Introduction to MITRE ATT&CK utilization tools by multiple LLM agents and RAG

JSAC2025

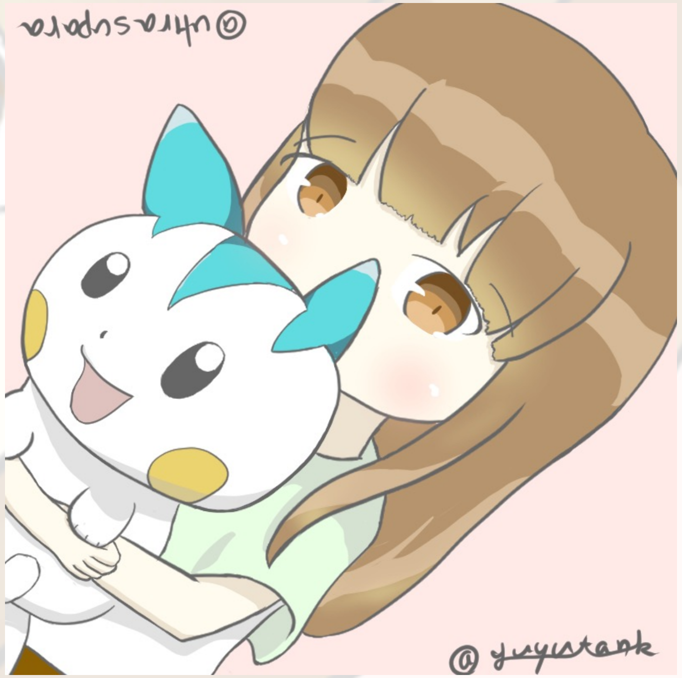
@Tokyo

January 21-22,2025

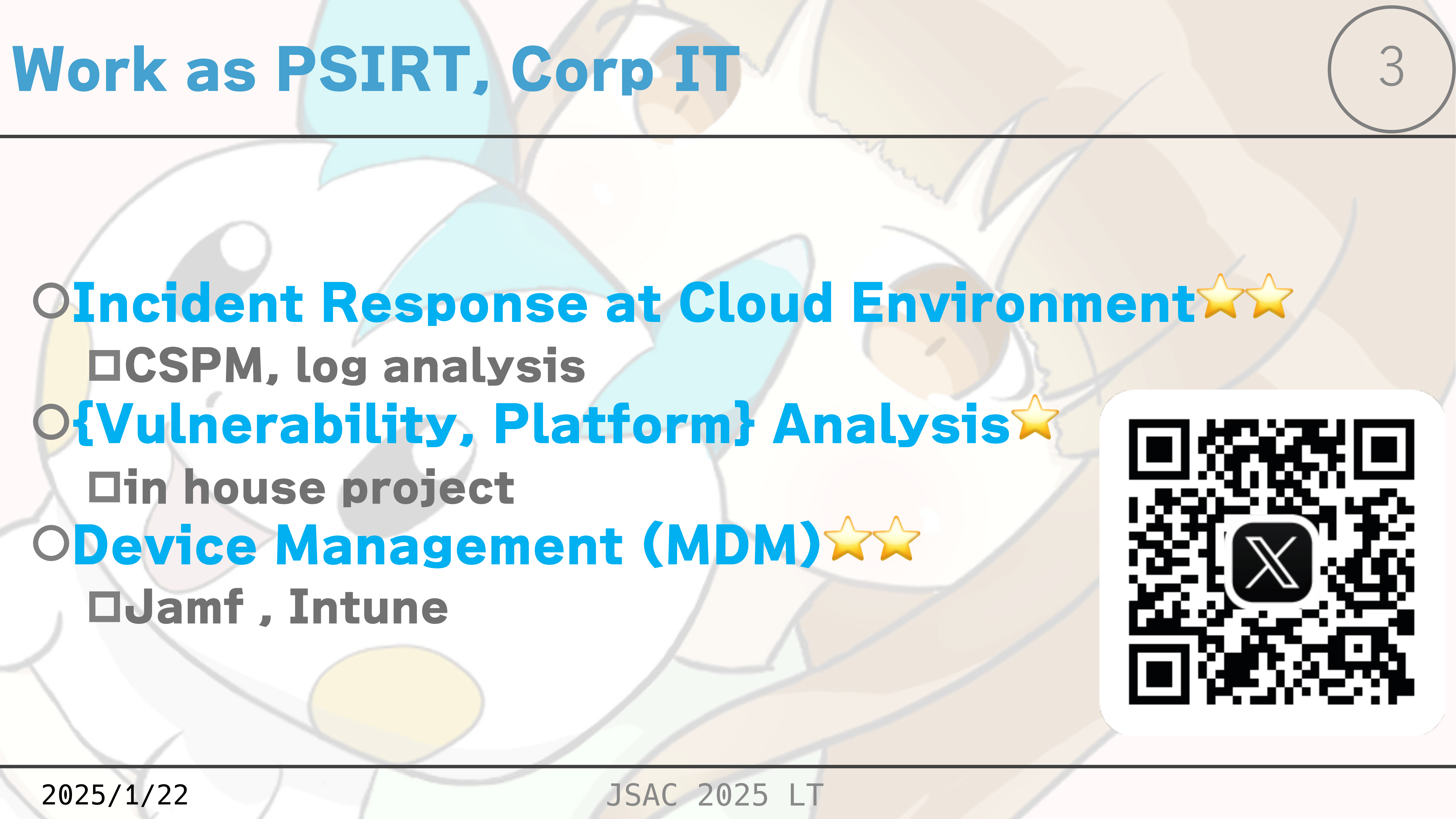
@4su_para

$ aws sts get-caller-indentity

- atsushi, sada a.k.a @4su_para
- Bachelor of Computer Science
- Security Engineer（24卒)
- PSIRT, Corp IT
- OSS dev, LLM lover
- Seccamp/SecHack365 OB
- Speaker @ BlackHat Arsenal



