

# 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



- 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)
  - Al engineer @ Fujitsu Defense & National Security Limited
  - Developer of LLM and other generative AI application



#### **Motivations**



- 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

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

# **ATT&CK**<sup>®</sup>

Extract critical TTPs for the environment

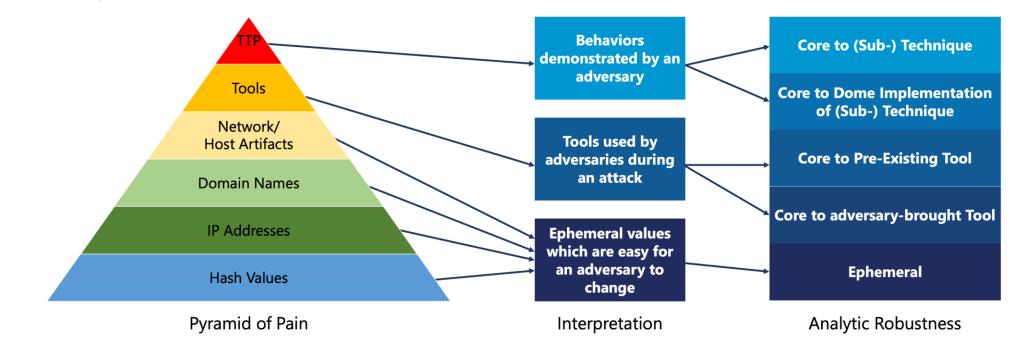
MITRE   ATT&CK°	Matrices - Tactics - Techniques - Defenses	s - CTI - Resources - Benefact	ors Blog 🖓			
	Reminder: the TAXII 2.0 server will be retiring on December 18. Please switch to the TAXII 2.1 server to ensure uninterrup	oted service.				
TECHNIQUES Security Account Manager	Home > Techniques > Enterprise > OS Credential Dumping > DCSync OS Credential Dumping: DCSync					
LSA Secrets Cached Domain Credentials	Other sub-techniques of OS Credential Dumping (8)             	ID: T1003.006 Sub-technique of: T1003				
DCSync Proc Filesystem	Adversaries may attempt to access credentials and other sensitive information by abusing a Windows Domain Controller's application programming interface (APP) <sup>11</sup> [2] [4] 4 to simulate the replication process from a remote domain controller using a technique called DCSync.	Tactic: Credential Access     Platforms: Windows     Contributors: ExtraHop; Vincent Le Toux     Version: 1.1				
/etc/passwd and /etc/shadow Steal Application Access Token	Members of the Administrators, Domain Admins, and Enterprise Admin groups or computer accounts on the domain controller are able to run DCSync to pull password data <sup>[5]</sup> from Active Directory, which may include current and historical hashes of					
Steal or Forge Authentication Certificates	potentially useful accounts such as KRBTGT and Administrators. The hashes can then in turn be used to create a Golden Ticket for use in Pass the Ticket <sup>[6]</sup> or change an account's password as noted in Account Manipulation. <sup>[7]</sup>	Created: 11 February 2020 Last Modified: 15 October 2024				
Steal or Forge Kerberos V Tickets	DCSync functionality has been included in the "Isadump" module in Mirnikatz. <sup>[9]</sup> Lsadump also includes NetSync, which performs DCSync over a legacy replication protocol. <sup>[9]</sup>	Version Permalink				



#### **Summiting the Pyramid (StP)**



- 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

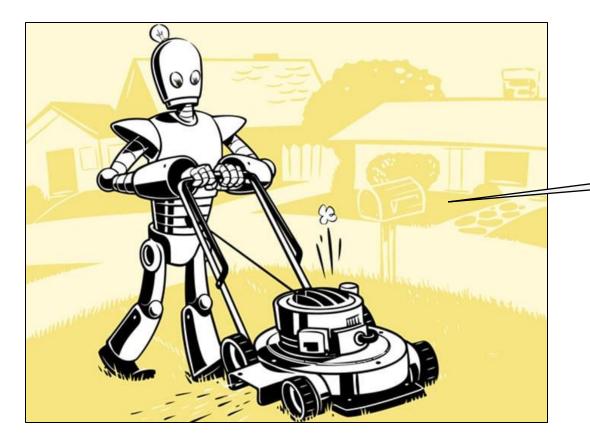


- StP can define the threat hunting levels from 1 to 5.
- The higher the level, the more false positives are detected, making it necessary to have more sensitive information for accurate threat hunting.

