MITRE ATT&CK Driven Threat Hunting Automated by Local LLM

Fujitsu Defense & National Security

Jun Miura

Toshitaka Satomi

Eri Miura

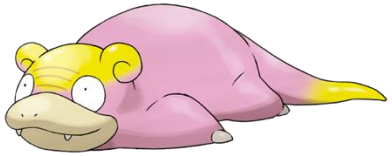
Agenda

- Introduction
- Our Concepts
- Demo
- Key Points

Introduction

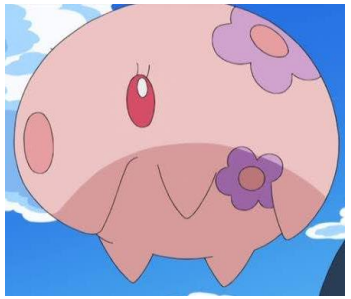
Who are we?

- Jun Miura (LinkedIn: jyadon-sec)
  - Offensive security researcher @Fujitsu Defense & National Security Limited
  - Experienced penetration tester and red teamer
  - OSCP, OSWP, GPEN, CARTP



- Toshitaka Satomi (LinkedIn: stmtstk)
  - Security researcher @ Fujitsu Defense & National Security Limited
  - Cyber Threat Intelligence (CTI) researcher
  - CISSP

- Eri Miura (LinkedIn: ereborn)
  - AI engineer @ Fujitsu Defense & National Security Limited
  - Developer of LLM and other generative AI application



Motivations

FUJITSU

- Modern cyber attacks are becoming more complex and sophisticated.
  - It is difficult to detect and prevent all threats using security solutions such as EDR.
- Threat hunting is becoming more important.
  - Threat hunting is a proactive approach to identifying undetected threats within an organization's environment.
  - There are some challenges related to threat hunting.
    - Various proposed ways to perform threat hunting
    - Necessity of advanced skills

Our proposal: "MITRE ATT&CK Driven Threat Hunting"

Our Concepts

MITRE ATT&CK Driven Threat Hunting

FUJITSU

- One of the goals is to create hunting rules from MITRE ATT&CK.