Work as PSIRT, Corp IT



○Incident Response at Cloud Environment⭐⭐

□CSPM, log analysis

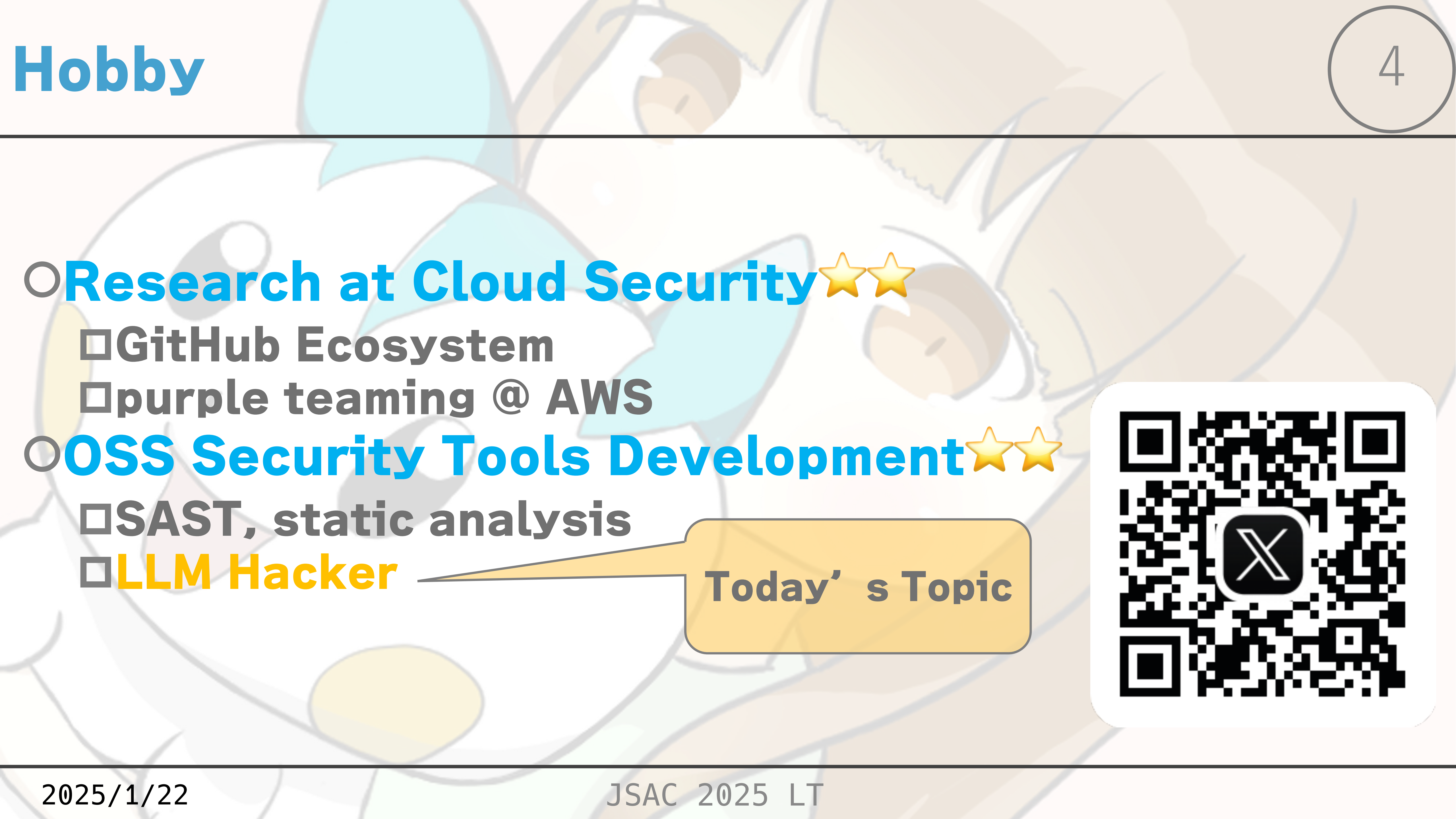
○{Vulnerability, Platform} Analysis⭐

□in house project

○Device Management (MDM)⭐⭐

□Jamf , Intune

Hobby



- ○Research at Cloud Security⭐⭐
  - □GitHub Ecosystem
  - □purple teaming @ AWS
- ○OSS Security Tools Development⭐⭐
  - □SAST, static analysis
  - □LLM Hacker

Today’ s Topic

Overview

○LLMs and AI tech are evolving explosively

  □So, it is a priority to consider how LLM can be used in security and incident response as well!

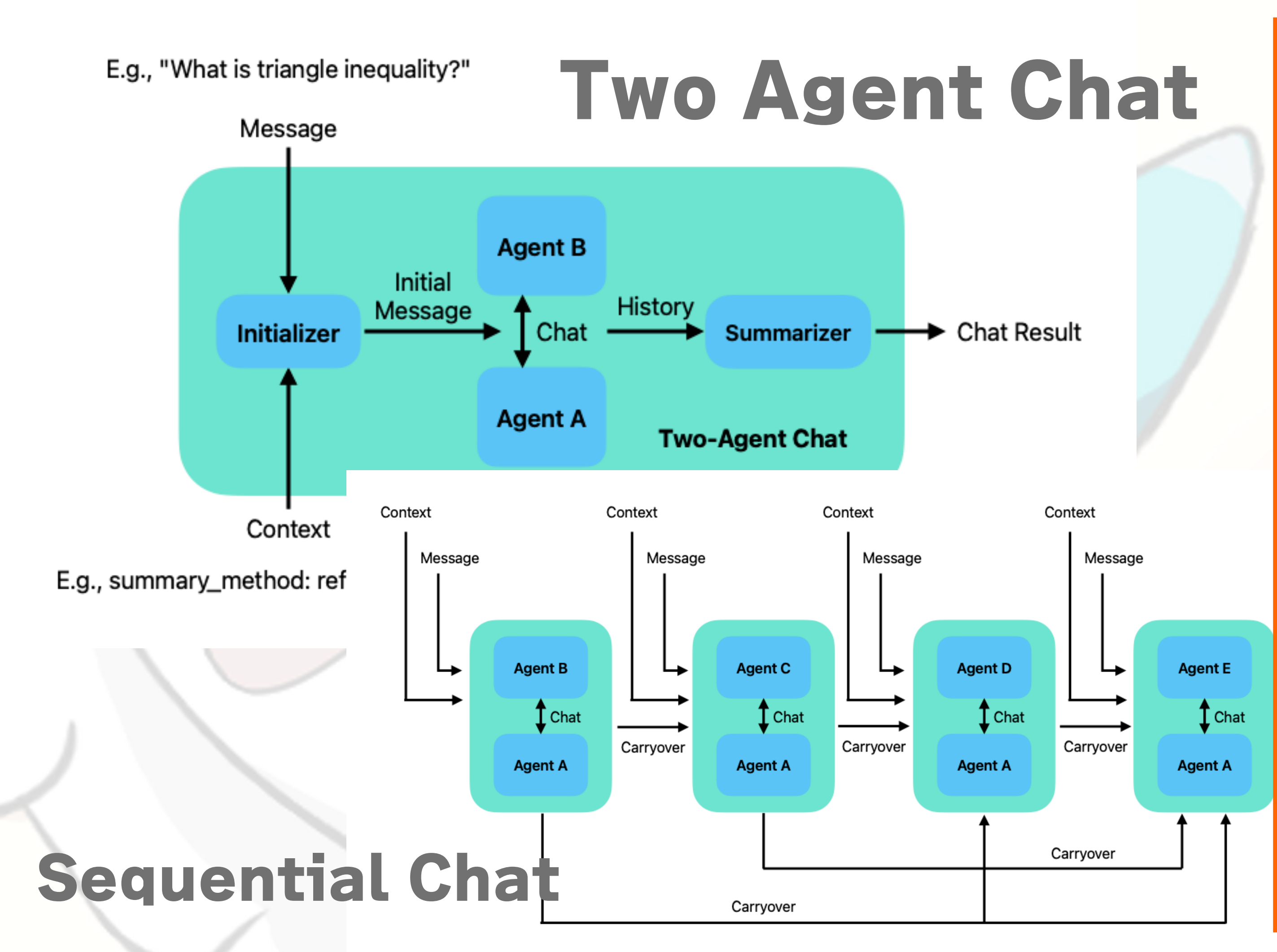
○AI Agents

  □AI Agent is a framework based on LLMs that autonomously achieves goals set by humans