J		Our target it takes long time to create	
Source	Description	Our target, it takes long time to create	
Core to (Sub-) Technique	Observables associated with "chokepoints" or "invariant behaviors" of the (Sub-)Technique, unavoidable by any implementation.		
Core to Dome Implementation of (Sub-) Technique	Observables associated with low-variance behaviors of the (Sub-) Technique, unavoidable without a substantially different implementation.		
Core to Pre-Existing Tool	ing Tool Observables associated with tools available to the defenders before adversary use and difficult for an adversary to modify.		
Core to adversary-brought Tool	Observables which are associated with tools that are brought in by an adversary to accomplish an attack.		
Ephemeral	Observables that are t without adversary inte	rivial for an adversary to change, or that change even rvention.	
	Core to (Sub-) Technique Core to Dome Implementation of (Sub-) Technique Core to Pre-Existing Tool Core to adversary-brought Tool	Core to (Sub-) TechniqueObservables associate (Sub-)Technique, unav Observables associate unavoidable without a Observables associate unavoidable without aCore to Pre-Existing ToolObservables associate unavoidable without a Observables associate use and difficult for an adversary to accompliCore to adversary-brought ToolObservables which are adversary to accompliEphemeralObservables that are t	

#### Using Large Language Model (LLM)

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

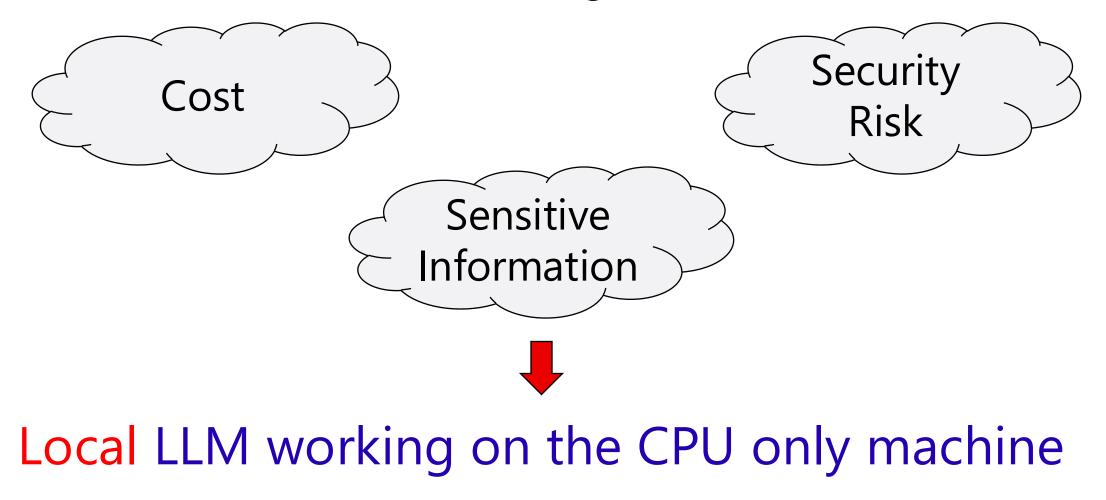


Automating the boring stuff with **Python LLM**. Human concentrate on only interesting things!

