# Further Powering Up ATT&CK Powered Suit with GenAI

Toshitaka Satomi
Fujitsu Defense & National Security Limited

# Outline

1. Who am I?
2. What is APS?
3. CTID Cooperation
4. Challenges
5. Solution
6. Use Cases
7. New Research Area
8. Takeaways

Generated by AI (DALL-E)

©2024 Fujitsu Defense & National Security Limited

# Outline

1. Who am I?
2. What is APS?
3. CTID Cooperation
4. Challenges
5. Solution
6. Use Cases
7. New Research Area
8. Takeaways

Generated by AI (DALL-E)

©2024 Fujitsu Defense & National Security Limited

# Who am I?

- “Toshi” taka Satomi (Tokyo, JP)
- Fujitsu Defense & National Security Limited
  - One of the Founding CTID members
- CTI Researcher
- Presentations
  - Black Hat 2020
  - FIRSTCON 2020, 2022, 2023
- All MITRE ATT&CK Defender Badge Holder
- Contributor
  - S-TIP ([https://github.com/s-tip](https://github.com/s-tip))
  - ATT&CK Powered Suit (APS)

©2024 Fujitsu Defense & National Security Limited

# Outline

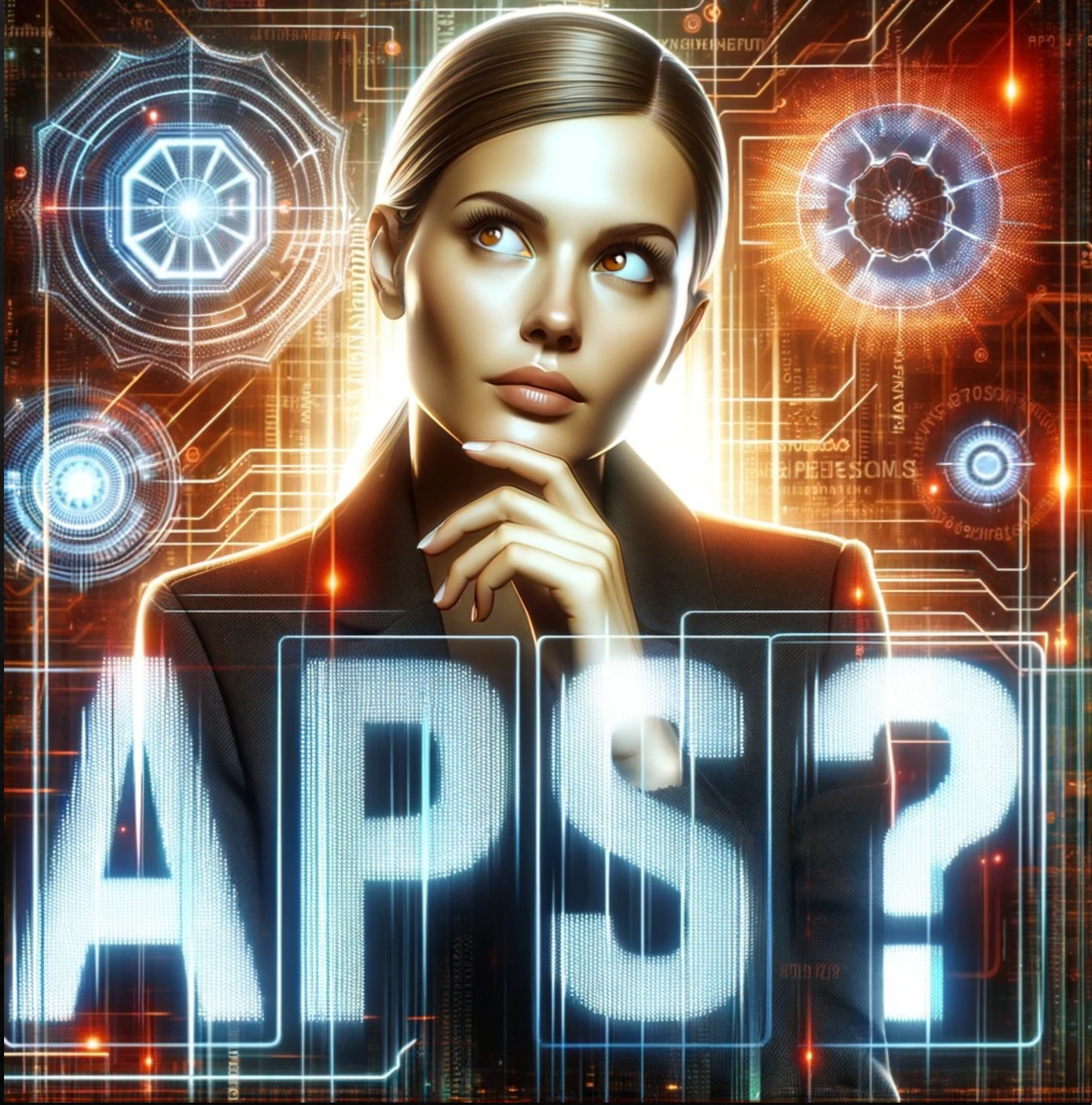
1. Who am I?
2. What is APS?
3. CTID Cooperation
4. Challenges
5. Solution
6. Use Cases
7. New Research Area
8. Takeaways

©2024 Fujitsu Defense & National Security Limited

Generated by AI (DALL-E)

# What is APS?

- Promoted by CTID
- PUT MITRE ATT&CK® AT YOUR FINGERTIPS
- Browser extension for quick access to ATT&CK knowledge base
- Works with popular browsers (Downloads until April 4th)
    - Chrome (5,937)
    - Firefox (173)
    - Edge (548)
    - Safari (Unknown)
- Now available from each browser store
- Can get code from GitHub

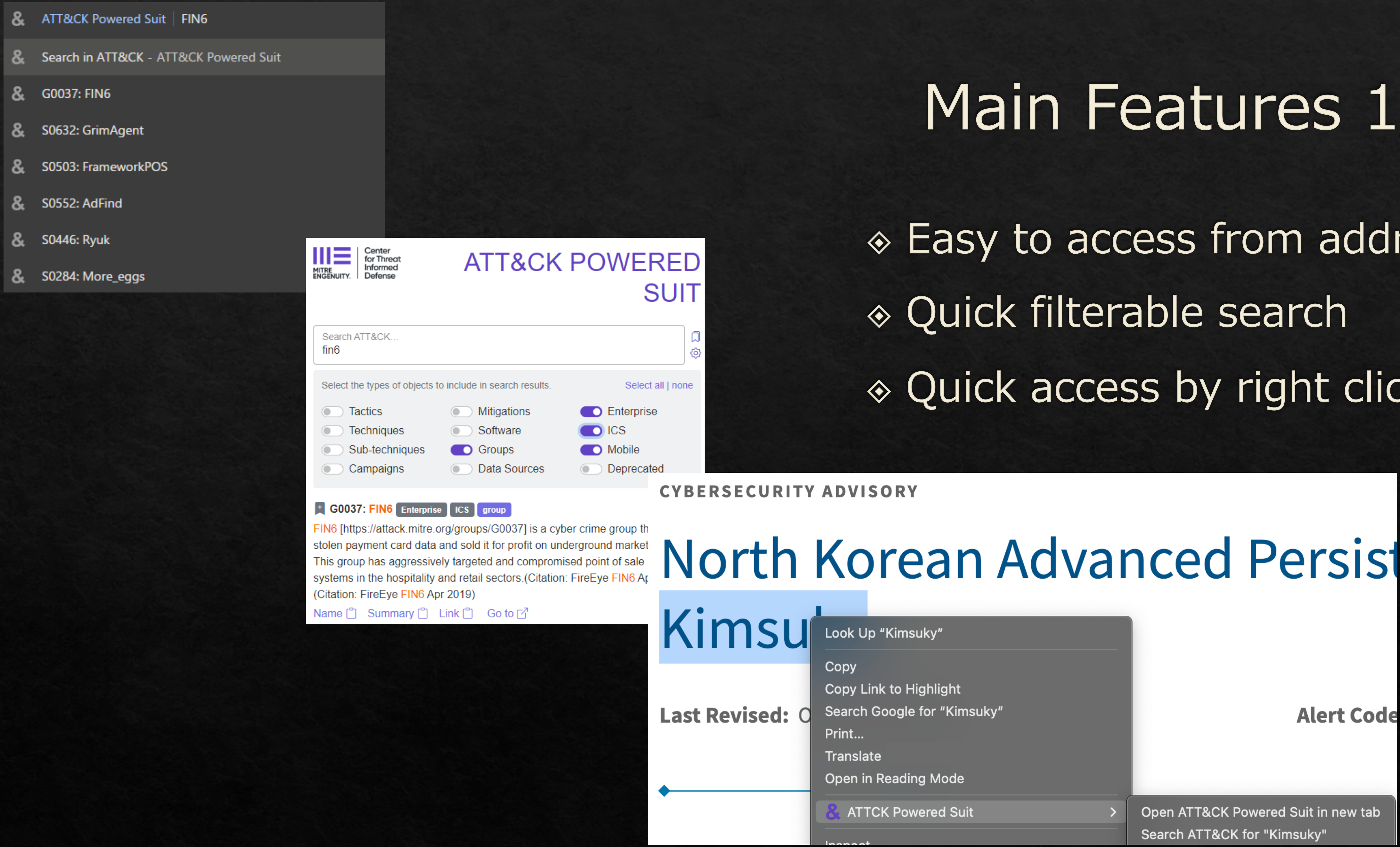


Generated by AI (DALL-E)

©2024 Fujitsu Defense & National Security Limited

# Main Features 1/2

- Easy to access from address bar
- Quick filterable search
- Quick access by right click



fin6

Select the types of objects to include in search results.

