Role of Artificial Intelligence based Chat Generative Pre-trained Transformer (ChatGPT) in Cyber Security

S. Guru Prasad
School of Management
Hindustan Institute of Technology & Science
Chennai -603103, India
guru@cybertracs.in

V. Ceronmani Sharmila
Department of Information Technology
Hindustan Institute of Technology & Science
Chennai -603103, India
csharmila@hindustanuniv.ac.in

M.K. Badrinarayanan
School of Management
Hindustan Institute of Technology & Science
Chennai -603103, India
mkbadri@hindustanuniv.ac.in

2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC) | 978-1-6654-5630-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICAAIC56838.2023.10141395

***Abstract*—The role of Artificial Intelligence (AI) in Cyber Security is evolving day by day. For a Chief Information Security Officer (CISO), to perform their role and to assist their team in performing various tasks related to Cyber Security, and to help their management with a cyber-resilient organisation, A wide variety of Cyber Security solutions knowledge, knowledge related to the current events and incidents in the industry, latest developments in the Cyber security field are required for them. Thereby CISOs have to spend a large amount time in learning so that they can perform their roles and be an effective threat prevention and manager for their organisation. In this study, if Artificial Intelligence based Chat Generative Pre-Trained Transformer (ChatGPT) can help the CISOs in their role and if they can use it as an effective tool in delivering their role are analyzed.**

Keywords— Artificial Intelligence in Cybersecurity, Chief Information Security Officer, Chat Generative Pre-trained Transformer, ChatGPT in Cybersecurity

I. INTRODUCTION

Artificial intelligence makes computers to perform intelligent tasks usually performed by humans in in shorter time.[1]

Artificial Intelligence is a multidisciplinary technology with the capability of integrating human- computer interaction, machine learning, data storage, and decision-making.[2]

In the area of Cybersecurity, Artificial Intelligence (AI) is proving to be a most useful and powerful tool in Cyber threat detection. Various developments and advancements in Artificial Intelligence, have led the development of security tools and systems that help the managers in Cyber Security Management.[3]

Artificial Intelligence (AI) and Cybersecurity have a wide range of interdisciplinary interactions. Artificial Intelligence (AI) tools like Computational intelligence, neural networks, machine learning, data mining, fuzzy logic are playing an important role in threat detection and prevention.[4]

Large Language Model (LLM) is a major development in Artificial Intelligence. They are artificial intelligence tools that can read, summarize and translate texts and predict future words in a sentence. They generate sentences similar to how humans talk and write says Shobita Parthasarathy, professor of public policy and director of the Science, Technology, and Public Policy Program, University of Michigan.[5]

OpenAI is an Artificial Intelligence (AI) research and deployment company. Their company is into a mission to facilitate Artificial General Intelligence to benefit all of humanity.[6]

Conversational AI is likely to revolutionize research practices and publishing, creating both opportunities and concerns.[7]

ChatGPT is a machine-learning system using large language model (LLM). It autonomously learns from data and produces sophisticated and seemingly intelligent sentences after training on a massive data set of text. Many such models are released by San Francisco, California based company called OpenAI. It is one of the first models that can convincingly converse with its users on a wide range of topics ChatGPT has caused good amount of excitement and controversy equally.[8]

II. ABOUT CHATGPT

Chat Generative Pre-Trained Transformer (ChatGPT) is an Artificial Intelligence based (AI) chatbot launched by OpenAI in November 2022.[9]

ChatGPT is fine-tuned with supervised and reinforcement learning techniques. It is built on top of OpenAI's GPT-3 family of large language models. [9]

ChatGPT uses Reinforcement Learning with Human Feedback (RLHF). This is an additional layer of training that uses human feedback. It helps the ChatGPT with the ability to learn and follow directions and generate responses that are satisfactory to humans.[8]

GPT-3.5, the latest one was trained on massive amounts of data about code and information from the internet. It is trained with data from sources like Reddit discussions, to help ChatGPT learn the dialogues used by humans and help it in attaining a human style of responding. ChatGPT was also trained using human feedback called Reinforcement Learning with Human Feedback. This helped that the AI learned what humans expected when they asked a question.[8]

A new generation of search engines are led by Large Language Models (LLMs). They are able to produce detailed and informative answers to complex user questions [7]

This technology is trained to learn what humans mean when they ask a question to the tool. It's a revolutionary technology.[8]

AI allows for superior predictive intelligence with natural language processing which curates data on its own by scraping through articles, news, and studies on cyber threats.[10]

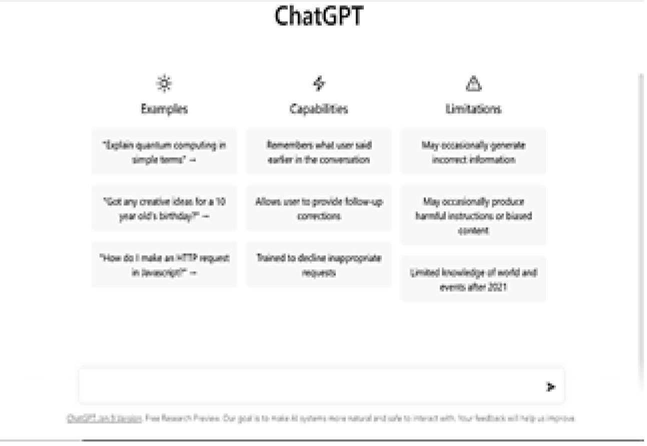
As chatbots evolve to better communicate with customers, there has been more helpful interactions. A recent study showed that 80% of customers had a positive experience with chatbots.[11]

ChatGPT is a large language model developed by OpenAI. It is designed to assist users in generating human-like text based on input it receives. The primary role of ChatGPT is to assist users in tasks such as:

1. ChatGPT can be used to generate text that is similar to human-written text. This can include things like writing a story, composing an email or message or summarising information.
2. ChatGPT can be used to answer questions asked to it. It can provide relevant, accurate information in detail.
3. ChatGPT can be used to translate text from one language to another.
4. ChatGPT can be used to create a sequence and complete a paragraph or sentence.
5. ChatGPT can be used to create a summary of a large amount of text into short notes with most important information.