#### Automation by "Local" LLM



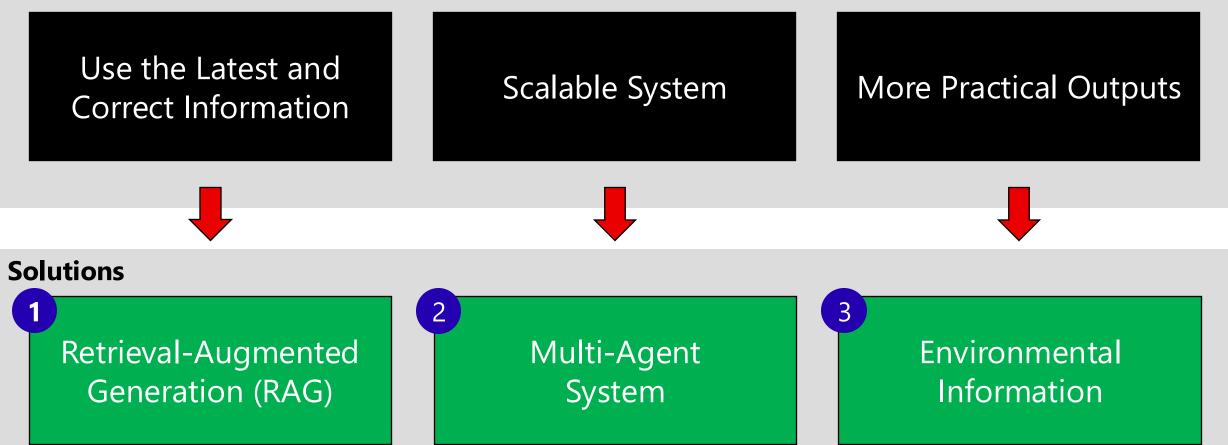
• There are some concerns about using LLM.



