITRE T1552 (+10)

📊 Structured Output Available (JSON): 2507 chars

💬 Session: 1 exchanges for analyst42

QUERY 2: MEMORY RETENTION - Chat History

```
👤 Analyst ID: analyst42
🔍 Query: What were the source IPs involved in those attacks?

=====
⌚ Processing with Vector RAG...

⌚ SOC ANALYST RESPONSE:
The source IP addresses involved in the past security incidents are as follows:

1. Incident #034: 10.22.3.9 (Blocked traffic; Conducted IOC scan)
2. Incident #012: 172.22.9.54 (Blocked IP; Alerted network team)
3. Incident #038: Not explicitly mentioned in the provided context (Isolated server; Investigated data)
4. Incident #007: 10.2.4.9 (Blocked IP; Enabled fail2ban; Reset credentials)

In addition to these specific incidents, it is important to note that there are other IP addresses of interest in the entity memory: 192.168.55.20 and 10.1.1.9. To maintain a proactive security posture, I recommend implementing the following actionable recommendations based on the retrieved incidents and referencing MITRE techniques:

1. Implement IP reputation services or blocklists to automatically block known malicious IP addresses (MITRE T1078). This can help prevent attacks originating from known malicious regions.

2. Regularly audit and revoke SSH keys, especially in cases where suspicious key usage has been detected (MITRE T1552). Enforcing regular rotation of SSH keys can also help maintain the security of your systems.

3. Implement a rate limiting mechanism for SSH login attempts to reduce the likelihood of successful brute-force attacks (MITRE T1110.001). This can be achieved by configuring fail2ban or similar tools that automatically block IP addresses after a certain number of failed login attempts within a specific timeframe.

4. Monitor outbound traffic for large data transfers and investigate the cause when such events occur (MITRE T1041). Implementing network monitoring tools can help detect anomalous outbound traffic patterns.

5. Educate users about the risks associated with SSH attacks and best practices for securing their accounts. This includes advice on creating strong passwords, enabling MFA, and being cautious when receiving unsolicited emails or messages that may contain links to phishing sites.

⌚ Entity Memory:
IPs: 10.2.4.9, 10.1.1.9, 10.22.3.9
OS: RedHat 8, Ubuntu 22
Hostname: SRV-LNX-12, SRV-APP2, SRV-DB01
MITRE: T1046, T1041, T1071, T1110.001, T1078, T1552
Severity: Critical, High

⌚ Threat Enrichment:
• T1110.001: Brute Force - Common credential attack, implement rate limiting & MFA
• IP 10.2.4.9: Internal network (check for lateral movement)
• IP 10.1.1.9: Internal network (check for lateral movement)
• IP 10.22.3.9: Internal network (check for lateral movement)
• Ubuntu 22: Review /var/log/auth.log, enable auditd

⚠ Threat Score: 100/100 (Risk Level: CRITICAL)
Factors: Severity=Critical (+40), Severity=High (+30), MITRE T1046 (+10)

📊 Structured Output Available (JSON): 2573 chars

💬 Session: 2 exchanges for analyst42
```

