Task 2 – Enhanced Offline SIEM AI Agent Report

1. Overview
This enhanced offline SIEM AI agent demonstrates how an AI-powered SOC assistant can analyze logs, detect threat intents, and trigger automated security playbooks — all without requiring internet connectivity. The agent simulates real SOC workflows and enhances accuracy, consistency, and response speed.

2. Agent Capabilities
• Offline ML-based intent classification (failed login, malware, suspicious IP, brute force, etc.)
• YAML-based automated playbook execution
• Log analysis for repeated login failures and malicious IP extraction
• Realistic SOC-style response messages
• 100% offline execution for high-security environments

3. Architecture Diagram

User Input
↓
Intent Classifier (Offline ML)
↓
Playbook Engine (YAML)
↓
Log Analyzer
↓
Final SOC Response

4. Intent Categories

Intent	Description	Playbook Triggered
failed login	Multiple authentication failures	Lock account, check source IP
malware detected	Malware indicators identified	Isolate host, run AV scan
suspicious IP	Untrusted IP activity	Block IP, notify SOC
brute force	Rapid repeated login attempts	Block IP + lock account

5. Example Interaction Transcript

Analyst> analyze logs

Log Summary:

• Failed Login Attempts: 27

• Unique Source IPs: 5

• Suspicious IPs: 45.77.23.19

■ **Potential Brute Force Detected**

Recommended Response:

1. Lock affected accounts

2. Block IP 45.77.23.19

3. Notify Tier-2 SOC

6. Why Offline?

• No sensitive data leaves SOC perimeter
• Works even without internet (critical for secure environments)
• Compliant with BFSI, Healthcare, and Government regulations
• Zero cloud dependency increases reliability

7. Conclusion
The enhanced offline SIEM agent demonstrates practical SOC automation with ML intent detection, log processing, and YAML-driven playbooks. It aligns perfectly with SIEM workflows and shows strong understanding of cybersecurity automation and AI-based threat detection.