#### **Technical Solutions**

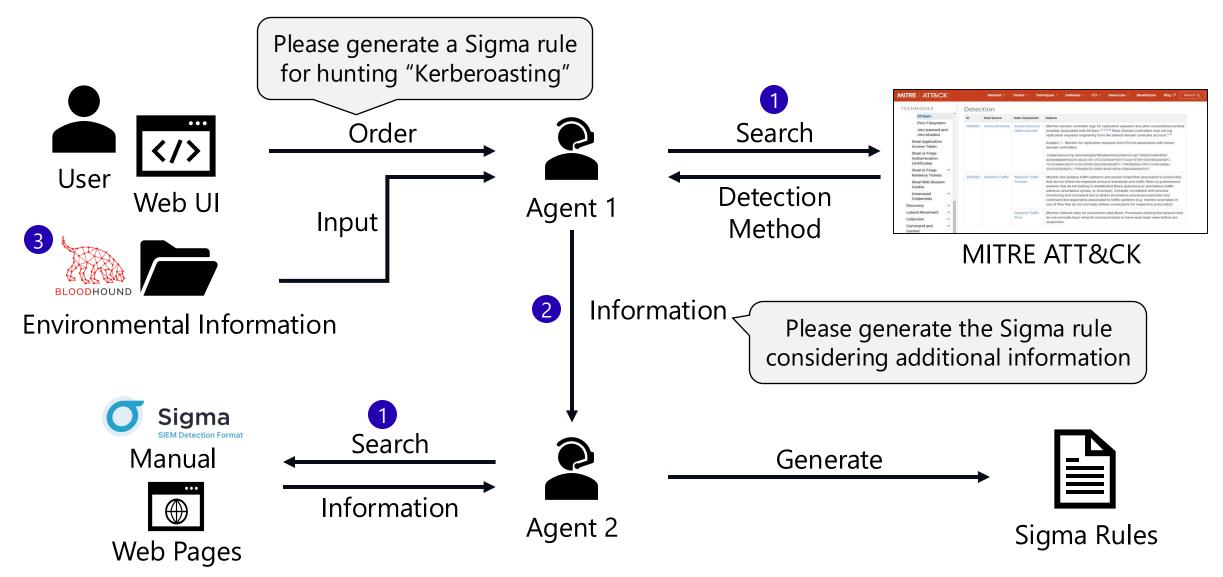






#### **Generation Flow**







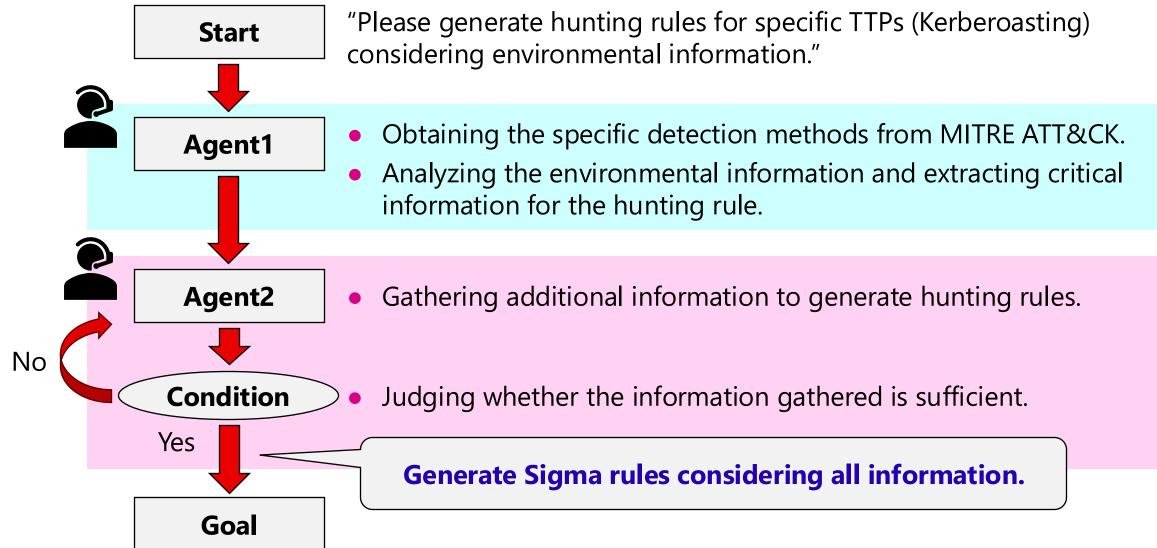
#### Demo



# **Key Points**

#### **Deep Dive into Generation Process**





#### **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.

4662(S, F): An operation w	vas	Event XML:
Article • 09/07/2021 • 1 contributor         Image: Control of the second seco	Subcategory: Audit Directory Service Access	<ul> <li>- <event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"></event></li> <li>- <system></system></li> <li><provider guid="{54849625-5478-4994&lt;/li&gt;     &lt;li&gt;&lt;PrentID&gt;4662-FVentID&gt;&lt;/li&gt;     &lt;li&gt;&lt;Version&gt;0&lt;/Version&gt;&lt;/li&gt;     &lt;li&gt;&lt;Level&gt;0&lt;/Level&gt;&lt;/li&gt;     &lt;li&gt;&lt;Task-14080&lt;/li&gt; &lt;/ul&gt;&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Subject:&lt;br&gt;Security ID:&lt;br&gt;Account Name:&lt;br&gt;Account Domain:&lt;br&gt;CONTOSO&lt;br&gt;Logon ID:&lt;br&gt;Object:&lt;br&gt;Object Serve:&lt;br&gt;Object Serve:&lt;br&gt;Object Type:&lt;br&gt;Object CN=MpC&lt;br&gt;Object Name:&lt;br&gt;Object Name:&lt;br&gt;Object Name:&lt;br&gt;Object Name:&lt;br&gt;Object Access&lt;br&gt;Accesse:&lt;br&gt;DELETE&lt;br&gt;Access Mask:&lt;br&gt;Otoporation:&lt;br&gt;Propertie:&lt;br&gt;DELETE&lt;br&gt;Access Mask:&lt;br&gt;Otoporation:&lt;br&gt;Propertie:&lt;br&gt;DELETE&lt;br&gt;Access Mask:&lt;br&gt;DELETE&lt;br&gt;Access Mask:&lt;br&gt;DELETE&lt;br&gt;Propertie:&lt;br&gt;DELETE&lt;br&gt;Propertie:&lt;br&gt;DELETE&lt;br&gt;Access Mask:&lt;br&gt;DELETE&lt;br&gt;Access Mask:&lt;br&gt;DELETE&lt;br&gt;Access Mask:&lt;br&gt;DELETE&lt;br&gt;Access Mask:&lt;br&gt;DELETE&lt;br&gt;Access Mask:&lt;br&gt;DELETE&lt;br&gt;Propertie:&lt;br&gt;DELETE&lt;br&gt;Propertie:&lt;br&gt;Parameter 1:&lt;br&gt;Parameter 2:&lt;br&gt;DELETE&lt;br&gt;Access Mask:&lt;br&gt;DELETE&lt;br&gt;Access Mask:&lt;br&gt;DELETE&lt;br&gt;Access Mask:&lt;br&gt;DELETE&lt;br&gt;Access Mask:&lt;br&gt;DELETE&lt;br&gt;DELETE&lt;br&gt;Access Mask:&lt;br&gt;DELETE&lt;br&gt;Access Mask:&lt;br&gt;DEL&lt;/td&gt;&lt;td&gt;&lt;ul&gt;     &lt;li&gt;Event Description:&lt;/li&gt;     &lt;li&gt;This event generates&lt;br&gt;every time when an&lt;br&gt;operation was&lt;br&gt;performed on an Active&lt;br&gt;Directory object.&lt;/li&gt;     &lt;li&gt;This event generates&lt;br&gt;only if appropriate SACL&lt;br&gt;was set for Active&lt;br&gt;Directory object and&lt;br&gt;performed operation&lt;br&gt;meets this SACL.&lt;/li&gt; &lt;/ul&gt;&lt;/td&gt;&lt;td&gt;&lt;pre&gt;&lt;ul&gt;     &lt;li&gt;&lt;Dpcode=0&lt;/Dpcode&gt;&lt;/keywords&gt;&lt;/keywords&gt;&lt;/keywords&gt;000000000000000000000000000000000000&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Log Name:         Security           Source:         Microsoft Windows set Logged:         8/27/2015 6:58:36 PM           Event ID:         462         Task Category:         Directory Service Access           Level:         Information         Keywords:         Audit Success           User:         N/A         Computer:         DC01 contoso.local           OpCode:         Information:         Event Log Online.&lt;/td&gt;&lt;td&gt;If operation failed then&lt;br&gt;Failure event will be&lt;br&gt;generated.&lt;br&gt;You will get one 4662&lt;br&gt;for each operation type&lt;br&gt;which was performed.&lt;/td&gt;&lt;td&gt;&lt;pre&gt;&lt;Data Name=" handleid"="" name="Microsoft-Windows-Security-Auditing">0x0 <data name="AccessList">%1537</data> <data name="AccessList">%1537</data> <data %20x10000<="" data="" name="AccessMask"> <data name="AdditionalInfo">~</data> <data name="AdditionalInfo">~</data> <data name="AdditionalInfo"></data>&lt;</data> <data name="AdditionalInfo"></data>&lt; <data name="AdditionalInfo"></data>&lt; <data name="AdditionalInfo"></data>&lt; <data name="AdditionalInfo"></data>&lt;  </provider></li></ul>

