Risks and benefits of ChatGPT 4 in defensive operations

Chris Hammond-Thrasher CISSP-ISSMP

For Cyber Alberta

06 March 2024

Chris Hammond-Thrasher CISSP-ISSMP
Fujitsu North America
Director, Enterprise and Cyber Security Consulting
Chris.Hammond-Thrasher@Fujitsu.com

Credit where credit is due

Daemon Behr

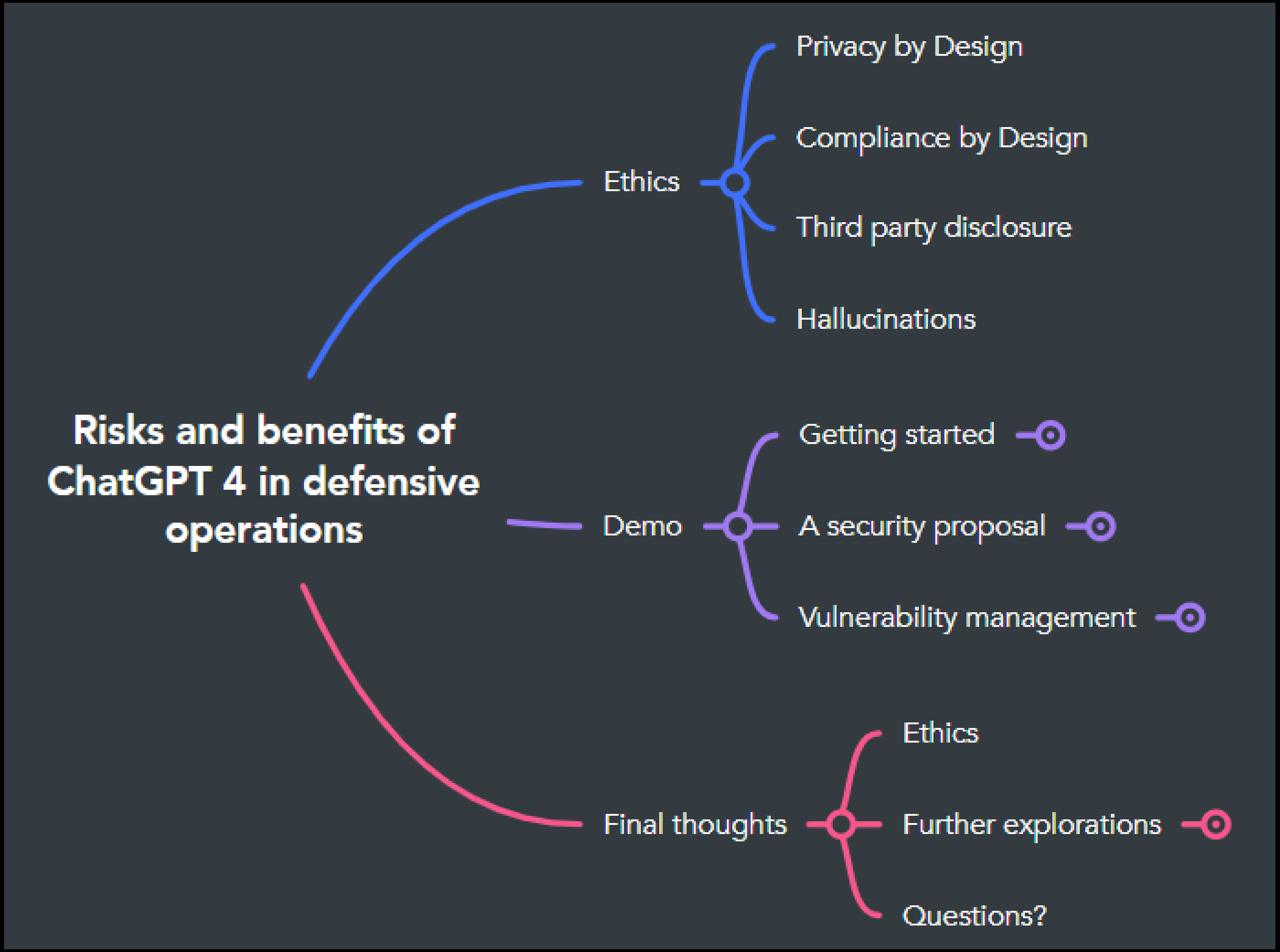
Executive Chair

Canadian Cyber Auxiliary

https://cca-cac.ca/

I would not be presenting about ChatGPT 4 without having been inspired by Daemon's brilliant presentation following the 2023 ICS2 Security Congress

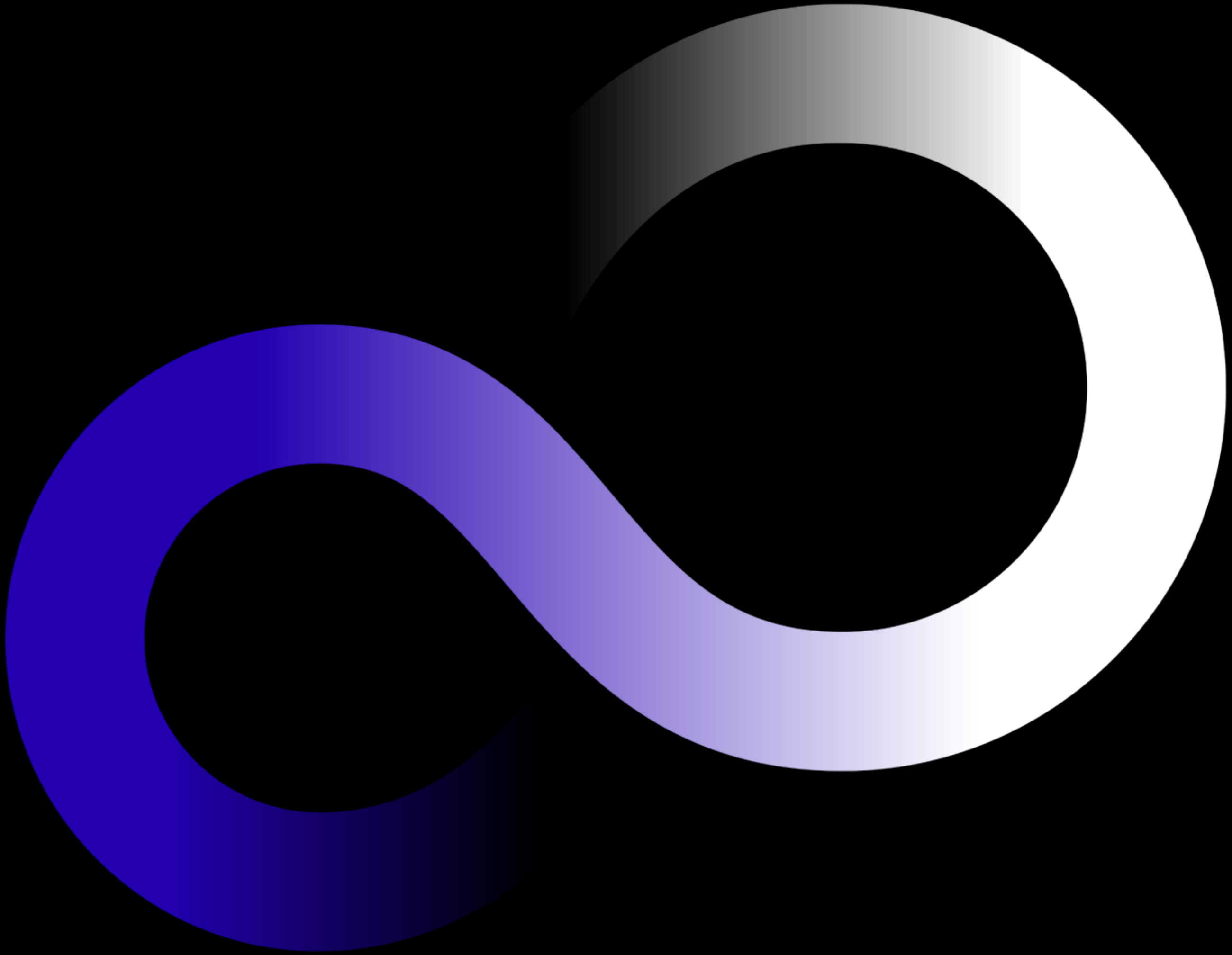
Agenda



Risks and benefits of ChatGPT 4 in defensive operations

- Ethics
  - Privacy by Design
  - Compliance by Design
  - Third party disclosure
  - Hallucinations
- Demo
  - Getting started
  - A security proposal
  - Vulnerability management
- Final thoughts
  - Ethics
  - Further explorations
  - Questions?

Ethics

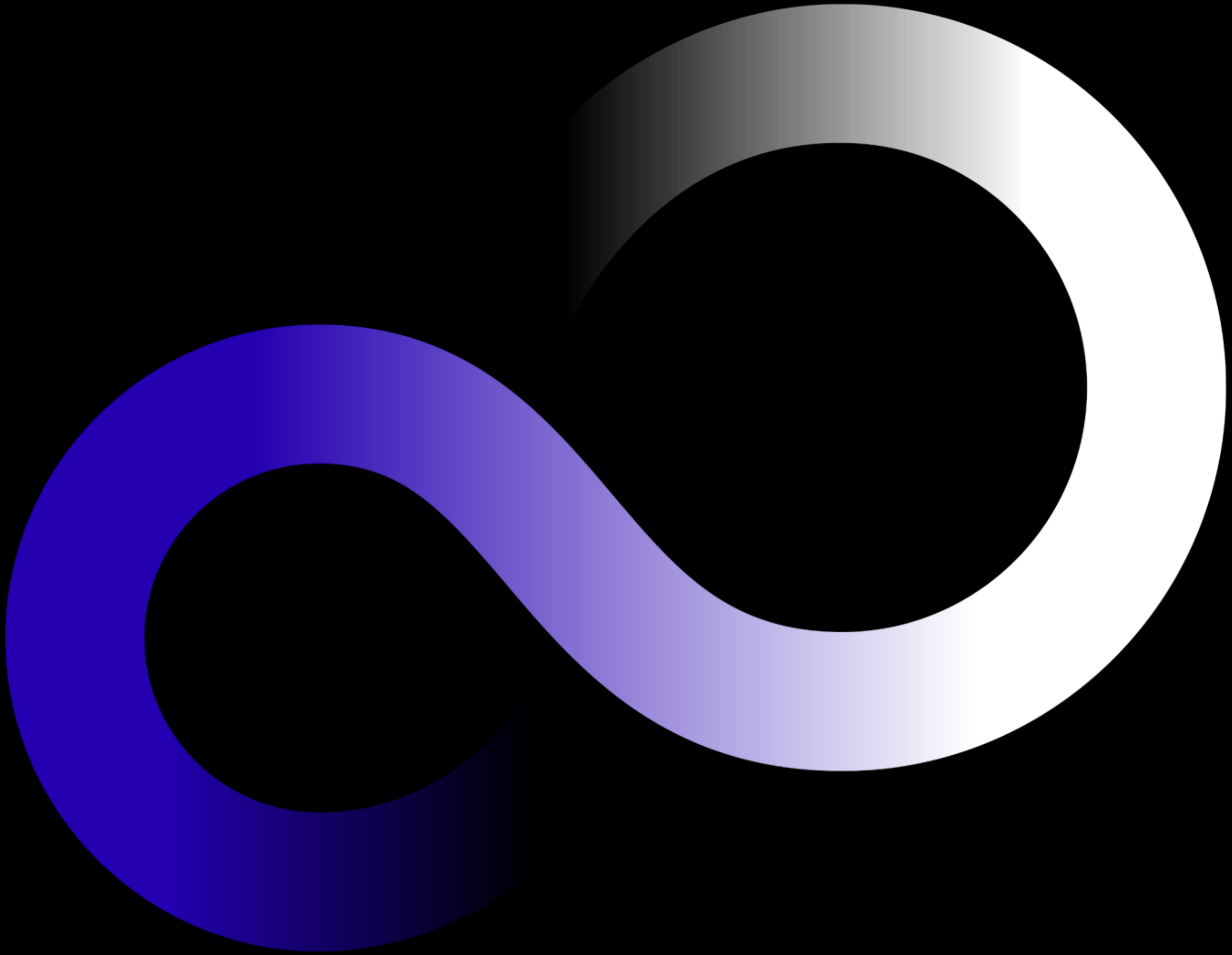


Ethics

- Privacy by design
- Compliance by design
- Third party disclosure
- Hallucinations

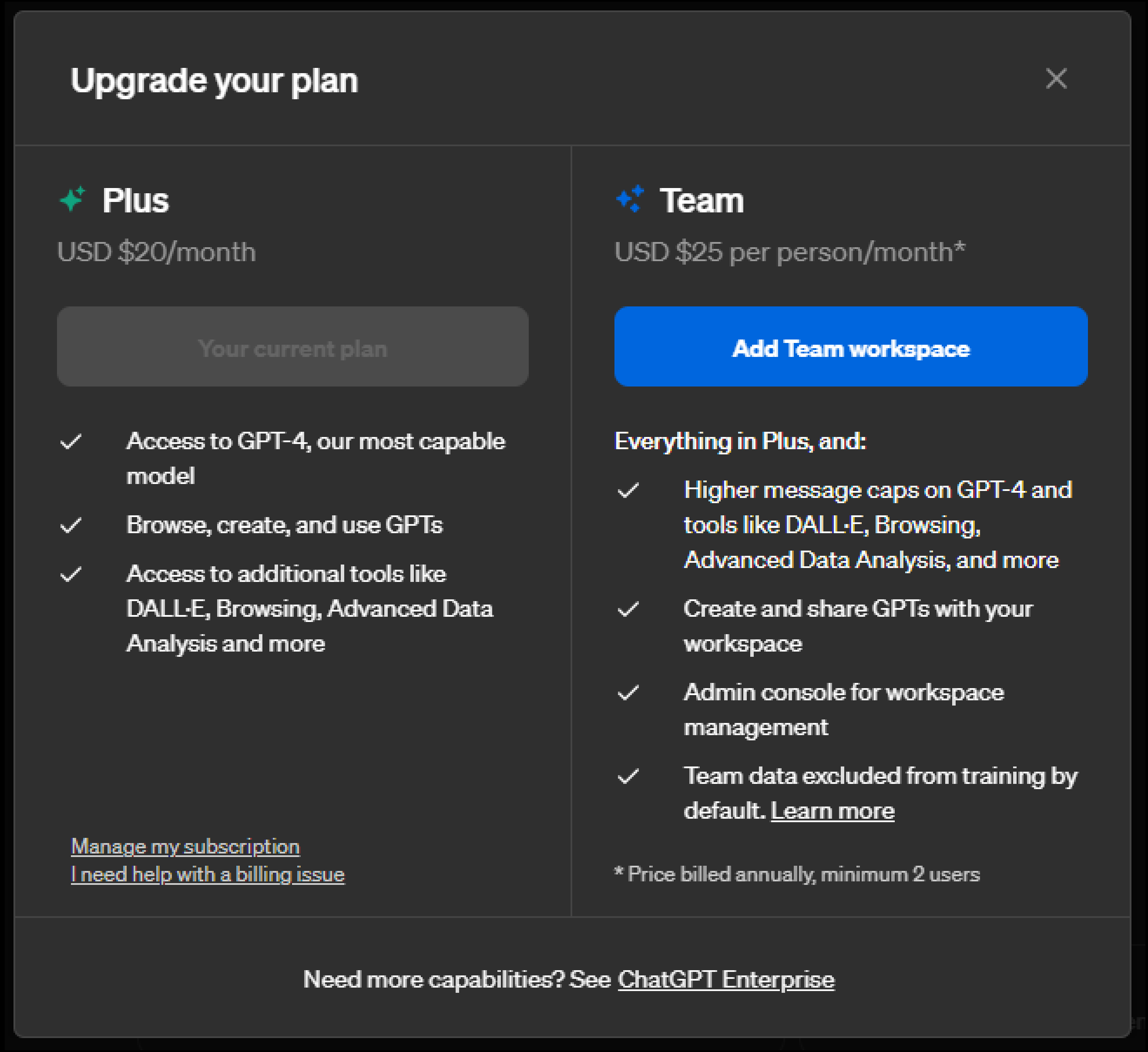
Demo 1

Be smart getting started with ChatGPT 4



Getting started

https://openai.com/



Upgrade your plan

Plus

USD $20/month

- ✓ Access to GPT-4, our most capable model
- ✓ Browse, create, and use GPTs
- ✓ Access to additional tools like DALL·E, Browsing, Advanced Data Analysis and more

Manage my subscription
I need help with a billing issue

Team

USD $25 per person/month*

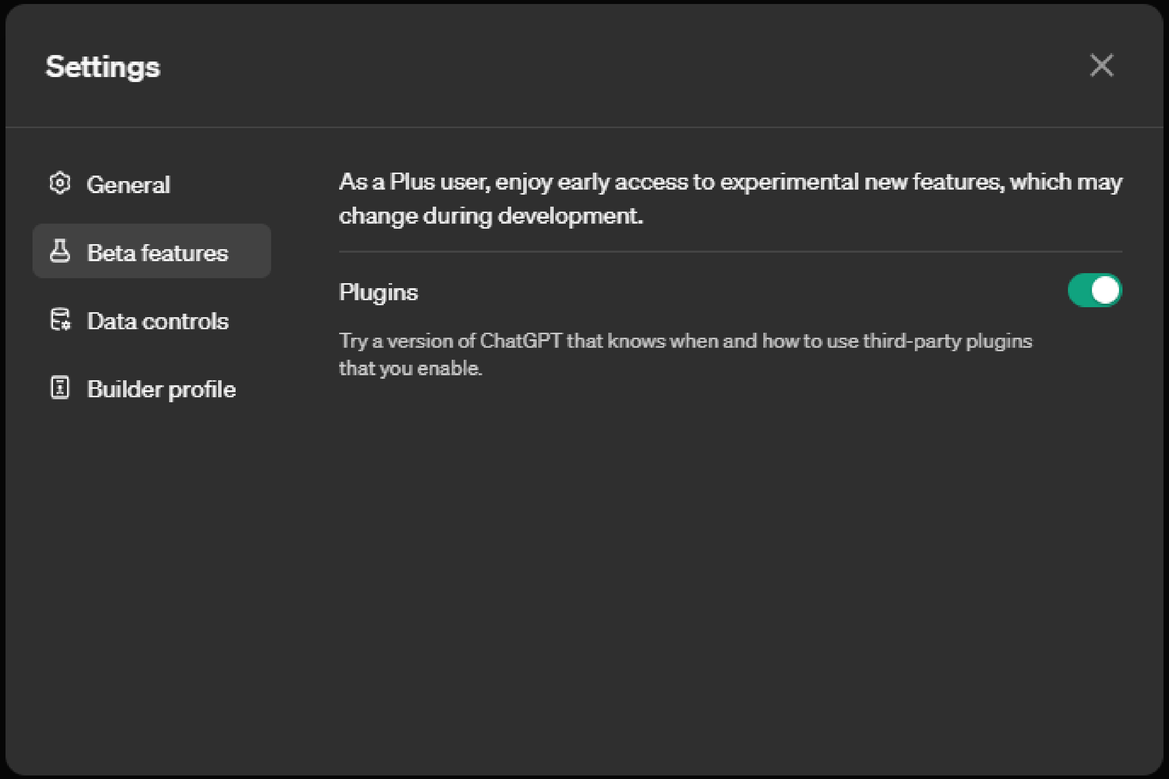
Everything in Plus, and:

- ✓ Higher message caps on GPT-4 and tools like DALL·E, Browsing, Advanced Data Analysis, and more
- ✓ Create and share GPTs with your workspace
- ✓ Admin console for workspace management
- ✓ Team data excluded from training by default. Learn more

* Price billed annually, minimum 2 users

Need more capabilities? See ChatGPT Enterprise

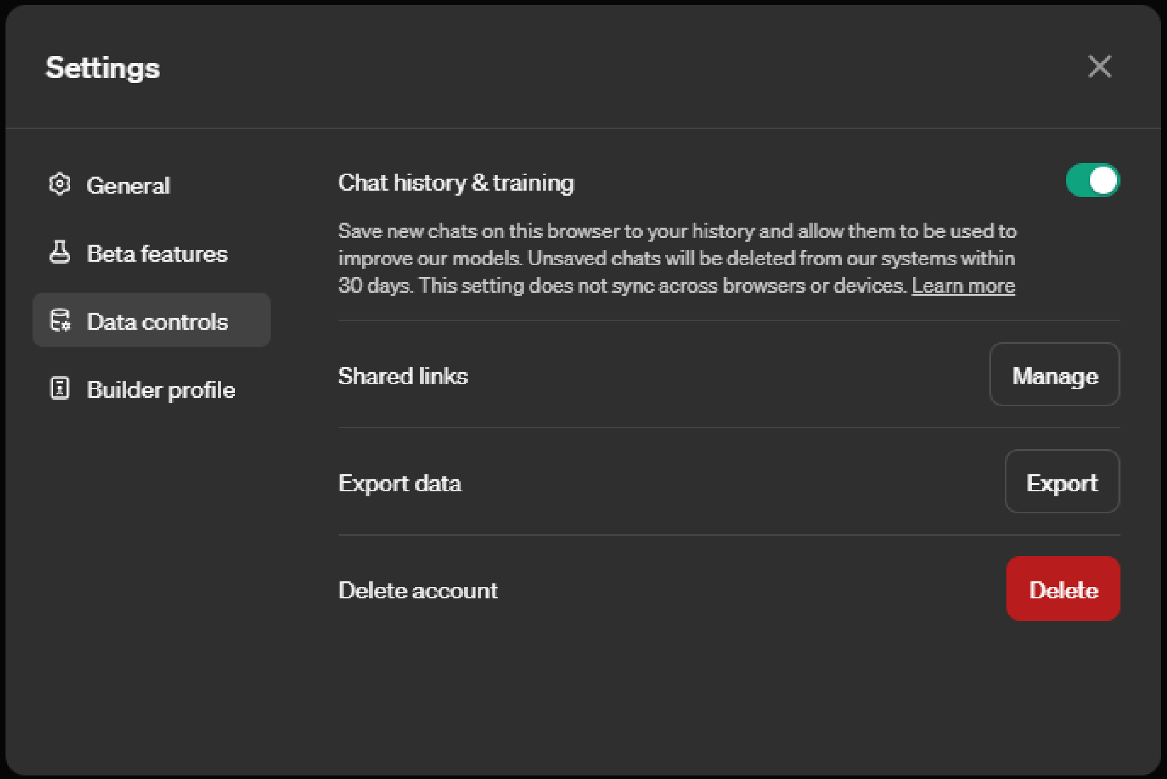
Privacy-informed settings



As a Plus user, enjoy early access to experimental new features, which may change during development.

Plugins ●

Try a version of ChatGPT that knows when and how to use third-party plugins that you enable.



Chat history & training ●

Save new chats on this browser to your history and allow them to be used to improve our models. Unsaved chats will be deleted from our systems within 30 days. This setting does not sync across browsers or devices. Learn more

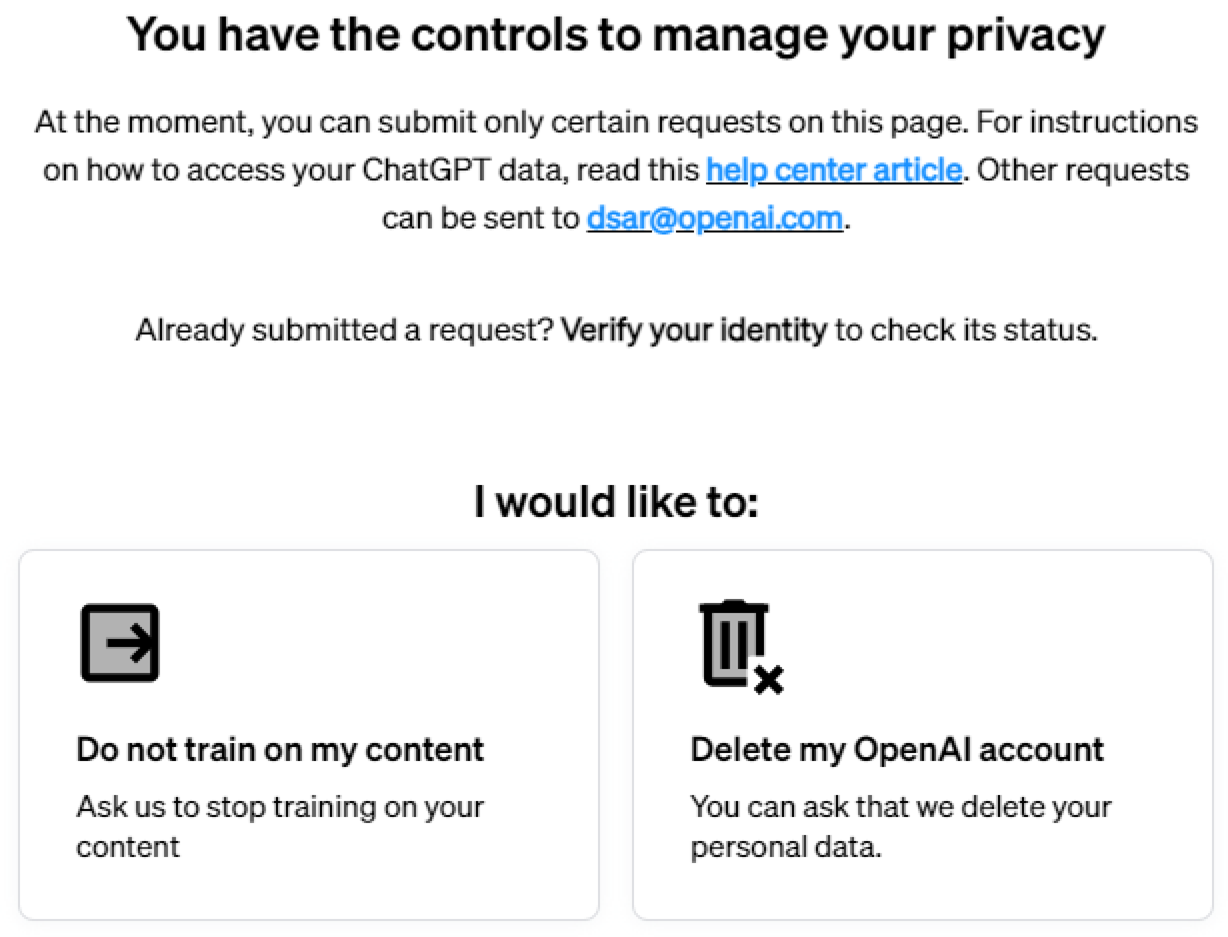
Shared links — Manage

Export data — Export

Delete account — Delete

Privacy opt-out

https://privacy.openai.com



You have the controls to manage your privacy

At the moment, you can submit only certain requests on this page. For instructions on how to access your ChatGPT data, read this help center article. Other requests can be sent to dsar@openai.com.

Already submitted a request? **Verify your identity** to check its status.

I would like to:

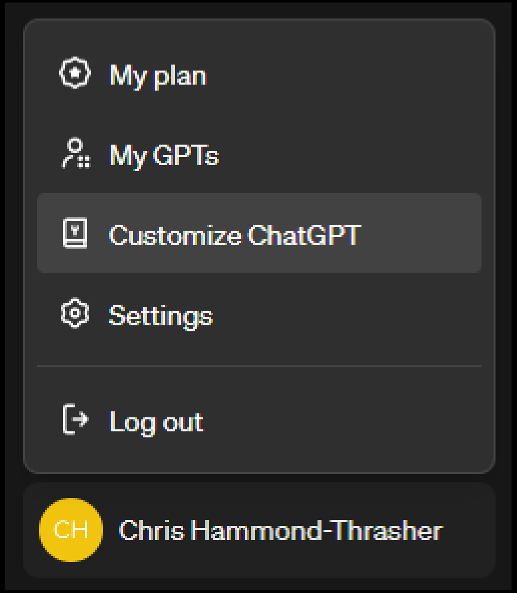
Do not train on my content

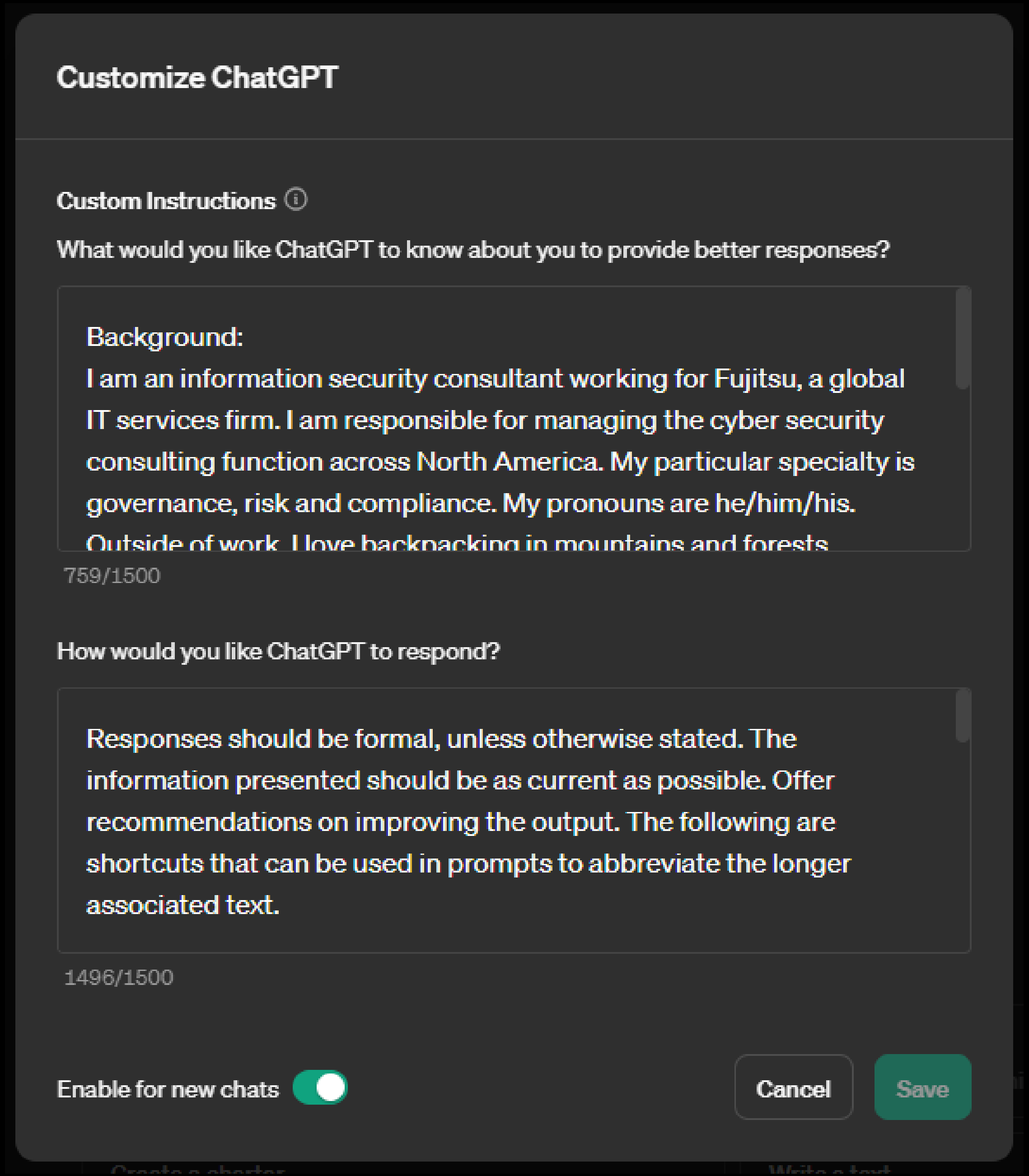
Ask us to stop training on your content

Delete my OpenAI account

You can ask that we delete your personal data.

“Profile” settings





What would you like ChatGPT to know about you to provide better responses?

Background:
I am an information security consultant working for Fujitsu, a global IT services firm. I am responsible for managing the cyber security consulting function across North America. My particular specialty is governance, risk and compliance. My pronouns are he/him/his.
Outside of work, I love backpacking in mountains and forests

759/1500

How would you like ChatGPT to respond?

Responses should be formal, unless otherwise stated. The information presented should be as current as possible. Offer recommendations on improving the output. The following are shortcuts that can be used in prompts to abbreviate the longer associated text.

1496/1500

Enable for new chats: ●

What would you like ChatGPT to know about you to provide better responses?

Background:
I am an information security consultant working for Fujitsu, a global IT services firm. I am responsible for managing the cyber security consulting function across North America. My particular specialty is governance, risk and compliance. My pronouns are he/him/his. Outside of work, I love backpacking in mountains and forests.

Objectives:
Consulting: Keeping up to date on consulting theory and "soft skills" with a particular interest in applying strategy to information security.
Compliance: Keeping up on major IT and OT security standards including ISO 27001, NIST-CSF and IEC 62443.
Risk: Improving my understanding of information security risk methodologies and approaches.
Privacy: Keeping up on changes to privacy theory and regulation.

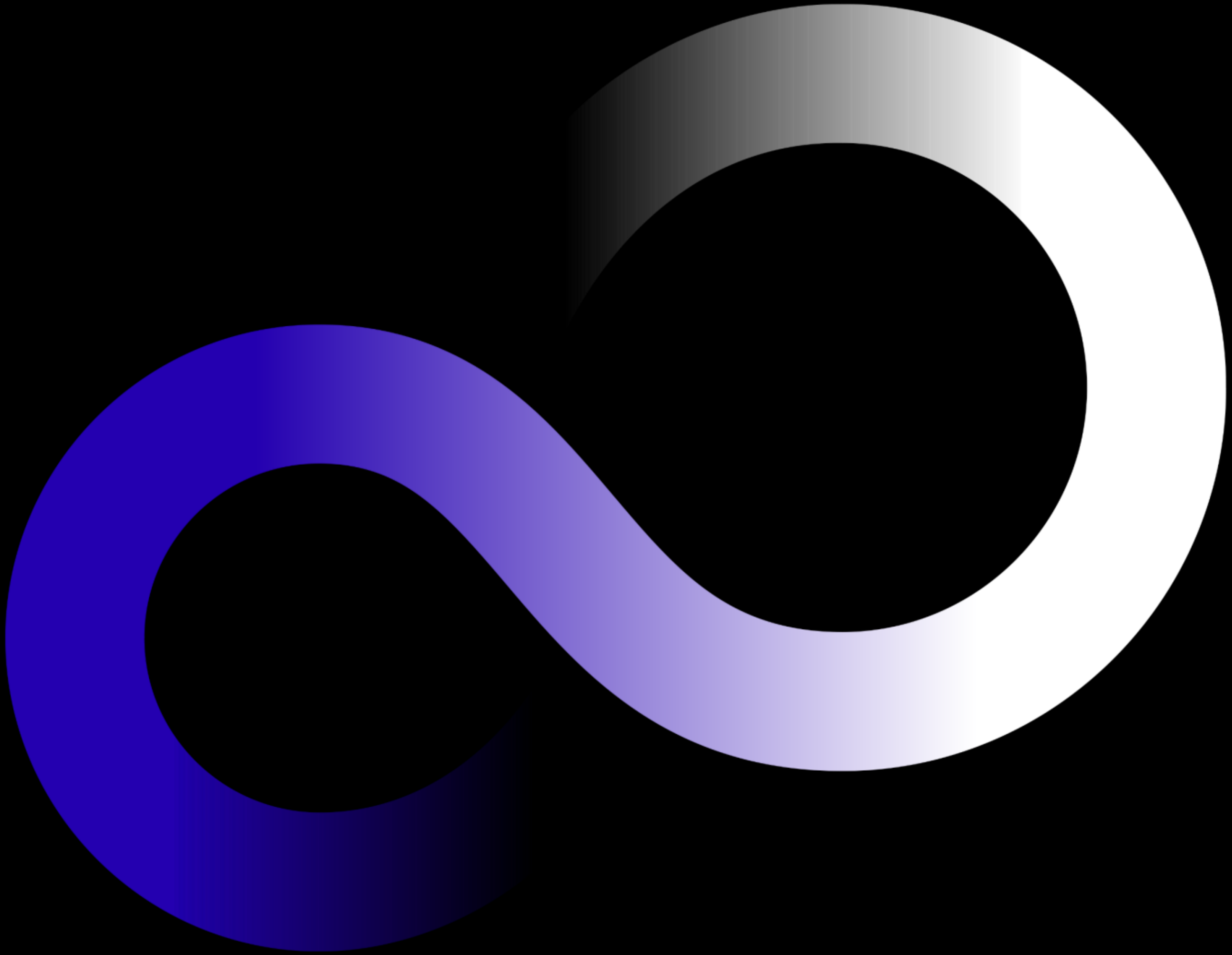
How would you like ChatGPT to respond?

Responses should be formal, unless otherwise stated. The information presented should be as current as possible. Offer recommendations on improving the output. The following are shortcuts that can be used in prompts to abbreviate the longer associated text.

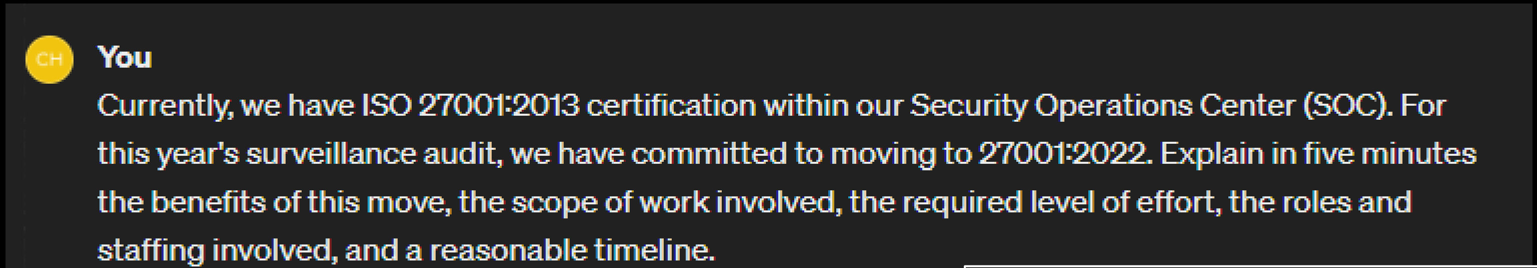
/list: provide a list of all short codes currently configured in my custom instructions
/sum: summarize the following transcript in detail in point form.
/longsum: summarize the following in a detailed, well structured manner that can be shared with colleagues.
/patch-alert: Generate a brief summary of newly released security patches along with a list of affected systems within the organization.
/risk-assess: Conduct a quick risk assessment on a specified system, application, or process. Provide an estimated risk score and recommended mitigations.
/comp-check: Assess compliance with a specified standard (e.g., GDPR, HIPAA, ISO 27001) and provide a compliance score along with any non compliant areas.
/inv-review: Perform an inventory review and list all hardware and software assets, highlighting any that are unaccounted for or unsecured.
/user-audit: Provide an audit report on user access rights, specifically looking for overly permissive or unnecessary privileges.
/incid-report: Produce a standardized incident report form for a specified cybersecurity event, including key facts, affected systems, and immediate action items.