ATT&CK®

Extract critical TTPs for the environment

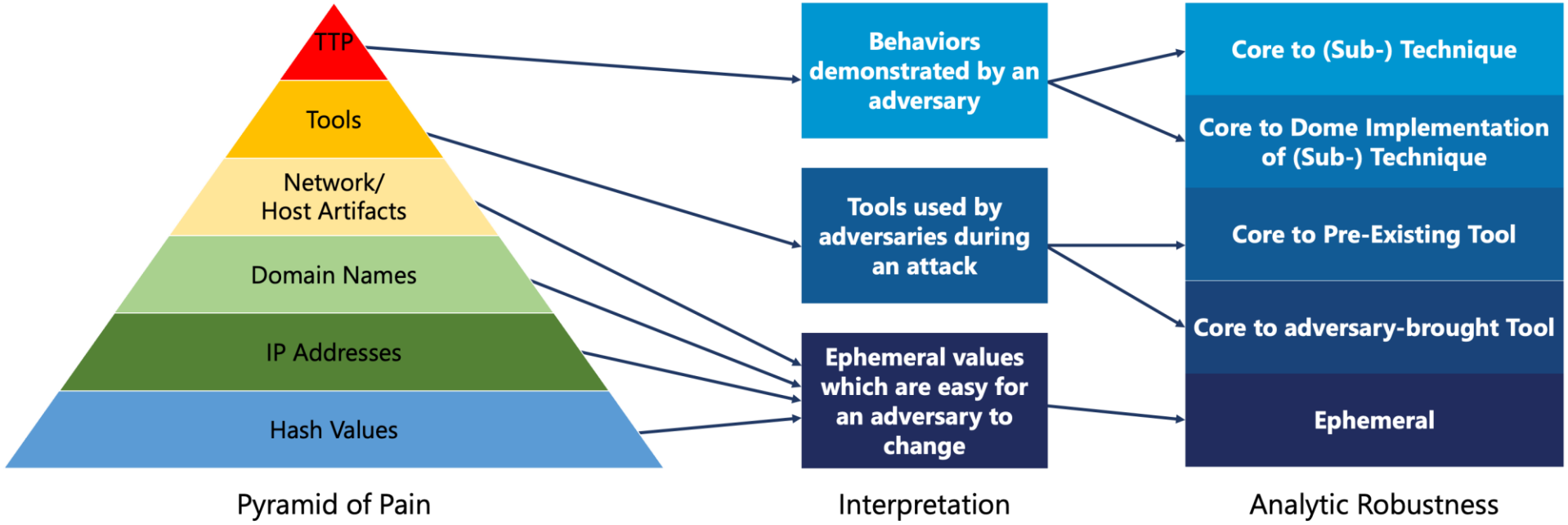
Create hunting rules

Sigma SIEM Detection Format splunk> elasticsearch

Summiting the Pyramid (StP)

FUJITSU

- Our threat hunting method is based on the concept of StP.
- "Create and apply a methodology to evaluate the dependencies inside analytics and make them more robust by focusing on adversary behaviors." (*)



(*): https://ctid.mitre.org/projects/summiting-the-pyramid

StP and Threat Hunting

FUJITSU

- StP can define the threat hunting levels from 1 to 5.
- The higher the level, the more false positives are detected, making it necessary to have more sensitive information for accurate threat hunting.

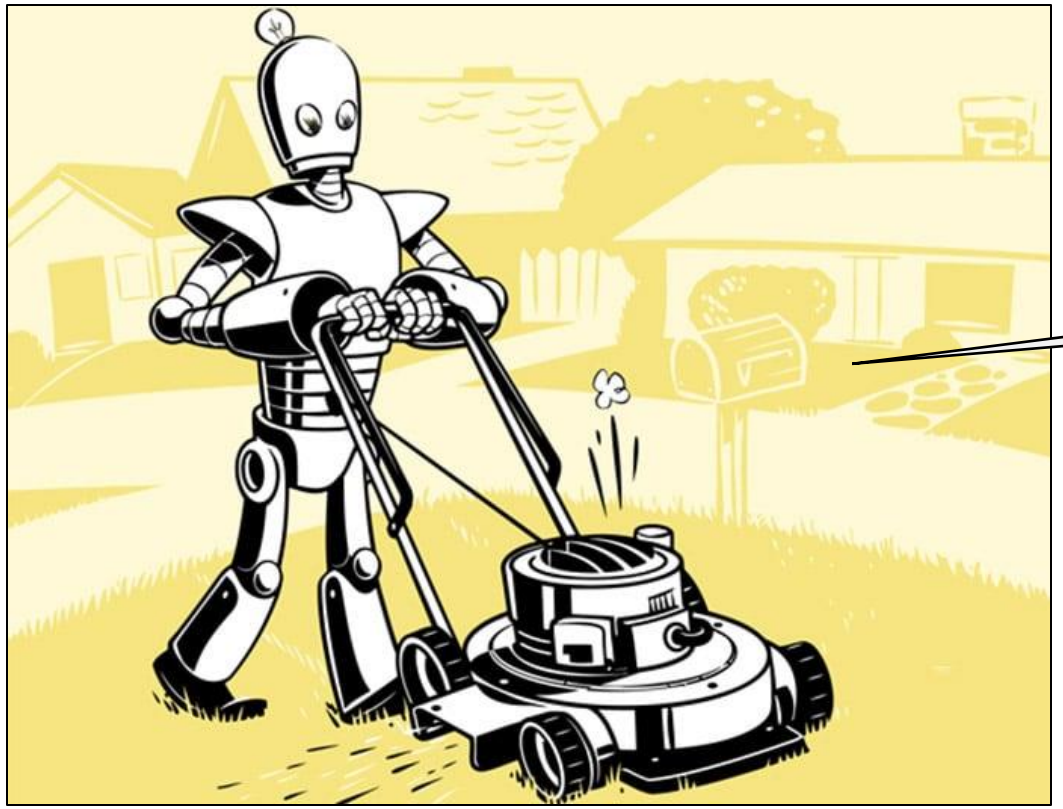
Our target, it takes long time to create