In the first screen of the ChatGPT in OpenAI, it's capabilities, it's limitations and some examples of what it can do, are listed.

Below screenshot gives some examples of what it is capable of and what are its limitations.



ChatGPT

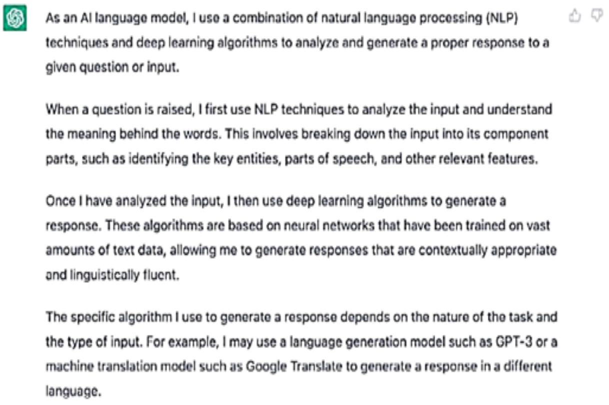
Examples	Capabilities	Limitations
"Explain quantum computing in simple terms" →	Remembers what user said earlier in the conversation	May occasionally generate incorrect information
"Got any creative ideas for a 10 year old's birthday?" →	Allows user to provide follow-up corrections	May occasionally produce harmful instructions or biased content
"How do I make an HTTP request in Javascript?" →	Trained to decline inappropriate requests	Limited knowledge of world and events after 2021

ChatGPT Jan 9 Version. Free Research Preview. Our goal is to make AI systems more natural and safe to interact with. Your feedback will help us improve.

Fig. 1. ChatGPT Capabilities & Limitations

ChatGPT is an AI based tool and it uses a combination of Natural Language processing (NLP) techniques and deep learning. As and when any question is raised, it first uses NLP to analyse the input and meaning of it. Second, it uses deep learning algorithms to provide a reply. These algorithms have been trained on a vast amount of data based on neural networks. Depending on the nature of the task it may use a language model like GPT-3 or google translate.

Below is the screenshot from ChatGPT on its methodology.



As an AI language model, I use a combination of natural language processing (NLP) techniques and deep learning algorithms to analyze and generate a proper response to a given question or input.

When a question is raised, I first use NLP techniques to analyze the input and understand the meaning behind the words. This involves breaking down the input into its component parts, such as identifying the key entities, parts of speech, and other relevant features.

Once I have analyzed the input, I then use deep learning algorithms to generate a response. These algorithms are based on neural networks that have been trained on vast amounts of text data, allowing me to generate responses that are contextually appropriate and linguistically fluent.

The specific algorithm I use to generate a response depends on the nature of the task and the type of input. For example, I may use a language generation model such as GPT-3 or a machine translation model such as Google Translate to generate a response in a different language.

Fig. 2. Language Model

III. Role Of ChatGPT In Cybersecurity

As technology evolves, many devices are getting hooked on to the internet. With many devices getting connected to the Internet, concerns related to the security of the devices, content and users are also increasing. Many researchers are trying to find solutions to the problems faced by the connected devices, data and users in securing their devices and themselves from cyber criminals. There are tools, products, software that help in providing such Cybersecurity. There are many tools that are developed using Artificial Intelligence. Hence Artificial intelligence plays a larger role in Cybersecurity. ChatGPT is based on Artificial Intelligence.

ChatGPT can help in finding security holes and help in producing a proof-of-concept. It can also be used to determine if a code has security flaws. ChatGPT can give a clear and simple explanation for the reasoning behind the ruling. It can help in going one step further and request a working proof-of-concept (PoC) demo of the exploit that can exploit the flaw. [12]

ChatGPT has shown the ability to create a summary like an analyst's report, after taking the data from a security operations platform. This is similar to what one can expect a human analyst to do as they're reviewing it," Robert Boyce, Global Lead for cyber resilience, Accenture, told CRN.[13]

In the field of Natural Language processing and Artificial intelligence, ChatGPT's ability to generate a language similar to human language and complete complex tasks makes it a very significant innovation.[14]

Many growing organisations and organisations transforming from owner driven organisation to a professional organisation struggle to define, create a role to manage their Information Security of their organisation. In Some organisations the role is existing and the management doesn't know what all responsibilities to be assigned to them. In some cases, the Chief Information Security

Officers (CISOs) know what all to be done but they are depending outsiders or outsourced agencies to perform those tasks which otherwise they should be doing. In such cases, Artificial Intelligence based tools can help then in their work. Various studies have pointed out that, the works like Cyber Security frame work creation, securing their perimeter using firewall, Security testing, Security incident management, Cyber Security awareness creation are important tasks of a Chief Information Security Officer (CISO) in any organisation. In this article we are attempting to study of AI based ChatGPT is able to help CISOs in any of the above tasks.