#### **Conclusion & Future Works**



#### 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**



- 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.

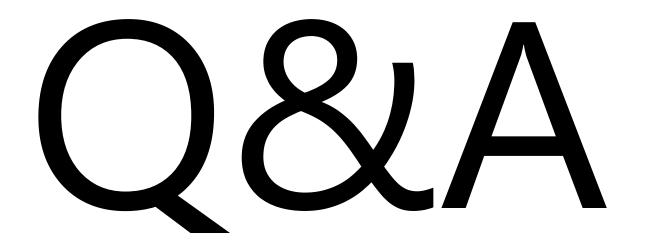


# Thank you!



Q&A







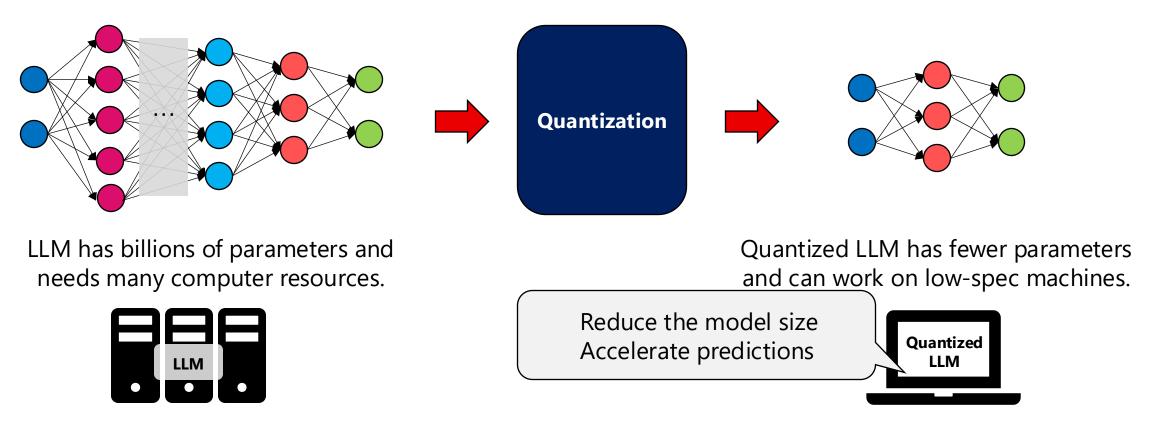
# Appendix

#### **Quantized LLM**



#### • What is Quantized LLM?

• Expressing the model parameters using fewer bits while minimizing accuracy loss