| | | |
|---|---|---|
| ○ Tactics | ○ Mitigations | ● Enterprise |
| ○ Techniques | ○ Software | ● ICS |
| ○ Sub-techniques | ● Groups | ● Mobile |
| ○ Campaigns | ○ Data Sources | ○ Deprecated |

**G0037: FIN6** Enterprise ICS group

FIN6 [https://attack.mitre.org/groups/G0037] is a cyber crime group th stolen payment card data and sold it for profit on underground market This group has aggressively targeted and compromised point of sale systems in the hospitality and retail sectors.(Citation: FireEye FIN6 Ap (Citation: FireEye FIN6 Apr 2019)

CYBERSECURITY ADVISORY

North Korean Advanced Persist

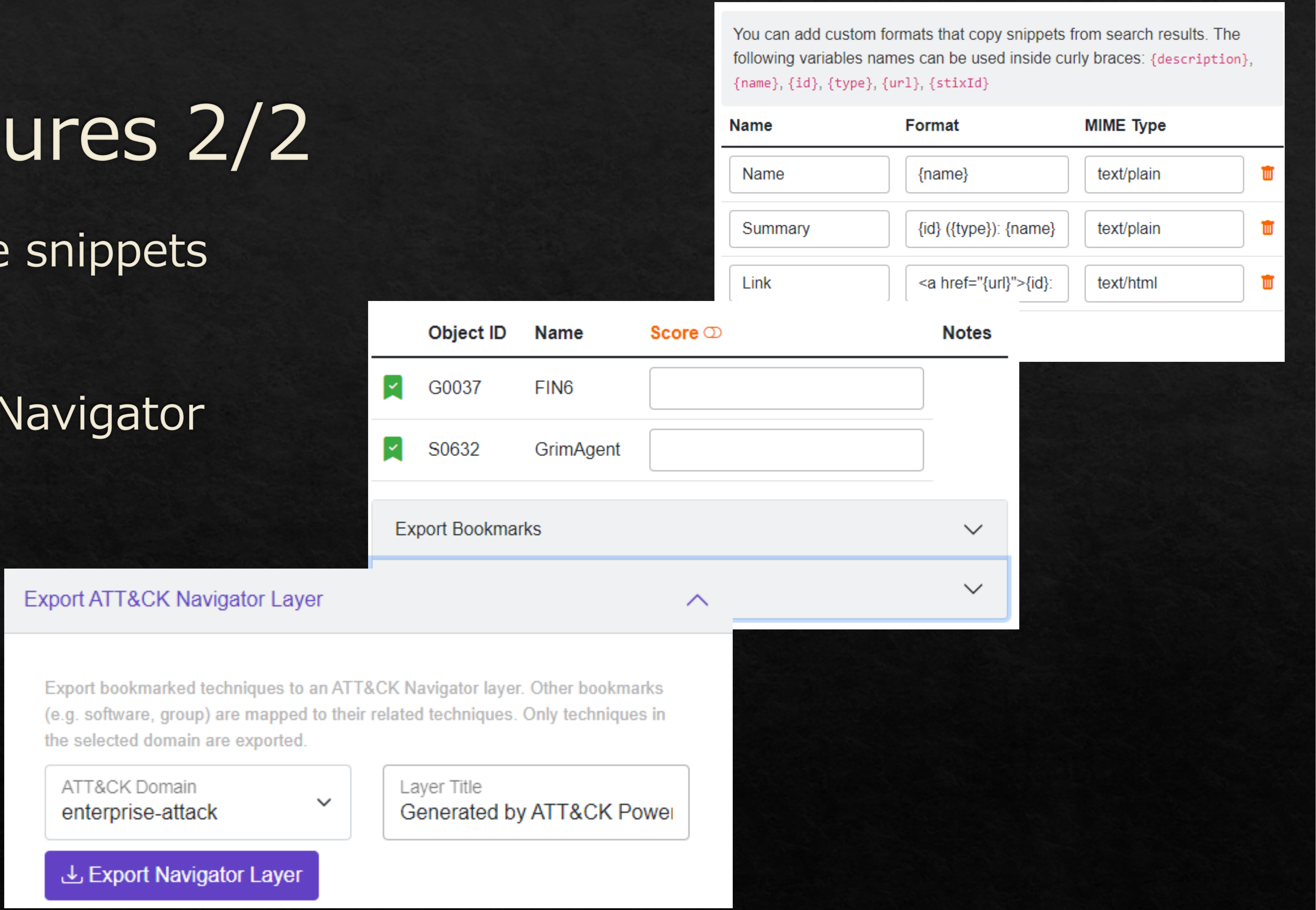
Kimsu

**Last Revised:** O

**Alert Code**

# Main Features 2/2

- Easy to generate snippets
- Bookmarkable
- Export ATT&CK Navigator layer JSON file



You can add custom formats that copy snippets from search results. The following variables names can be used inside curly braces: `{description}`, `{name}`, `{id}`, `{type}`, `{url}`, `{stixId}`

| Name | Format | MIME Type |
|---|---|---|
| Name | {name} | text/plain |
| Summary | {id} ({type}): {name} | text/plain |
| Link | <a href="{url}">{id}: | text/html |

| | Object ID | Name | Score | Notes |
|---|---|---|---|---|
| ✓ | G0037 | FIN6 | | |
| ✓ | S0632 | GrimAgent | | |

Export ATT&CK Navigator Layer

Export bookmarked techniques to an ATT&CK Navigator layer. Other bookmarks (e.g. software, group) are mapped to their related techniques. Only techniques in the selected domain are exported.

ATT&CK Domain: enterprise-attack

Layer Title: Generated by ATT&CK Powe

# Outline

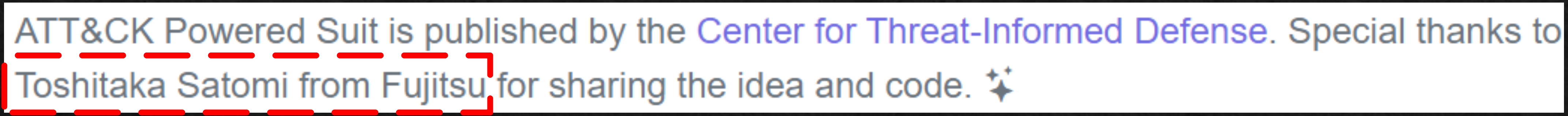
1. Who am I?
2. What is APS?
3. CTID Cooperation
4. Challenges
5. Solution
6. Use Cases
7. New Research Area
8. Takeaways

Generated by AI (DALL-E)

©2024 Fujitsu Defense & National Security Limited

# To Tell the Truth…

- I am the initial developer of ATT&CK Powered Suit



ATT&CK Powered Suit is published by the Center for Threat-Informed Defense. Special thanks to Toshitaka Satomi from Fujitsu for sharing the idea and code. ✨

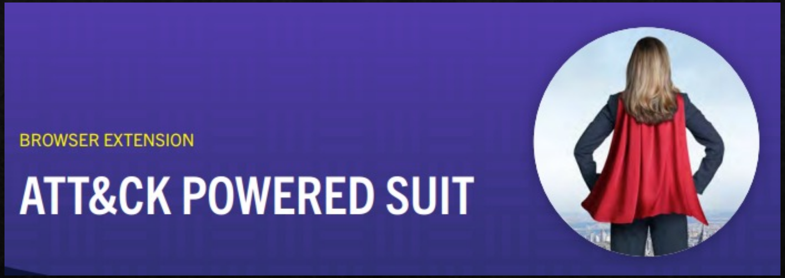
- Motivations
  - A certain security blog typo
  - Search speed of the official ATT&CK
- Developed ATT&CK Powered Suit as a prototype
- Internal members trial
- However, I wanted many defenders to use APS

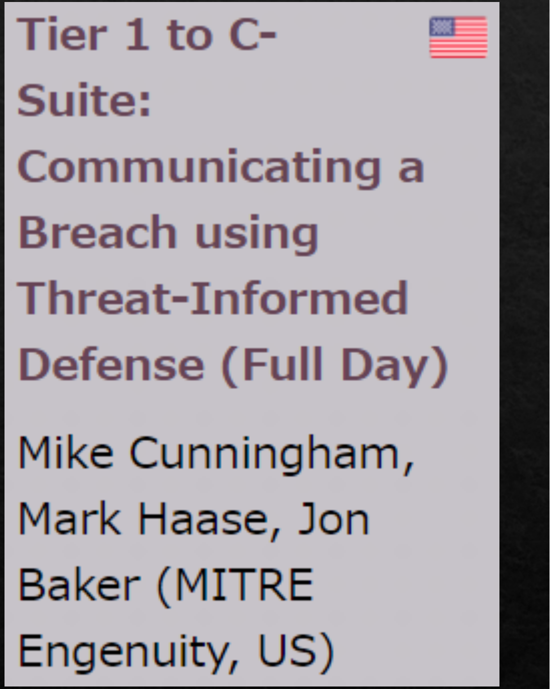
©2024 Fujitsu Defense & National Security Limited

Generated by AI (DALL-E)

# CTID Cooperation

- I demonstrated APS prototype and conveyed my passion with CTID
- CTID supports…
  - Brush up the source code I contributed
  - Publishing source code to GitHub
  - Support for major browsers
- Introduce APS widely to defenders
  - FIRSTCON23 Workshop
  - Impact Report 2022
- I am very glad many defenders use APS for improving own security posture
- **I also want to again thank CTID members for their continued support**




**Tier 1 to C-Suite: Communicating a Breach using Threat-Informed Defense (Full Day)**

Mike Cunningham, Mark Haase, Jon Baker (MITRE Engenuity, US)