Demo 2

A security compliance project

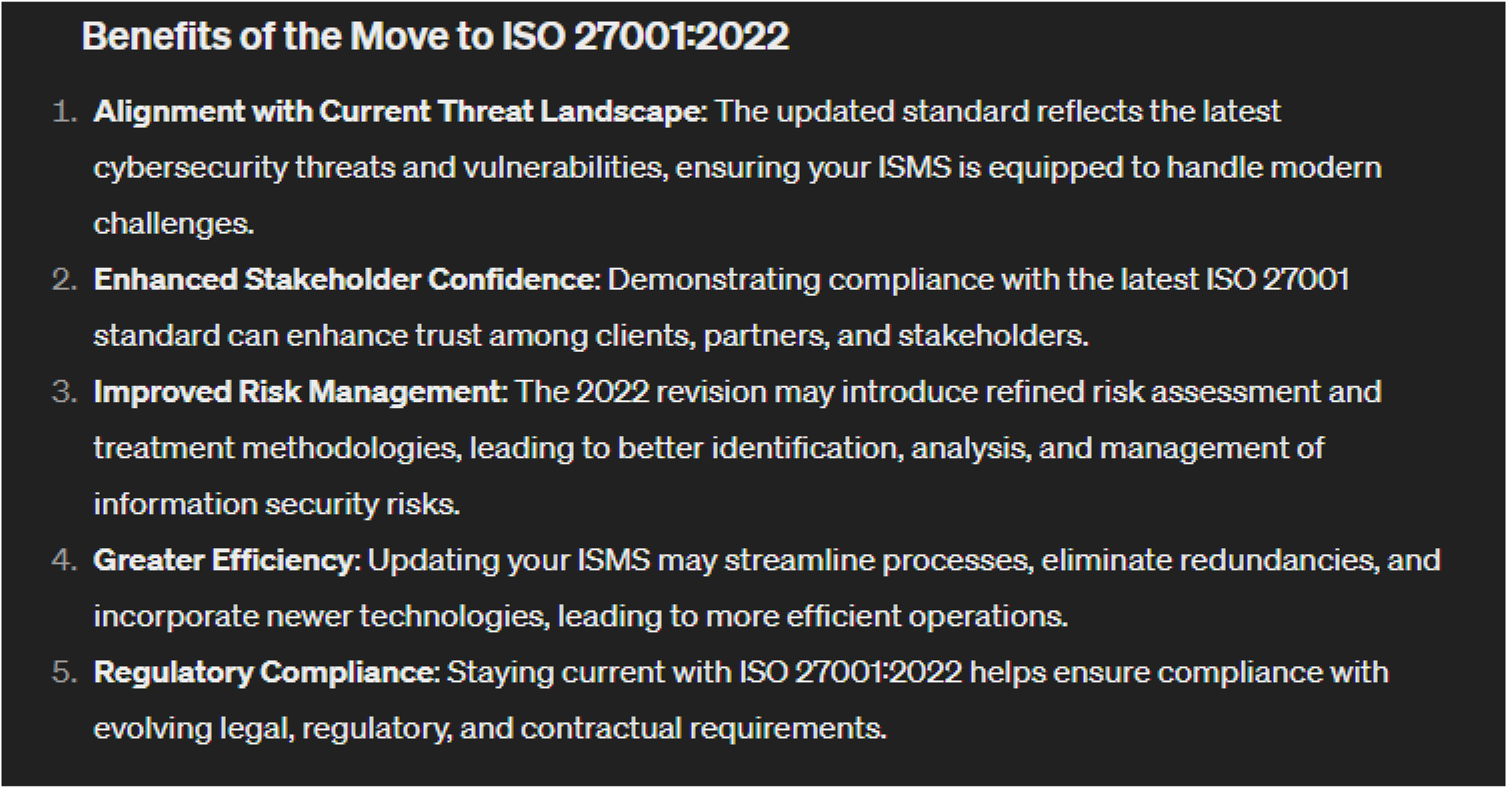


ISO 27001:2013 to 2022 Transition



You

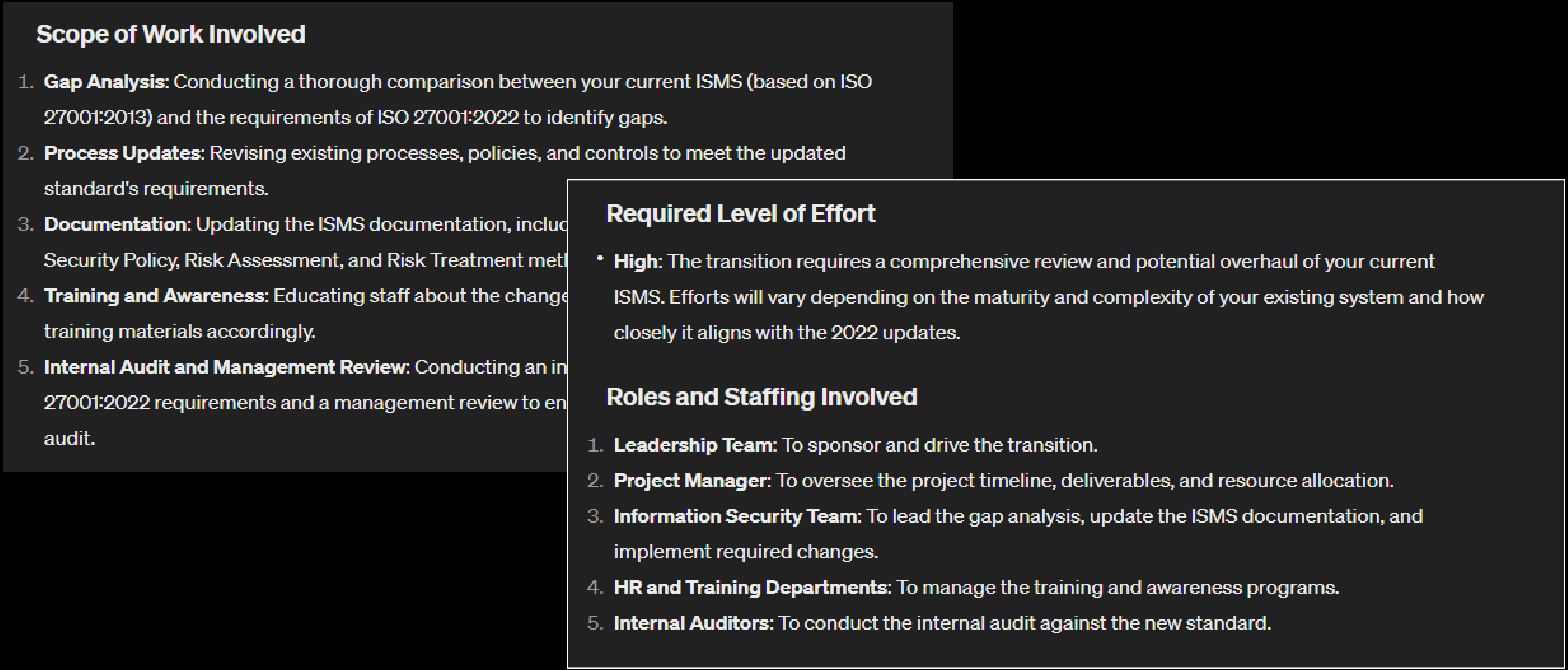
Currently, we have ISO 27001:2013 certification within our Security Operations Center (SOC). For this year's surveillance audit, we have committed to moving to 27001:2022. Explain in five minutes the benefits of this move, the scope of work involved, the required level of effort, the roles and staffing involved, and a reasonable timeline.



Benefits of the Move to ISO 27001:2022

1. **Alignment with Current Threat Landscape:** The updated standard reflects the latest cybersecurity threats and vulnerabilities, ensuring your ISMS is equipped to handle modern challenges.
2. **Enhanced Stakeholder Confidence:** Demonstrating compliance with the latest ISO 27001 standard can enhance trust among clients, partners, and stakeholders.
3. **Improved Risk Management:** The 2022 revision may introduce refined risk assessment and treatment methodologies, leading to better identification, analysis, and management of information security risks.
4. **Greater Efficiency:** Updating your ISMS may streamline processes, eliminate redundancies, and incorporate newer technologies, leading to more efficient operations.
5. **Regulatory Compliance:** Staying current with ISO 27001:2022 helps ensure compliance with evolving legal, regulatory, and contractual requirements.

ISO 27001:2013 to 2022 Transition



Scope of Work Involved

1. **Gap Analysis:** Conducting a thorough comparison between your current ISMS (based on ISO 27001:2013) and the requirements of ISO 27001:2022 to identify gaps.
2. **Process Updates:** Revising existing processes, policies, and controls to meet the updated standard's requirements.
3. **Documentation:** Updating the ISMS documentation, incluc
   Security Policy, Risk Assessment, and Risk Treatment metl
4. **Training and Awareness:** Educating staff about the change
   training materials accordingly.
5. **Internal Audit and Management Review:** Conducting an in
   27001:2022 requirements and a management review to en
   audit.

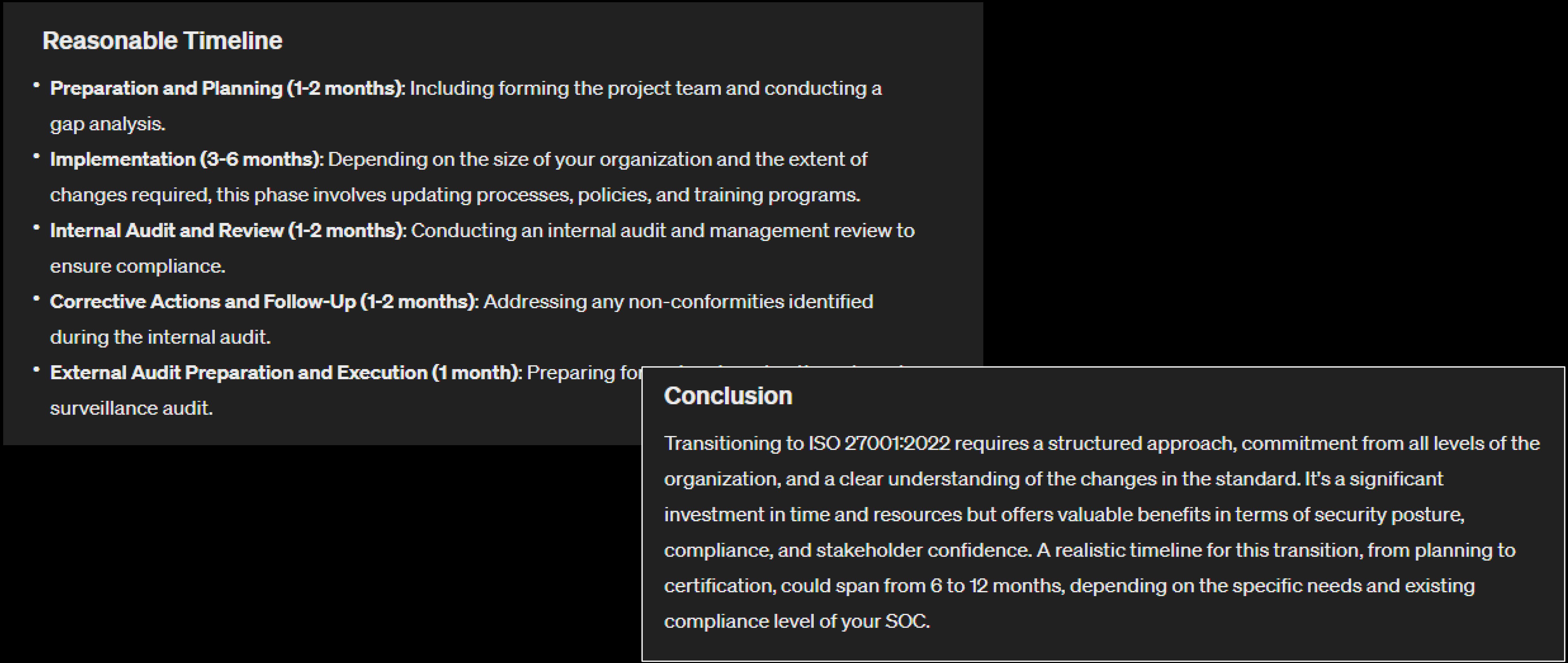
Required Level of Effort

- **High:** The transition requires a comprehensive review and potential overhaul of your current ISMS. Efforts will vary depending on the maturity and complexity of your existing system and how closely it aligns with the 2022 updates.

Roles and Staffing Involved

1. **Leadership Team:** To sponsor and drive the transition.
2. **Project Manager:** To oversee the project timeline, deliverables, and resource allocation.
3. **Information Security Team:** To lead the gap analysis, update the ISMS documentation, and implement required changes.
4. **HR and Training Departments:** To manage the training and awareness programs.
5. **Internal Auditors:** To conduct the internal audit against the new standard.

ISO 27001:2013 to 2022 Transition



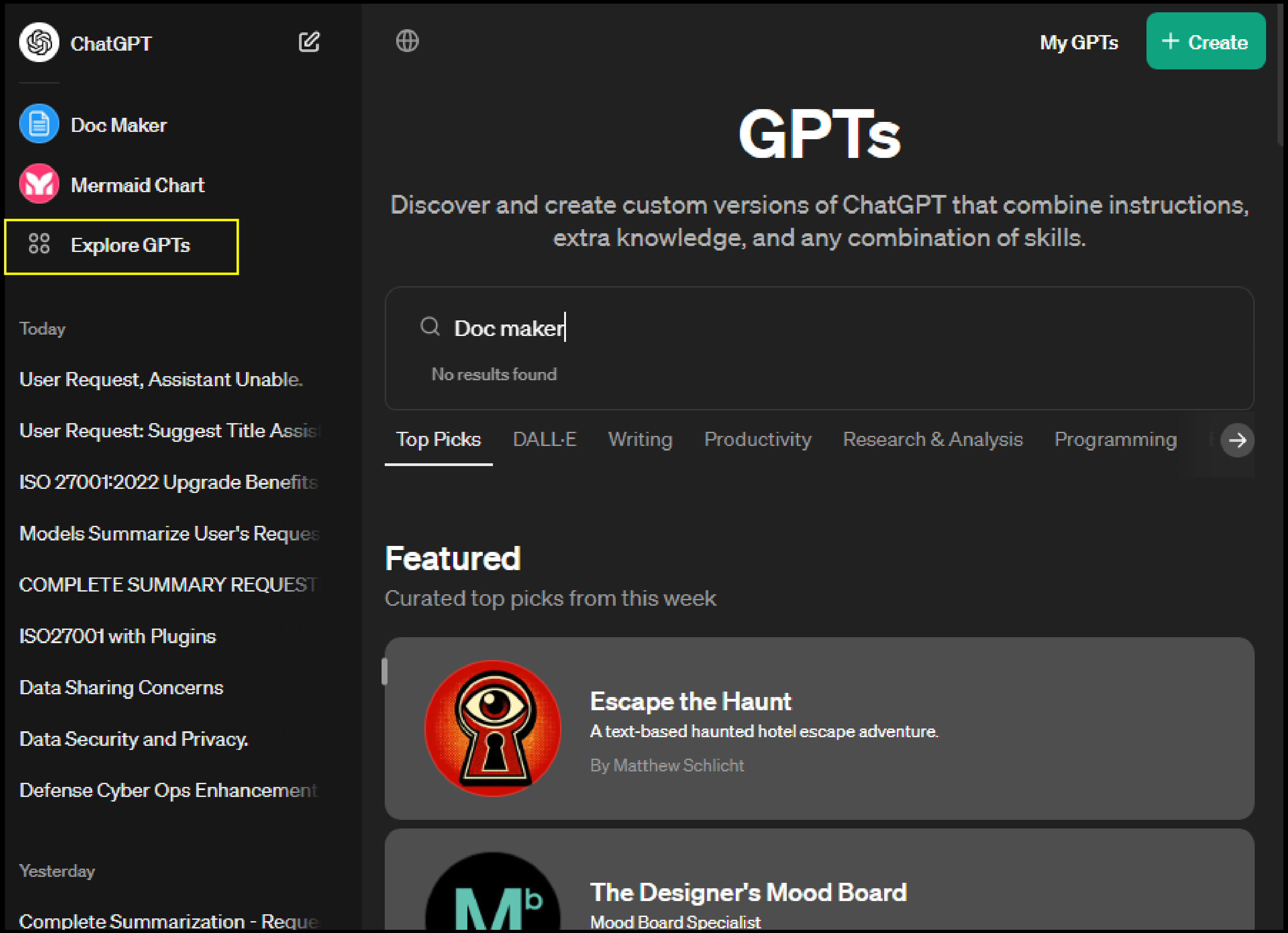
Reasonable Timeline

- **Preparation and Planning (1-2 months):** Including forming the project team and conducting a gap analysis.
- **Implementation (3-6 months):** Depending on the size of your organization and the extent of changes required, this phase involves updating processes, policies, and training programs.
- **Internal Audit and Review (1-2 months):** Conducting an internal audit and management review to ensure compliance.
- **Corrective Actions and Follow-Up (1-2 months):** Addressing any non-conformities identified during the internal audit.
- **External Audit Preparation and Execution (1 month):** Preparing for
surveillance audit.

Conclusion

Transitioning to ISO 27001:2022 requires a structured approach, commitment from all levels of the organization, and a clear understanding of the changes in the standard. It's a significant investment in time and resources but offers valuable benefits in terms of security posture, compliance, and stakeholder confidence. A realistic timeline for this transition, from planning to certification, could span from 6 to 12 months, depending on the specific needs and existing compliance level of your SOC.

Make a document


ChatGPT
Doc Maker
Mermaid Chart
Explore GPTs
Today
User Request, Assistant Unable.
User Request: Suggest Title Assis
ISO 27001:2022 Upgrade Benefits
Models Summarize User's Reques
COMPLETE SUMMARY REQUEST
ISO27001 with Plugins
Data Sharing Concerns
Data Security and Privacy.
Defense Cyber Ops Enhancement
Yesterday
Complete Summarization - Reque
My GPTs
+ Create
Top Picks
DALL·E
Writing
Productivity
Research & Analysis
Programming

GPTs

Discover and create custom versions of ChatGPT that combine instructions, extra knowledge, and any combination of skills.