  □introduce sample PoC : disarmBot

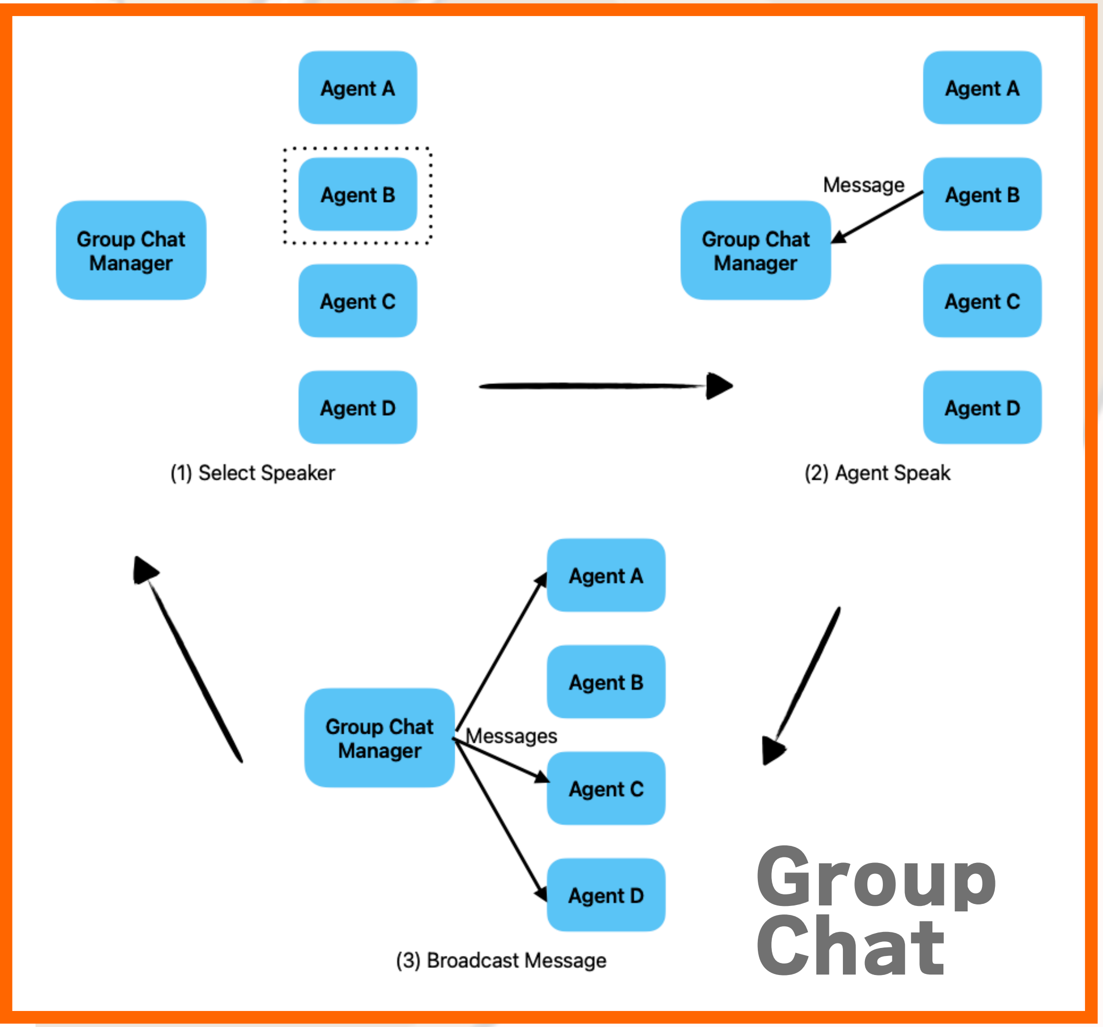
    AutoGen, AutoGPT, crew AI ・・・

AutoGen by Microsoft, execution pattern



Two Agent Chat

Sequential Chat



Group Chat

AutoGen usecases

- ○A1.Math Problem
- ○A2.RAG Chat
- ○A3.ALF Chat
- ○A4.Multi-agent Coding
- ○A5.Group Chat
- ○A6. Chess