©2024 Fujitsu Defense & National Security Limited

Quoted from Impact Report 2022 and FIRSTCON23 program

# Outline

1. Who am I?
2. What is APS?
3. CTID Cooperation
4. Challenges
5. Solution
6. Use Cases
7. New Research Area
8. Takeaways

Generated by AI (DALL-E)

©2024 Fujitsu Defense & National Security Limited

# Challenge 1/2: Discovering Insights beyond ATT&CK

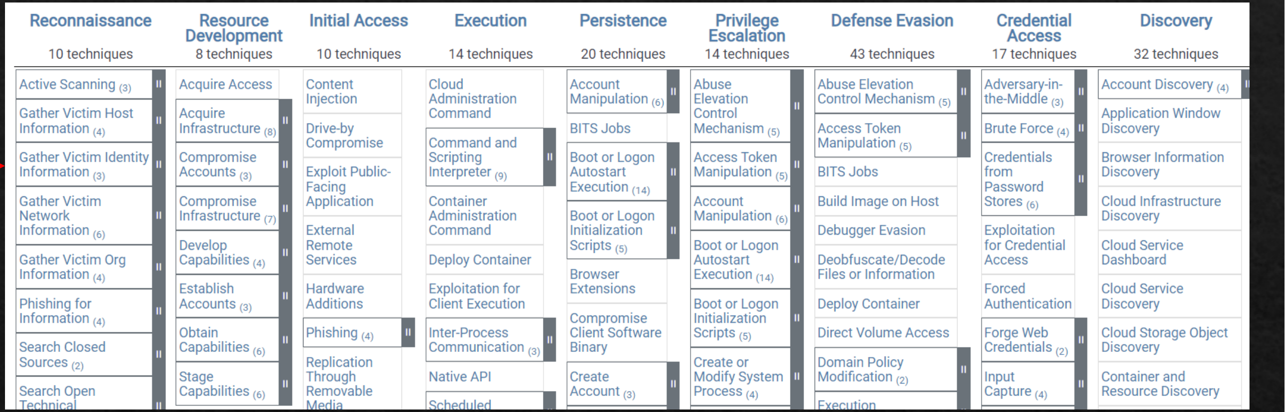
- Limitation: Search that APS provides is very useful for many defenders, however, there are still limitations.
    - APS supports only **full text search**
    - APS provides intelligence **only** from ATT&CK

- Challenge: Get some new insights beyond simply searching only ATT&CK

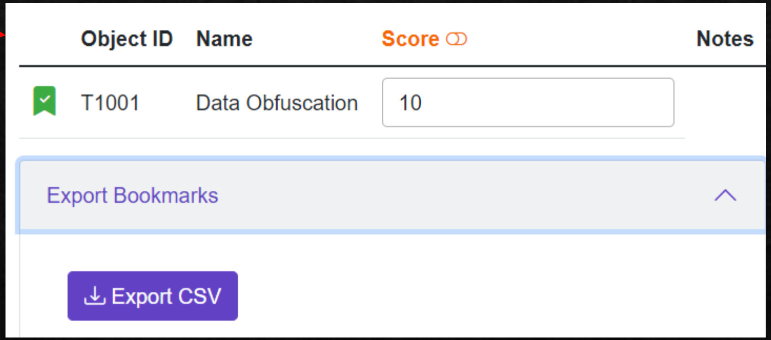
©2024 Fujitsu Defense & National Security Limited

# Challenge 2/2: Generating a Wide Variety of Contents

- Limitation: APS Generates two Kinds of artifacts
    - ATT&CK Navigator JSON
    - Bookmark
- Challenge: Generating more useful artifacts
    - Rule files (Suricata, Snort, Yara)
    - STIX
    - Correlation diagram



| Reconnaissance<br>10 techniques | Resource Development<br>8 techniques | Initial Access<br>10 techniques | Execution<br>14 techniques | Persistence<br>20 techniques | Privilege Escalation<br>14 techniques | Defense Evasion<br>43 techniques | Credential Access<br>17 techniques | Discovery<br>32 techniques |
|---|---|---|---|---|---|---|---|---|
| Active Scanning (3) | Acquire Access | Content Injection | Cloud Administration Command | Account Manipulation (6) | Abuse Elevation Control Mechanism (5) | Abuse Elevation Control Mechanism (5) | Adversary-in-the-Middle (3) | Account Discovery (4) |
| Gather Victim Host Information (4) | Acquire Infrastructure (8) | Drive-by Compromise | Command and Scripting Interpreter (9) | BITS Jobs | Access Token Manipulation (5) | Access Token Manipulation (5) | Brute Force (4) | Application Window Discovery |
| Gather Victim Identity Information (3) | Compromise Accounts (3) | Exploit Public-Facing Application | Container Administration Command | Boot or Logon Autostart Execution (14) | Account Manipulation (6) | BITS Jobs | Credentials from Password Stores (6) | Browser Information Discovery |
| Gather Victim Network Information (6) | Compromise Infrastructure (7) | External Remote Services | Deploy Container | Boot or Logon Initialization Scripts (5) | Boot or Logon Autostart Execution (14) | Build Image on Host | Exploitation for Credential Access | Cloud Infrastructure Discovery |
| Gather Victim Org Information (4) | Develop Capabilities (4) | Hardware Additions | Exploitation for Client Execution | Browser Extensions | Boot or Logon Initialization Scripts (5) | Debugger Evasion | Forced Authentication | Cloud Service Dashboard |
| Phishing for Information (4) | Establish Accounts (3) | Phishing (4) | Inter-Process Communication (3) | Compromise Client Software Binary | Create or Modify System Process (4) | Deobfuscate/Decode Files or Information | Forge Web Credentials (2) | Cloud Service Discovery |
| Search Closed Sources (2) | Obtain Capabilities (6) | Replication Through Removable Media | Native API | Create Account (3) | | Deploy Container | Input Capture (4) | Cloud Storage Object Discovery |
| Search Open Technical | Stage Capabilities (6) | | Scheduled | | | Direct Volume Access | | Container and Resource Discovery |
| | | | | | | Domain Policy Modification (2) | | |
| | | | | | | Execution | | |



| | Object ID | Name | Score | Notes |
|---|---|---|---|---|
| ✓ | T1001 | Data Obfuscation | 10 | |

©2024 Fujitsu Defense & National Security Limited

# Further Powering Up APS

If these challenges are realized, defenders with ATT&CK Powered Suit can advance one step further ahead

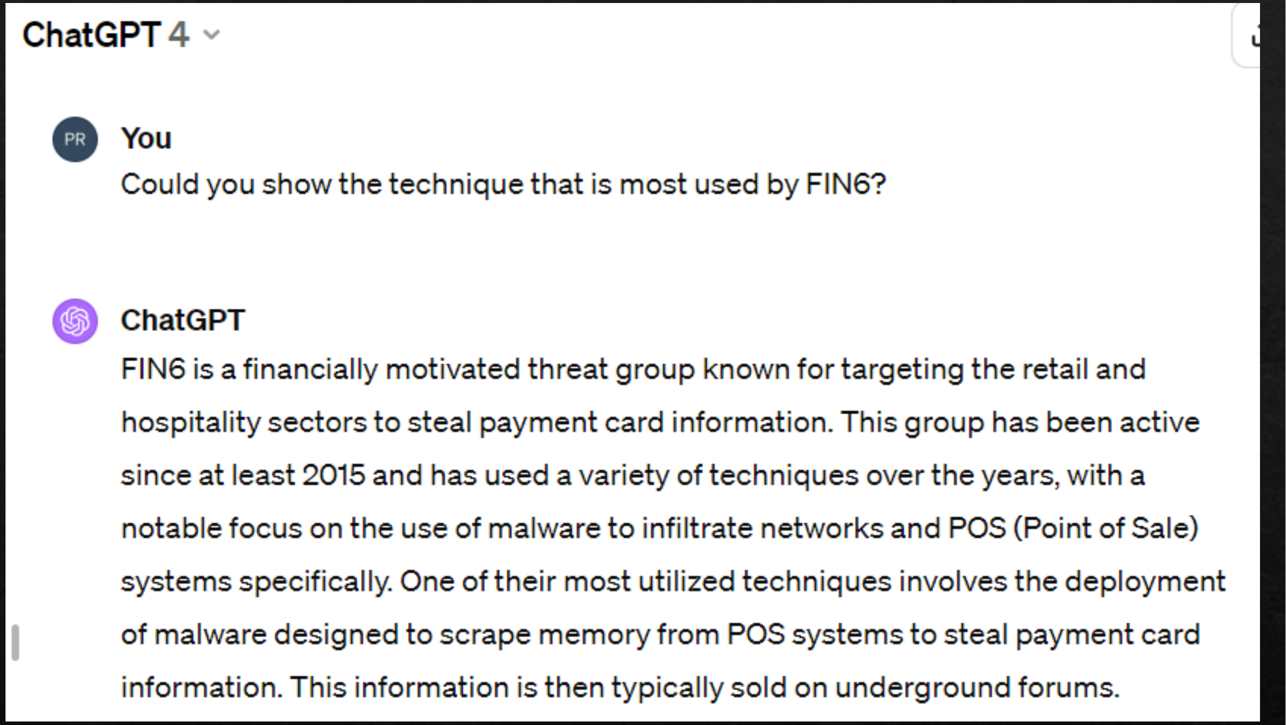
# Outline

1. Who am I?
2. What is APS?
3. CTID Cooperation
4. Challenges
5. Solution
6. Use Cases
7. New Research Area
8. Takeaways

Generated by AI (DALL-E)

# Solution for the Challenges

- We can already use Generative AI on your browser or application
- Generative AI can also …
  - Generate intelligence beyond search from ATT&CK (overcome Challenge 1)
  - Generate many artifacts like STIX 2.1, IDS rule files (overcome Challenge 2)



**You**

Could you show the technique that is most used by FIN6?