Level	Source	Description
5	Core to (Sub-) Technique	Observables associated with “chokepoints” or “invariant behaviors” of the (Sub-)Technique, unavoidable by any implementation.
4	Core to Dome Implementation of (Sub-) Technique	Observables associated with low-variance behaviors of the (Sub-) Technique, unavoidable without a substantially different implementation.
3	Core to Pre-Existing Tool	Observables associated with tools available to the defenders before adversary use and difficult for an adversary to modify.
2	Core to adversary-brought Tool	Observables which are associated with tools that are brought in by an adversary to accomplish an attack.
1	Ephemeral	Observables that are trivial for an adversary to change, or that change even without adversary intervention.

Using Large Language Model (LLM)

FUJITSU

- Threat Hunting has a lot of steps…
- Human resources, time, money…



Automating the boring stuff with ~~**Python**~~ **LLM**.
Human concentrate on only interesting things!

Automation by “Local” LLM

FUJITSU

- There are some concerns about using LLM.

Cost

Security Risk

Sensitive Information

Local LLM working on the CPU only machine

Technical Solutions

FUJITSU

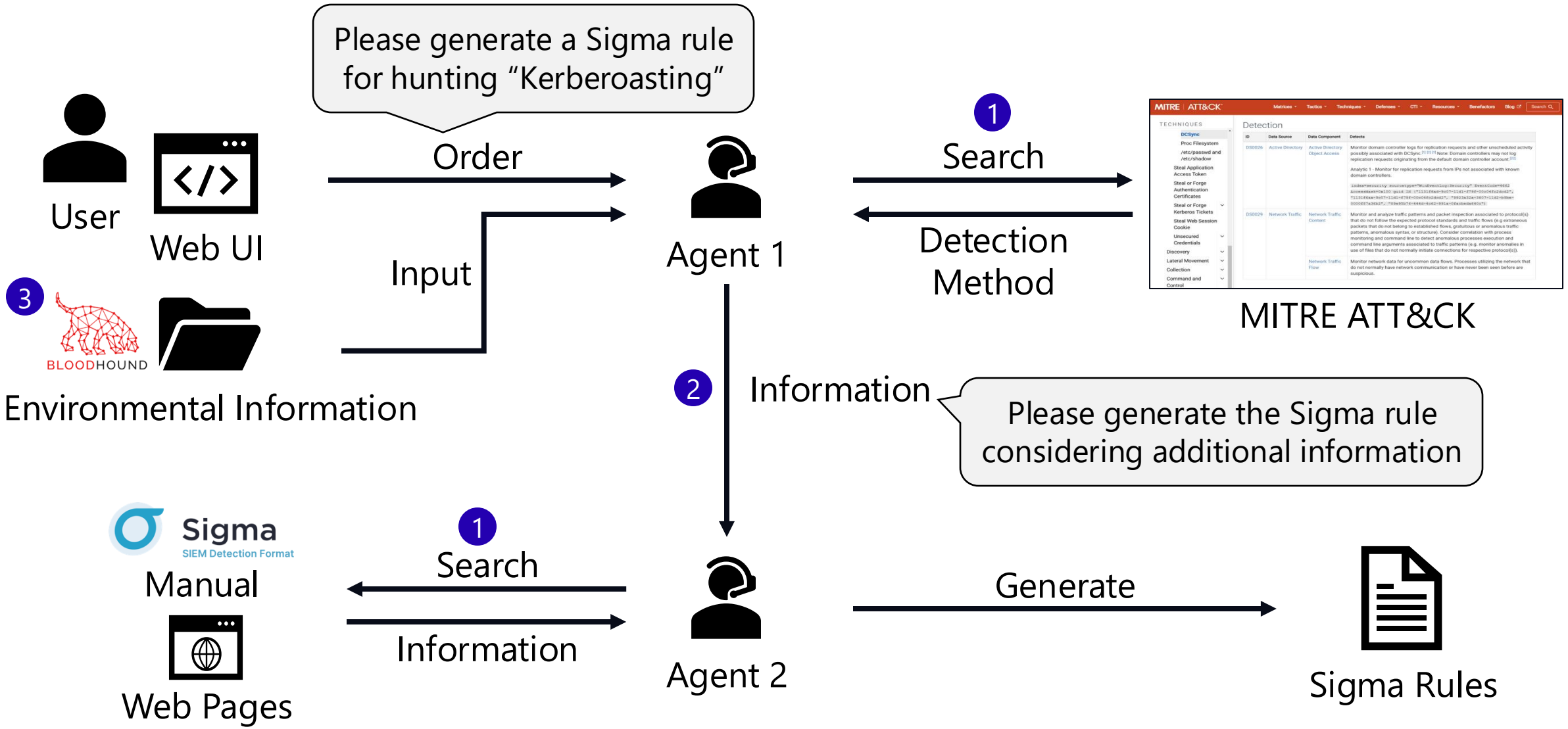
Challenges

- Use the Latest and Correct Information
- Scalable System
- More Practical Outputs

Solutions

1. Retrieval-Augmented Generation (RAG)
2. Multi-Agent System
3. Environmental Information

Generation Flow

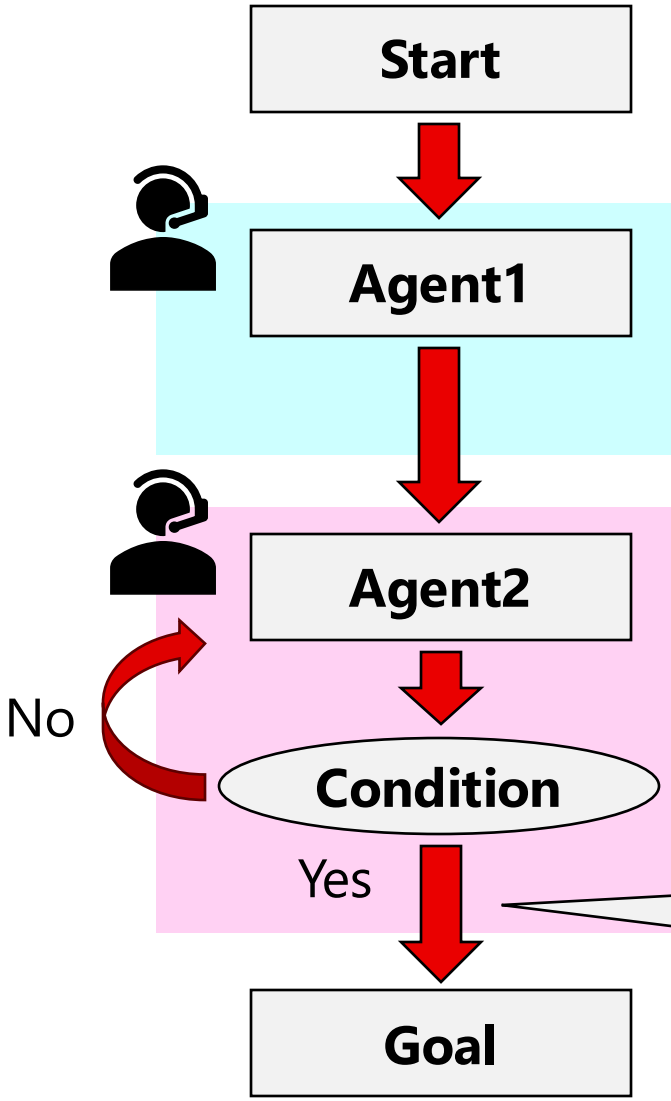


Demo

Key Points

Deep Dive into Generation Process

FUJITSU



"Please generate hunting rules for specific TTPs (Kerberoasting) considering environmental information."