#### **Key-points of Quantized LLM**



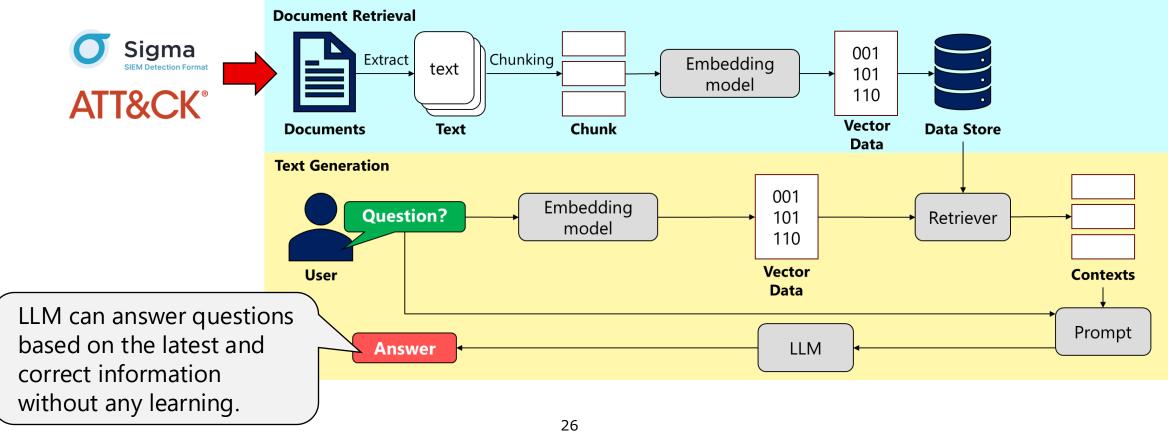
- There are various quantization methods:
  - In the CPU only environment, quantization with "llama.cpp" is the best solution.
  - There are also various LLMs quantized with "llama.cpp".
    - It is essential to consider the trade-off between response quality and speed due to the model size after quantization.

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.	<b>Q4_K_M</b> keeps quality while reducing model size.	
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.		

#### **Retrieval-Augmented Generation (RAG)**

#### • What is RAG?

• Improve the accuracy of answers using external information retrieval in generating texts with LLM.



#### **Multi-Agent System**



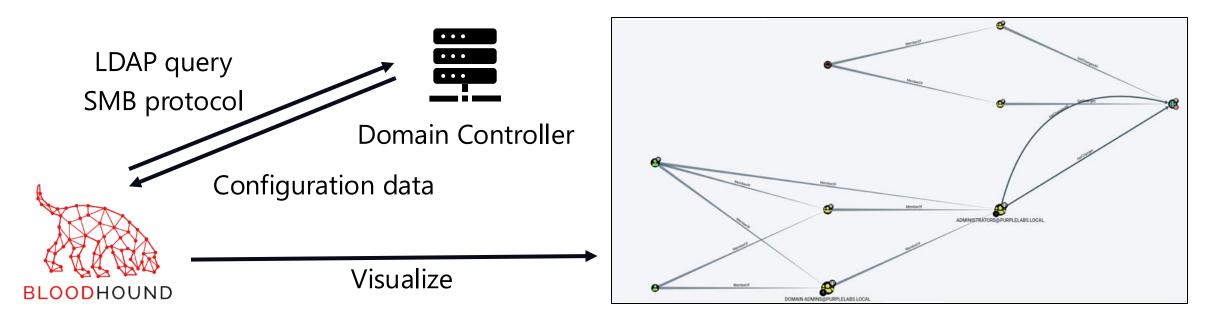
- What is a Multi-Agent System?
  - An approach in which specialized agents work together to accomplish complex tasks rather than one agent doing everything.
- Benefits of multi-agent system:
  - Getting each agent to focus on fewer tasks can improve generated results.
  - Each agent can be powered by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





• 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.





- 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.