**ChatGPT**

FIN6 is a financially motivated threat group known for targeting the retail and hospitality sectors to steal payment card information. This group has been active since at least 2015 and has used a variety of techniques over the years, with a notable focus on the use of malware to infiltrate networks and POS (Point of Sale) systems specifically. One of their most utilized techniques involves the deployment of malware designed to scrape memory from POS systems to steal payment card information. This information is then typically sold on underground forums.

- If Generative AI could be easily accessed from APS, it would be more useful

©2024 Fujitsu Defense & National Security Limited

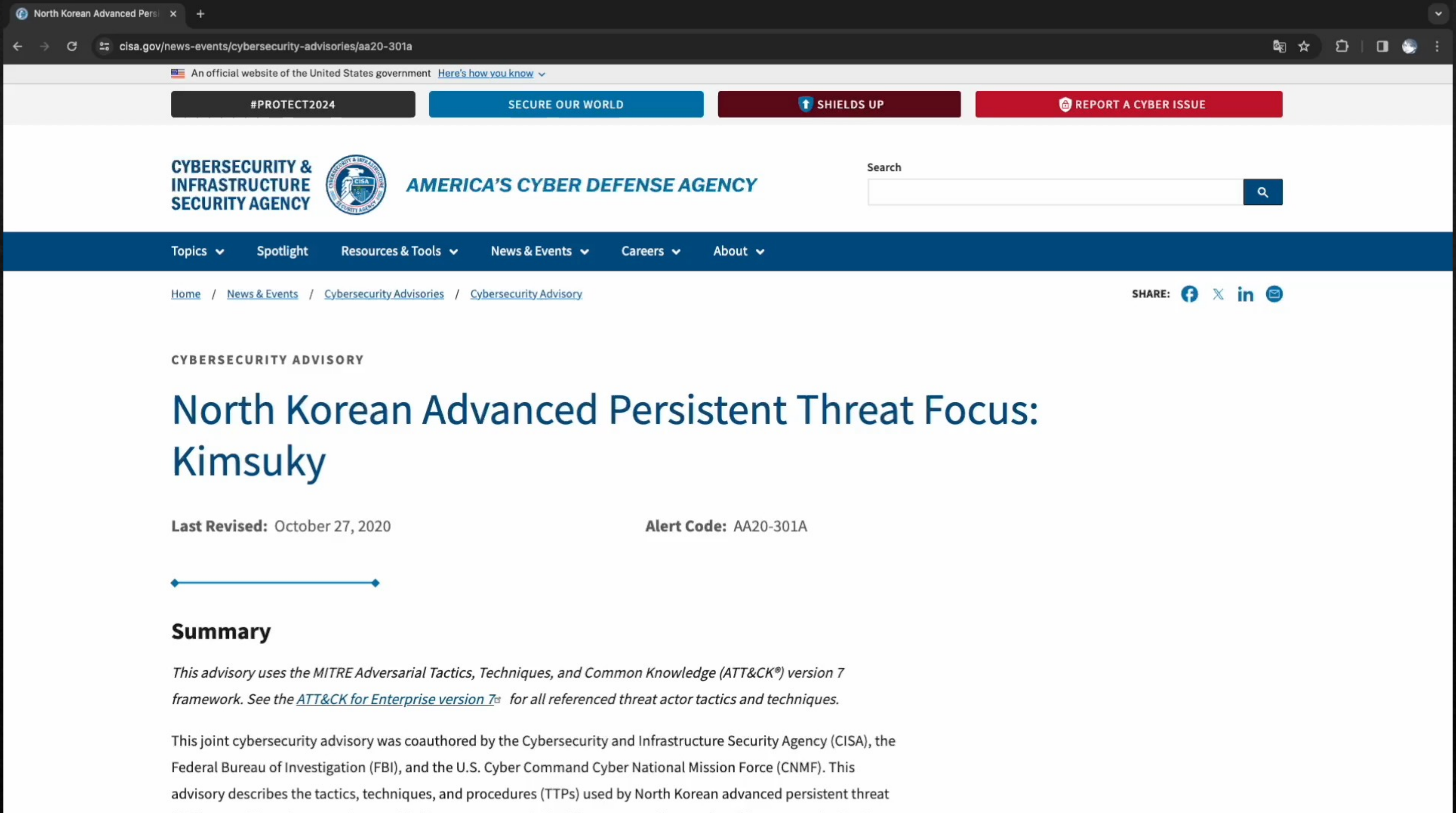
Generated by AI (DALL-E)

# APS Meets OpenAI

- Engaging with OpenAI easily from APS
- With the following parameters, APS can connect with OpenAI easily
  - API Key
  - Models
  - System Instructions
  - Prompt format
- So, I just implemented it

Generated by AI (DALL-E)

# How to Use New Functionality (Demo Movie)


North Korean Advanced Pers
cisa.gov/news-events/cybersecurity-advisories/aa20-301a
An official website of the United States government Here's how you know
#PROTECT2024
SECURE OUR WORLD
SHIELDS UP
REPORT A CYBER ISSUE
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
AMERICA'S CYBER DEFENSE AGENCY
Search
Topics
Spotlight
Resources & Tools
News & Events
Careers
About
Home / News & Events / Cybersecurity Advisories / Cybersecurity Advisory
SHARE:

CYBERSECURITY ADVISORY

North Korean Advanced Persistent Threat Focus: Kimsuky

**Last Revised:** October 27, 2020

**Alert Code:** AA20-301A

**Summary**

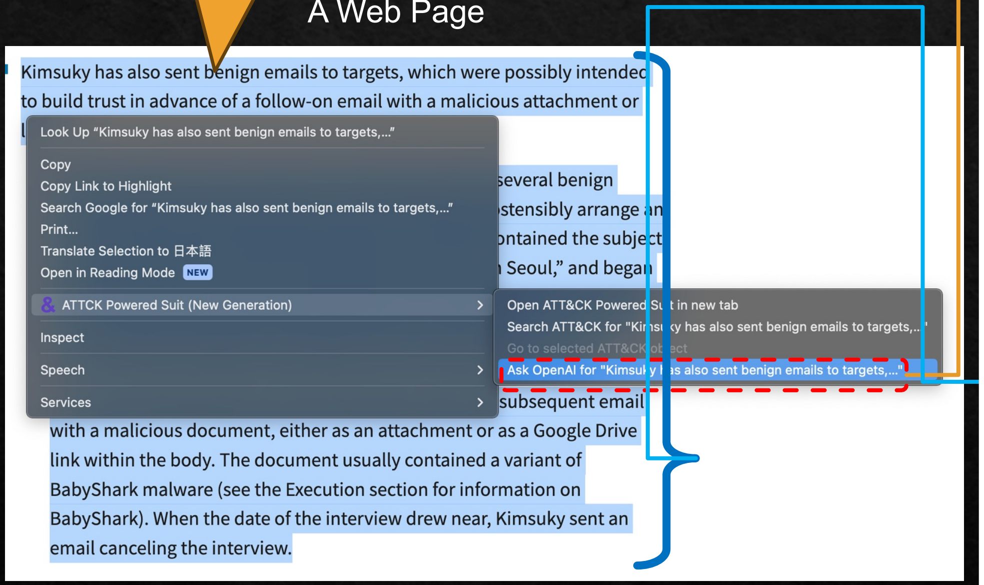
*This advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) version 7 framework. See the ATT&CK for Enterprise version 7 for all referenced threat actor tactics and techniques.*

This joint cybersecurity advisory was coauthored by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the U.S. Cyber Command Cyber National Mission Force (CNMF). This advisory describes the tactics, techniques, and procedures (TTPs) used by North Korean advanced persistent threat

# How to Use New Functionality

Your Browser (select the text block)

A Web Page



Kimsuky has also sent benign emails to targets, which were possibly intended to build trust in advance of a follow-on email with a malicious attachment or