QUERY 3: BONUS - Hybrid Retrieval with Exact Match

```
=====
👤 Analyst ID: analyst42
🔍 Query: Find incidents on host WKS-22
=====

⌚ Processing with Vector RAG...
=====

⌚ SOC ANALYST RESPONSE:
Based on the provided context of past security incidents and entity memory, I have identified several actionable recommendations to improve your organization's security posture:

1. Implement a network intrusion detection system (NIDS) or host-based intrusion prevention system (HIPS) to monitor for and alert on suspicious activities such as port scanning (MITRE T1046). This can help detect potential reconnaissance activities before they escalate into more serious attacks.

2. Configure firewalls to block outbound traffic from high-risk ports, especially when large data transfers have been detected (MITRE T1041). Implementing network monitoring tools can help detect anomalous outbound traffic patterns and alert on potential data exfiltration attempts.

3. Regularly audit and revoke SSH keys, especially in cases where suspicious key usage has been detected (MITRE T1552). Enforcing regular rotation of SSH keys can also help maintain the security of your systems.

4. Implement a rate limiting mechanism for SSH login attempts to reduce the likelihood of successful brute-force attacks (MITRE T1110.001). This can be achieved by configuring fail2ban or similar tools that automatically block IP addresses after a certain number of failed login attempts within a specific timeframe.

5. Implement IP reputation services or blocklists to automatically block known malicious IP addresses (MITRE T1078). This can help prevent attacks originating from known malicious regions.

6. Educate users about the risks associated with SSH attacks and best practices for securing their accounts. This includes advice on creating strong passwords, enabling MFA, and being cautious when receiving unsolicited emails or messages that may contain links to phishing sites.

Regarding incidents on host WKS-22, I could not find any specific incidents in the provided context. However, it is important to regularly monitor hosts for suspicious activities and implement the recommended security measures to maintain a proactive security posture.

⌚ Entity Memory:
IPs: 172.22.9.54
OS: RedHat 8, Windows 11
Hostname: SRV-APP2, WKS-64, SRV-WIN-02
MITRE: T1046, T1041, T1552, T1110.001, T1078, T1053, T1090
Severity: Critical, Medium, High

⌚ Threat Enrichment:


- T1110.001: Brute Force - Common credential attack, implement rate limiting & MFA
- IP 172.22.9.54: External source (recommend block at perimeter)
- Windows 11: Enable Windows Defender ATP, check Event IDs 4624/4625



⚠ Threat Score: 100/100 (Risk Level: CRITICAL)
Factors: Severity=Critical (+40), Severity=Medium (+15), Severity=High (+30)

📊 Structured Output Available (JSON): 2736 chars
💬 Session: 3 exchanges for analyst42
=====
```

QUERY 4: BONUS - Entity Memory Accumulation

```
⌚ Analyst ID: analyst42
🔍 Query: Show me ransomware incidents

=====
⌚ Processing with Vector RAG...

🧠 SOC ANALYST RESPONSE:
Based on the provided context of past security incidents and entity memory, I have identified several actionable recommendations to help prevent and respond to ransomware attacks:

1. Implement a network intrusion detection system (NIDS) or host-based intrusion prevention system (HIPS) to monitor for and alert on suspicious activities such as port scanning (MITRE T1046). This can help detect potential reconnaissance activities before they escalate into more serious attacks, including ransomware.

2. Regularly back up critical data and test the recovery process to ensure that it is working correctly (MITRE T1486). In the event of a ransomware attack, having a reliable backup can help minimize downtime and reduce the impact on your organization.

3. Implement email filtering solutions to block phishing emails containing malicious attachments or links (MITRE T1566). Educate users about the risks associated with opening suspicious emails and the importance of not clicking on links or downloading attachments from unknown sources.

4. Configure firewalls to block outbound traffic from high-risk ports, especially when large data transfers have been detected (MITRE T1041). Implementing network monitoring tools can help detect anomalous outbound traffic patterns and alert on potential data exfiltration attempts.

5. Regularly audit and revoke SSH keys, especially in cases where suspicious key usage has been detected (MITRE T1552). Enforcing regular rotation of SSH keys can also help maintain the security of your systems.
```

6. Implement a rate limiting mechanism for SSH login attempts to reduce the likelihood of successful brute-force attacks (MITRE T1110.001). This can be achieved by configuring fail2ban or similar tools that automatically block IP addresses after a certain number of failed login attempts within a specific timeframe.

7. Implement IP reputation services or blocklists to automatically block known malicious IP addresses (MITRE T1078). This can help prevent attacks originating from known malicious regions.

