Introduction

Objective:

- The goal of this project is to develop a system that uses large language models (LLMs) to translate complex Intrusion Detection System (IDS) alerts into plain language that non-experts can easily understand.

- This will enable broader awareness and quicker response to potential security threats within organizations, even by those who may not have a deep technical background.

Issue:

- Logs are difficult to read and not outputted in a user-frienfly manner.

Oct 22, 2020	event.dataset	Message
		ents":{"added":3,"done":3},"harvester":{"closed":1,"files":{"56a95aa9-536c-4be3-8864-0c5efc146e6b":{"last_event_published_time":"2020-10-23T03:49:43.721Z","last_event_timestamp":"2020-10-23T03:49:38.720Z","read_offset":1437,"size":1247}},"open_files":2,"running":2}},"libbeat":{"config":{"module":{"running":1}},"output":{"events":{"acked":2,"batches":2,"total":2},"read":{"bytes":12},"write":{"bytes":2052}},"pipeline":{"clients":3,"events":{"active":0,"filtered":1,"published":2,"total":3},"queue":{"acked":2}}},"registrar":{"states":{"current":4,"update":3},"writes":{"success":3,"total":3}},"system":{"load":{"1":0,"15":0.03,"5":0.04,"norm":{"1":0,"15":0.015,"5":0.02}}}}}}
22:50:38.723	system.syslog	Oct 23 03:50:31 straw-server filebeat[1483]: 2020-10-23T03:50:31.743Z#011INFO#011[monitoring]#011log/log.go:145#011Non-zero metrics in the last 30s#011{"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":570,"time":{"ms":2}},"total":{"ticks":1880,"time":{"ms":13},"value":1880},"user":{"ticks":1310,"time":{"ms":11}}},"handles":{"limit":{"hard":4096,"soft":1024},"open":13},"info":{"ephemeral_id":"75e1c01a-4cf1-4133-9494-f7a7c545ee3e","uptime":{"ms":480237}},"memstats":{"gc_next":21600080,"memory_alloc":20337216,"memory_total":171655616},"runtime":{"goroutines":60}},"filebeat":{"events":{"added":1,"done":1},"harvester":{"files":{"56a95aa9-536c-4be3-8864-0c5efc146e6b":{"last_event_published_time":"2020-10-23T03:50:08.722Z","last_event_timestamp":"2020-10-23T03:50:03.722Z","read_offset":1271,"size":1461}},"open_files":2,"running":

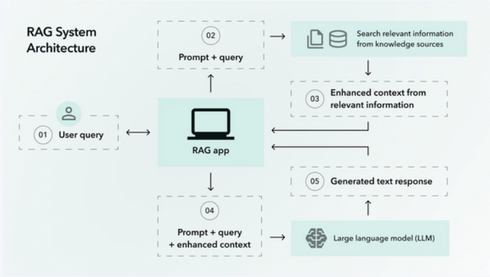
Goal:

- Create a chat bot that translates complex IDS alerts into easy-to-understand language for non-technical users by using an open-source large language model(LLM) deployed locally.

Procedure

- We plan to use Retrieval Augmented Generation (RAG).

- By using domain-specific data, RAG helps the LLM generate more precise and user-friendly outputs tailored to the specific needs of the domain



- Using libraries like QLoRA we can fine-tune the LLM on consumer grade systems to fit within limited hardware resources.

Techniques used:

- **Page Optimizers**: Manage memory efficiently by swapping data between GPU and CPU as needed, helping to handle larder modern models than would fit in GPU memory alone.

- **Single/Double Quantization**: reduces the precision of the model weights (8-bit to lower), significantly decreasing memory usage and allowing for efficient training on less powerful hardware

Results

Example

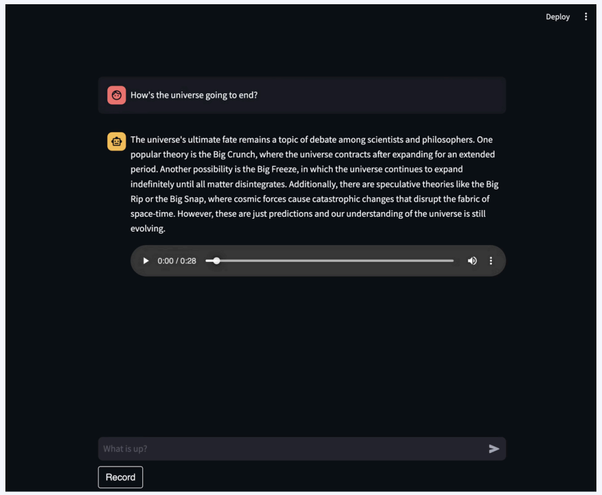
- 2024-09-15 14:32:45 [INFO] - User login attempt failed. Username: jdoe, IP: 192.168.1.100, Reason: Incorrect password

User Interface:

- A front-end user interface will also be implemented to provide a user-friendly experience, rather than just providing a console output.

- The expectation is to host this user interface on a web server, with the LLM connected to it, which then interacts with the database.

Example Interface:



- The interface will include the ability to search for specific alerts and display outputs of existing logs from a SIEM solution in a way that is understandable to the user.