several benign

stensibly arrange an

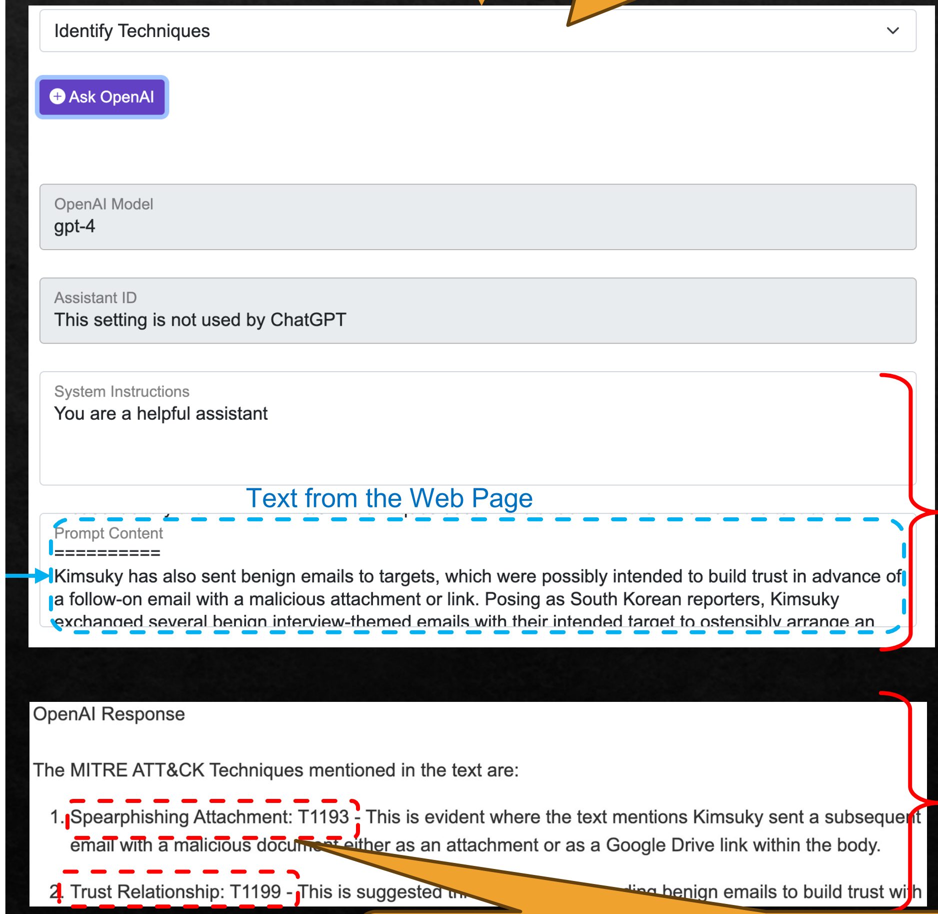
ontained the subject

Seoul," and began

subsequent email with a malicious document, either as an attachment or as a Google Drive link within the body. The document usually contained a variant of BabyShark malware (see the Execution section for information on BabyShark). When the date of the interview drew near, Kimsuky sent an email canceling the interview.

Look Up "Kimsuky has also sent benign emails to targets,..."
Copy
Copy Link to Highlight
Search Google for "Kimsuky has also sent benign emails to targets,..."
Print...
Translate Selection to 日本語
Open in Reading Mode NEW
ATTCK Powered Suit (New Generation)
Inspect
Speech
Services
Open ATT&CK Powered Su t in new tab
Search ATT&CK for "Kimsu ky has also sent benign emails to targets,..."
Go to selected ATT&CK ob ect
Ask OpenAI for "Kimsuky has also sent benign emails to targets,..."

Jump to APS landing page



OpenAI Model
gpt-4

Assistant ID
This setting is not used by ChatGPT

System Instructions
You are a helpful assistant

Prompt Content
==========
Kimsuky has also sent benign emails to targets, which were possibly intended to build trust in advance of a follow-on email with a malicious attachment or link. Posing as South Korean reporters, Kimsuky exchanged several benign interview-themed emails with their intended target to ostensibly arrange an

OpenAI Response

The MITRE ATT&CK Techniques mentioned in the text are:

1. Spearphishing Attachment: T1193 - This is evident where the text mentions Kimsuky sent a subsequent email with a malicious document either as an attachment or as a Google Drive link within the body.
2. Trust Relationship: T1199 - This is suggested th

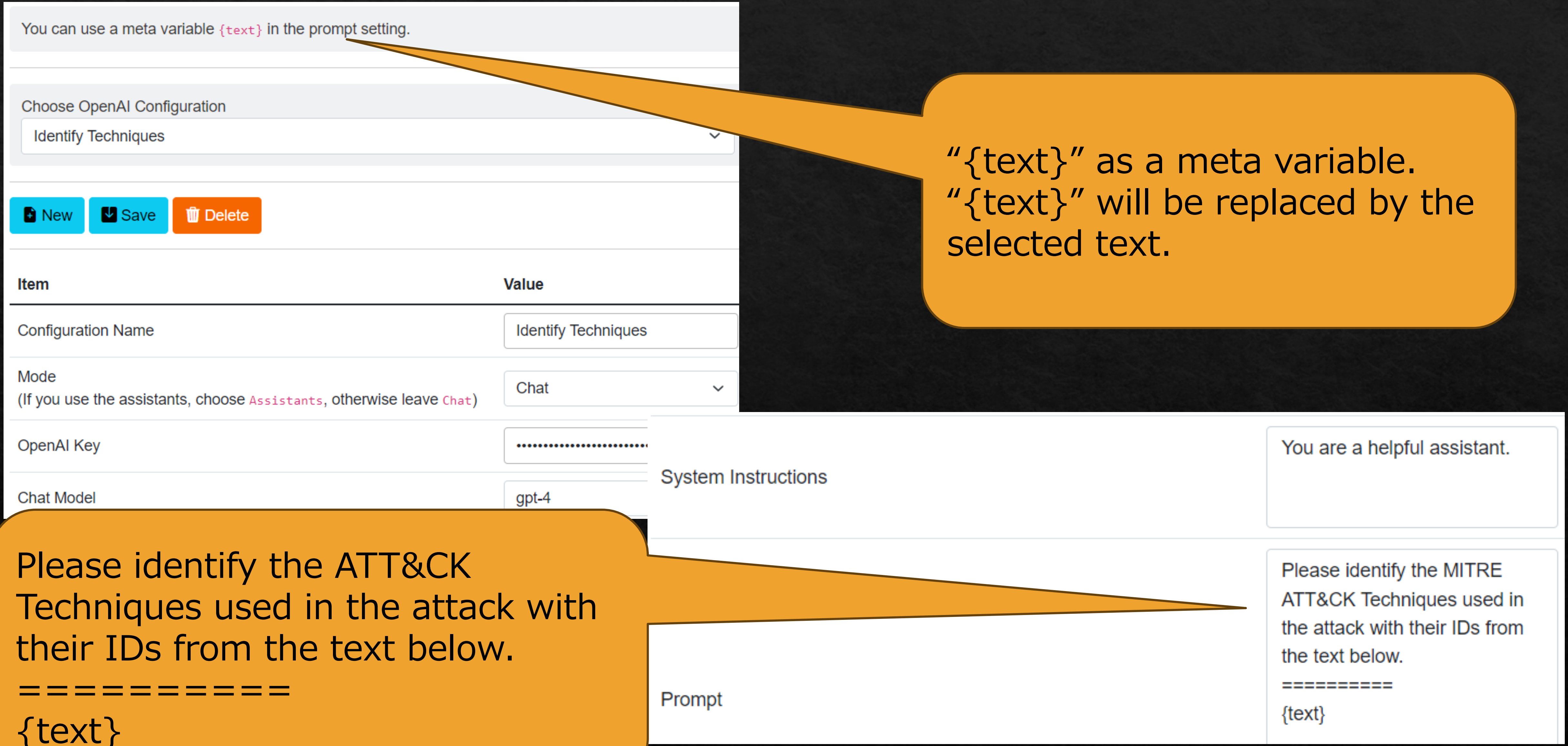
ding benign emails to build trust with

Communicate to OpenAI via REST API

API

OpenAI response with techniques

# Configurations



You can use a meta variable `{text}` in the prompt setting.

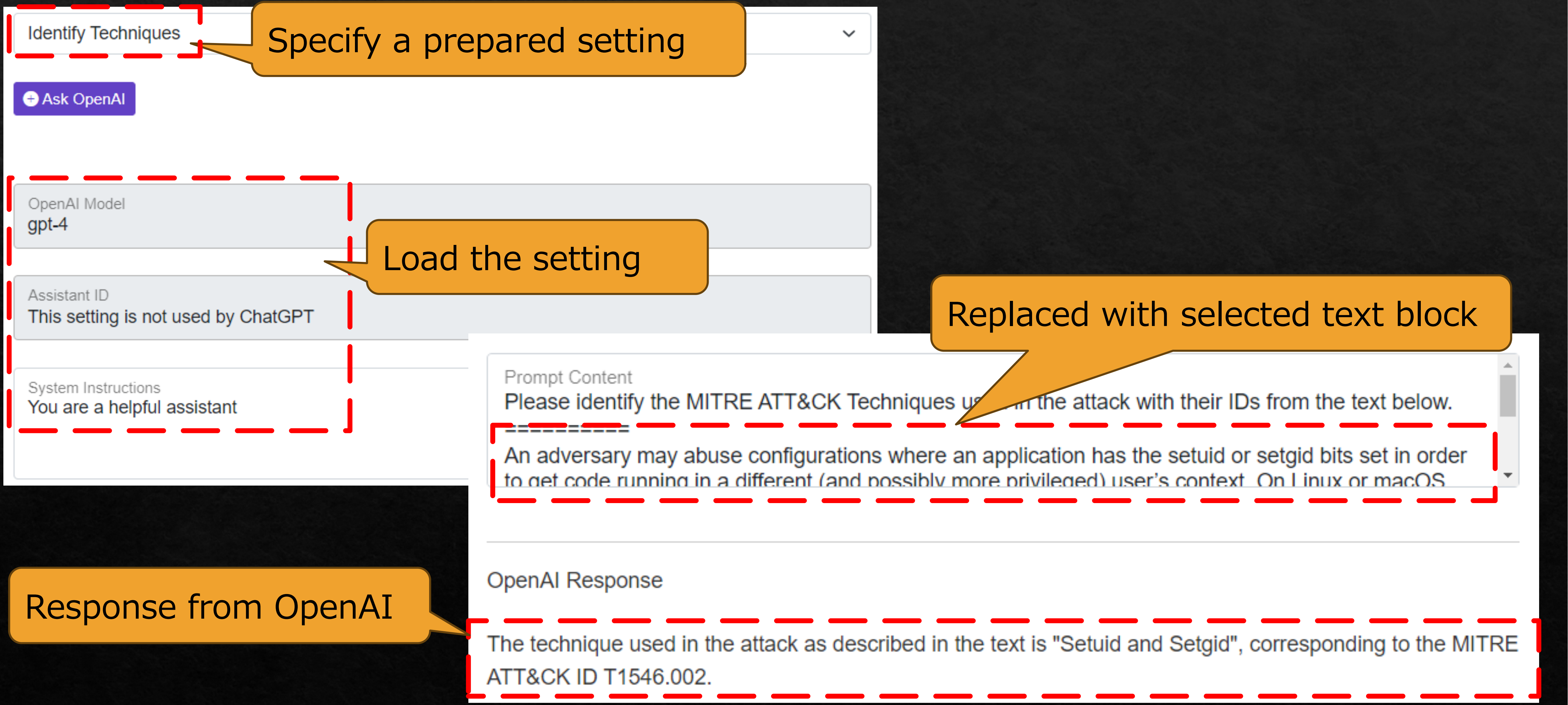
Choose OpenAI Configuration: Identify Techniques

| Item | Value |
|---|---|
| Configuration Name | Identify Techniques |
| Mode<br>(If you use the assistants, choose `Assistants`, otherwise leave `Chat`) | Chat |
| OpenAI Key | •••••••••••••••••••••••••• |
| Chat Model | gpt-4 |
| System Instructions | You are a helpful assistant. |
| Prompt | Please identify the MITRE ATT&CK Techniques used in the attack with their IDs from the text below.<br>==========<br>{text} |

"{text}" as a meta variable.
"{text}" will be replaced by the selected text.