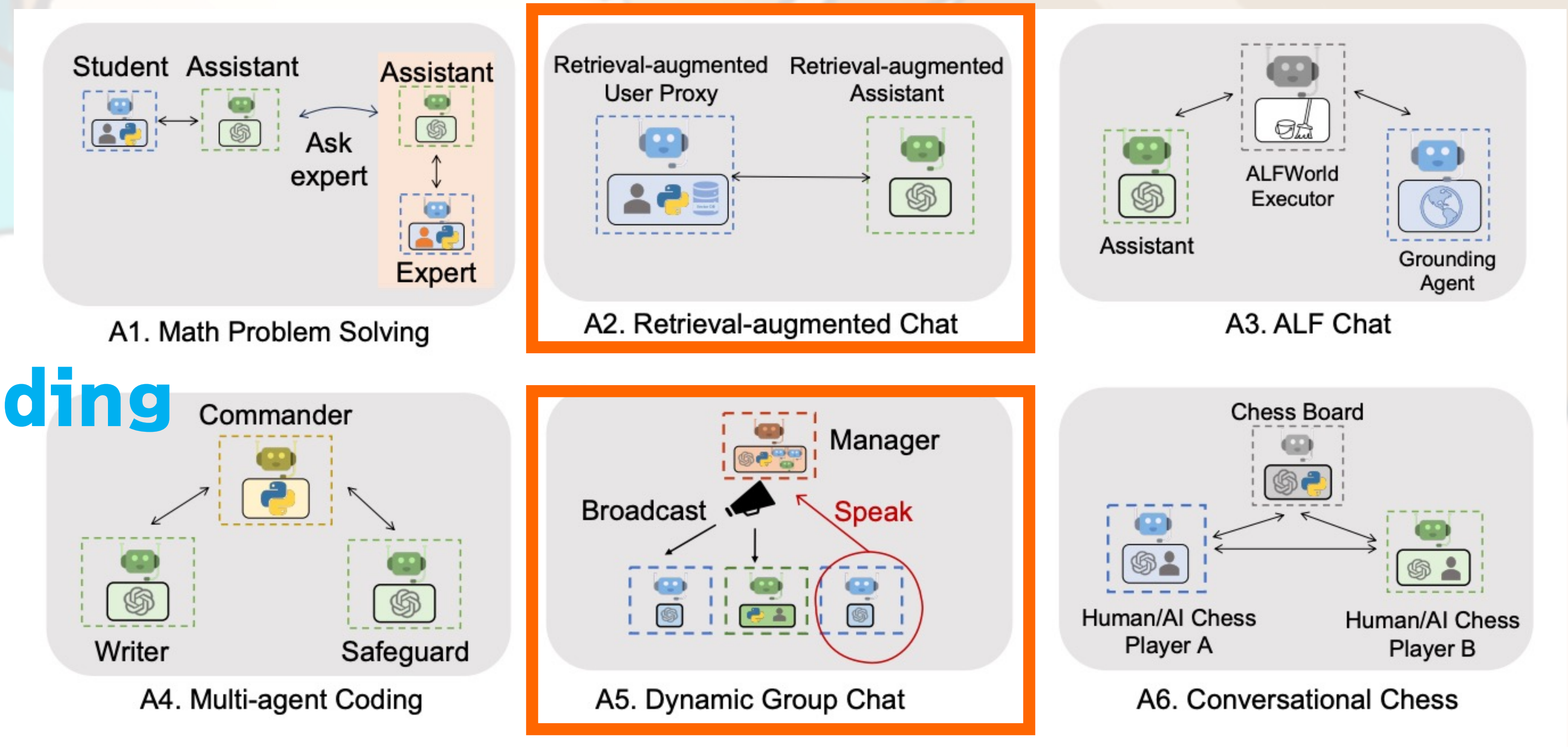
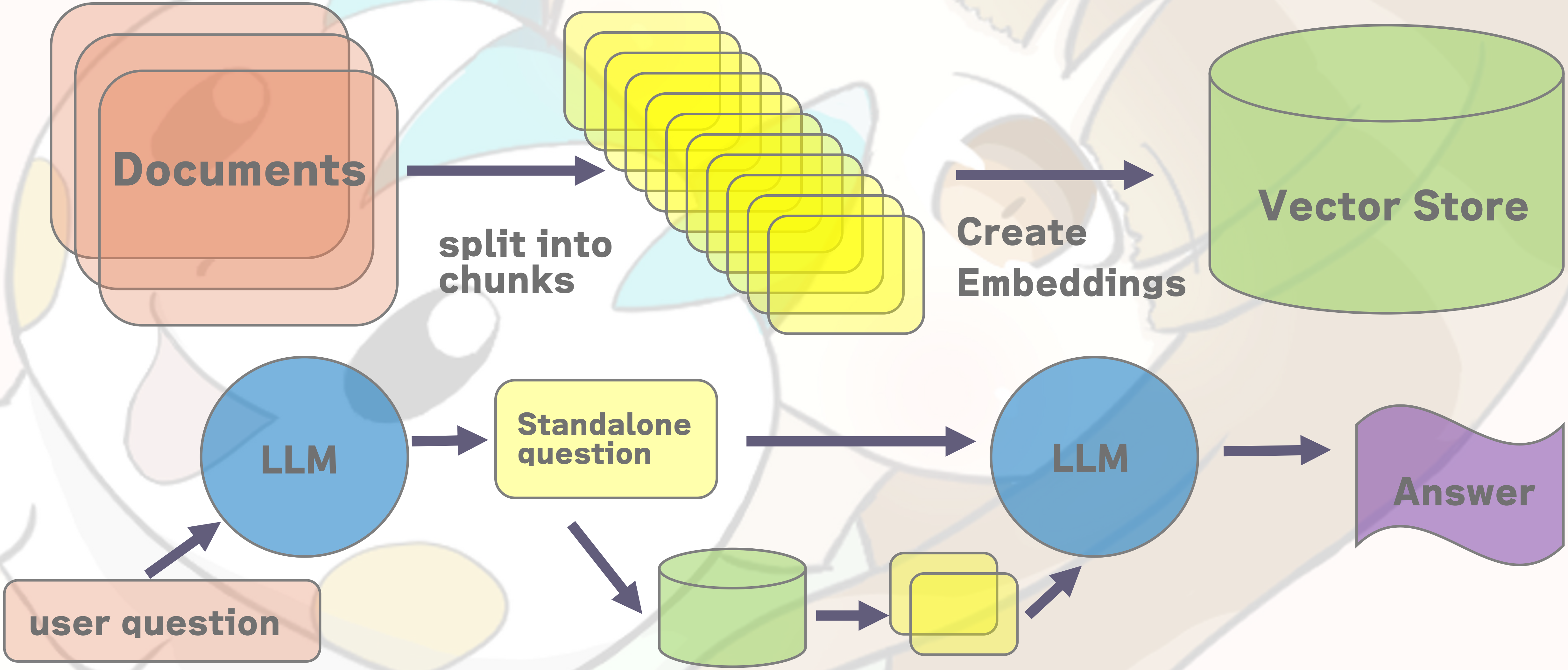


Figure 3: Six examples of diverse applications built using AutoGen. Their conversation patterns show AutoGen's flexibility and power.

The key to innovation is mixed!!

AutoGen: Enabling Next-Gen LLM Applications via Multi-Agent Conversation (2023) , https://arxiv.org/abs/2308.08155

RAG（retrieval-augmented generation）



Main Theme in the Threat Intelligence

- ○Effective use of data and theory
  - □Framework such as MITRE ATT&CK
  - □The strength of user-side companies are their ability to utilize vast amounts of internal information

[redacted]

Information needs to be transformed into something useful in some way.

情報分析力

小泉悠

YU KOIZUMI

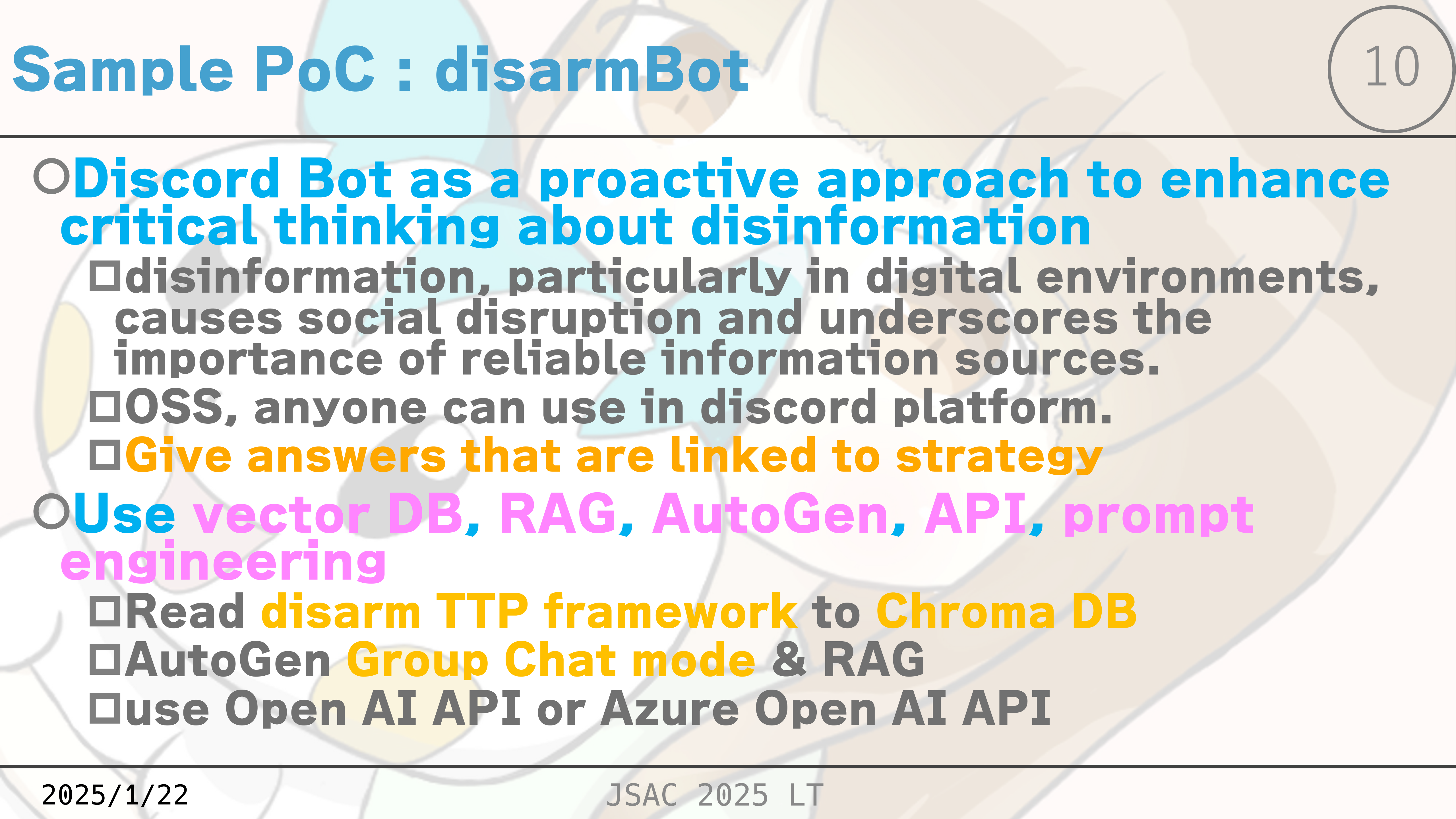
プロはどう集め、読み、
アウトプットするのか？
情報に溺れ
ないための
「分析装置」の
作り方