In the case of ransomware incidents, it is crucial to have an incident response plan in place. The resolution steps for each incident may vary, but some common steps include:

- * Isolating the affected host(s) to prevent further spread (as seen in Incident #003).
- * Triggering the incident response plan (as seen in Incident #003).
- * Restoring from backup (as seen in Incident #003).
- * Performing malware analysis and cleaning the environment (as seen in Incident #006).

⌚ Entity Memory:

OS: Ubuntu 22, Windows 10

Hostname: LAB-07, FIN12, WKS-11

MITRE: T1046, T1041, T1091, T1552, T1566, T1110.001, T1078, T1486, T1053, T1059.006

Severity: Critical, Medium, High

🛡 Threat Enrichment:

- T1110.001: Brute Force - Common credential attack, implement rate limiting & MFA
- T1486: Data Encrypted for Impact (Ransomware) - CRITICAL: Isolate immediately
- T1059.006: Command/Script Interpreter - Monitor PowerShell/bash execution
- Ubuntu 22: Review /var/log/auth.log, enable auditd
- Windows 10: Enable Windows Defender ATP, check Event IDs 4624/4625

⚠ Threat Score: 100/100 (Risk Level: CRITICAL)

Factors: Severity=Critical (+40), Severity=Medium (+15), Severity=High (+30)

📊 Structured Output Available (JSON): 3269 chars

💬 Session: 4 exchanges for analyst42

=====

QUERY 5: BONUS - Threat Score Calculation

👤 Analyst ID: analyst42
🔍 Query: Analyze the threat level of credential dumping attacks

=====

⌚ Processing with Vector RAG...

⌚ SOC ANALYST RESPONSE:

Based on the provided context of past security incidents and entity memory, I have identified several actionable recommendations to help prevent and respond to credential dumping attacks:

1. Implement a network intrusion detection system (NIDS) or host-based intrusion prevention system (HIPS) to monitor for and alert on suspicious activities such as port scanning (MITRE T1046). This can help detect potential reconnaissance activities before they escalate into more serious attacks, including credential dumping.
2. Regularly audit and revoke SSH keys, especially in cases where suspicious key usage has been detected (MITRE T1552). Enforcing regular rotation of SSH keys can also help maintain the security of your systems.
3. Implement a rate limiting mechanism for SSH login attempts to reduce the likelihood of successful brute-force attacks (MITRE T1110.001). This can be achieved by configuring fail2ban or similar tools that automatically block IP addresses after a certain number of failed login attempts within a specific timeframe.
4. Implement IP reputation services or blocklists to automatically block known malicious IP addresses (MITRE T1078). This can help prevent attacks originating from known malicious regions.
5. Educate users about the risks associated with credential dumping and best practices for securing their accounts. This includes advice on creating strong passwords, enabling MFA, and being cautious when receiving unsolicited emails or messages that may contain links to phishing sites.

In the case of credential dumping incidents, it is crucial to have an incident response plan in place. The resolution steps for each incident may vary, but some common steps include:

- * Isolating the affected host(s) to prevent further spread (as seen in Incident #033).
- * Terminating the process responsible for credential dumping (as seen in Incident #033).
- * Performing memory analysis to identify any additional malware or compromised accounts (as seen in Incident #033).
- * Revoking privileges, rotating credentials, and monitoring user actions when privilege escalation attempts have been detected (as seen in Incident #005).
- * Revoking DB access and rotating DB keys when unauthorized DB dump attempts have been detected (as seen in Incident #013).
- * Throttling login attempts and enabling MFA when spikes in failed login attempts have been detected (as seen in Incident #008).