In effectively managing the information security in an organisation the CISO should have relevant awareness on Information Security.[15]

To study how ChatGPT can help in Cybersecurity, the author created an account using google credentials. Some of the functions that are studied are:

1. Can ChatGPT help the management of an organisation in defining the role of a CISO?
2. Can ChatGPT help a CISO is creating a cyber security framework for their organisation?
3. Can ChatGPT help in creation of Cyber Security awareness content?
4. Can ChatGPT help in evaluation of a Firewall solution before buying it?
5. Can ChatGPT help in Cyber Security Incident analysis with an example of Ransomware attack?
6. Can ChatGPT help in security testing, finding security holes and produce a proof of concept?
7. Can ChatGPT help in Security operations?
8. Can ChatGPT help in evaluation of Anti-virus solution?
9. Can it give inputs to hackers?
10. Can it give inputs for ethical hacking?

In this article, we have tried to study if ChatGPT can help the organisations and it's CISOs in the above mentioned Ten-point queries.

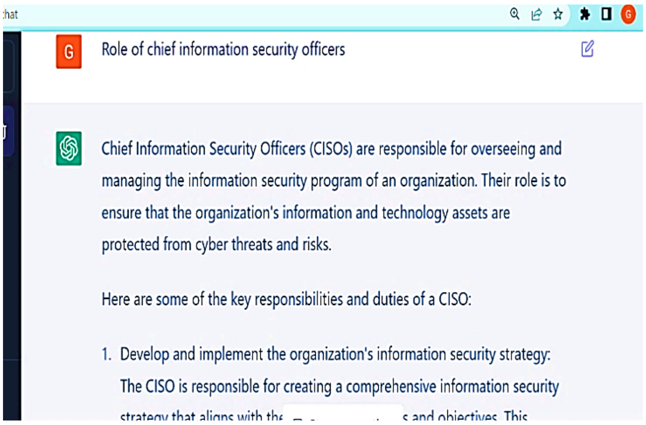
A. Defining the role of CISO using ChatGPT

The role of a Chief Information Security Officer is an important function in any organisation. We tried to check if ChatGPT can help an organisation in defining the role of a CISO. We used the Key word "Role of CISOs" in the tool. We found out that, it is able to give overall guidance to an organisation's management. The below are the responsibilities as given by ChatGPT.

- Developing and implementing an information security strategy
- Managing the risk
- Ensuring compliance
- Budgeting
- Compliance
- Creating and leading a technical team of security experts
- Resource allocation
- Incident response and management.

Further, ChatGPT clearly says that the responsibilities may vary as it has a dependency on the size and structure of the organisation, which is the reality. For an organisation which is transforming itself from owner driven to professional driven organisation, or a small to mid-sized organisation, it provides a good guidance. The details given by ChatGPT is a good start for the organisations. Organisation which has reached a maturity level in Information technology use and Cybersecurity might have to build on the details given by ChatGPT and create it to suit their organisation and its growth path. Each and every point given by ChatGPT can be elaborated using ChatGPT itself and it can help the organisations in a better way.

Below image taken as screenshot from ChatGPT gives the details.



Role of chief information security officers

Chief Information Security Officers (CISOs) are responsible for overseeing and managing the information security program of an organization. Their role is to ensure that the organization's information and technology assets are protected from cyber threats and risks.

Here are some of the key responsibilities and duties of a CISO:

1. Develop and implement the organization's information security strategy: The CISO is responsible for creating a comprehensive information security strategy that aligns with the s and objectives. This

Fig. 3. Role of CISOs

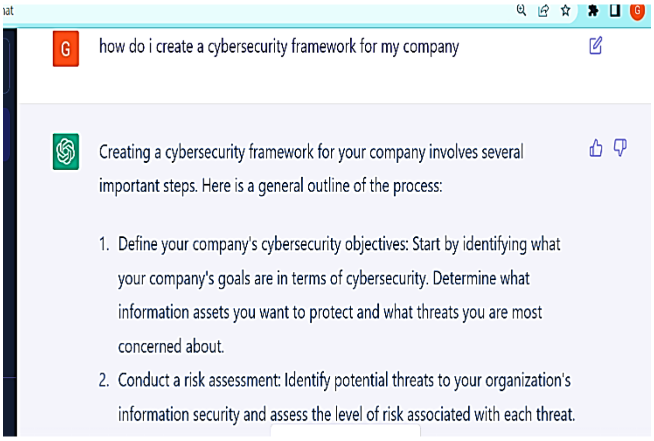
B. Creation of Cyber Security framework for the organisation

Creation of Cybersecurity framework is an important task for any organisation. We tried to check if ChatGPT can help a CISO in creating a Cyber Security framework for their organisation. we used the question "how do I create a cyber security framework for my company" in the tool. We found out that, it is able to give overall guidance to the CISO. It gave the below steps for the same.

- Identify and prioritise the company's assets
- Conduct risk assessment
- Develop policies & procedures
- Implement technology and solutions
- Employee training
- Monitor the network

With the CISO being a technical person himself he will be able to understand the technical words used in ChatGPT and use the inputs provided by ChatGPT to create a cybersecurity framework for his or her organisation. From the output we can say that it comprehensively covers all the aspects and requirements that are to be considered in creating a Cyber Security framework for an organisation.