Please identify the ATT&CK Techniques used in the attack with their IDs from the text below.
===========
{text}

# Landing Page



Identify Techniques

Specify a prepared setting

OpenAI Model
gpt-4

Load the setting

Assistant ID
This setting is not used by ChatGPT

System Instructions
You are a helpful assistant

Replaced with selected text block

Prompt Content
Please identify the MITRE ATT&CK Techniques u n the attack with their IDs from the text below.
==========
An adversary may abuse configurations where an application has the setuid or setgid bits set in order to get code running in a different (and possibly more privileged) user's context. On Linux or macOS

OpenAI Response

Response from OpenAI

The technique used in the attack as described in the text is "Setuid and Setgid", corresponding to the MITRE ATT&CK ID T1546.002.

# Outline

1. Who am I?
2. What is APS?
3. CTID Cooperation
4. Challenges
5. Solution
6. Use Cases
7. New Research Area
8. Takeaways

Generated by AI (DALL-E)

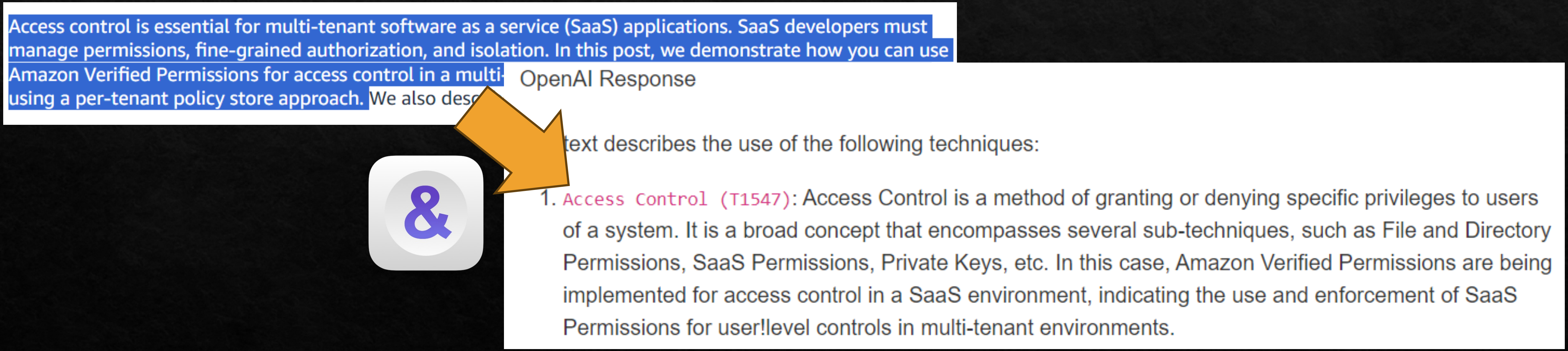
# Use Cases: Inferring Techniques

Challenge 1 is clear

- We can use APS to infer techniques like TRAM!!
- System Instructions configuration

```
Please list the techniques used in the text below with explanations.
---
{text}
```

- Select text block and click right button



Access control is essential for multi-tenant software as a service (SaaS) applications. SaaS developers must manage permissions, fine-grained authorization, and isolation. In this post, we demonstrate how you can use Amazon Verified Permissions for access control in a multi-
using a per-tenant policy store approach. We also desc

OpenAI Response

text describes the use of the following techniques:

1. `Access Control (T1547)`: Access Control is a method of granting or denying specific privileges to users of a system. It is a broad concept that encompasses several sub-techniques, such as File and Directory Permissions, SaaS Permissions, Private Keys, etc. In this case, Amazon Verified Permissions are being implemented for access control in a SaaS environment, indicating the use and enforcement of SaaS Permissions for user!level controls in multi-tenant environments.

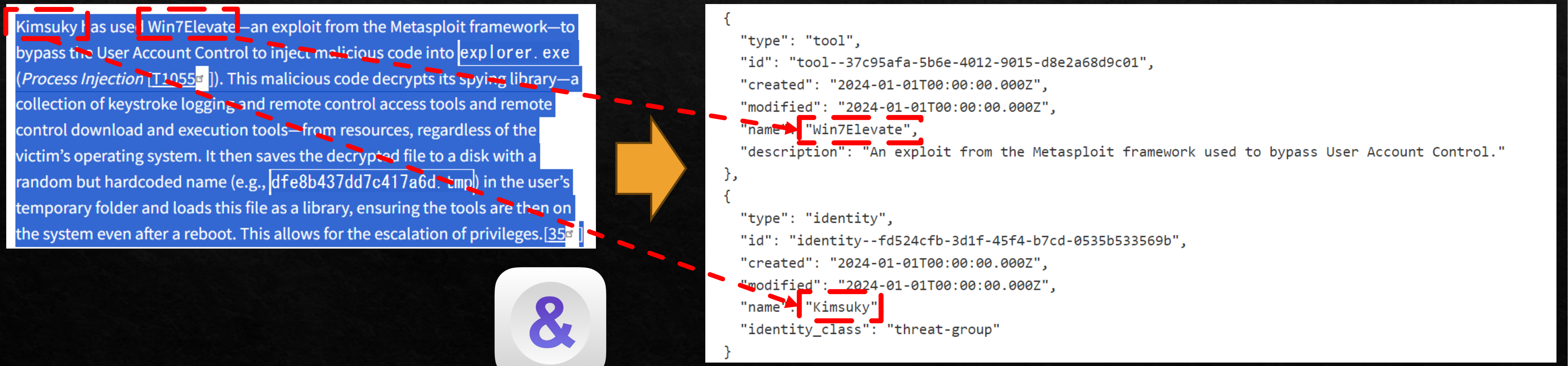
©2024 Fujitsu Defense & National Security Limited

# Use Cases: Generate STIX Content

Challenge 2 is clear

- We can also use APS to generate STIX content related to the selected text

Below is a quote from the blog article.
Create STIX 2.1 from this quote.
Please set the timestamp to 2024/1/1.
---
{text}



Kimsuky has used Win7Elevate—an exploit from the Metasploit framework—to bypass the User Account Control to inject malicious code into `explorer.exe` (*Process Injection* [T1055]). This malicious code decrypts its spying library—a collection of keystroke logging and remote control access tools and remote control download and execution tools—from resources, regardless of the victim's operating system. It then saves the decrypted file to a disk with a random but hardcoded name (e.g., `dfe8b437dd7c417a6d.tmp`) in the user's temporary folder and loads this file as a library, ensuring the tools are then on the system even after a reboot. This allows for the escalation of privileges.[35]

```
{
  "type": "tool",
  "id": "tool--37c95afa-5b6e-4012-9015-d8e2a68d9c01",
  "created": "2024-01-01T00:00:00.000Z",
  "modified": "2024-01-01T00:00:00.000Z",
  "name": "Win7Elevate",
  "description": "An exploit from the Metasploit framework used to bypass User Account Control."
},
{
  "type": "identity",
  "id": "identity--fd524cfb-3d1f-45f4-b7cd-0535b533569b",
  "created": "2024-01-01T00:00:00.000Z",
  "modified": "2024-01-01T00:00:00.000Z",
  "name": "Kimsuky",
  "identity_class": "threat-group"
}
```

# New APS Use Cases: Infinite

```
Please attribute an attacker from this text
block and tell me how to deal with it.
---
{text}
```

- Defenders can change the sentence of these parameters to suit their own needs
- With system introductions and prompt, there are no limits!