⌚ Entity Memory:
OS: RedHat 8, Windows 10
Hostname: SRV-DB03, SRV-APP2, WKS-98
MITRE: T1046, T1068, T1110.001, T1003, T1005, T1078, T1110, T1552
Severity: Medium, High

🛡 Threat Enrichment:

- T1068: Exploitation for Privilege Escalation - Patch systems urgently
- T1110.001: Brute Force - Common credential attack, implement rate limiting & MFA
- T1003: OS Credential Dumping - Domain compromise likely, rotate credentials
- T1110: Brute Force - Common credential attack, implement rate limiting & MFA
- Windows 10: Enable Windows Defender ATP, check Event IDs 4624/4625

⚠ Threat Score: 100/100 (Risk Level: CRITICAL)
Factors: Severity=Medium (+15), Severity=High (+30), MITRE T1046 (+10)

📊 Structured Output Available (JSON): 3072 chars

💬 Session: 5 exchanges for analyst42

QUERY 6: BONUS - Full JSON Output Display

```
=====
👤 Analyst ID: analyst42
🔍 Query: What PowerShell attacks have we seen?

=====
⌚ Processing with Vector RAG...

👤 SOC ANALYST RESPONSE:
Based on the provided context of past security incidents and entity memory, I have identified several PowerShell-related attacks that your organization has encountered:

1. Encoded command detection (T1059): This technique involves using PowerShell to execute encoded commands, which can be used for various malicious purposes such as downloading and executing additional payloads or exfiltrating data. Resolution steps include terminating the process responsible for the encoded command, disabling PowerShell v2, and quarantining any related artifacts (as seen in Incident #002).

2. PowerShell Empire beacon (T1090): This technique involves using PowerShell to establish a persistent backdoor on a compromised host, allowing an attacker to maintain access for future activities. Resolution steps include isolating the affected host and removing any persistence mechanisms (as seen in Incident #025).

3. PowerShell IEX download command (T1059.001): This technique involves using PowerShell's IEX cmdlet to download and execute a script from a remote location, which can be used for various malicious purposes such as installing additional malware or exfiltrating data. Resolution steps include killing the process responsible for the download command, quarantining the related file, and blocking the domain from which the script was downloaded (as seen in Incident #009).

4. Obfuscated JavaScript execution (T1059.007): This technique involves using obfuscated JavaScript to execute malicious code on a compromised host. Resolution steps include blocking the JavaScript and investigating the source of the file (as seen in Incident #039).

To prevent similar PowerShell attacks, I recommend implementing the following actionable recommendations:
```

1. Implement a network intrusion detection system (NIDS) or host-based intrusion prevention system (HIPS) to monitor for and alert on suspicious PowerShell activities such as encoded commands, downloads, and executions (MITRE T1059, T1059.001).
2. Configure PowerShell to require user approval for scripts from unknown sources (as seen in Incident #039).
3. Implement IP reputation services or blocklists to automatically block known malicious IP addresses (MITRE T1078). This can help prevent attacks originating from known malicious regions.
4. Educate users about the risks associated with PowerShell attacks and best practices for securing their systems, such as enabling MFA, creating strong passwords, and being cautious when receiving unsolicited emails or messages that may contain links to phishing sites.

⌚ Entity Memory:

OS: Windows 10, Windows 11

Hostname: WKS-64, WKS-22, WKS-81

MITRE: T1059.001, T1059.007, T1078, T1059, T1090

Severity: Critical, High

🛡 Threat Enrichment:

- T1059.001: Command/Script Interpreter - Monitor PowerShell/bash execution
- T1059.007: Command/Script Interpreter - Monitor PowerShell/bash execution
- T1059: Command/Script Interpreter - Monitor PowerShell/bash execution
- Windows 10: Enable Windows Defender ATP, check Event IDs 4624/4625
- Windows 11: Enable Windows Defender ATP, check Event IDs 4624/4625

⚠ Threat Score: 100/100 (Risk Level: CRITICAL)

Factors: Severity=Critical (+40), Severity=High (+30), MITRE T1059.001 (+10)