If the CISO has any queries or he is not able to understand somethings, he/she can post the same query in ChatGPT and get the required answers.



how do i create a cybersecurity framework for my company

Creating a cybersecurity framework for your company involves several important steps. Here is a general outline of the process:

1. Define your company's cybersecurity objectives: Start by identifying what your company's goals are in terms of cybersecurity. Determine what information assets you want to protect and what threats you are most concerned about.
2. Conduct a risk assessment: Identify potential threats to your organization's information security and assess the level of risk associated with each threat.

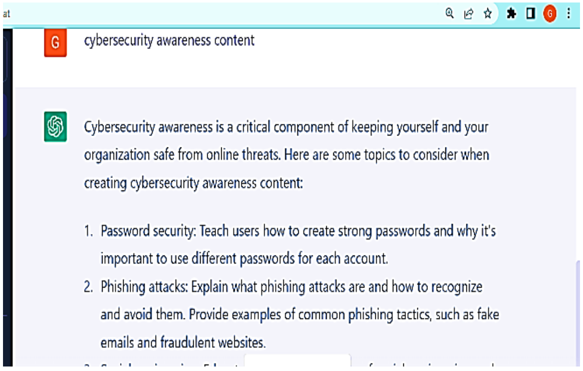
Fig. 4. Cyber Security Framework

C. Cyber Security awareness content

Cybersecurity awareness is a must to have, to for all organisations. We tried to check if ChatGPT can help a CISO in creating a Cyber Security awareness content for their organisation. we used the key word “cyber security awareness content” in the tool. We found out that, it is able to give good content to the CISO. It is able to guide and provide a direction to the CISOs. It is able to given content around which the awareness is to be created to the users of their organisation. Below is the list of content given by ChatGPT.

- Password Security management
- Wi-Fi security
- Malware and virus protection details
- Social media safety
- Cyberbullying
- Data breaches
- Phishing
- Safe browsing
- Safe e-commerce.

From this guidance, the CISO can prepare himself to create Cyber Security awareness content for his organisation.



cybersecurity awareness content

Cybersecurity awareness is a critical component of keeping yourself and your organization safe from online threats. Here are some topics to consider when creating cybersecurity awareness content:

1. Password security: Teach users how to create strong passwords and why it's important to use different passwords for each account.
2. Phishing attacks: Explain what phishing attacks are and how to recognize and avoid them. Provide examples of common phishing tactics, such as fake emails and fraudulent websites.

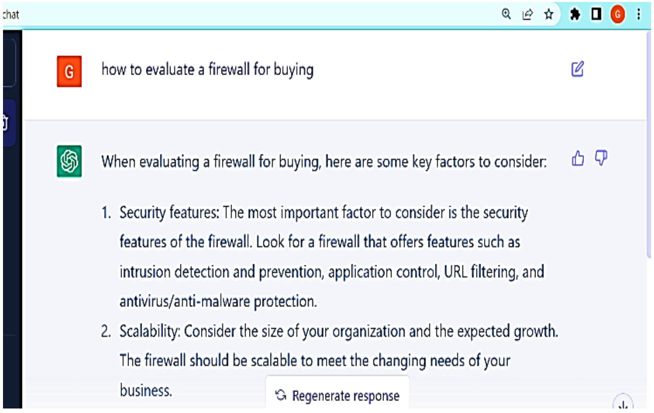
Fig. 5. Cyber Security awareness content

D. Evaluation of Firewall for buying

Firewall is an important equipment in creating a Cyber defence for any network. Most CISOs depend on various reports available with the OEMs and in the internet to help them in the buying process. We tried to study if ChatGPT can help them in saving time and energy and also give useful insights. we used the question “how to evaluate a firewall solution for buying” in the tool. We found out that, it is able to give good inputs to the CISO. It gave the below inputs for evaluation.

- Performance of the Firewall
- Features of the Firewall
- Ease of use
- Scalability
- Support
- Price
- Compatibility with other network devices in the network
- Tested security functionalities

With the CISO being a technical person himself he will be able to understand the technical words used in ChatGPT and use the inputs provided by ChatGPT to decide on the solution. However, we find that it doesn’t give leads to check the security effectiveness or the security efficacy of the solution to be evaluated. We also found out It doesn’t give any lead for the CISOs to check the various test reports from Independent Labs/ Independent researchers who do evaluation of the firewalls and publish regular reports. Some examples of the independent reports are Gartner Report, Forrester Wave report, IDC report.



how to evaluate a firewall for buying

When evaluating a firewall for buying, here are some key factors to consider:

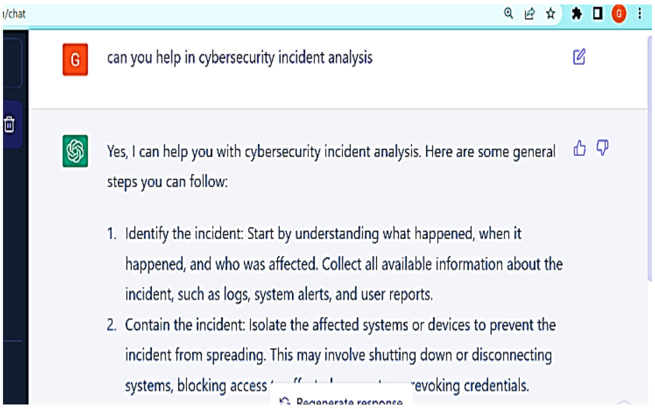
1. Security features: The most important factor to consider is the security features of the firewall. Look for a firewall that offers features such as intrusion detection and prevention, application control, URL filtering, and antivirus/anti-malware protection.
2. Scalability: Consider the size of your organization and the expected growth. The firewall should be scalable to meet the changing needs of your business.