- Obtaining the specific detection methods from MITRE ATT&CK.
- Analyzing the environmental information and extracting critical information for the hunting rule.

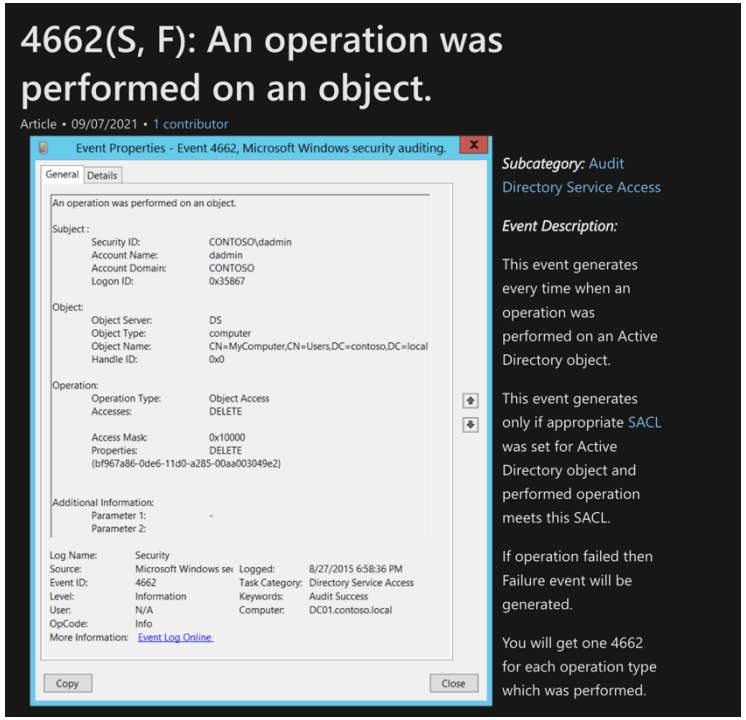
- Gathering additional information to generate hunting rules.

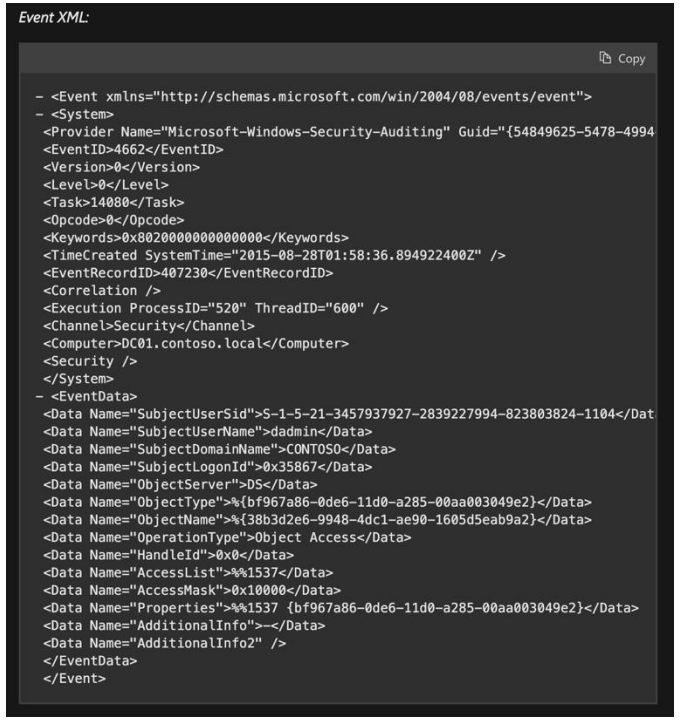
- Judging whether the information gathered is sufficient.