Generated by AI (DALL-E)

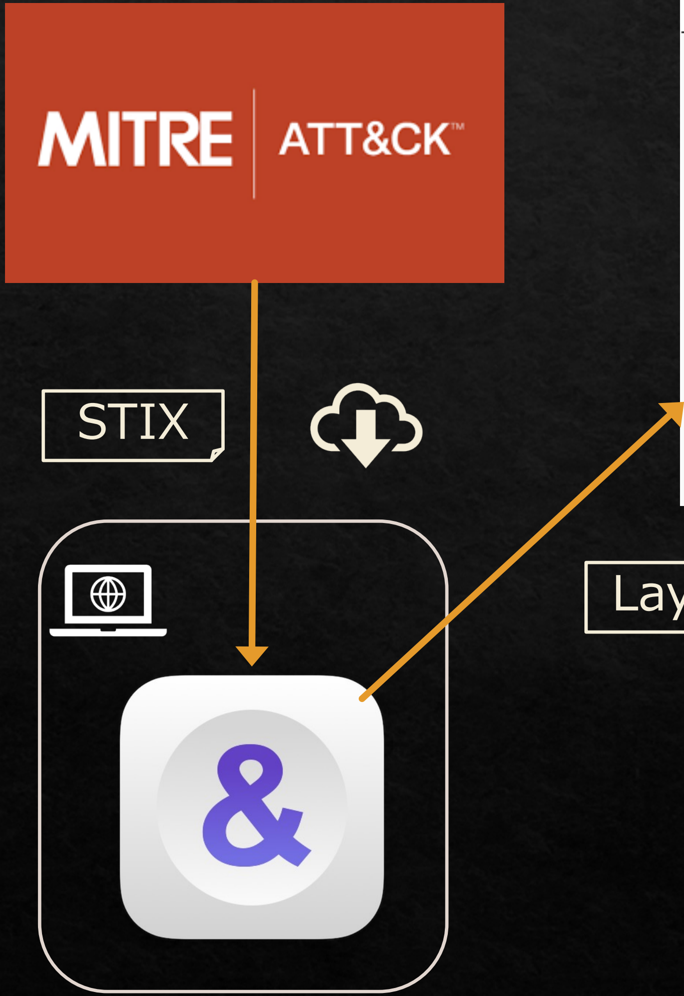
# Outline

1. Who am I?
2. What is APS?
3. CTID Cooperation
4. Challenges
5. Solution
6. Use Cases
7. <u>New Research Area</u>
8. Takeaways

Generated by AI (DALL-E)

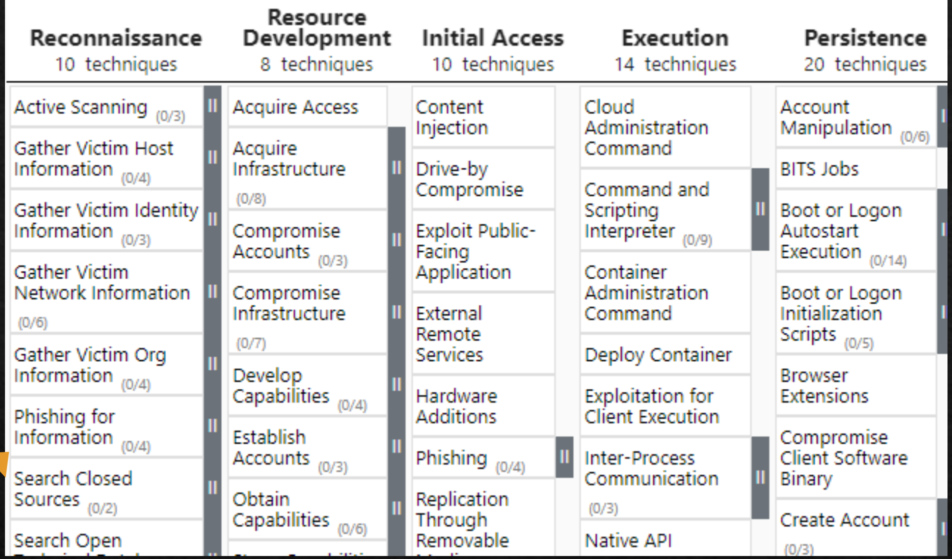
©2024 Fujitsu Defense & National Security Limited

# Current Overview



STIX

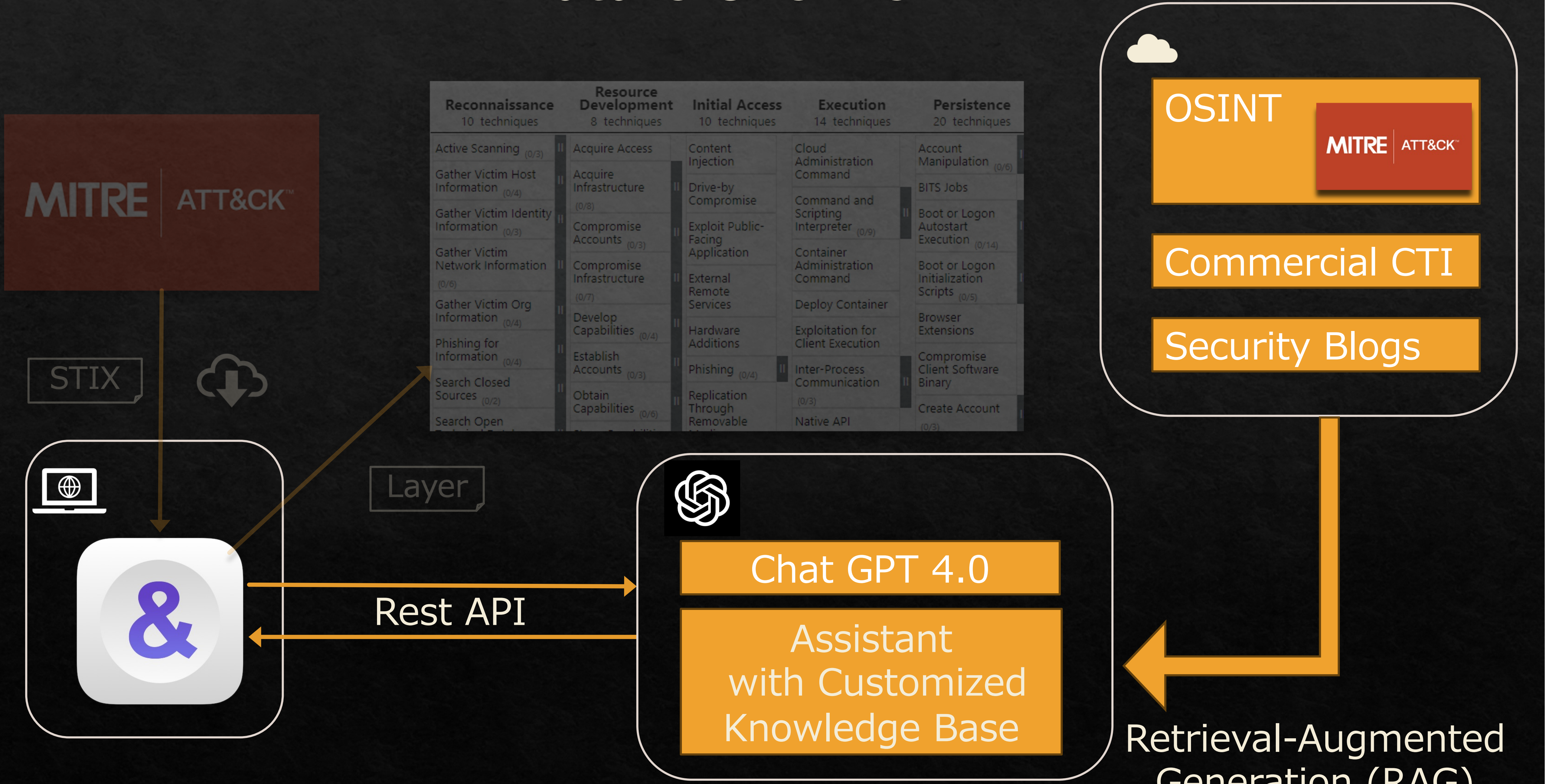
Layer



| Reconnaissance 10 techniques | Resource Development 8 techniques | Initial Access 10 techniques | Execution 14 techniques | Persistence 20 techniques |
|---|---|---|---|---|
| Active Scanning (0/3) | Acquire Access | Content Injection | Cloud Administration Command | Account Manipulation (0/6) |
| Gather Victim Host Information (0/4) | Acquire Infrastructure (0/8) | Drive-by Compromise | Command and Scripting Interpreter (0/9) | BITS Jobs |
| Gather Victim Identity Information (0/3) | Compromise Accounts (0/3) | Exploit Public-Facing Application | Container Administration Command | Boot or Logon Autostart Execution (0/14) |
| Gather Victim Network Information (0/6) | Compromise Infrastructure (0/7) | External Remote Services | Deploy Container | Boot or Logon Initialization Scripts (0/5) |
| Gather Victim Org Information (0/4) | Develop Capabilities (0/4) | Hardware Additions | Exploitation for Client Execution | Browser Extensions |
| Phishing for Information (0/4) | Establish Accounts (0/3) | Phishing (0/4) | Inter-Process Communication (0/3) | Compromise Client Software Binary |
| Search Closed Sources (0/2) | Obtain Capabilities (0/6) | Replication Through Removable | Native API | Create Account (0/3) |
| Search Open | | | | |

©2024 Fujitsu Defense & National Security Limited

# Future Overview



| Reconnaissance<br>10 techniques | Resource Development<br>8 techniques | Initial Access<br>10 techniques | Execution<br>14 techniques | Persistence<br>20 techniques |
|---|---|---|---|---|
| Active Scanning (0/3) | Acquire Access | Content Injection | Cloud Administration Command | Account Manipulation (0/6) |
| Gather Victim Host Information (0/4) | Acquire Infrastructure (0/8) | Drive-by Compromise | Command and Scripting Interpreter (0/9) | BITS Jobs |
| Gather Victim Identity Information (0/3) | Compromise Accounts (0/3) | Exploit Public-Facing Application | Container Administration Command | Boot or Logon Autostart Execution (0/14) |
| Gather Victim Network Information (0/6) | Compromise Infrastructure (0/7) | External Remote Services | Deploy Container | Boot or Logon Initialization Scripts (0/5) |
| Gather Victim Org Information (0/4) | Develop Capabilities (0/4) | Hardware Additions | Exploitation for Client Execution | Browser Extensions |
| Phishing for Information (0/4) | Establish Accounts (0/3) | Phishing (0/4) | Inter-Process Communication (0/3) | Compromise Client Software Binary |
| Search Closed Sources (0/2) | Obtain Capabilities (0/6) | Replication Through Removable | Native API | Create Account (0/3) |
| Search Open | | | | |