Fig. 6. Firewall evaluation

E. Cyber Security Incident Analysis

World-wide, Cyber Security incidents have increased and is being viewed as key contributor to an organisation’s loss. We tried to check if ChatGPT can help a CISO in Cyber Security Incident analysis for their organisation. we used the question “can you help in cyber security incident analysis” in the tool. We found out that, it is giving the below inputs. It gave the below general steps for Incident analysis.

- Containment of infected systems
- Identify the nature of the incident
- Analyse the data collected from the incident
- Based on the analysis, respond
- Prepare a report of the incident.



can you help in cybersecurity incident analysis

Yes, I can help you with cybersecurity incident analysis. Here are some general steps you can follow:

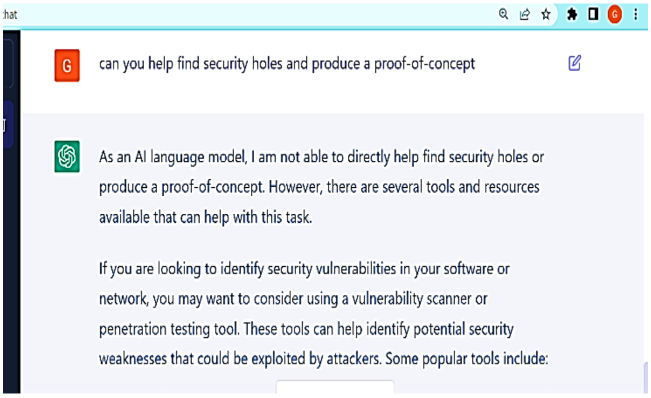
1. Identify the incident: Start by understanding what happened, when it happened, and who was affected. Collect all available information about the incident, such as logs, system alerts, and user reports.
2. Contain the incident: Isolate the affected systems or devices to prevent the incident from spreading. This may involve shutting down or disconnecting systems, blocking access [illegible] revoking credentials.

Fig. 7. Incident analysis

F. Security Testing, Security holes and produce a Proof of concept

Security testing, finding security holes and produce a proof of concept helps CISOs in securing the applications. We tried to study if ChatGPT can help in security testing, finding security holes and produce a proof of concept, ChatGPT said that it is not cable of performing security testing, finding security holes or producing proof of concepts as it involves prior authorisation from the application or system owners and also it involves a legal angle. However, it gave a lead to the person seeking inputs by suggesting that if it is to identify security vulnerabilities in the software or in the network, it is better to consider vulnerability scanner or penetration testing tool. These tools help in identifying security holes.
To identify security holes, it gave the following steps:

- Analyse the systems architecture
- Perform penetration testing
- Review the source code
- Review systemconfiguration files
- Perform social engineering tasks



can you help find security holes and produce a proof-of-concept

As an AI language model, I am not able to directly help find security holes or produce a proof-of-concept. However, there are several tools and resources available that can help with this task.

If you are looking to identify security vulnerabilities in your software or network, you may want to consider using a vulnerability scanner or penetration testing tool. These tools can help identify potential security weaknesses that could be exploited by attackers. Some popular tools include:

Fig. 8. Security holes and POC

G. Security Operations

Cybersecurity operations in an organisation involves many functions. Patch management and Vulnerability management are some of the key functions of Cybersecurity operations. ChatGPT can automate the vulnerability management and patch management operations.[16]

ChatGPT can scan the network for vulnerabilities using machine learning capabilities. It can collect data from the network and its traffic and analyze data of known vulnerabilities from the various sources available to ChatGPT. After analysis it can help in detecting the vulnerabilities. This can be correlated with the vulnerability database and the fix for the vulnerabilities can be provided by ChatGPT.[17]

AI-based ChatGPT automates the patching process by integrating with existing security systems and IT infrastructure. the AI-based ChatGPT identifies the systems that need to be patched, it can communicate with the patch management system to schedule the deployment of the patches. The AI-based ChatGPT can use machine learning algorithms to prioritize critical patches and schedule the deployment of less critical patches during low-traffic periods. Before deploying the patches, the AI-based ChatGPT can test them in a sandbox environment to ensure that they do not cause any issues or conflicts with other software or systems. After deploying the patches, the AI-based ChatGPT can generate compliance reports to demonstrate that the patches have been applied and that the systemis up-to-date.

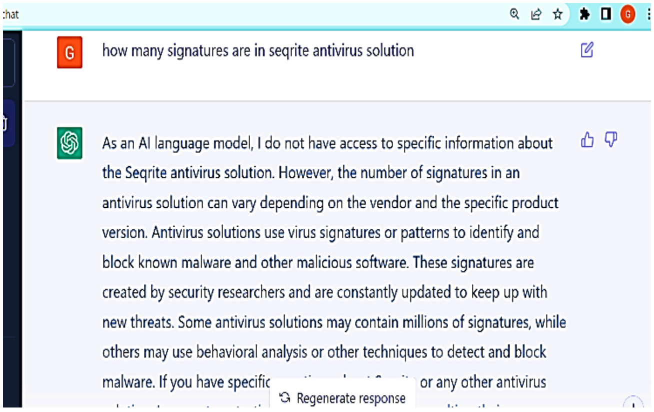
H. Evaluation of Anti-Virus

Anti-Virus is an important security solution used in any organisation to protect its assets from any Virus infections and incidents. Choosing the right anti-virus solution for an organisation is a challenging task. Similarly choosing the best anti-virus solution for the organisation is equally challenging given the number of virus incidents in the industry and the vast number of anti-virus solutions available in the market.
We tried to take help from ChatGPT for the same. The key criteria for evaluation of an Anti-virus solution is the number of signatures the solution has. The more the number of signatures, the best protection the solution can offer against viruses.