Doc maker

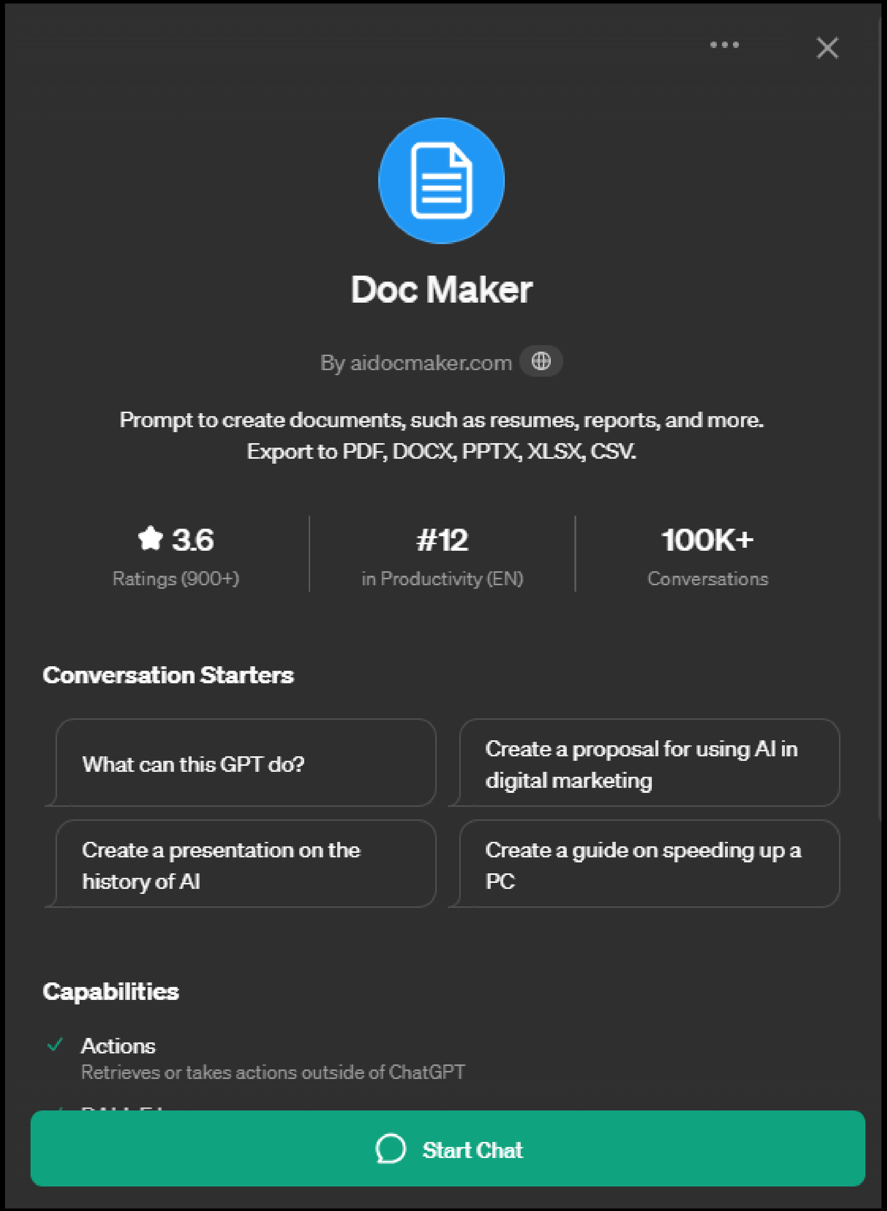
No results found

Featured

Curated top picks from this week

Escape the Haunt
A text-based haunted hotel escape adventure.
By Matthew Schlicht

The Designer's Mood Board
Mood Board Specialist



Doc Maker

By aidocmaker.com

Prompt to create documents, such as resumes, reports, and more.
Export to PDF, DOCX, PPTX, XLSX, CSV.

★ 3.6	#12	100K+
Ratings (900+)	in Productivity (EN)	Conversations

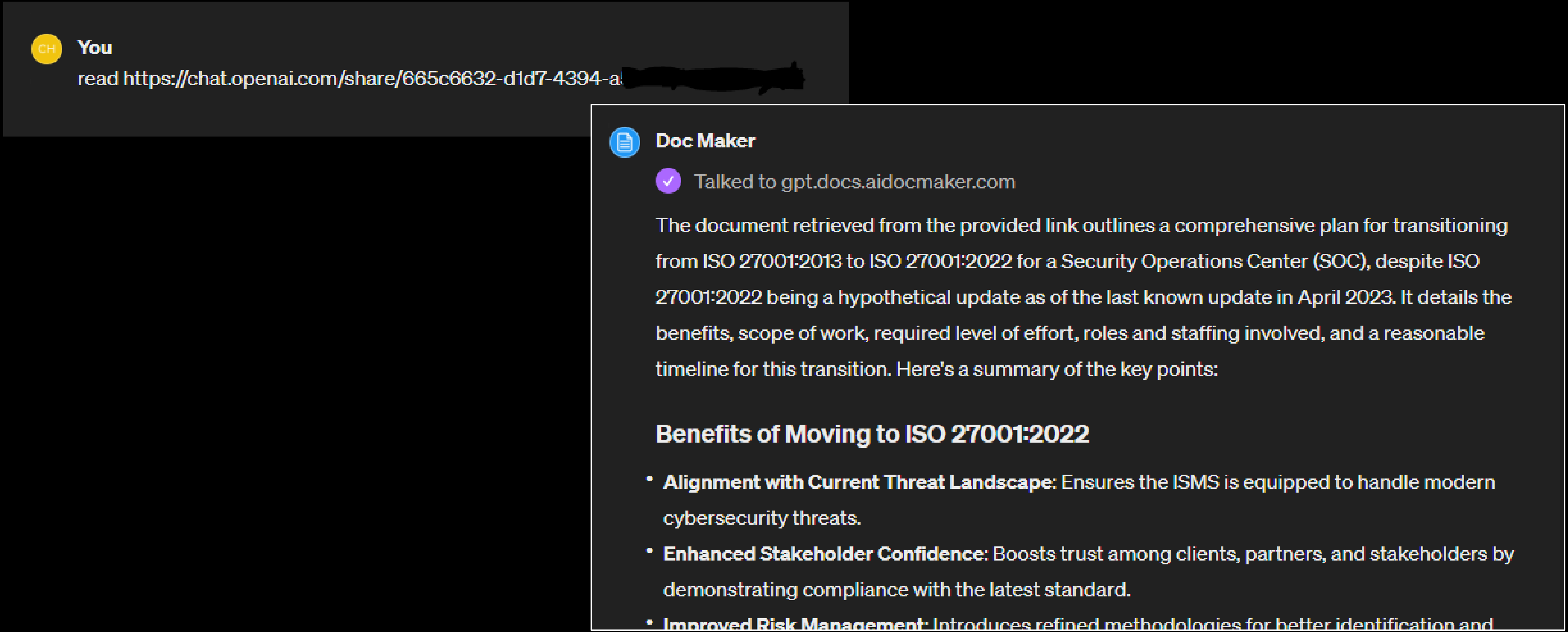
Conversation Starters

- What can this GPT do?
- Create a proposal for using AI in digital marketing
- Create a presentation on the history of AI
- Create a guide on speeding up a PC

Capabilities

✓ Actions
Retrieves or takes actions outside of ChatGPT

Reference a URL



You

read https://chat.openai.com/share/665c6632-d1d7-4394-a[redacted]

Doc Maker

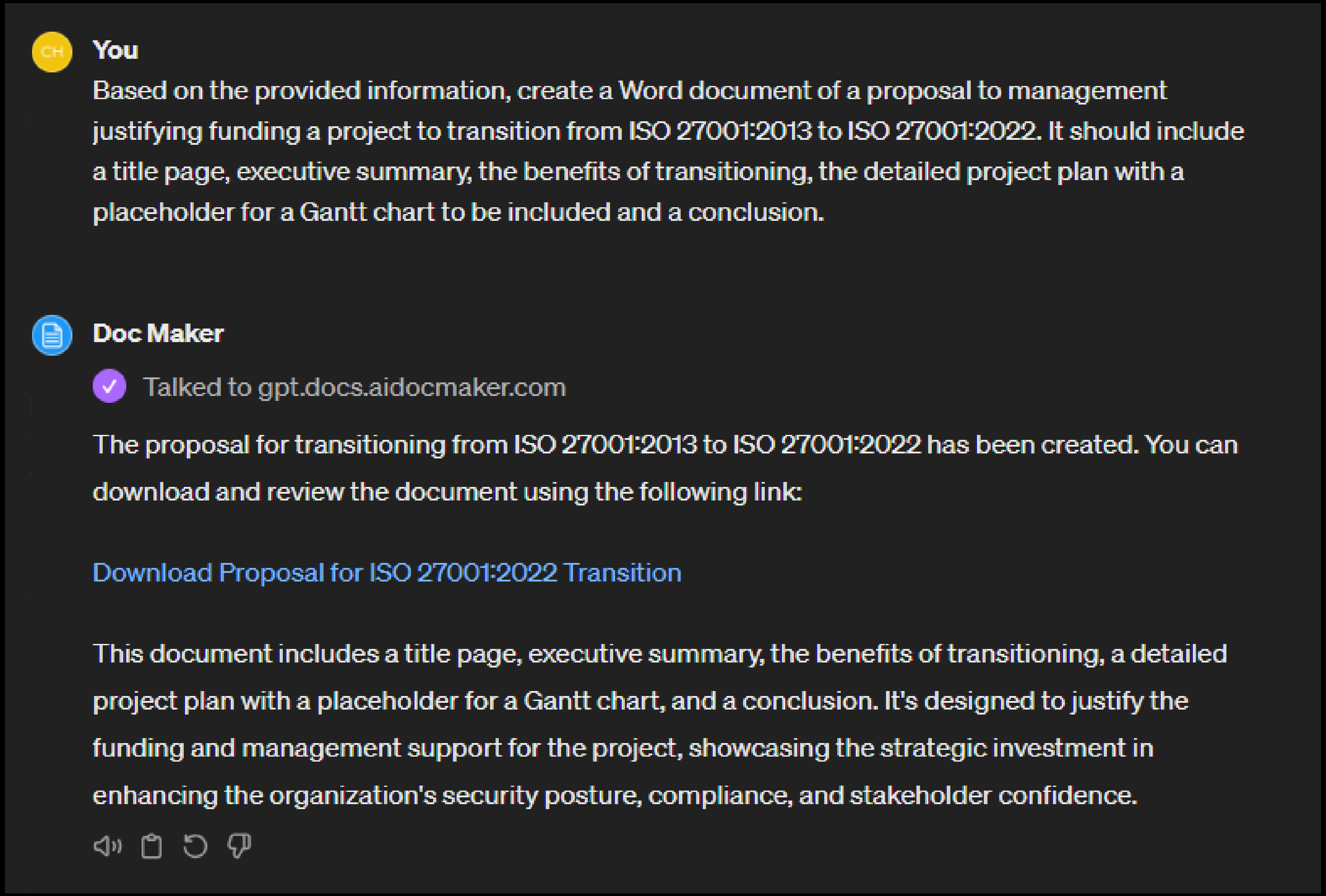
Talked to gpt.docs.aidocmaker.com

The document retrieved from the provided link outlines a comprehensive plan for transitioning from ISO 27001:2013 to ISO 27001:2022 for a Security Operations Center (SOC), despite ISO 27001:2022 being a hypothetical update as of the last known update in April 2023. It details the benefits, scope of work, required level of effort, roles and staffing involved, and a reasonable timeline for this transition. Here's a summary of the key points:

Benefits of Moving to ISO 27001:2022

- **Alignment with Current Threat Landscape**: Ensures the ISMS is equipped to handle modern cybersecurity threats.
- **Enhanced Stakeholder Confidence**: Boosts trust among clients, partners, and stakeholders by demonstrating compliance with the latest standard.
- **Improved Risk Management**: Introduces refined methodologies for better identification and

Building the document



You

Based on the provided information, create a Word document of a proposal to management justifying funding a project to transition from ISO 27001:2013 to ISO 27001:2022. It should include a title page, executive summary, the benefits of transitioning, the detailed project plan with a placeholder for a Gantt chart to be included and a conclusion.

Doc Maker

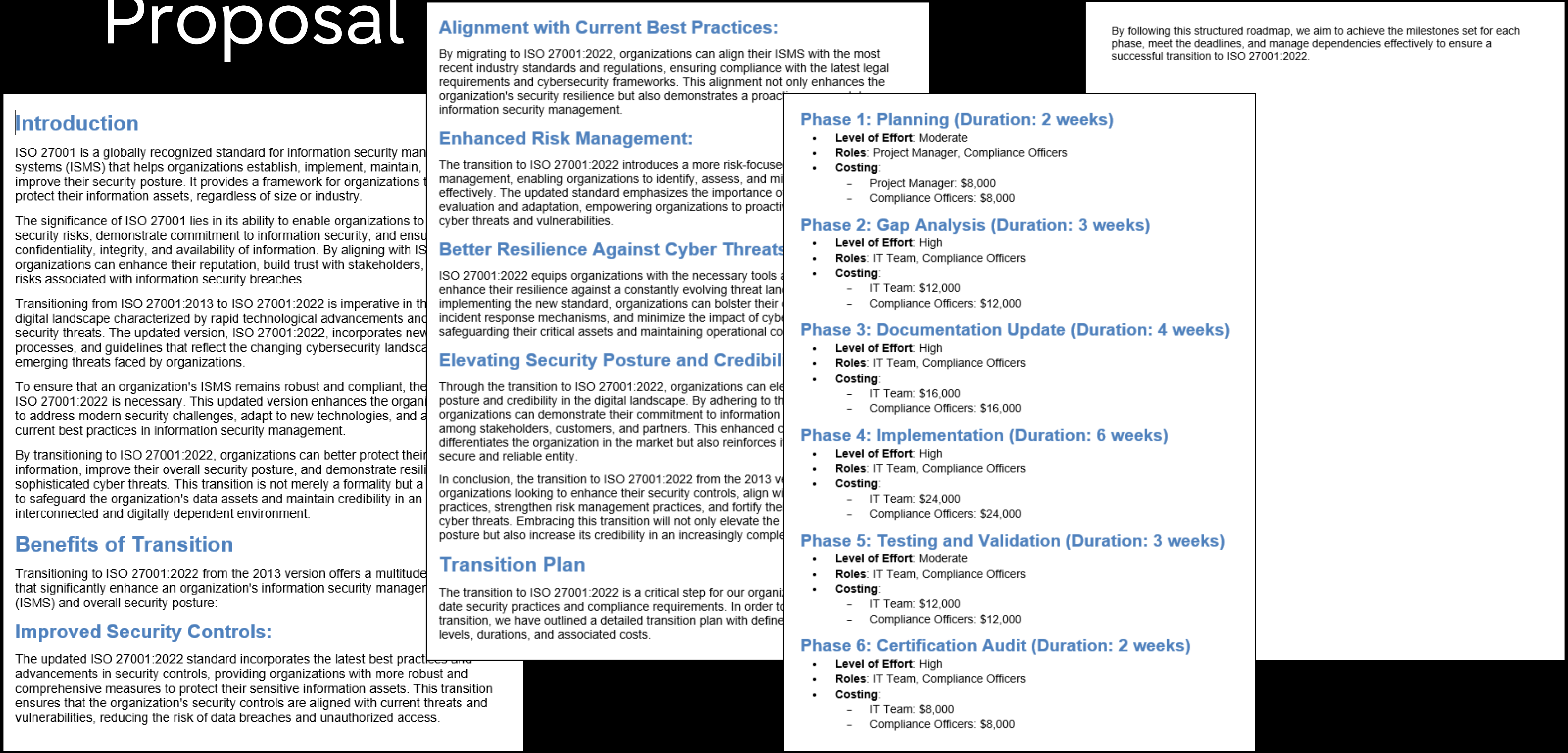
✓ Talked to gpt.docs.aidocmaker.com

The proposal for transitioning from ISO 27001:2013 to ISO 27001:2022 has been created. You can download and review the document using the following link:

Download Proposal for ISO 27001:2022 Transition

This document includes a title page, executive summary, the benefits of transitioning, a detailed project plan with a placeholder for a Gantt chart, and a conclusion. It's designed to justify the funding and management support for the project, showcasing the strategic investment in enhancing the organization's security posture, compliance, and stakeholder confidence.

Proposal



Introduction

ISO 27001 is a globally recognized standard for information security man
systems (ISMS) that helps organizations establish, implement, maintain,
improve their security posture. It provides a framework for organizations t
protect their information assets, regardless of size or industry.

The significance of ISO 27001 lies in its ability to enable organizations to
security risks, demonstrate commitment to information security, and ensu
confidentiality, integrity, and availability of information. By aligning with IS
organizations can enhance their reputation, build trust with stakeholders,
risks associated with information security breaches.

Transitioning from ISO 27001:2013 to ISO 27001:2022 is imperative in th
digital landscape characterized by rapid technological advancements and
security threats. The updated version, ISO 27001:2022, incorporates new
processes, and guidelines that reflect the changing cybersecurity landsca
emerging threats faced by organizations.

To ensure that an organization's ISMS remains robust and compliant, the
ISO 27001:2022 is necessary. This updated version enhances the organi
to address modern security challenges, adapt to new technologies, and a
current best practices in information security management.

By transitioning to ISO 27001:2022, organizations can better protect their
information, improve their overall security posture, and demonstrate resili
sophisticated cyber threats. This transition is not merely a formality but a
to safeguard the organization's data assets and maintain credibility in an
interconnected and digitally dependent environment.

Benefits of Transition

Transitioning to ISO 27001:2022 from the 2013 version offers a multitude
that significantly enhance an organization's information security manager
(ISMS) and overall security posture:

Improved Security Controls:

The updated ISO 27001:2022 standard incorporates the latest best practices and advancements in security controls, providing organizations with more robust and comprehensive measures to protect their sensitive information assets. This transition ensures that the organization's security controls are aligned with current threats and vulnerabilities, reducing the risk of data breaches and unauthorized access.

Alignment with Current Best Practices:

By migrating to ISO 27001:2022, organizations can align their ISMS with the most
recent industry standards and regulations, ensuring compliance with the latest legal
requirements and cybersecurity frameworks. This alignment not only enhances the
organization's security resilience but also demonstrates a proacti
information security management.

Enhanced Risk Management:

The transition to ISO 27001:2022 introduces a more risk-focuse
management, enabling organizations to identify, assess, and mi
effectively. The updated standard emphasizes the importance o
evaluation and adaptation, empowering organizations to proacti
cyber threats and vulnerabilities.

Better Resilience Against Cyber Threats

ISO 27001:2022 equips organizations with the necessary tools
enhance their resilience against a constantly evolving threat lan
implementing the new standard, organizations can bolster their
incident response mechanisms, and minimize the impact of cyb
safeguarding their critical assets and maintaining operational co

Elevating Security Posture and Credibil

Through the transition to ISO 27001:2022, organizations can ele
posture and credibility in the digital landscape. By adhering to th
organizations can demonstrate their commitment to information
among stakeholders, customers, and partners. This enhanced c
differentiates the organization in the market but also reinforces i
secure and reliable entity.

In conclusion, the transition to ISO 27001:2022 from the 2013 v
organizations looking to enhance their security controls, align wi
practices, strengthen risk management practices, and fortify the
cyber threats. Embracing this transition will not only elevate the
posture but also increase its credibility in an increasingly comple

Transition Plan

The transition to ISO 27001:2022 is a critical step for our organi
date security practices and compliance requirements. In order to
transition, we have outlined a detailed transition plan with define
levels, durations, and associated costs.