Generate Sigma rules considering all information.

Know-How and Tips

- Filtering the detection methods in MITRE ATT&CK is critical.
- In multi-agent system, token parameters should be adjusted.
- The Windows Event Log formats are different for each Event ID.





Conclusion & Future Works

FUJITSU

- Conclusion
  - Developed the application using local LLM for our MITRE ATT&CK driven threat hunting.
  - It is possible to generate a Sigma rule automatically for detecting specific attacks.
- Future Works
  - Stability
  - Machine resources
  - Further improvements and expansions

Take Aways

FUJITSU

- Based on the concept of Summiting the Pyramid, high-level threat hunting can be defined, which is difficult for attackers to avoid with any techniques.
- Since sensitive information, especially environmental information, is essential for threat hunting, local LLM is one of the best options to assist the process.
- Running local LLM on a CPU only machine is challenging in machine resources. They can be improved by some technologies, such as RAG, and multi-agent systems.

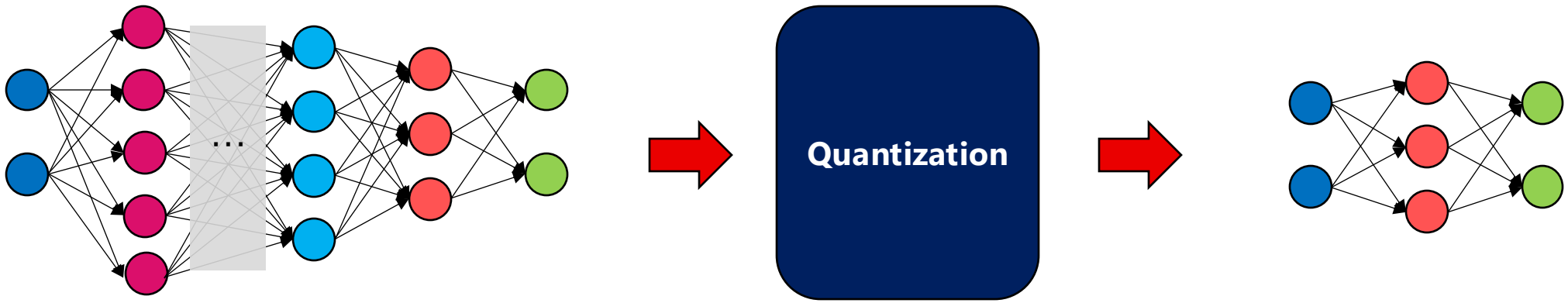
Thank you!

Q&A

Appendix

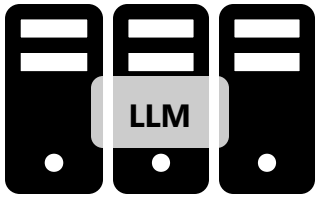
Quantized LLM

- What is Quantized LLM?
  - Expressing the model parameters using fewer bits while minimizing accuracy loss



LLM has billions of parameters and needs many computer resources.

Quantized LLM has fewer parameters and can work on low-spec machines.



Reduce the model size
Accelerate predictions

Key-points of Quantized LLM

FUJITSU

- There are various quantization methods:
  - In the CPU only environment, quantization with "llama.cpp" is the best solution.
  - There are also various LLMs quantized with "llama.cpp".
    - It is essential to consider the trade-off between response quality and speed due to the model size after quantization.