💡 Structured Output Available (JSON): 3134 chars

💬 Session: 6 exchanges for analyst42

=====

QUERY 7: Different User - Session Isolation and EXIT

```
=====
👤 Analyst ID: new_analyst
🔍 Query: Show me privilege escalation incidents

=====
🕒 Processing with Vector RAG...

⌚ SOC ANALYST RESPONSE:
Based on the retrieved context of privilege escalation incidents, here are some actionable recommendations to enhance security measures:

1. Implement Multi-Factor Authentication (MFA): To prevent unauthorized access and reduce the risk of privilege escalation attempts, consider implementing MFA for all users across Windows and Linux platforms. This will add an extra layer of security by requiring users to provide two or more verification factors to gain access. (MITRE: T1185)

2. Regularly Review and Monitor System Privileges: Keep a close eye on system privileges, especially for high-risk users or administrators. Regular audits can help identify any unusual changes in user permissions that might indicate privilege escalation attempts. (MITRE: T1068)

3. Limit User Privileges: By default, users should be granted the least privilege necessary to perform their job functions. Implementing the principle of least privilege (PoLP) can help minimize the potential impact of a successful privilege escalation attempt. (MITRE: T1078)

4. Enforce Strong Password Policies: Strengthen password policies by requiring complex, unique passwords and enforcing regular password changes. This can make it more difficult for attackers to gain access through brute force or credential reuse attacks. (MITRE: T1078)

5. Monitor Scheduled Tasks: Regularly review scheduled tasks on Windows systems to detect any malicious or unexpected activities. If a suspicious task is found, investigate its parent process and remove it if necessary. (MITRE: T1053)
```

```
6. Secure the sudoers File: On Linux systems, ensure that the sudoers file is properly secured and regularly reviewed for any unusual or unauthorized changes. This can help prevent unauthorized access and privilege escalation through sudo usage. (MITRE: T1053)

7. Implement User Lockout Policies: To protect against brute-force attacks, implement user lockout policies that limit the number of failed login attempts before locking the account. This can help prevent attackers from repeatedly trying to guess passwords or exploit weak credentials. (MITRE: T1110)

8. Alert Rule Creation: Create alert rules for frequent failed sudo attempts, as this could indicate a potential brute-force attack or an attempt to gain unauthorized access. (MITRE: T1110)
```

```
🔍 Entity Memory:
OS: Ubuntu 18, Windows 11
Hostname: SRV-LNX-05, WKS-77, DEV-01
MITRE: T1185, T1068, T1078, T1110, T1053
Severity: Medium, High
```

```
🛡 Threat Enrichment:
• T1068: Exploitation for Privilege Escalation - Patch systems urgently
• T1110: Brute Force - Common credential attack, implement rate limiting & MFA
• Ubuntu 18: Review /var/log/auth.log, enable auditd
• Windows 11: Enable Windows Defender ATP, check Event IDs 4624/4625
```

```
⚠ Threat Score: 100/100 (Risk Level: CRITICAL)
Factors: Severity=Medium (+15), Severity=High (+30), MITRE T1185 (+10)
```

```
📊 Structured Output Available (JSON): 2820 chars
```

```
🔍 Entity Memory:  
OS: Ubuntu 18, Windows 11  
Hostname: SRV-LNX-05, WKS-77, DEV-01  
MITRE: T1185, T1068, T1078, T1110, T1053  
Severity: Medium, High  
  
🛡 Threat Enrichment:  
• T1068: Exploitation for Privilege Escalation - Patch systems urgently  
• T1110: Brute Force - Common credential attack, implement rate limiting & MFA  
• Ubuntu 18: Review /var/log/auth.log, enable auditd  
• Windows 11: Enable Windows Defender ATP, check Event IDs 4624/4625
```

```
⚠ Threat Score: 100/100 (Risk Level: CRITICAL)  
Factors: Severity=Medium (+15), Severity=High (+30), MITRE T1185 (+10)
```

```
📊 Structured Output Available (JSON): 2820 chars
```

```
💬 Session: 1 exchanges for new_analyst  
=====
```

```
👤 Analyst ID: exit
```

```
✓ Exiting SOC RAG Assistant...
```

```
✓ Stay vigilant! 🔒
```

```
(.venv) C:\Users\User\Desktop\mockmock>
```