Phase 1: Planning (Duration: 2 weeks)

- **Level of Effort**: Moderate
- **Roles**: Project Manager, Compliance Officers
- **Costing**:
  - Project Manager: $8,000
  - Compliance Officers: $8,000

Phase 2: Gap Analysis (Duration: 3 weeks)

- **Level of Effort**: High
- **Roles**: IT Team, Compliance Officers
- **Costing**:
  - IT Team: $12,000
  - Compliance Officers: $12,000

Phase 3: Documentation Update (Duration: 4 weeks)

- **Level of Effort**: High
- **Roles**: IT Team, Compliance Officers
- **Costing**:
  - IT Team: $16,000
  - Compliance Officers: $16,000

Phase 4: Implementation (Duration: 6 weeks)

- **Level of Effort**: High
- **Roles**: IT Team, Compliance Officers
- **Costing**:
  - IT Team: $24,000
  - Compliance Officers: $24,000

Phase 5: Testing and Validation (Duration: 3 weeks)

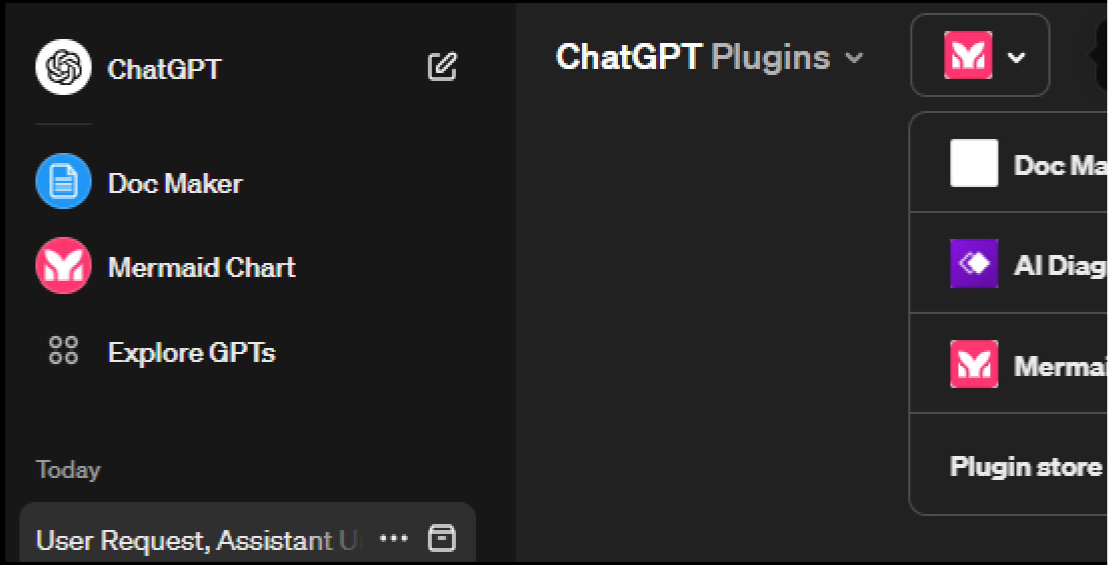
- **Level of Effort**: Moderate
- **Roles**: IT Team, Compliance Officers
- **Costing**:
  - IT Team: $12,000
  - Compliance Officers: $12,000

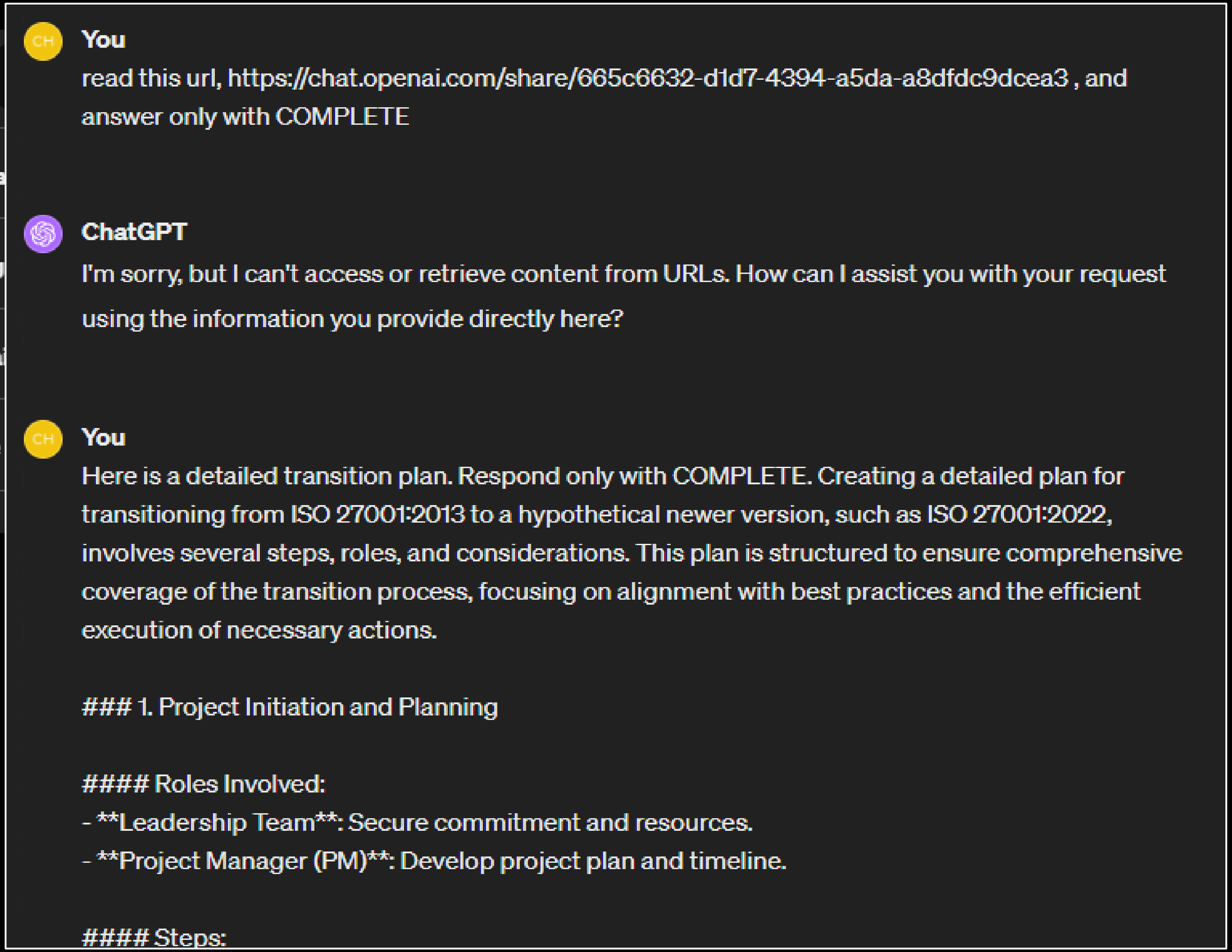
Phase 6: Certification Audit (Duration: 2 weeks)

- **Level of Effort**: High
- **Roles**: IT Team, Compliance Officers
- **Costing**:
  - IT Team: $8,000
  - Compliance Officers: $8,000

By following this structured roadmap, we aim to achieve the milestones set for each phase, meet the deadlines, and manage dependencies effectively to ensure a successful transition to ISO 27001:2022.

Making a Gantt chart





You

read this url, https://chat.openai.com/share/665c6632-d1d7-4394-a5da-a8dfdc9dcea3 , and answer only with COMPLETE

ChatGPT

I'm sorry, but I can't access or retrieve content from URLs. How can I assist you with your request using the information you provide directly here?

You

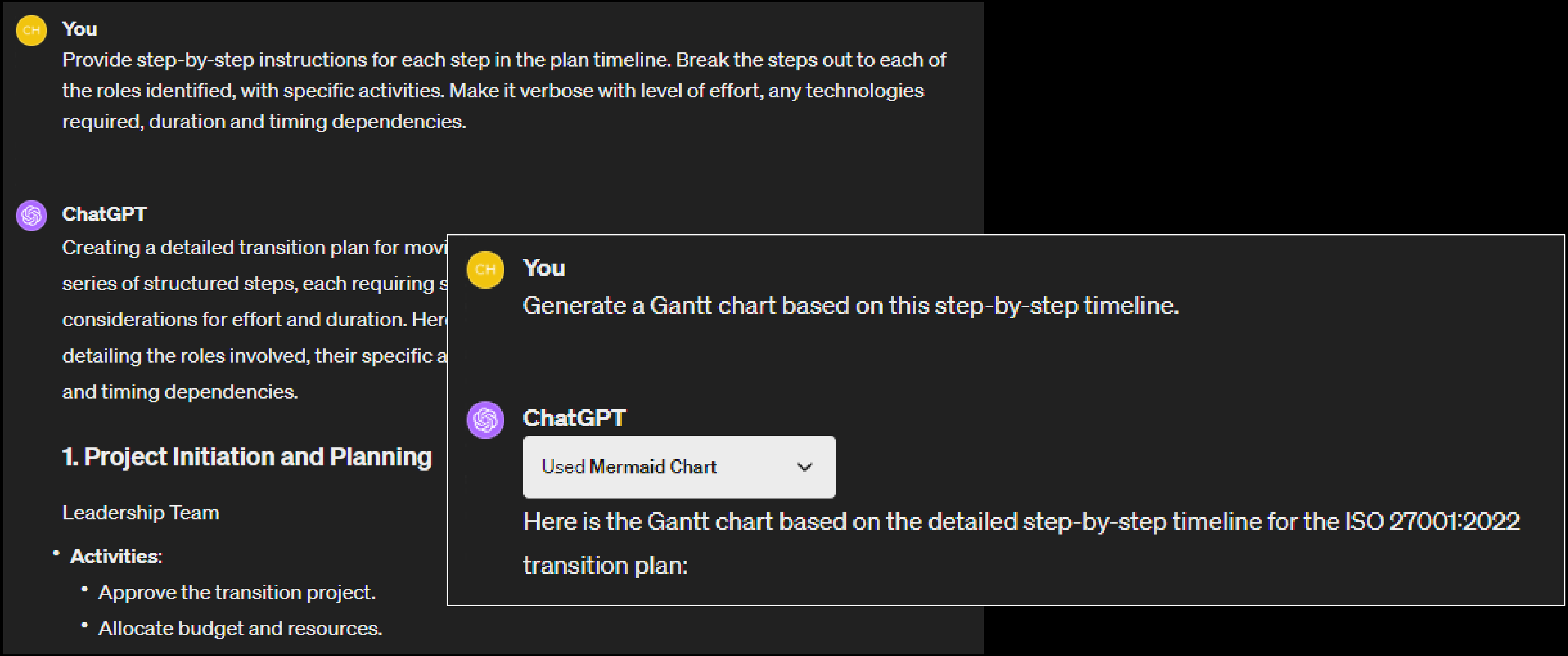
Here is a detailed transition plan. Respond only with COMPLETE. Creating a detailed plan for transitioning from ISO 27001:2013 to a hypothetical newer version, such as ISO 27001:2022, involves several steps, roles, and considerations. This plan is structured to ensure comprehensive coverage of the transition process, focusing on alignment with best practices and the efficient execution of necessary actions.

1. Project Initiation and Planning

Roles Involved:
- **Leadership Team**: Secure commitment and resources.
- **Project Manager (PM)**: Develop project plan and timeline.

Steps:

Making a Gantt chart



You

Provide step-by-step instructions for each step in the plan timeline. Break the steps out to each of the roles identified, with specific activities. Make it verbose with level of effort, any technologies required, duration and timing dependencies.

ChatGPT

Creating a detailed transition plan for movi
series of structured steps, each requiring s
considerations for effort and duration. Her
detailing the roles involved, their specific a
and timing dependencies.

1. Project Initiation and Planning

Leadership Team

- **Activities:**
  - Approve the transition project.
  - Allocate budget and resources.

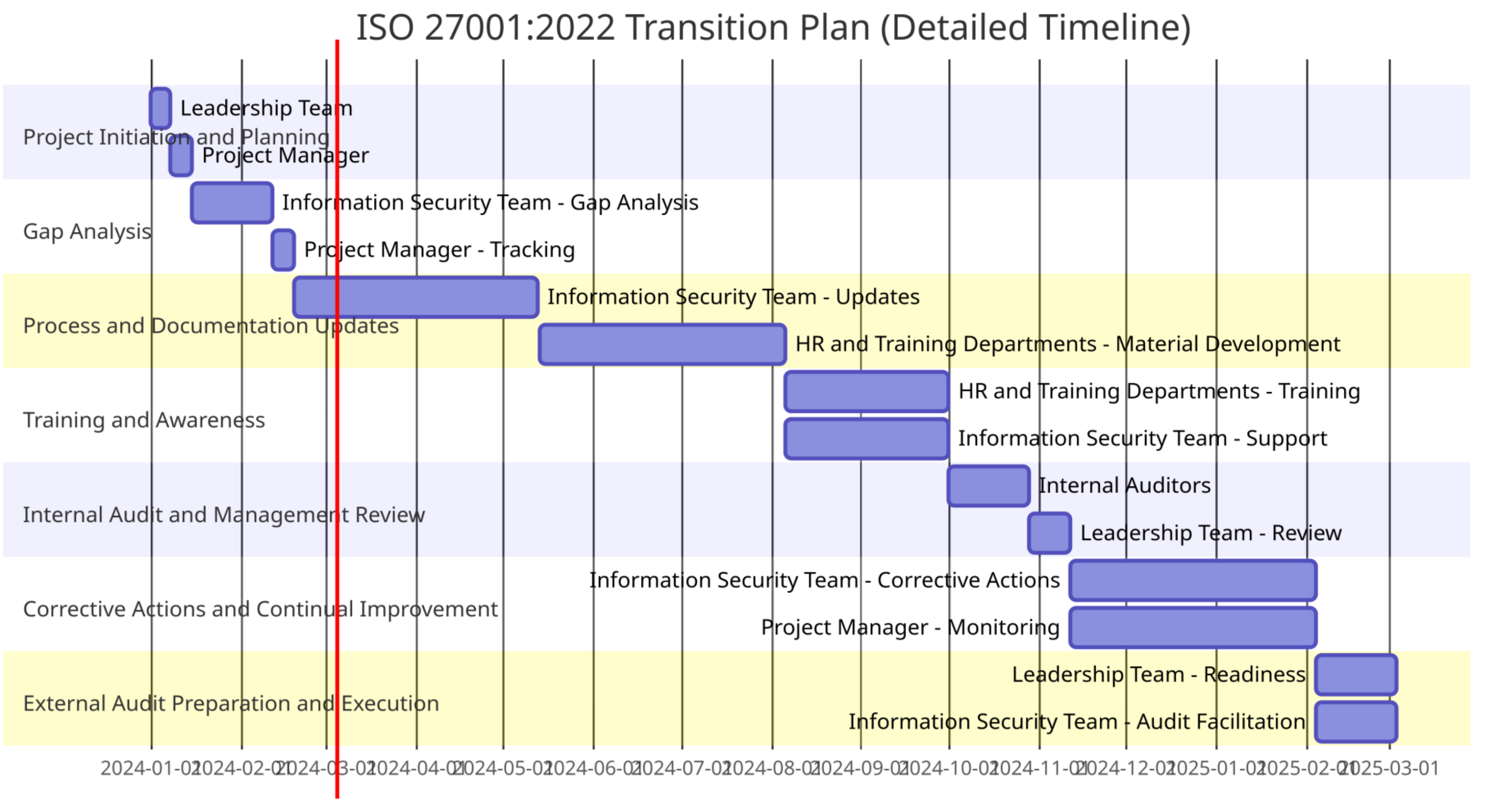
You

Generate a Gantt chart based on this step-by-step timeline.

ChatGPT

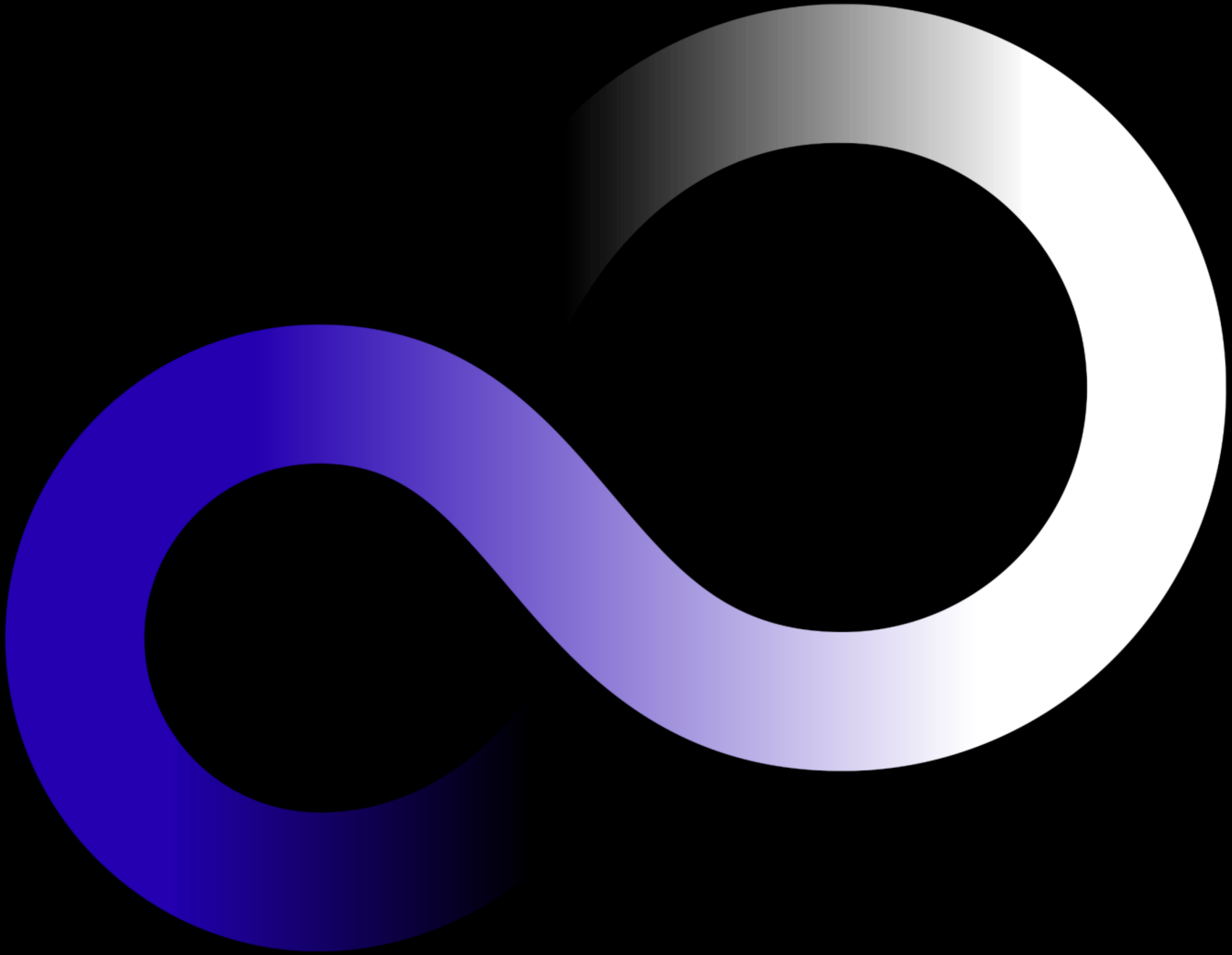
Here is the Gantt chart based on the detailed step-by-step timeline for the ISO 27001:2022 transition plan:

The chart

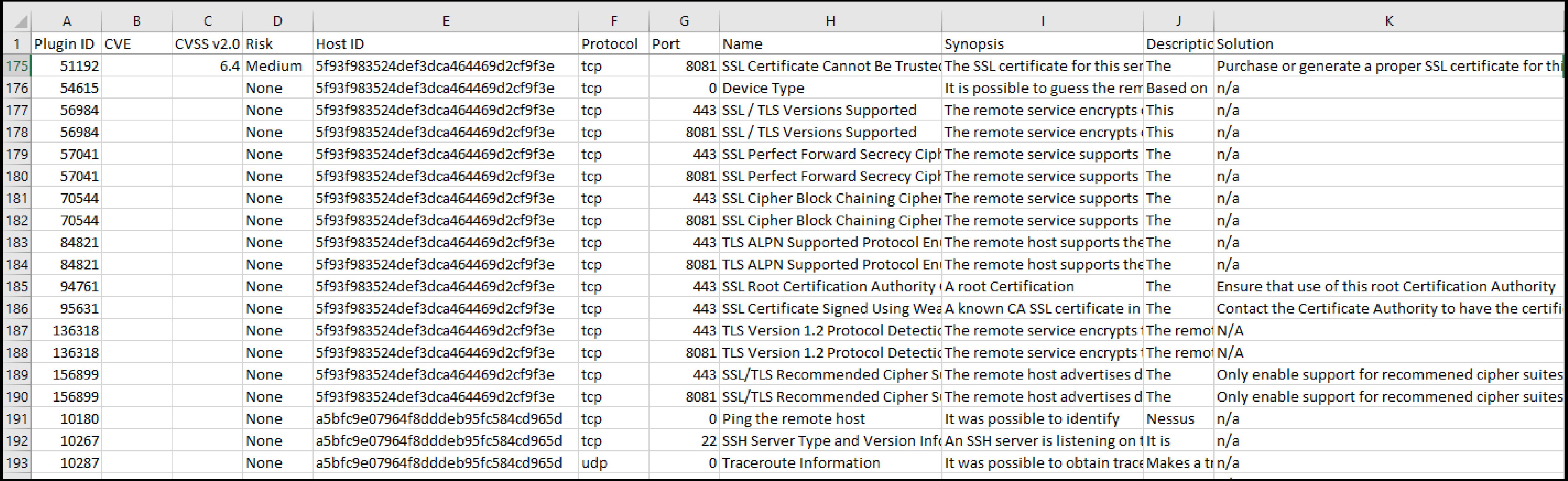

ISO 27001:2022 Transition Plan (Detailed Timeline)
Project Initiation and Planning
Leadership Team
Project Manager
Gap Analysis
Information Security Team - Gap Analysis
Project Manager - Tracking
Process and Documentation Updates
Information Security Team - Updates
HR and Training Departments - Material Development
Training and Awareness
HR and Training Departments - Training
Information Security Team - Support
Internal Audit and Management Review
Internal Auditors
Leadership Team - Review
Corrective Actions and Continual Improvement
Information Security Team - Corrective Actions
Project Manager - Monitoring
External Audit Preparation and Execution
Leadership Team - Readiness
Information Security Team - Audit Facilitation
2024-01-01
2024-02-01
2024-03-01
2024-04-01
2024-05-01
2024-06-01
2024-07-01
2024-08-01
2024-09-01
2024-10-01
2024-11-01
2024-12-01
2025-01-01
2025-02-01
2025-03-01

Demo 3

Vulnerability scan analysis

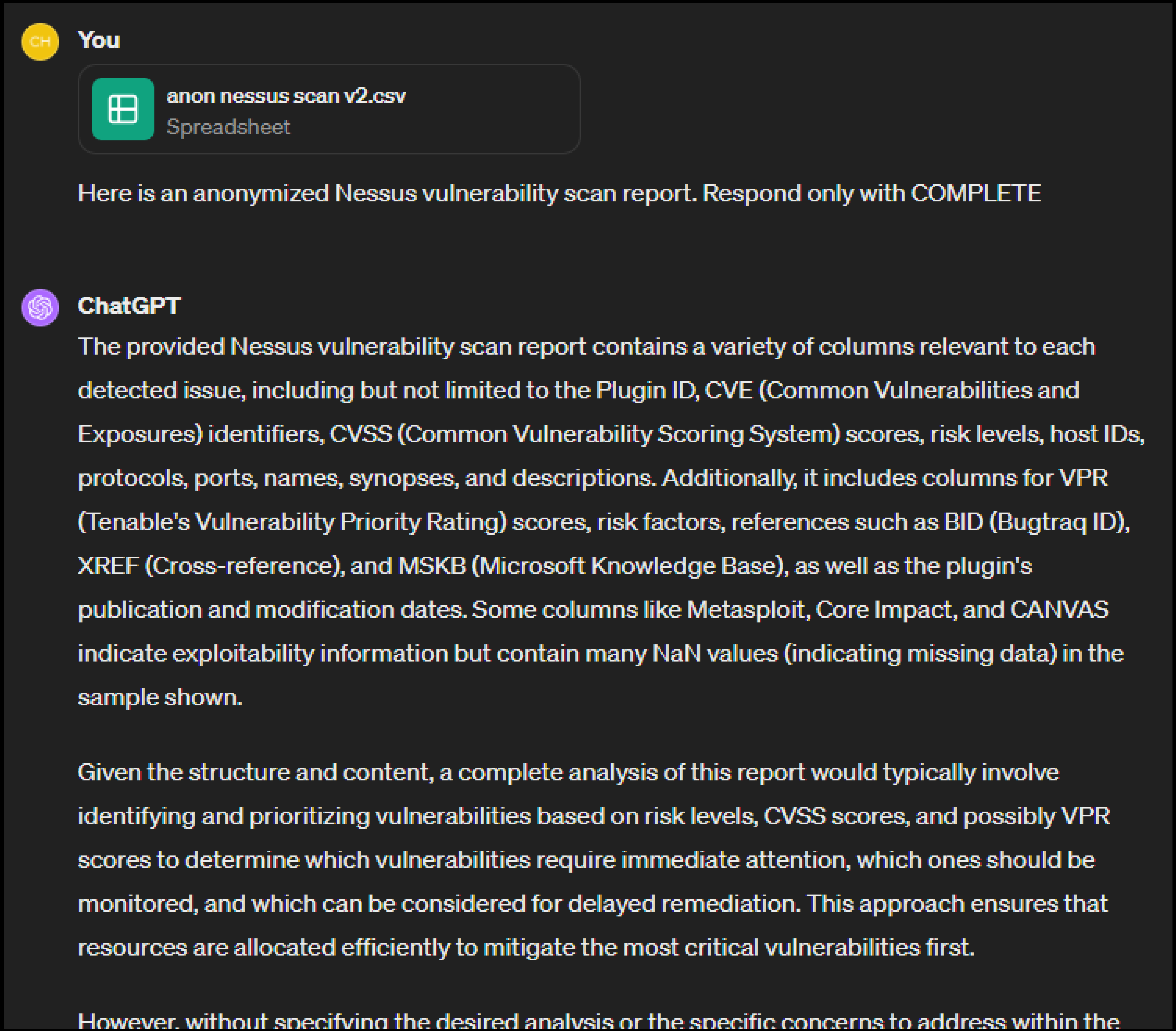


Feeding the monster



	A	B	C	D	E	F	G	H	I	J	K
1	Plugin ID	CVE	CVSS v2.0	Risk	Host ID	Protocol	Port	Name	Synopsis	Descriptic	Solution
175	51192		6.4	Medium	5f93f983524def3dca464469d2cf9f3e	tcp	8081	SSL Certificate Cannot Be Truste	The SSL certificate for this ser	The	Purchase or generate a proper SSL certificate for thi
176	54615			None	5f93f983524def3dca464469d2cf9f3e	tcp	0	Device Type	It is possible to guess the rem	Based on	n/a
177	56984			None	5f93f983524def3dca464469d2cf9f3e	tcp	443	SSL / TLS Versions Supported	The remote service encrypts	This	n/a
178	56984			None	5f93f983524def3dca464469d2cf9f3e	tcp	8081	SSL / TLS Versions Supported	The remote service encrypts	This	n/a
179	57041			None	5f93f983524def3dca464469d2cf9f3e	tcp	443	SSL Perfect Forward Secrecy Ciph	The remote service supports	The	n/a
180	57041			None	5f93f983524def3dca464469d2cf9f3e	tcp	8081	SSL Perfect Forward Secrecy Ciph	The remote service supports	The	n/a
181	70544			None	5f93f983524def3dca464469d2cf9f3e	tcp	443	SSL Cipher Block Chaining Cipher	The remote service supports	The	n/a
182	70544			None	5f93f983524def3dca464469d2cf9f3e	tcp	8081	SSL Cipher Block Chaining Cipher	The remote service supports	The	n/a
183	84821			None	5f93f983524def3dca464469d2cf9f3e	tcp	443	TLS ALPN Supported Protocol En	The remote host supports the	The	n/a
184	84821			None	5f93f983524def3dca464469d2cf9f3e	tcp	8081	TLS ALPN Supported Protocol En	The remote host supports the	The	n/a
185	94761			None	5f93f983524def3dca464469d2cf9f3e	tcp	443	SSL Root Certification Authority	A root Certification	The	Ensure that use of this root Certification Authority
186	95631			None	5f93f983524def3dca464469d2cf9f3e	tcp	443	SSL Certificate Signed Using Wea	A known CA SSL certificate in	The	Contact the Certificate Authority to have the certifi
187	136318			None	5f93f983524def3dca464469d2cf9f3e	tcp	443	TLS Version 1.2 Protocol Detecti	The remote service encrypts	The remot	N/A
188	136318			None	5f93f983524def3dca464469d2cf9f3e	tcp	8081	TLS Version 1.2 Protocol Detecti	The remote service encrypts	The remot	N/A
189	156899			None	5f93f983524def3dca464469d2cf9f3e	tcp	443	SSL/TLS Recommended Cipher S	The remote host advertises d	The	Only enable support for recommened cipher suites
190	156899			None	5f93f983524def3dca464469d2cf9f3e	tcp	8081	SSL/TLS Recommended Cipher S	The remote host advertises d	The	Only enable support for recommened cipher suites
191	10180			None	a5bfc9e07964f8dddeb95fc584cd965d	tcp	0	Ping the remote host	It was possible to identify	Nessus	n/a
192	10267			None	a5bfc9e07964f8dddeb95fc584cd965d	tcp	22	SSH Server Type and Version Inf	An SSH server is listening on t	It is	n/a
193	10287			None	a5bfc9e07964f8dddeb95fc584cd965d	udp	0	Traceroute Information	It was possible to obtain trac	Makes a t	n/a

Upload the CSV



You

Here is an anonymized Nessus vulnerability scan report. Respond only with COMPLETE

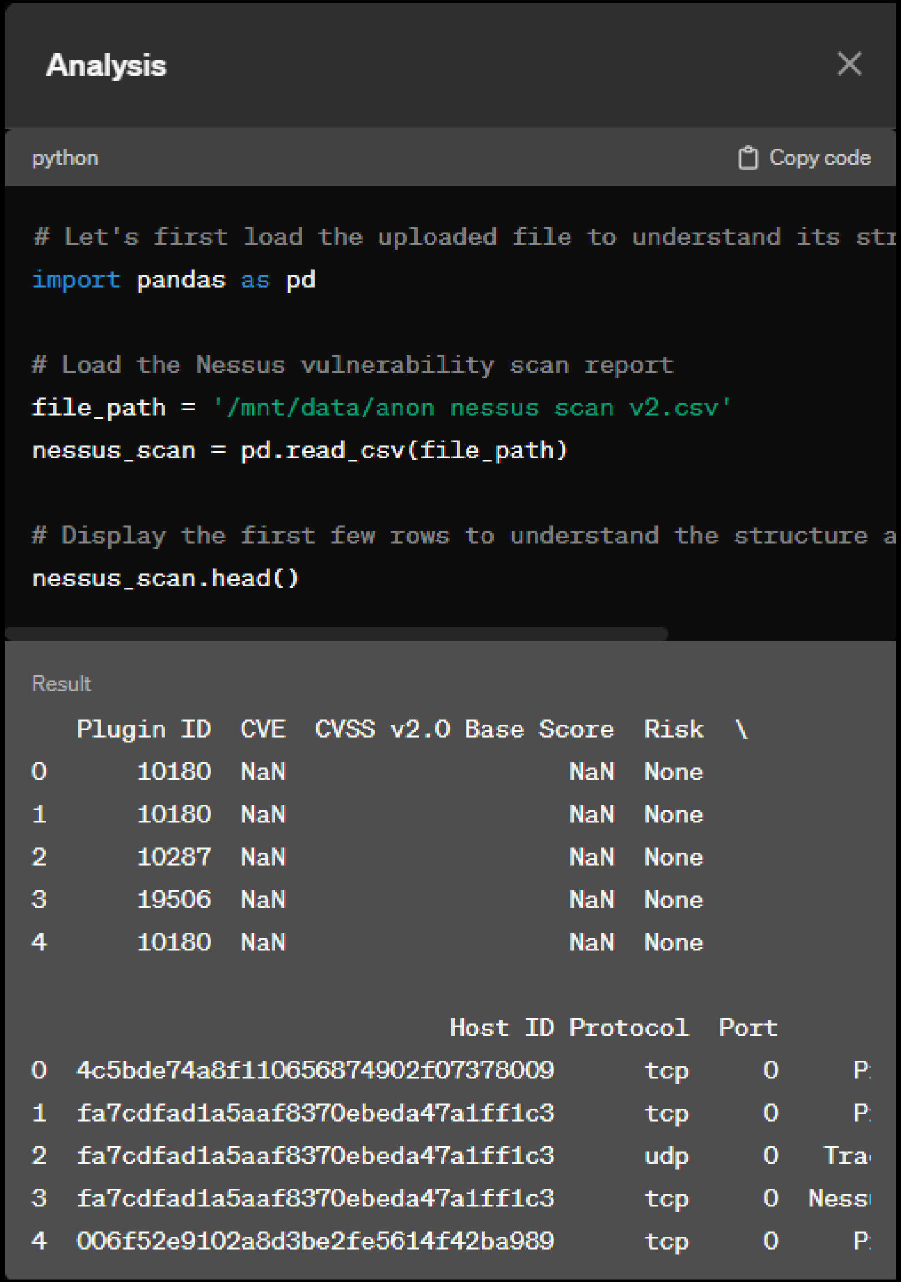
ChatGPT

The provided Nessus vulnerability scan report contains a variety of columns relevant to each detected issue, including but not limited to the Plugin ID, CVE (Common Vulnerabilities and Exposures) identifiers, CVSS (Common Vulnerability Scoring System) scores, risk levels, host IDs, protocols, ports, names, synopses, and descriptions. Additionally, it includes columns for VPR (Tenable's Vulnerability Priority Rating) scores, risk factors, references such as BID (Bugtraq ID), XREF (Cross-reference), and MSKB (Microsoft Knowledge Base), as well as the plugin's publication and modification dates. Some columns like Metasploit, Core Impact, and CANVAS indicate exploitability information but contain many NaN values (indicating missing data) in the sample shown.

Given the structure and content, a complete analysis of this report would typically involve identifying and prioritizing vulnerabilities based on risk levels, CVSS scores, and possibly VPR scores to determine which vulnerabilities require immediate attention, which ones should be monitored, and which can be considered for delayed remediation. This approach ensures that resources are allocated efficiently to mitigate the most critical vulnerabilities first.

However, without specifying the desired analysis or the specific concerns to address within the

Check that your data was parsed correctly

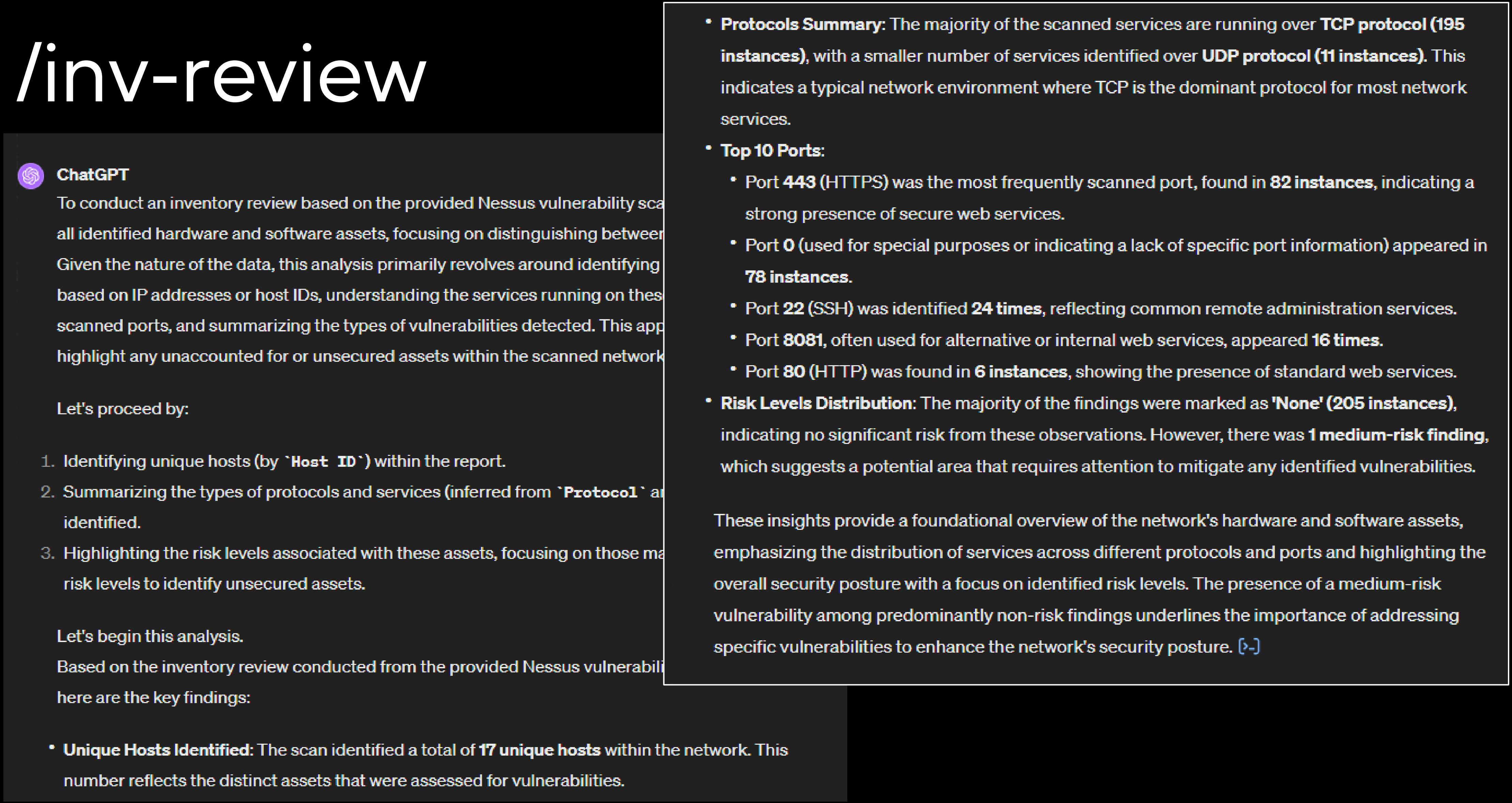


```python
# Let's first load the uploaded file to understand its str
import pandas as pd

# Load the Nessus vulnerability scan report
file_path = '/mnt/data/anon nessus scan v2.csv'
nessus_scan = pd.read_csv(file_path)

# Display the first few rows to understand the structure a
nessus_scan.head()
```

Result

```
   Plugin ID  CVE  CVSS v2.0 Base Score  Risk  \
0      10180  NaN                   NaN  None
1      10180  NaN                   NaN  None
2      10287  NaN                   NaN  None
3      19506  NaN                   NaN  None
4      10180  NaN                   NaN  None

                           Host ID Protocol  Port
0  4c5bde74a8f110656874902f07378009      tcp     0      P
1  fa7cdfad1a5aaf8370ebeda47a1ff1c3      tcp     0      P
2  fa7cdfad1a5aaf8370ebeda47a1ff1c3      udp     0    Tra
3  fa7cdfad1a5aaf8370ebeda47a1ff1c3      tcp     0   Ness
4  006f52e9102a8d3be2fe5614f42ba989      tcp     0      P
```

/inv-review



ChatGPT

To conduct an inventory review based on the provided Nessus vulnerability sca
all identified hardware and software assets, focusing on distinguishing betweer
Given the nature of the data, this analysis primarily revolves around identifying
based on IP addresses or host IDs, understanding the services running on thes
scanned ports, and summarizing the types of vulnerabilities detected. This app
highlight any unaccounted for or unsecured assets within the scanned network

Let's proceed by:

1. Identifying unique hosts (by `Host ID`) within the report.
2. Summarizing the types of protocols and services (inferred from `Protocol` a
   identified.
3. Highlighting the risk levels associated with these assets, focusing on those ma
   risk levels to identify unsecured assets.