ビジネスパーソンから学生まで。
ロシアの軍事・安全保障専門の著者による
情報分析力
入門講義

祥伝社

定価 1760円
（10％税込）

Sample PoC : disarmBot



○Discord Bot as a proactive approach to enhance critical thinking about disinformation

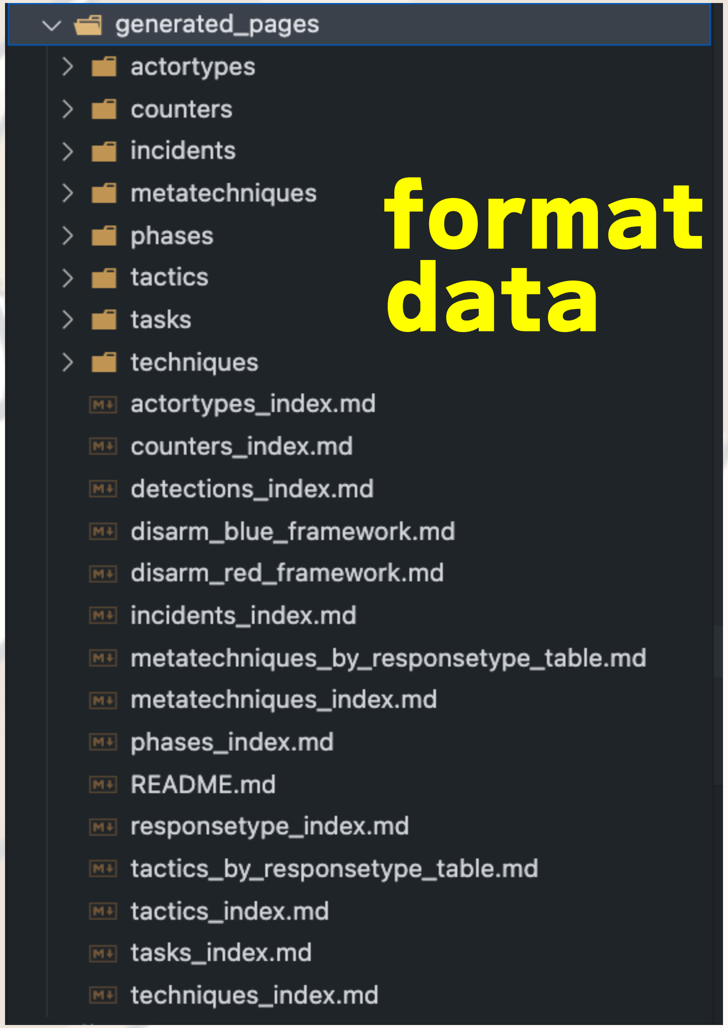
- □disinformation, particularly in digital environments, causes social disruption and underscores the importance of reliable information sources.
- □OSS, anyone can use in discord platform.
- □Give answers that are linked to strategy

○Use vector DB, RAG, AutoGen, API, prompt engineering

- □Read disarm TTP framework to Chroma DB
- □AutoGen Group Chat mode & RAG
- □use Open AI API or Azure Open AI API