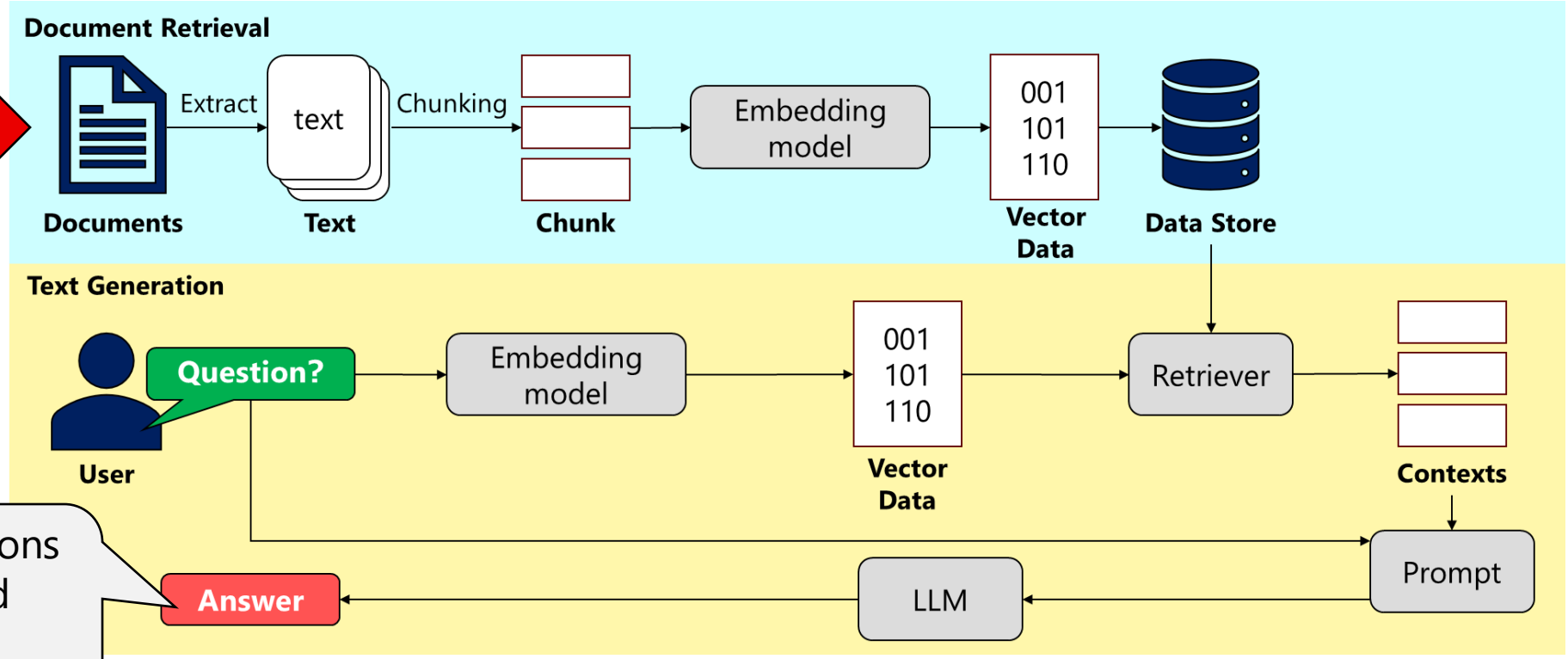
model	Model size	Details
Q8_0	8.54GB	Extremely high quality, generally unneeded but max available quant.
Q6_K	6.59GB	Very high quality, near perfect, recommended.
Q5_K_M	5.73GB	High quality, recommended.
Q5_K_S	5.59GB	High quality, recommended.
Q4_K_M	4.92GB	Good quality, uses about 4.83 bits per weight, recommended.
Q4_K_S	4.69GB	Slightly lower quality with more space savings, recommended.
Q3_K_L	4.32GB	Lower quality but usable, good for low RAM availability.

Q4_K_M keeps quality while reducing model size.

