**https://www.kaggle.com/code/rav1ndra/notebookb72d17fd5d/edit/run/234871787**

**AI SOC Analyst Assistant (Text Gen + Reasoning)**

**What it does:** Takes in cybersecurity alerts/logs and explains them in simple language, recommends next steps.  
**Tech Used:** GPT/Gemini + LangChain tools  
**Innovation Angle:** Useful in real-world SOC operations, demo MITRE ATT&CK mapping with LLM logic.

**Capstone Project Documentation: AI SOC Analyst Assistant using Gemini API**

**Project Title:** AI SOC Analyst Assistant: Leveraging Generative AI for Cybersecurity Alert Triage

**Author:** [RRR]  
**Platform:** Kaggle (Capstone - GenAI Intensive Course 2025Q1)  
**Date:** April 2025

**1. Project Overview**

The "AI SOC Analyst Assistant" is a generative AI agent designed to assist cybersecurity analysts in Security Operations Centers (SOCs). The goal of this capstone project is to leverage modern Large Language Models (LLMs), specifically Google Gemini, to analyze raw security logs and generate structured, contextual, and actionable insights.

This project demonstrates the practical application of generative AI in a high-stakes domain such as cybersecurity by:

* Parsing and understanding complex log entries
* Producing structured summaries
* Mapping incidents to MITRE ATT&CK techniques
* Suggesting relevant response actions
* Using Retrieval-Augmented Generation (RAG) to simulate an agent with memory

**2. Capstone Requirements Satisfied**

This solution fulfills multiple required GenAI capabilities:

1. **Few-shot Prompting**: Used to guide the Gemini model with examples of logs, summaries, and actions.
2. **Structured Output / Controlled Generation**: Prompts explicitly format outputs into summary, MITRE technique, and actions.
3. **Retrieval-Augmented Generation (RAG)**: Employs FAISS vector search to provide historical log context to the model.
4. **Agents**: Simulated reasoning behavior by prompting Gemini to analyze logs with contextual data.

**3. Dataset and Input**

The dataset used is a sample CSV file (cybersecurity\_attacks.csv) uploaded to Kaggle. It contains simulated SOC alert logs with fields such as:

* source\_ip, destination\_ip
* user, event, command\_line
* timestamp, etc.

Each row is treated as a unique security event to be analyzed.

**4. Technical Architecture**

**Tools Used:**

* **Google Gemini Pro API** (via google.generativeai Python SDK)
* **Kaggle Secrets** to securely manage API keys
* **FAISS + TF-IDF Vectorizer** for similarity search (RAG)
* **Pandas** for data handling

**Main Components:**

1. **Gemini Summarizer Function:**
   * Takes a raw log as input
   * Uses few-shot prompting to produce:
     + Human-readable summary
     + MITRE ATT&CK technique
     + Suggested remediation actions
2. **RAG Search:**
   * Embeds all logs using TF-IDF
   * Uses FAISS to find top-k similar logs
   * Supplies these as context to Gemini
3. **Agent Reasoning Prompt:**
   * Combines log + RAG context
   * Gemini analyzes and infers high-level security observations

**5. Example Workflow**

**Input Log:**

User: jsmith

Command: powershell -enc JAB...

Event: Obfuscated PowerShell command

**Gemini Output:**

Summary: User 'jsmith' executed a suspicious obfuscated PowerShell command.

MITRE: T1059.001 (Command and Scripting Interpreter - PowerShell)

Actions: Review execution history, isolate the system, scan for persistence mechanisms.

**Agent Reasoning (with RAG Context):**

Based on historical logs with similar PowerShell activity, this could indicate initial access or lateral movement. Recommend isolating host, checking AD authentication, and searching for privilege escalation attempts.

**6. Security & Best Practices**

* **No hardcoded secrets**: API key is securely retrieved using Kaggle Secrets.
* **Stateless design**: No sensitive data is persisted.
* **Modular notebook**: Functions separated for clarity, debugging, and reuse.

**7. Limitations & Future Work**

**Limitations:**

* Requires Gemini API access and proper key setup
* Logs are simulated; real-world data may vary significantly
* No external threat intelligence APIs integrated yet

**Future Enhancements:**

* Integrate MITRE ATT&CK JSON database for structured lookups
* Add visualization dashboards (Streamlit or Plotly)
* Include external document/pdf understanding for incident reports
* Extend to support multi-modal inputs (screenshots, configs)

**8. Conclusion**

This project illustrates how Generative AI, particularly Gemini, can transform security operations. By turning raw alert data into contextual intelligence, the AI SOC Analyst Assistant bridges the gap between signal and decision, offering scalable support for real-world cybersecurity teams.