disarm TTP framework・・・

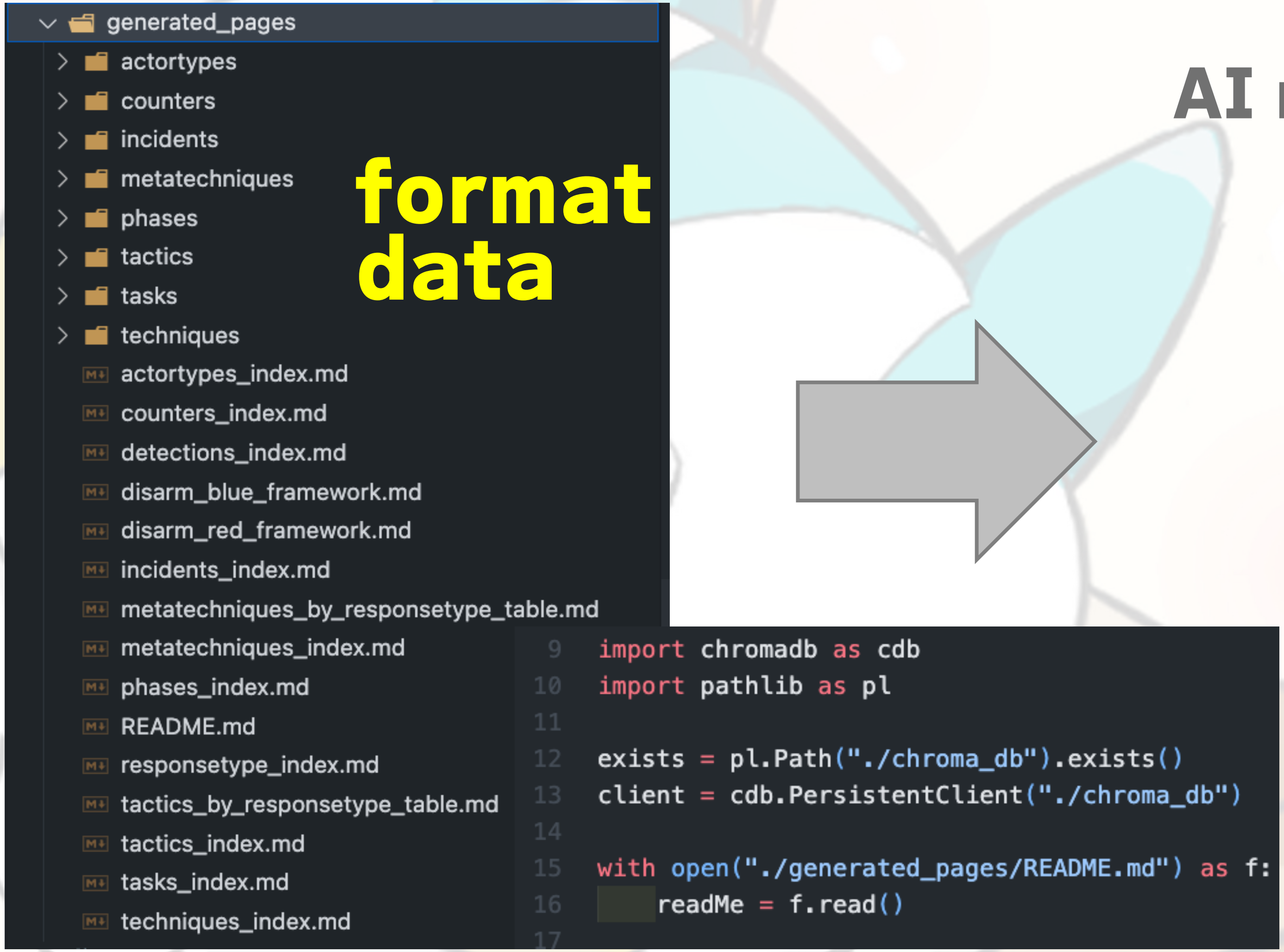
- MITRE ATT&CK frameworks designed for describing and understanding disinformation incidents
  - □ Red Team framework
  - □ Blue Team framework
- TTP (Tactics, Techniques, Procedures)
  - □ Phases: higher-level groupings of tactics, created so we could check we didn't miss anything
  - □ Tactics: stages that someone running a misinformation incident is likely to use
  - □ Techniques: activities that might be seen at each stage
  - □ Tasks: things that need to be done at each stage. Tasks are things you do . Techniques are how you do them.
  - □ Counters: countermeasures to DISARM TTPs.
  - □ Actor Types: resources needed to run countermeasures
  - □ Response types: the course-of-action categories we used to create counters
  - □ Metatechniques: a higher-level grouping for countermeasures
  - □ Incidents: incident descriptions used to create the DISARM frameworks



```
generated_pages
  actortypes
  counters
  incidents
  metatechniques
  phases
  tactics
  tasks
  techniques
  actortypes_index.md
  counters_index.md
  detections_index.md
  disarm_blue_framework.md
  disarm_red_framework.md
  incidents_index.md
  metatechniques_by_responsetype_table.md
  metatechniques_index.md
  phases_index.md
  README.md
  responsetype_index.md
  tactics_by_responsetype_table.md
  tactics_index.md
  tasks_index.md
  techniques_index.md
```

format data

Insert data to local Embedding DB

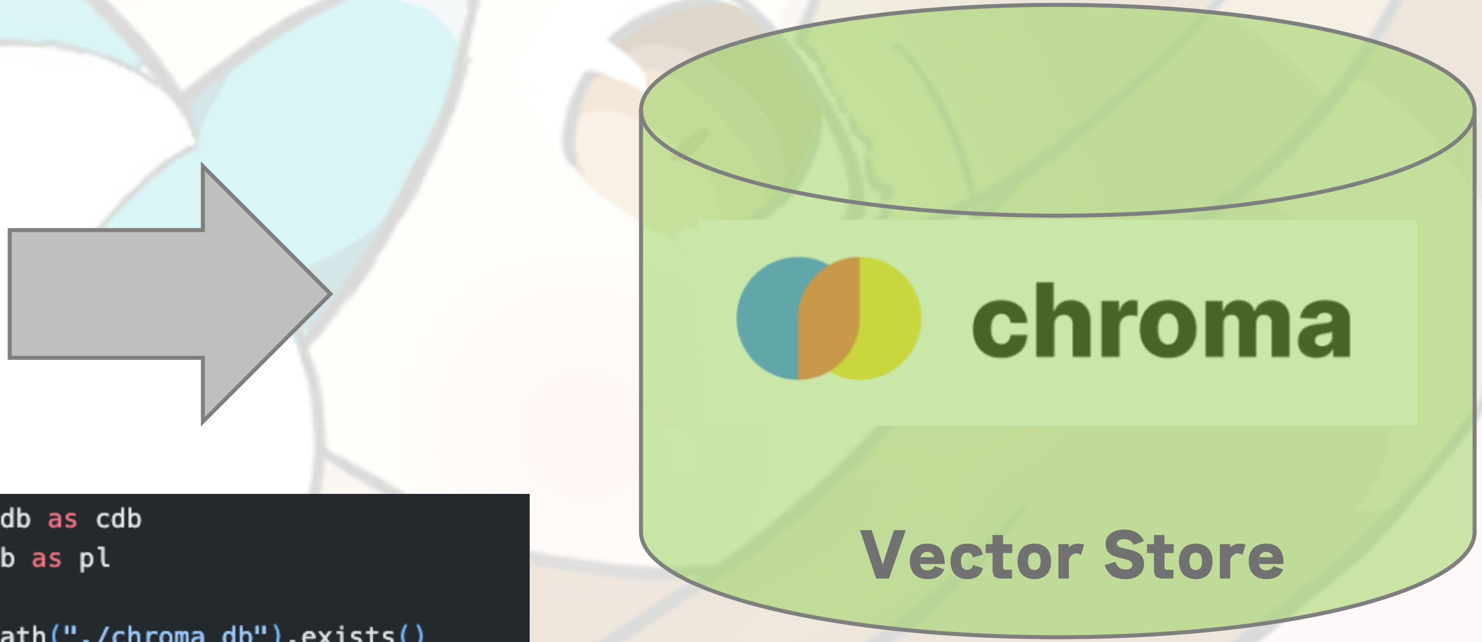


- generated_pages
  - actortypes
  - counters
  - incidents
  - metatechniques
  - phases
  - tactics
  - tasks
  - techniques
  - actortypes_index.md
  - counters_index.md
  - detections_index.md
  - disarm_blue_framework.md
  - disarm_red_framework.md
  - incidents_index.md
  - metatechniques_by_responsetype_table.md
  - metatechniques_index.md
  - phases_index.md
  - README.md
  - responsetype_index.md
  - tactics_by_responsetype_table.md
  - tactics_index.md
  - tasks_index.md
  - techniques_index.md

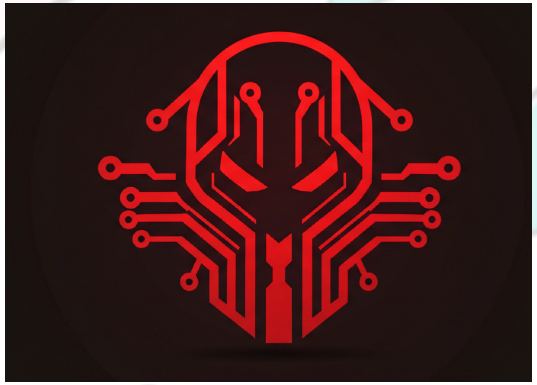
format data

```python
import chromadb as cdb
import pathlib as pl

exists = pl.Path("./chroma_db").exists()
client = cdb.PersistentClient("./chroma_db")

with open("./generated_pages/README.md") as f:
    readMe = f.read()
```