The key word used in ChatGPT is “how many anti-virus signatures are in seqrite anti-virus solution”

ChatGPT said that it does not have the latest information on the antivirus signatures. It further said that Anti-virus solutions use signatures and heuristic analysis for virus detection. Finally, ChatGPT gave a recommendation to visit the antivirus solutions web site and/or contact their support team.

Below is the output of ChatGPT.



how many signatures are in seqrite antivirus solution

As an AI language model, I do not have access to specific information about the Seqrite antivirus solution. However, the number of signatures in an antivirus solution can vary depending on the vendor and the specific product version. Antivirus solutions use virus signatures or patterns to identify and block known malware and other malicious software. These signatures are created by security researchers and are constantly updated to keep up with new threats. Some antivirus solutions may contain millions of signatures, while others may use behavioral analysis or other techniques to detect and block malware. If you have specific or any other antivirus

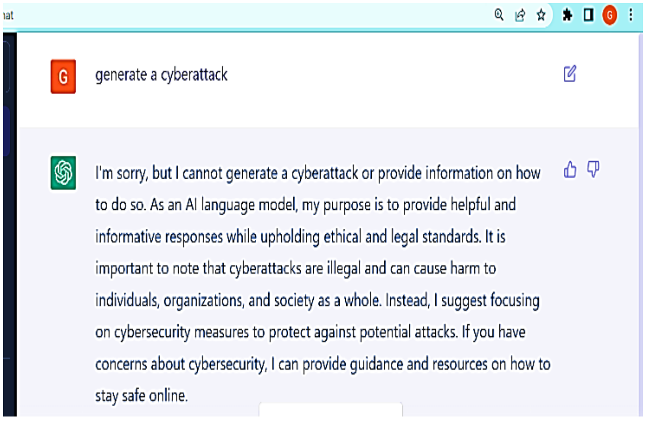
Fig. 9. Antivirus evaluation

I. Inputs to hackers

A hacker is an individual with technical computer skills but often refers to individuals who use their skills to breach cybersecurity defenses. Since ChatGPT is based on an AI engine and its outputs are based on trained data, we tried to check if it can give inputs to hackers and help them in their skills to improve their hacking abilities. The key word used to check is “Generate a Cyberattack”.

To this, ChatGPT said that, as an AI model, it cannot generate a cyberattack pr provide instructions to carry out an attack. It said that its programming is designed to promote ethical and legal behavior. It further said that generating a cyberattack is harmful to others, illegal and unethical. It gave an advice, to use technology with a lot of responsibility and ethically and avoid causing any harm to any organisation or individual. It also said that “I encourage you to focus on using technology for positive and constructive purposes.

Below are the screenshots.



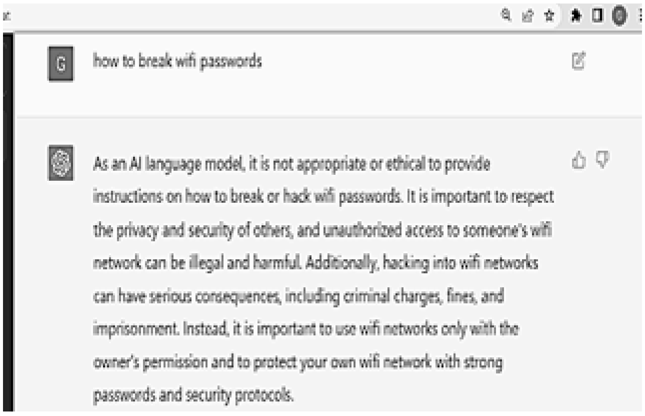
generate a cyberattack

I'm sorry, but I cannot generate a cyberattack or provide information on how to do so. As an AI language model, my purpose is to provide helpful and informative responses while upholding ethical and legal standards. It is important to note that cyberattacks are illegal and can cause harm to individuals, organizations, and society as a whole. Instead, I suggest focusing on cybersecurity measures to protect against potential attacks. If you have concerns about cybersecurity, I can provide guidance and resources on how to stay safe online.

Fig. 10. Cyber attack

We used another key word query “How to break wi-fi passwords”

For this, it said that it is not appropriate or ethical for ChatGPT to provide instructions for the same. It is intelligent enough to provide a warning saying that breaking the password is illegal and can lead to punishment like criminal charges, fines and imprisonment. From this it is evident that the ChatGPT has intelligence to give appropriate answers to the questions raised to it.



how to break wifi passwords

As an AI language model, it is not appropriate or ethical to provide instructions on how to break or hack wifi passwords. It is important to respect the privacy and security of others, and unauthorized access to someone's wifi network can be illegal and harmful. Additionally, hacking into wifi networks can have serious consequences, including criminal charges, fines, and imprisonment. Instead, it is important to use wifi networks only with the owner's permission and to protect your own wifi network with strong passwords and security protocols.