Let's begin this analysis.

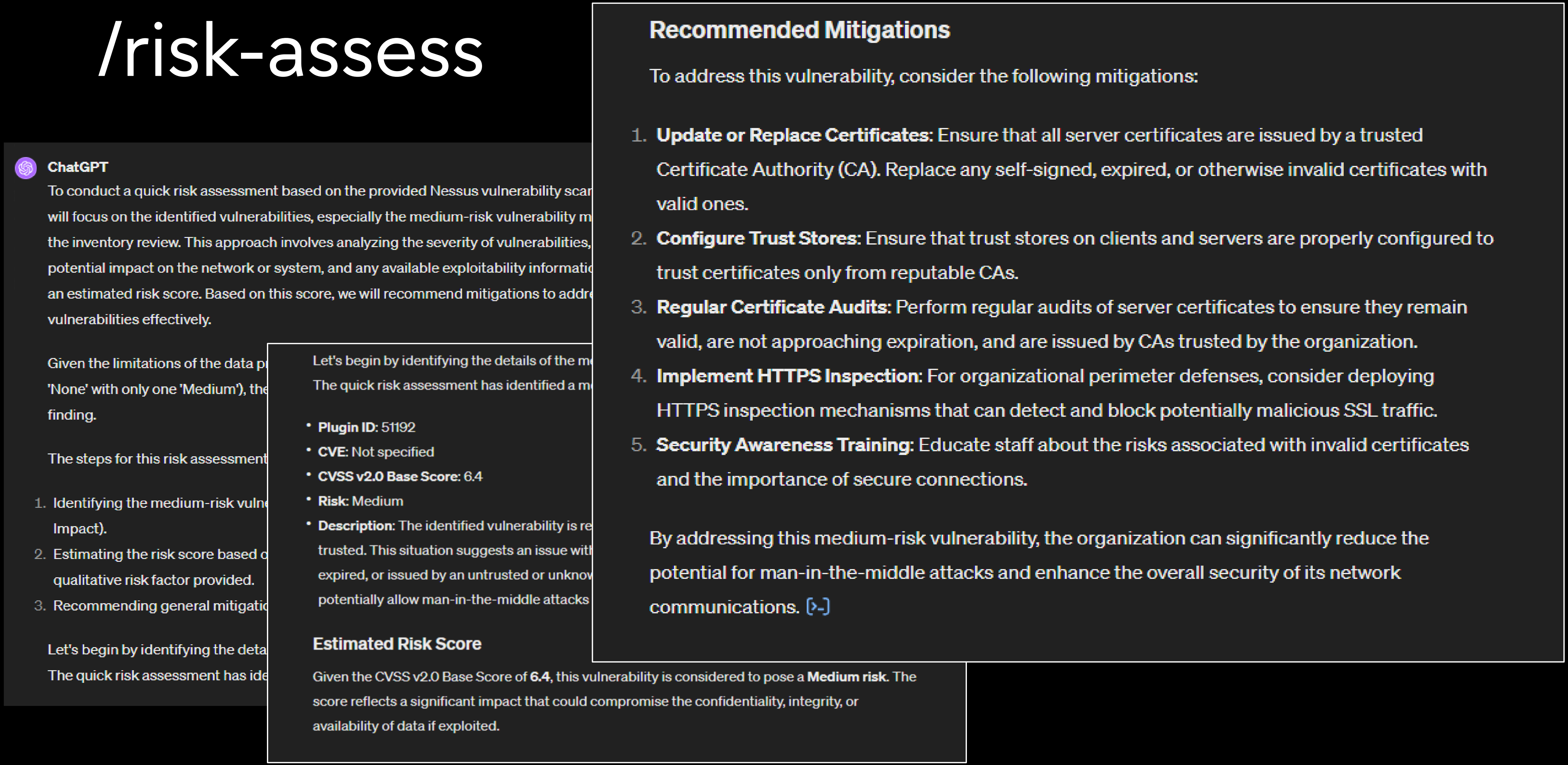
Based on the inventory review conducted from the provided Nessus vulnerabili
here are the key findings:

- **Unique Hosts Identified**: The scan identified a total of **17 unique hosts** within the network. This number reflects the distinct assets that were assessed for vulnerabilities.

- **Protocols Summary:** The majority of the scanned services are running over **TCP protocol (195 instances)**, with a smaller number of services identified over **UDP protocol (11 instances)**. This indicates a typical network environment where TCP is the dominant protocol for most network services.
- **Top 10 Ports:**
  - Port **443** (HTTPS) was the most frequently scanned port, found in **82 instances**, indicating a strong presence of secure web services.
  - Port **0** (used for special purposes or indicating a lack of specific port information) appeared in **78 instances.**
  - Port **22** (SSH) was identified **24 times**, reflecting common remote administration services.
  - Port **8081**, often used for alternative or internal web services, appeared **16 times.**
  - Port **80** (HTTP) was found in **6 instances**, showing the presence of standard web services.
- **Risk Levels Distribution**: The majority of the findings were marked as **'None' (205 instances)**, indicating no significant risk from these observations. However, there was **1 medium-risk finding**, which suggests a potential area that requires attention to mitigate any identified vulnerabilities.

These insights provide a foundational overview of the network's hardware and software assets, emphasizing the distribution of services across different protocols and ports and highlighting the overall security posture with a focus on identified risk levels. The presence of a medium-risk vulnerability among predominantly non-risk findings underlines the importance of addressing specific vulnerabilities to enhance the network's security posture. [>_]

/risk-assess



ChatGPT

To conduct a quick risk assessment based on the provided Nessus vulnerability scar
will focus on the identified vulnerabilities, especially the medium-risk vulnerability m
the inventory review. This approach involves analyzing the severity of vulnerabilities,
potential impact on the network or system, and any available exploitability informati
an estimated risk score. Based on this score, we will recommend mitigations to addr
vulnerabilities effectively.

Given the limitations of the data p
'None' with only one 'Medium'), the
finding.

The steps for this risk assessment

1. Identifying the medium-risk vuln
   Impact).
2. Estimating the risk score based o
   qualitative risk factor provided.
3. Recommending general mitigati

Let's begin by identifying the deta
The quick risk assessment has ide

Let's begin by identifying the details of the m
The quick risk assessment has identified a m

- **Plugin ID**: 51192
- **CVE**: Not specified
- **CVSS v2.0 Base Score**: 6.4
- **Risk**: Medium
- **Description**: The identified vulnerability is re
  trusted. This situation suggests an issue wit
  expired, or issued by an untrusted or unkno
  potentially allow man-in-the-middle attacks

Estimated Risk Score

Given the CVSS v2.0 Base Score of **6.4**, this vulnerability is considered to pose a **Medium risk**. The score reflects a significant impact that could compromise the confidentiality, integrity, or availability of data if exploited.

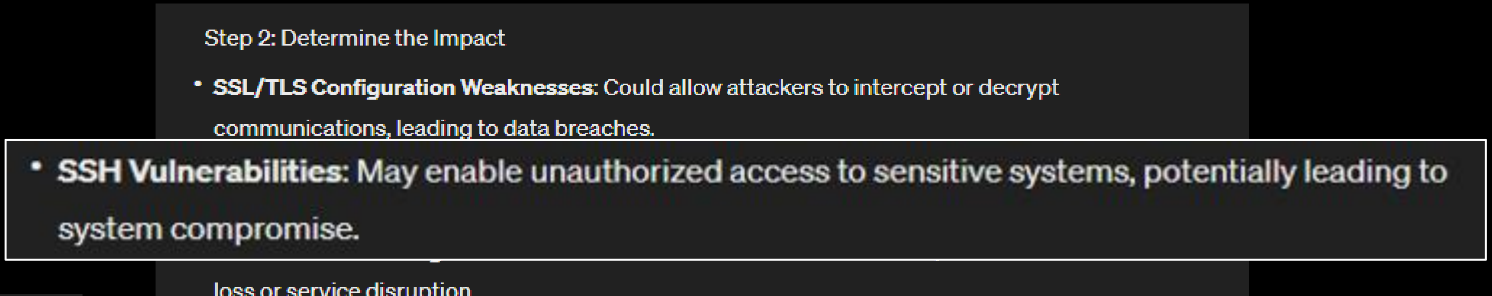
Recommended Mitigations

To address this vulnerability, consider the following mitigations:

1. **Update or Replace Certificates**: Ensure that all server certificates are issued by a trusted Certificate Authority (CA). Replace any self-signed, expired, or otherwise invalid certificates with valid ones.
2. **Configure Trust Stores**: Ensure that trust stores on clients and servers are properly configured to trust certificates only from reputable CAs.
3. **Regular Certificate Audits**: Perform regular audits of server certificates to ensure they remain valid, are not approaching expiration, and are issued by CAs trusted by the organization.
4. **Implement HTTPS Inspection**: For organizational perimeter defenses, consider deploying HTTPS inspection mechanisms that can detect and block potentially malicious SSL traffic.
5. **Security Awareness Training**: Educate staff about the risks associated with invalid certificates and the importance of secure connections.

By addressing this medium-risk vulnerability, the organization can significantly reduce the potential for man-in-the-middle attacks and enhance the overall security of its network communications.

Hallucinations

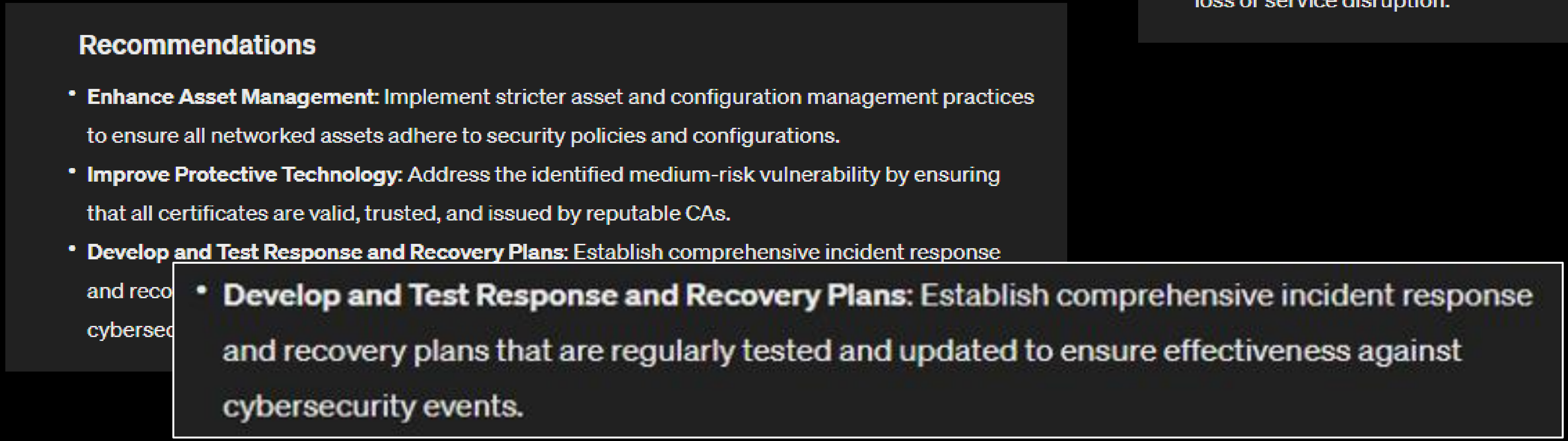


Step 2: Determine the Impact

- **SSL/TLS Configuration Weaknesses:** Could allow attackers to intercept or decrypt communications, leading to data breaches.

- **SSH Vulnerabilities:** May enable unauthorized access to sensitive systems, potentially leading to system compromise.

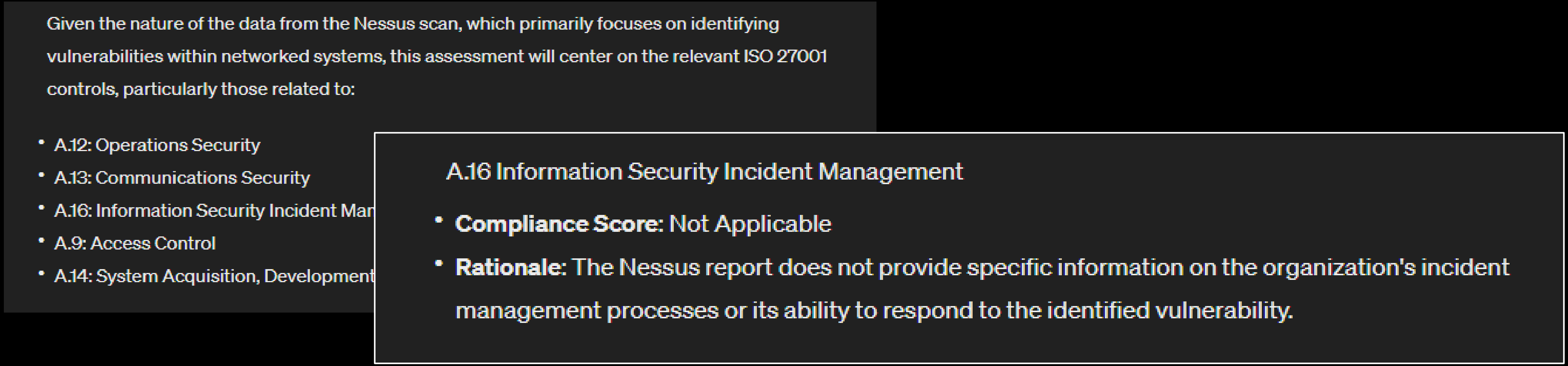
loss or service disruption.



Recommendations

- **Enhance Asset Management:** Implement stricter asset and configuration management practices to ensure all networked assets adhere to security policies and configurations.
- **Improve Protective Technology:** Address the identified medium-risk vulnerability by ensuring that all certificates are valid, trusted, and issued by reputable CAs.
- **Develop and Test Response and Recovery Plans:** Establish comprehensive incident response and reco cybersec

- **Develop and Test Response and Recovery Plans:** Establish comprehensive incident response and recovery plans that are regularly tested and updated to ensure effectiveness against cybersecurity events.



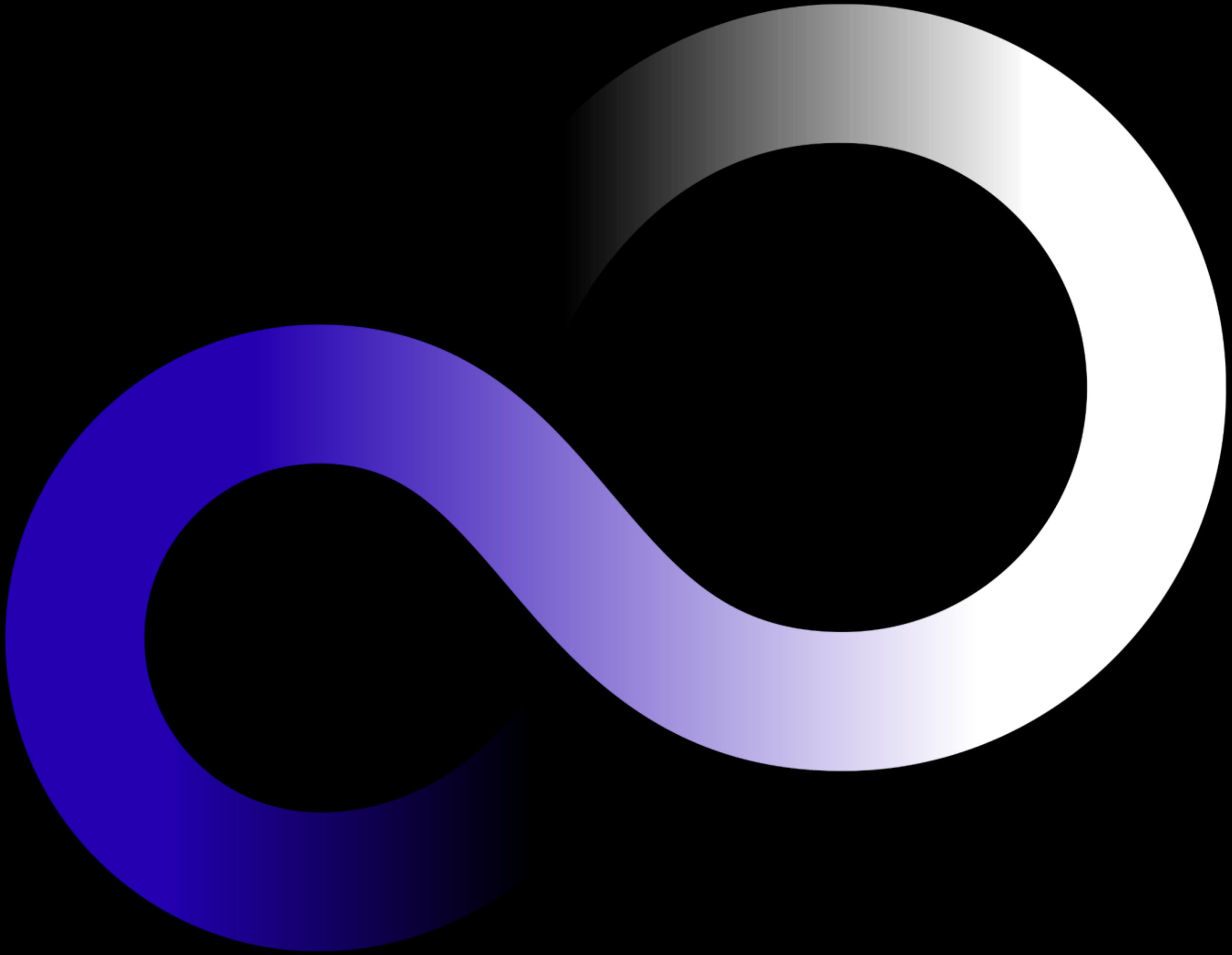
Given the nature of the data from the Nessus scan, which primarily focuses on identifying vulnerabilities within networked systems, this assessment will center on the relevant ISO 27001 controls, particularly those related to:

- A.12: Operations Security
- A.13: Communications Security
- A.16: Information Security Incident Man
- A.9: Access Control
- A.14: System Acquisition, Development

A.16 Information Security Incident Management

- **Compliance Score:** Not Applicable
- **Rationale:** The Nessus report does not provide specific information on the organization's incident management processes or its ability to respond to the identified vulnerability.