Retrieval-Augmented Generation (RAG)

FUJITSU

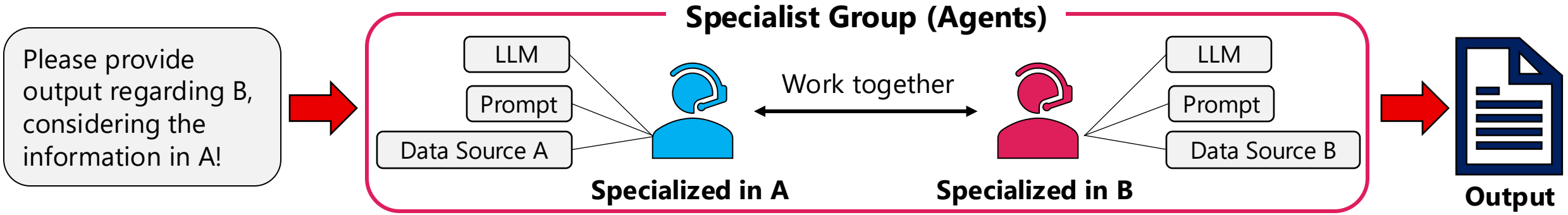
- What is RAG?
  - Improve the accuracy of answers using external information retrieval in generating texts with LLM.



LLM can answer questions based on the latest and correct information without any learning.

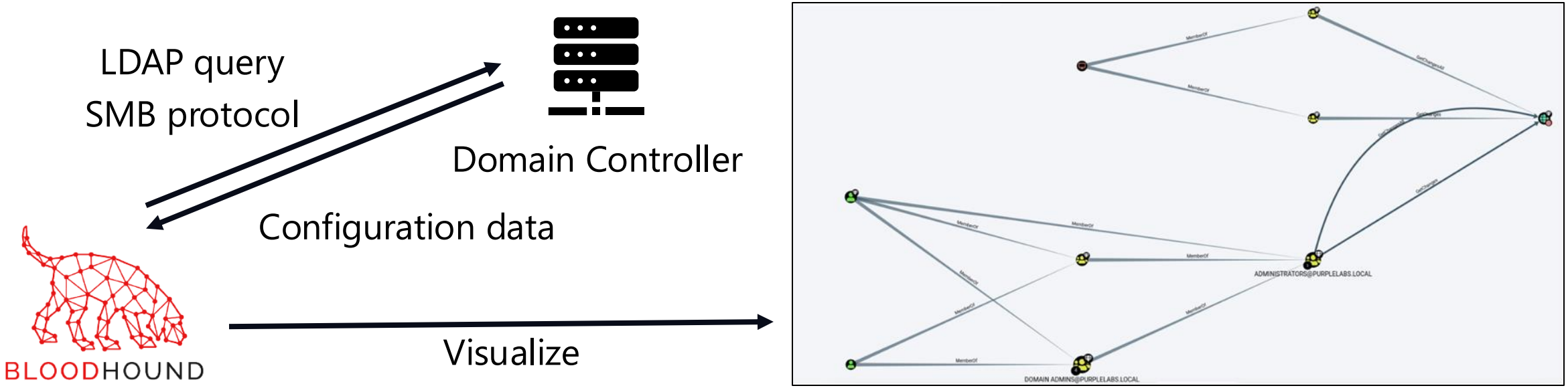
Multi-Agent System

- What is a Multi-Agent System?
  - An approach in which specialized agents work together to accomplish complex tasks rather than one agent doing everything.
- Benefits of multi-agent system:
  - Getting each agent to focus on fewer tasks can improve generated results.
  - Each agent can be powered by a separate prompt and LLM.
  - Evaluation and improvement of each agent can be done individually without any change to the entire application.



Environmental Information

- Many organizations use Active Directory to manage their resources.
  - e.g., accounts, computers, group policies
- In an Active Directory environment, the configuration data can be collected and visualized by Bloodhound.



Extract Critical TTPs

- LLM analyzes the collected data, identifies misconfigurations in the environment, and extracts critical TTPs.
- If a machine where the application runs belongs to an Active Directory domain, the data can be collected without any user input.