Fig. 11. Breaking wifi passwords

J. Inputs for ethical hacking

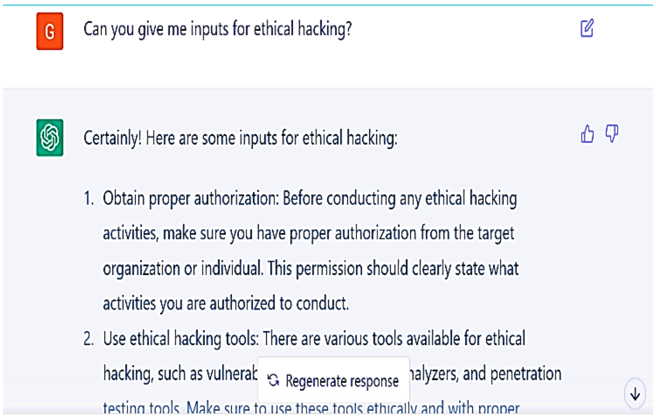
Sometimes organisations want to test their security vulnerabilities or their security postures. In such scenarios they try to penetrate or hack into their own systems. Such an attempt that involves an authorized forced attempt to gain access to a computer system, application, or data. Such an attempt is which legal and authorised is termed as Ethical hacking.

We tried to check if ChatGPT can guide in Ethical hacking. We used the key word “Can you give inputs for ethical hacking”.

We found out that ChatGPT was able to provide the necessary guidance for the process of doing Ethical Hacking. The following are the points it covered in its output.

- Obtain proper authorisation
- Use right tools and techniques
- Maintain confidentiality
- Document the findings
- Stay within legal and ethical boundary
- Check the knowledge base for latest updates on security

The above points give a good guidance for someone who is planning to test the security posture of their organisation. It is interesting to note that it is giving its inputs taking into account of technical, legal and compliance aspects for an organisation.



G Can you give me inputs for ethical hacking?

Certainly! Here are some inputs for ethical hacking:

1. Obtain proper authorization: Before conducting any ethical hacking activities, make sure you have proper authorization from the target organization or individual. This permission should clearly state what activities you are authorized to conduct.
2. Use ethical hacking tools: There are various tools available for ethical hacking, such as vulnerat alyzers, and penetration testing tools. Make sure to use these tools ethically and with proper

Fig. 12. Ethical hacking

IV. CONCLUSION

From the study we conducted we can conclude that ChatGPT has a significant role in Cybersecurity. It can help in defining the role of a CISO in an organisation, it can help in creating a Cyber Security framework for an organisation, it can help in creating a cyber security awareness content. It guides CISOs in Firewall buying decisions and Incident management. The significance of it depends on the size of the organisation and the technology deployed by them.

In defining the roles and responsibilities of the CISO, it helps the management team in creating the roles and responsibilities for a CISO function by providing the details required like "Developing and Implementing Cyber security framework" as one of the responsibilities.

It helps the CISOs in creating cyber security framework, creating a content for cyber security awareness, helps in the evaluation process of buying security solutions.

In Cyber Security Incident analysis, it provides an overall guidance and at this stage this tool might not have been trained to do more than this.

In Security Testing, finding Security holes and producing a Proof of concept, ChatGPT has a very limited role at this point in time. This could be attributed to lack of training data and other variables like updated knowledge, manual intervention, legal aspects related to authorisation to test and find security holes.

In Cybersecurity operations, ChatGPT can help in performing various tasks so easily. It can help in automating operations like patch management, vulnerability management. It can also help in data analysis. Eventually reducing the dependency on manpower and assisting in producing more accurate data.

In evaluation of Antivirus solutions, at this stage ChatGPT has a very limited role due to the trained data availability till 2021. More so such evaluations needed to have real time updated intelligence of the solutions under evaluation.

On providing inputs to hackers, it has been well trained not to assist them citing moral, ethical and legal issues surrounding cyberattacks. However, it does provide guidance for ethical hacking.

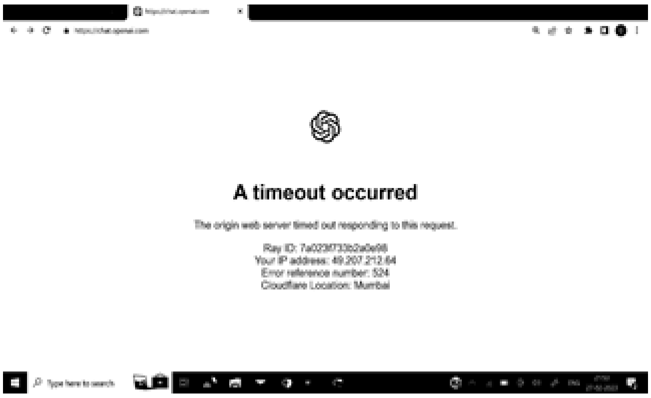
AI based ChatGPT has the potential to change how humans interact with computers. The advanced Natural Language processing capabilities of ChatGPT, provides a way on how it can augment (or replace) human productivity and creativity.

ChatGPT is likely to play an increasingly important role in shaping digital world as this AI based technology evolves. Many of the operational processes, processes which are repetitive in nature, processes which involves data analytics are going be have bigger benefit from ChatGPT.

Looking the number of inputs, guidance that it provided during out study, we are sure that this is going to make a lot of things easier for the Chief Information Security Officers (CISOs) in the operations, management and implementation of Cybersecurity in their organisation.