Rest API

Chat GPT 4.0

Assistant with Customized Knowledge Base

OSINT

MITRE | ATT&CK

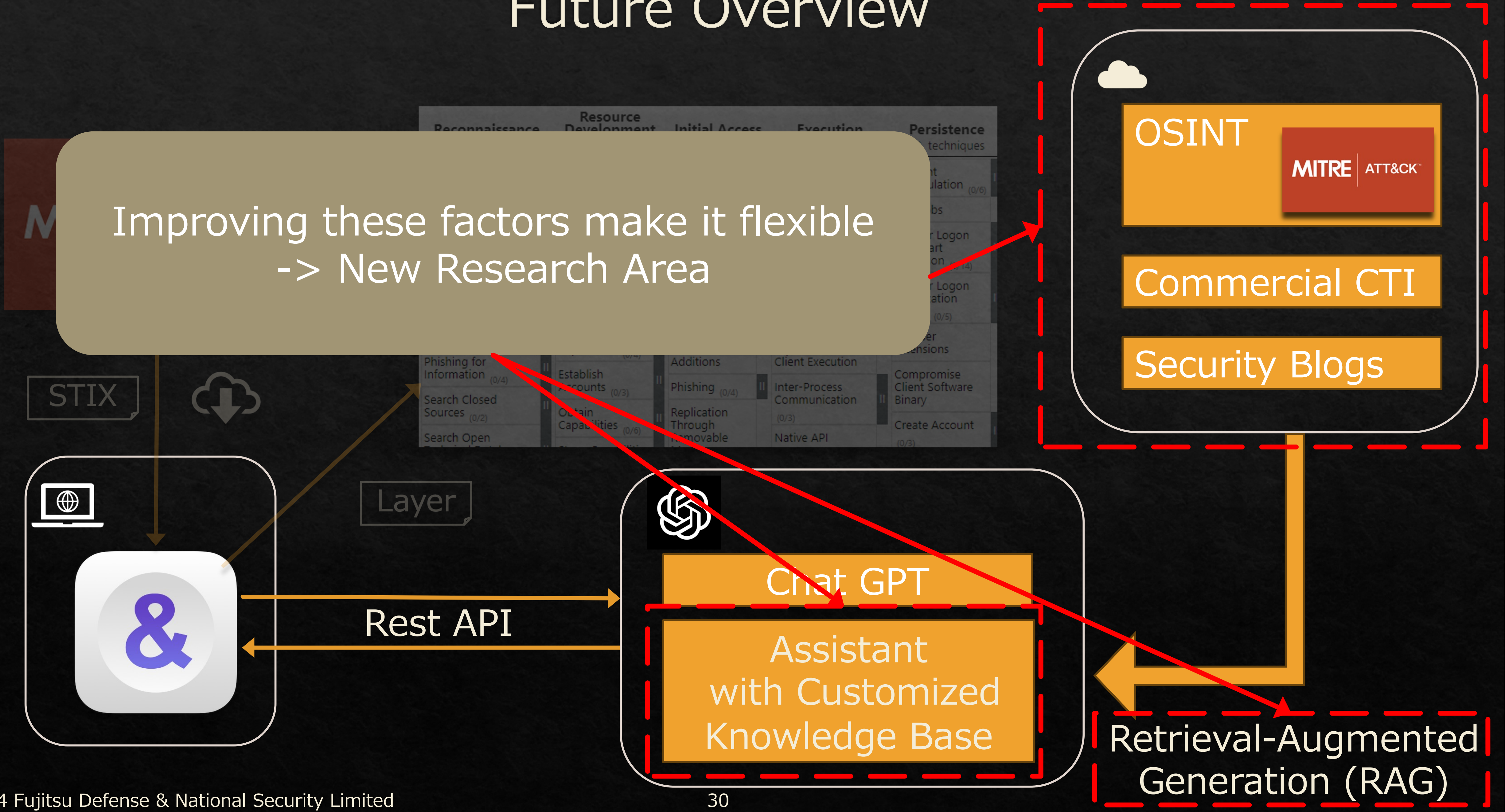
Commercial CTI

Security Blogs

Retrieval-Augmented Generation (RAG)

©2024 Fujitsu Defense & National Security Limited

# Future Overview



Improving these factors make it flexible
-> New Research Area

OSINT

Commercial CTI

Security Blogs

Rest API

Chat GPT

Assistant with Customized Knowledge Base

Retrieval-Augmented Generation (RAG)

©2024 Fujitsu Defense & National Security Limited

# New Research Area

- Assistant is just one of methods (= LLM with RAG + Rest API)
- Other services/approaches are being rolled out (i.e. Copilot Pro)
- Building an LLM for a CTI domain
  - ATT&CK knowledge base
  - CVE from MITRE
  - Commercial CTI
  - OSINT

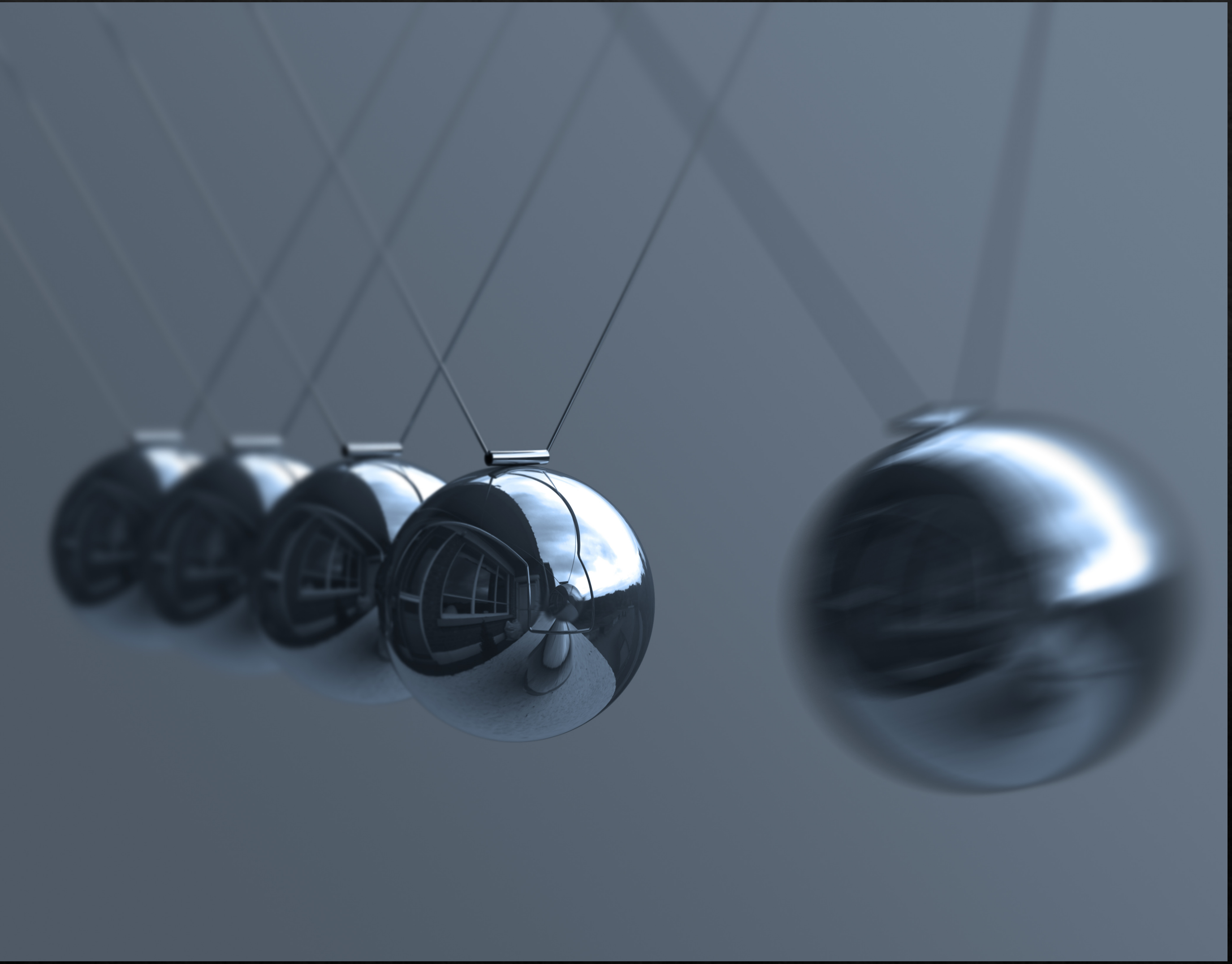
©2024 Fujitsu Defense & National Security Limited

# Outline

1. Who am I?
2. What is APS?
3. CTID Cooperation
4. Challenges
5. Solution
6. Use Cases
7. New Research Area
8. <u>Takeaways</u>

Generated by AI (DALL-E)

# Takeaways



- ATT&CK provides a common language for various layers of defenders
- ATT&CK Powered Suit was created to utilize ATT&CK
- Integration with Generative AI is incredibly beneficial
- With Model and Prompt configurations, possibilities are infinite
- CTI-domain LLM has new potential
- **ATT&CK Powered Suit can further power up defenders by being combined with Generative AI!!**

©2024 Fujitsu Defense & National Security Limited

# Thank you!!

- Toshitaka Satomi
- Fujitsu Defense & National Security Limited
- Researcher
- @stmtstk
- in @stmtstk
- 🤗 @stmtstk

©2024 Fujitsu Defense & National Security Limited