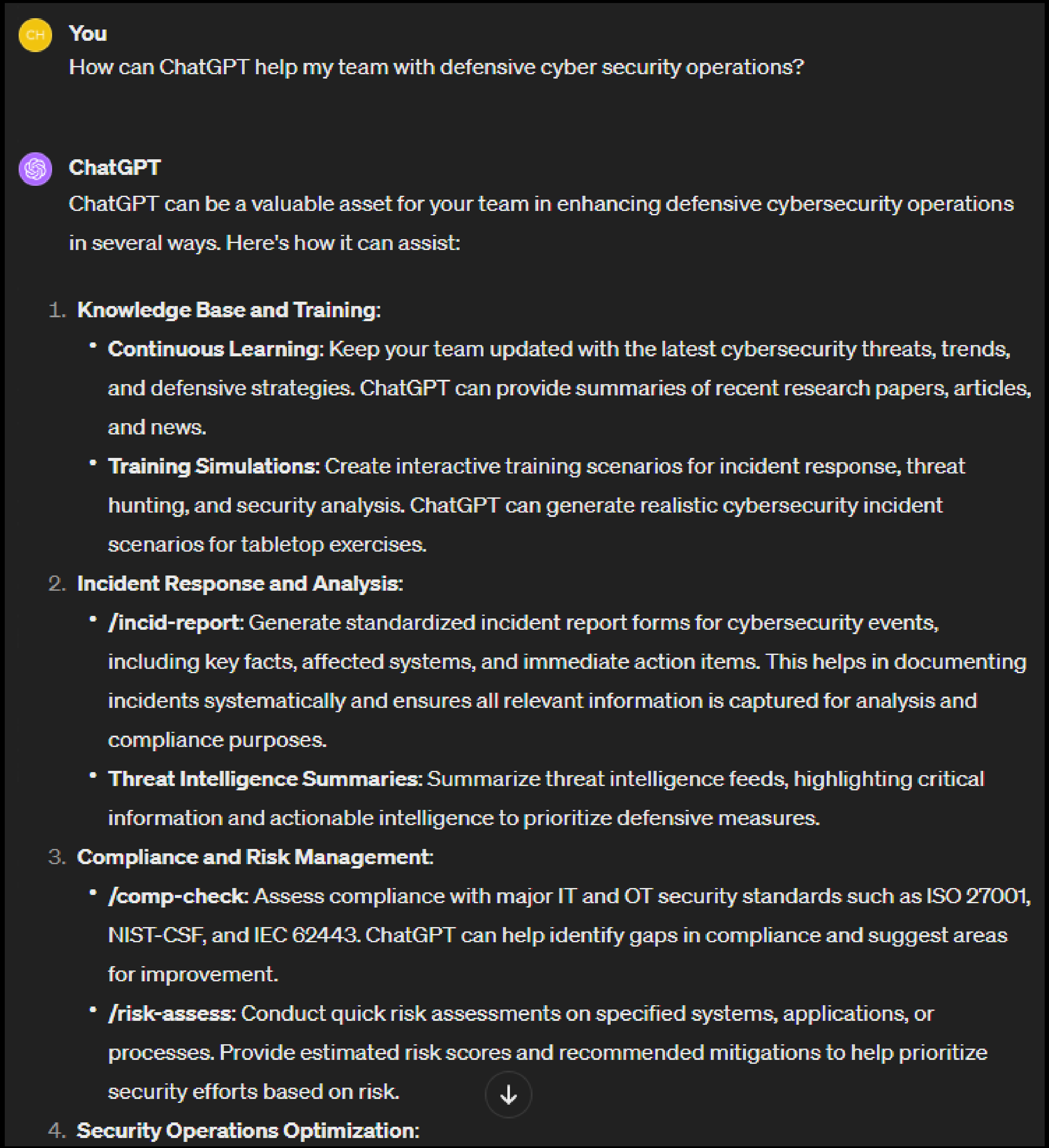
Final thoughts



Ethics

- Privacy by design
- Compliance by design
- Third party disclosure
- Hallucinations

Ask for suggestions



You

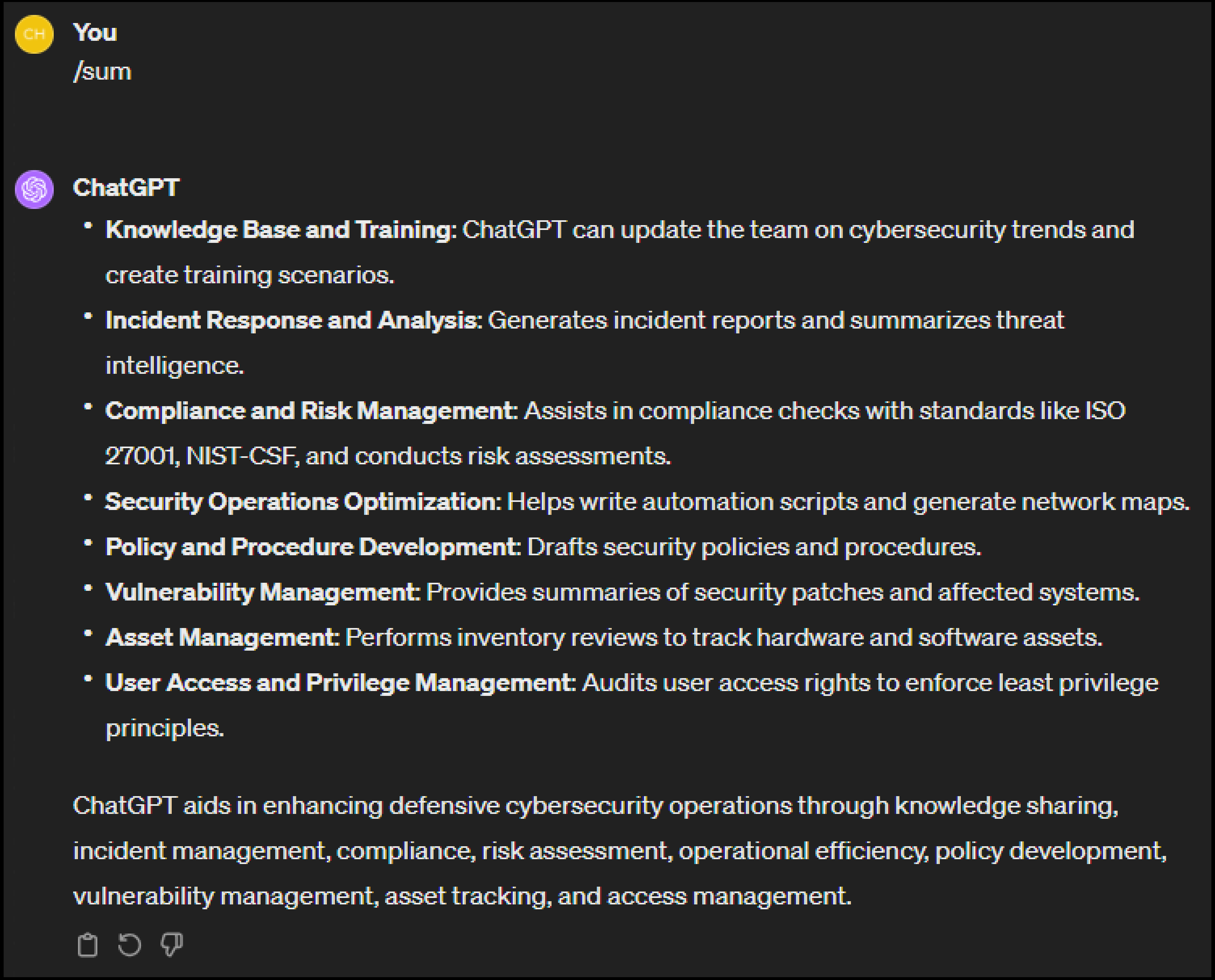
How can ChatGPT help my team with defensive cyber security operations?

ChatGPT

ChatGPT can be a valuable asset for your team in enhancing defensive cybersecurity operations in several ways. Here's how it can assist:

1. **Knowledge Base and Training**:
   - **Continuous Learning**: Keep your team updated with the latest cybersecurity threats, trends, and defensive strategies. ChatGPT can provide summaries of recent research papers, articles, and news.
   - **Training Simulations:** Create interactive training scenarios for incident response, threat hunting, and security analysis. ChatGPT can generate realistic cybersecurity incident scenarios for tabletop exercises.
2. **Incident Response and Analysis**:
   - **/incid-report**: Generate standardized incident report forms for cybersecurity events, including key facts, affected systems, and immediate action items. This helps in documenting incidents systematically and ensures all relevant information is captured for analysis and compliance purposes.
   - **Threat Intelligence Summaries:** Summarize threat intelligence feeds, highlighting critical information and actionable intelligence to prioritize defensive measures.
3. **Compliance and Risk Management**:
   - **/comp-check:** Assess compliance with major IT and OT security standards such as ISO 27001, NIST-CSF, and IEC 62443. ChatGPT can help identify gaps in compliance and suggest areas for improvement.
   - **/risk-assess:** Conduct quick risk assessments on specified systems, applications, or processes. Provide estimated risk scores and recommended mitigations to help prioritize security efforts based on risk.
4. **Security Operations Optimization**:

/sum



You

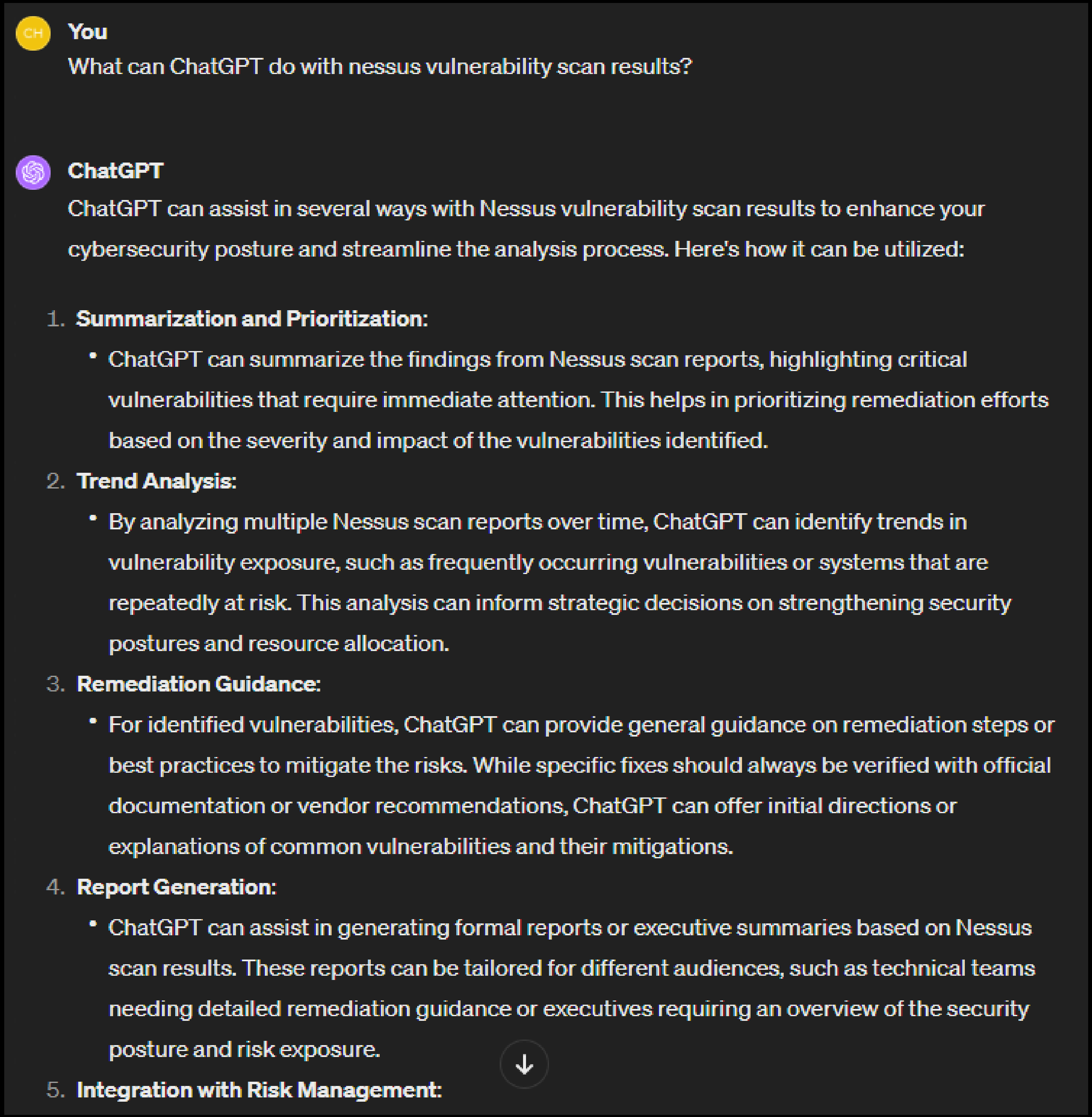
/sum

ChatGPT

- **Knowledge Base and Training:** ChatGPT can update the team on cybersecurity trends and create training scenarios.
- **Incident Response and Analysis:** Generates incident reports and summarizes threat intelligence.
- **Compliance and Risk Management:** Assists in compliance checks with standards like ISO 27001, NIST-CSF, and conducts risk assessments.
- **Security Operations Optimization:** Helps write automation scripts and generate network maps.
- **Policy and Procedure Development:** Drafts security policies and procedures.
- **Vulnerability Management:** Provides summaries of security patches and affected systems.
- **Asset Management:** Performs inventory reviews to track hardware and software assets.
- **User Access and Privilege Management:** Audits user access rights to enforce least privilege principles.

ChatGPT aids in enhancing defensive cybersecurity operations through knowledge sharing, incident management, compliance, risk assessment, operational efficiency, policy development, vulnerability management, asset tracking, and access management.

Ask about specific challenges



You

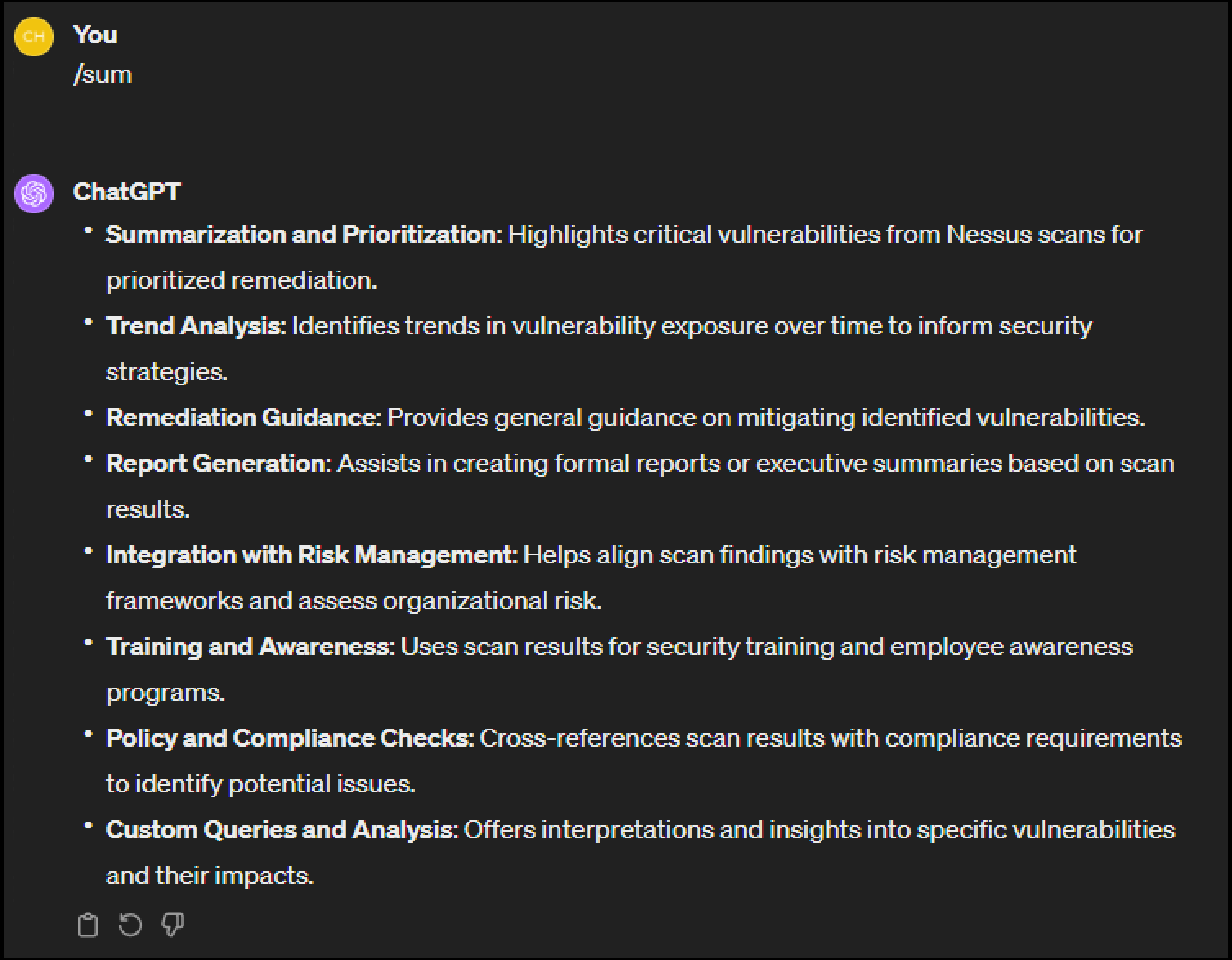
What can ChatGPT do with nessus vulnerability scan results?

ChatGPT

ChatGPT can assist in several ways with Nessus vulnerability scan results to enhance your cybersecurity posture and streamline the analysis process. Here's how it can be utilized:

1. **Summarization and Prioritization:**
   - ChatGPT can summarize the findings from Nessus scan reports, highlighting critical vulnerabilities that require immediate attention. This helps in prioritizing remediation efforts based on the severity and impact of the vulnerabilities identified.
2. **Trend Analysis:**
   - By analyzing multiple Nessus scan reports over time, ChatGPT can identify trends in vulnerability exposure, such as frequently occurring vulnerabilities or systems that are repeatedly at risk. This analysis can inform strategic decisions on strengthening security postures and resource allocation.
3. **Remediation Guidance:**
   - For identified vulnerabilities, ChatGPT can provide general guidance on remediation steps or best practices to mitigate the risks. While specific fixes should always be verified with official documentation or vendor recommendations, ChatGPT can offer initial directions or explanations of common vulnerabilities and their mitigations.
4. **Report Generation:**
   - ChatGPT can assist in generating formal reports or executive summaries based on Nessus scan results. These reports can be tailored for different audiences, such as technical teams needing detailed remediation guidance or executives requiring an overview of the security posture and risk exposure.
5. **Integration with Risk Management:**

/sum



You

/sum

ChatGPT

- **Summarization and Prioritization:** Highlights critical vulnerabilities from Nessus scans for prioritized remediation.
- **Trend Analysis:** Identifies trends in vulnerability exposure over time to inform security strategies.
- **Remediation Guidance:** Provides general guidance on mitigating identified vulnerabilities.
- **Report Generation:** Assists in creating formal reports or executive summaries based on scan results.
- **Integration with Risk Management:** Helps align scan findings with risk management frameworks and assess organizational risk.
- **Training and Awareness:** Uses scan results for security training and employee awareness programs.
- **Policy and Compliance Checks:** Cross-references scan results with compliance requirements to identify potential issues.
- **Custom Queries and Analysis:** Offers interpretations and insights into specific vulnerabilities and their impacts.

Questions?