AI Security Assistant Agent — SOC Case Study Report

Prepared by: Abdul Rehman| Role: SOC Analyst (Aspiring)| Date: December 2025

Executive Summary

This project focuses on building an AI-based Security Assistant Agent designed to support Security Operations Center (SOC) activities. The system automates log analysis, detects potential threats, and generates structured incident reports. The goal is to simulate a real SOC workflow using modern AI agent architecture.

Project Objective

The objective of this project is to design a system capable of analyzing raw security logs, identifying suspicious activities, and producing actionable insights similar to a Tier 1 SOC Analyst.

System Architecture

The system is built using a multi-agent workflow:

- Log Parser: Extracts important data such as IP addresses, failed login attempts, an suspicious keywords.
- Detector Agent: Identifies anomalies and possible threats.
- Analyst Agent: Converts findings into a clear incident report.
- Orchestrator: Manages the workflow and ensures smooth data flow between components.

Methodology

The workflow begins with raw log input, which is processed by the parser. The extracted data is analyzed by the Detector Agent to identify threats. The Analyst Agent then generates a human-readable report, and the Orchestrator compiles the final output.

Tools & Technologies

Python for log processing, Google ADK for agent development, and Kaggle Notebook for execution and testing.

Sample Incident Analysis

During testing, multiple failed login attempts were detected from IP address 192.168.1.10. The system flagged this as a potential brute-force attack based on repeated authentication failures and suspicious keywords such as 'unauthorized access'.

SOC Output

The system generated a structured report including:
- Indicators of Compromise (IOC): Suspicious IP
- Threat Type: Brute-force attack
- Severity Level: High (Potential Brute-Force Attack)
- Recommendation: Block the IP address and enable multi-factor authentication.

Practical Relevance

This project reflects real SOC responsibilities such as monitoring logs, identifying threats, and documenting incidents. It demonstrates the ability to apply AI in cybersecurity operations.

Conclusion

The project successfully demonstrates how AI agents can automate security analysis tasks. It highlights practical SOC skills and provides a foundation for advanced security automation systems.

Incident Timeline

- 10:02 AM – Multiple failed login attempts detected
- 10:03 AM – Suspicious IP flagged (192.168.1.10)
- 10:04 AM – Detector Agent triggered alert
- 10:05 AM – Analyst Agent generated report
- 10:06 AM – Final SOC report completed

Indicators of Compromise (IOCs)

- IP Address: 192.168.1.10
- Activity: Repeated failed login attempts
- Keyword: "unauthorized access"
- Behaviour: Brute-force pattern detected

Recommended Actions

- Block the suspicious IP address
- Enable multi-factor authentication (MFA)
- Monitor login attempts for similar patterns
- Update firewall rules

Appendix – Supporting Evidence

- Kaggle Notebook:
https://www.kaggle.com/code/shaikcyber66/capstone-ai-security-assistant-agent/notebook

- Certificate:
https://www.kaggle.com/certification/badges/shaikcyber66/105

- Note: https://notebooklm.google.com/notebook/892594ab-77e7-4cad-a1af-387e7b9ee031