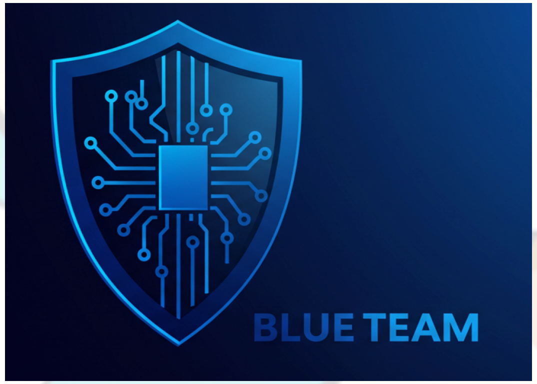
AI native embedding database



Group Chat Characters, 5 AI Agents



attacker side



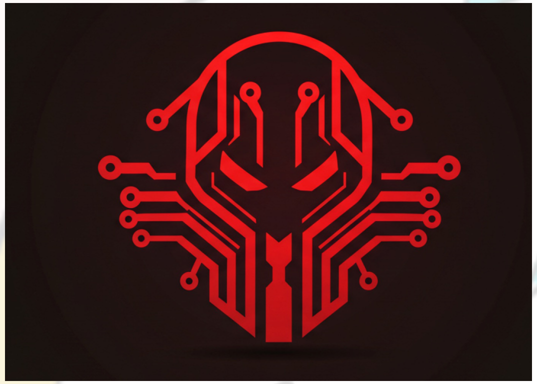
defender side

Skeptics

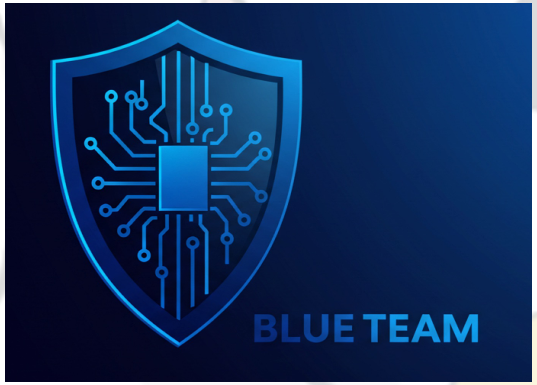
Solution architect

OSINT specialist

Character1,2 : A/D Agents



attacker side



defender side

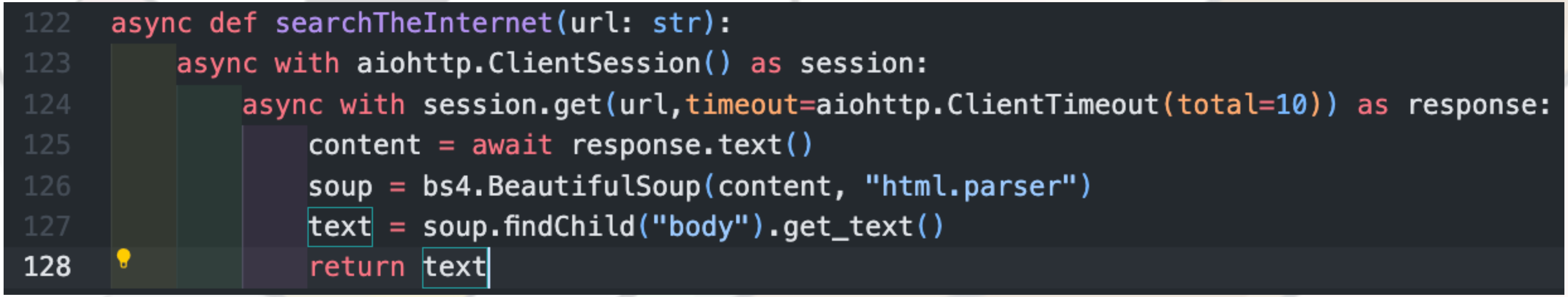
- ○Read Offensive TTP⭐⭐
  - □Prompt : You are an expert in disinformation attacks. Your role is to use your expertise in disinformation attacks to find vulnerabilities in the case. Use the searchDisarmFramework function to search for strategies/tactics related to the red framework and discuss them.
- ○Read Defensive TTP⭐⭐
  - □Prompt : You are a disinformation countermeasure/defense expert. It is your role to use your expertise on the disinformation defense side to think about responses to the vulnerabilities in the case. Use the searchDisarmFramework function to search for strategies/tactics related to blue framework and discuss them.

Character3：OSINT Specialist Agent

OSINT specialist

○Searches the internet and generates answers

- □Prompt：You are an Internet search expert. Your role is to introduce outside information and stimulate discussion. You must use the searchTheInternet function to search the Internet and summarize the information.



```python
async def searchTheInternet(url: str):
    async with aiohttp.ClientSession() as session:
        async with session.get(url,timeout=aiohttp.ClientTimeout(total=10)) as response:
            content = await response.text()
            soup = bs4.BeautifulSoup(content, "html.parser")
            text = soup.findChild("body").get_text()
            return text
```

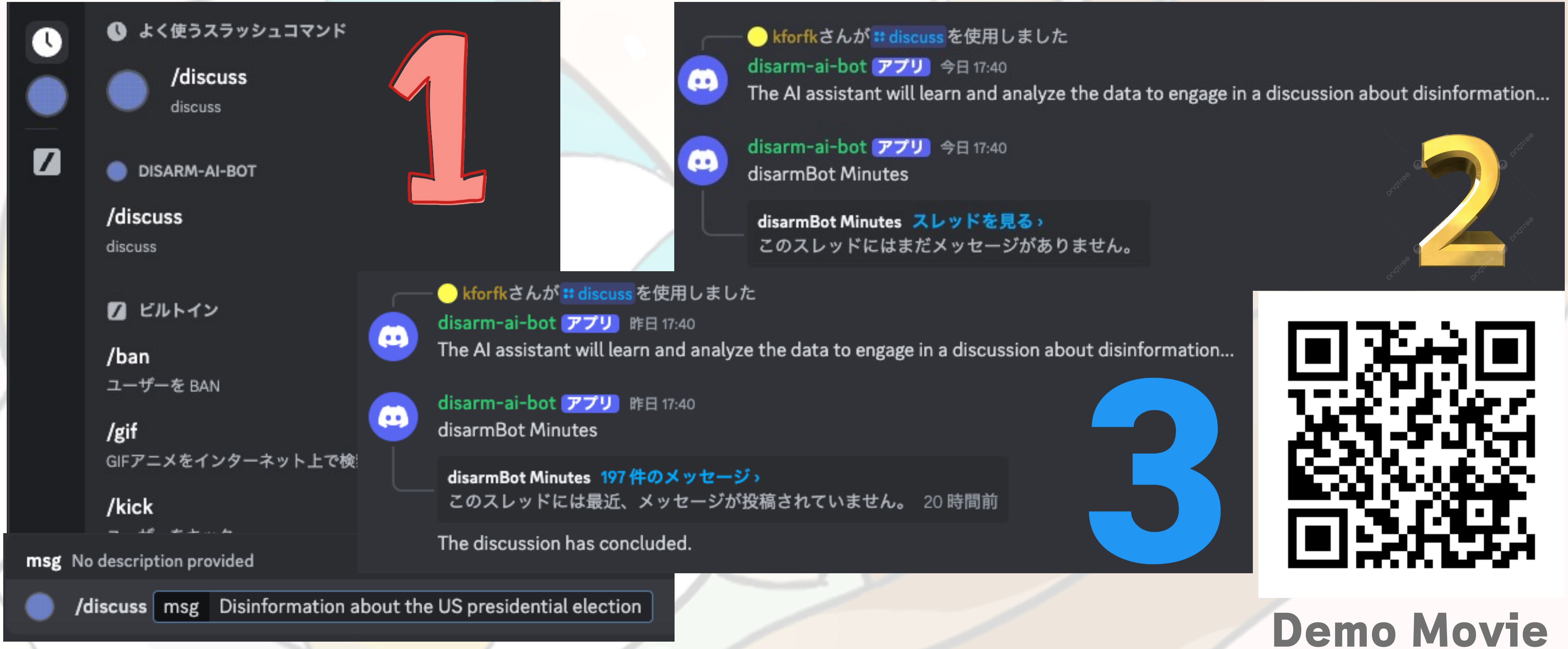
Characters4, 5 AI Agents

Skeptics

Solution architect

- ○Oppose other agents as a skeptic
  - □Prompt : You are a skeptic. Your role is to act as devil's advocate and provide a critical perspective on what other agents say. Use the searchDisarmFramework function to search for what other agents say and ask your skeptical questions.
- ○Solution Architect to bring it all together
  - □Prompt : You are a solution architect. Your role is to provide a solution to the problem using expert's information. Use the searchDisarmFramework functions to provide a solution..

Demonstration Snapshot



よく使うスラッシュコマンド

/discuss
discuss

DISARM-AI-BOT

/discuss
discuss

ビルトイン

/ban
ユーザーを BAN

/gif
GIFアニメをインターネット上で検

/kick

msg No description provided

/discuss msg Disinformation about the US presidential election

kforfkさんが discuss を使用しました

disarm-ai-bot アプリ 今日 17:40
The AI assistant will learn and analyze the data to engage in a discussion about disinformation...

disarm-ai-bot アプリ 今日 17:40
disarmBot Minutes

disarmBot Minutes スレッドを見る ›
このスレッドにはまだメッセージがありません。

kforfkさんが discuss を使用しました

disarm-ai-bot アプリ 昨日 17:40
The AI assistant will learn and analyze the data to engage in a discussion about disinformation...

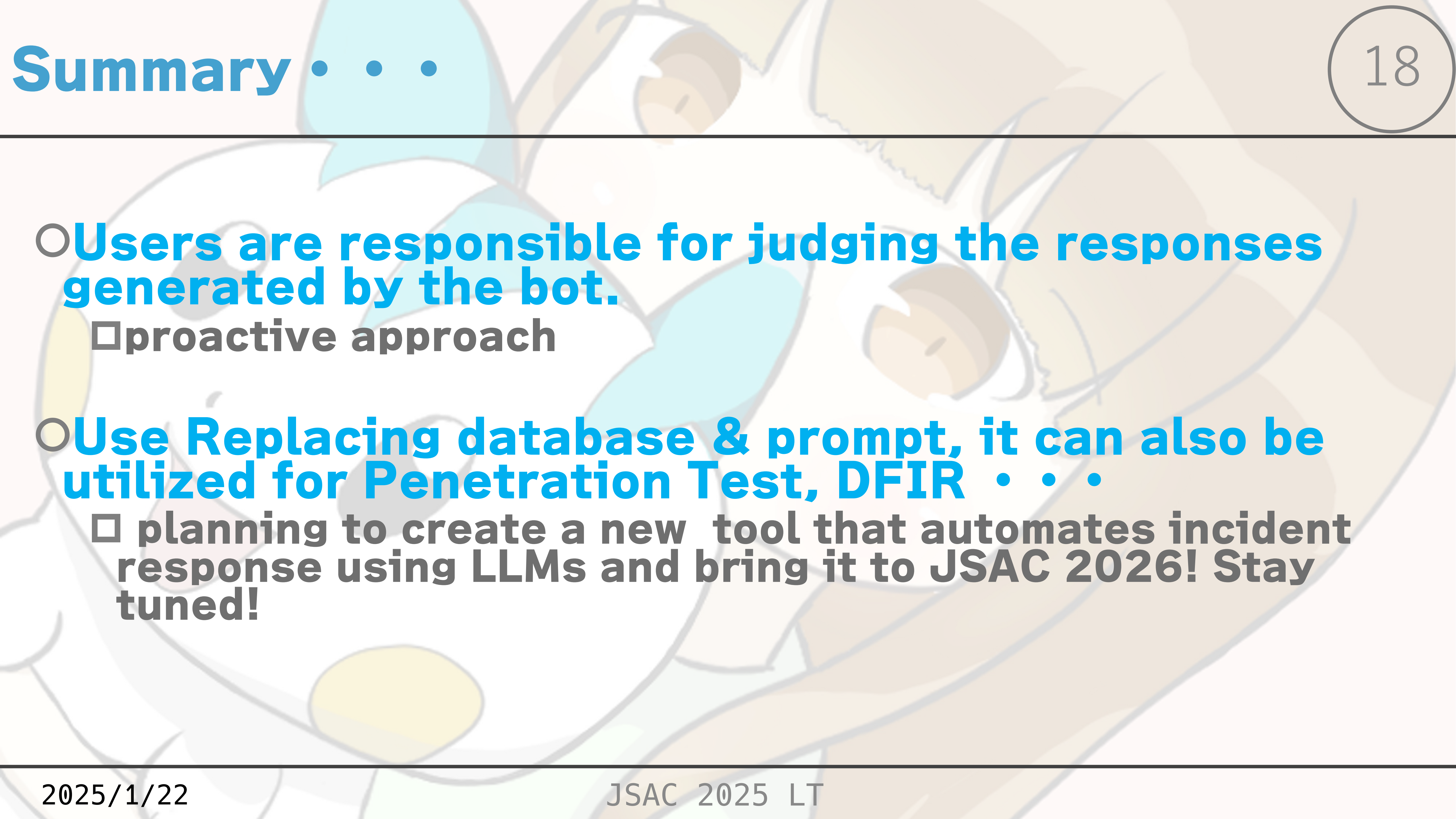
disarm-ai-bot アプリ 昨日 17:40
disarmBot Minutes

disarmBot Minutes 197 件のメッセージ ›
このスレッドには最近、メッセージが投稿されていません。 20 時間前

The discussion has concluded.

Demo Movie

Summary・・・



- ○Users are responsible for judging the responses generated by the bot.
  - □proactive approach
- ○Use Replacing database & prompt, it can also be utilized for Penetration Test, DFIR ・・・
  - □ planning to create a new tool that automates incident response using LLMs and bring it to JSAC 2026! Stay tuned!

Thanks!

https://github.com/ultra-supara/disarmBot

JSAC2025

@Tokyo

January 21-22,2025