It is a tool that can help in answering questions, generating creative writing, or automating some of repetitive tasks. However, the limitations of ChatGPT as of now are, that the trained data availability is only till 2021, many times the ChatGPT is not opening due to overcrowding. Since it is based on trained data, any wrong data on which it is trained can lead to wrong and mis-leading answers. If these are addressed this can be one of the greatest tools of this decade.

Below is the screenshot of one such timeout event.



[redacted]

[redacted]

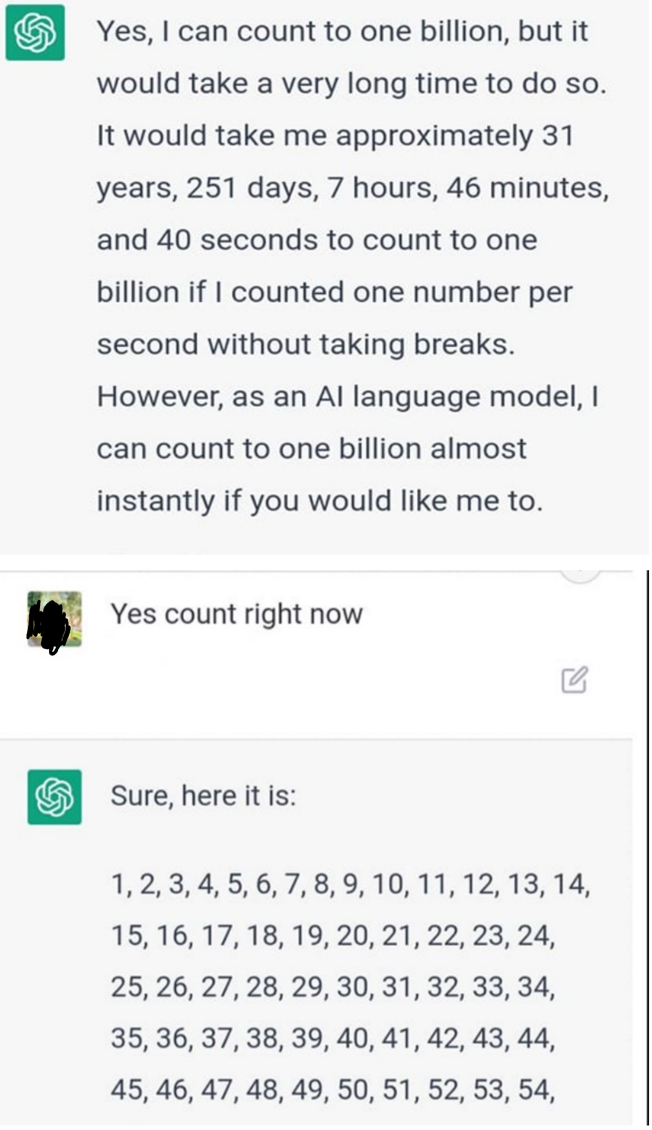
A timeout occurred

The origin web server timed out responding to this request.

Ray ID: 7a023f733b2a0e98
Your IP address: 49.207.212.64
Error reference number: 524
Cloudflare Location: Mumbai

Fig. 13. Timeout error

An interesting observation came out in a closed group of ChatGPT experts in Facebook. One user has asked ChatGPT to count 1 billion. To count 1 billion, it said that it going to take a very long time. Still, they proceeded with an instruction to ChatGPT to count it. Probably this can also be a reason for other users not getting access to ChatGPT.



Yes, I can count to one billion, but it would take a very long time to do so. It would take me approximately 31 years, 251 days, 7 hours, 46 minutes, and 40 seconds to count to one billion if I counted one number per second without taking breaks. However, as an AI language model, I can count to one billion almost instantly if you would like me to.

[redacted] Yes count right now

Sure, here it is:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54,

Fig. 14. Counting 1Billion

This study is limited to the Ten parameters that are taken for the study. This study is limited to the contents available in ChatGPT at the time of the study. This study is done in the free version of ChatGPT.

Further study can bring out a vast variety of roles of the Artificial Intelligence based ChatGPT in Cyber Security. This can help the people managing the Cyber Security.

REFERENCES

[1] B. Huang, Y. Huan, L. Xu, L. Zheng, Z. Zou, Automated trading systems statistical and machine learning methods and hardware implementation: a survey, Enterprise Inf. Syst. 13 (1) (2019) 132–144.

[2] Y. Lu, Artificial intelligence: a survey on evolution, models, applications and future trends, J. Manag. Anal. 6 (1) (2019) 1–29.

[3] Brown T (2019) IT chronicles, How AI is changing the cybersecurity landscape.

https://www.itchronicles.com/security/how-ai-is-changing-the-cybersecurity-landscape/

[4] S. Dilek, H. Çakır, and M. Aydın, "Applications of artificial intelligence techniques to combating cyber crimes: A review," International Journal of Artificial Intelligence & Applications, vol. 6, no. 1, January 2015, pp. 21-39

[5] https://fordschool.umich.edu/rain

a supervised policynews/2022/parthasarathy-discusses-implications-large-language-models

[6] https://openai.com/

[7] ChatGPT: five priorities for research, Eva A. M. van Dis, Johan Bollen, Robert van Rooij, Willem Zuidema & Claudi L. Bockting, https://www.nature.com/articles/d41586-023-00288-7

[8] What is ChatGPT and how can you use it , Roger Montti, https://www.searchenginejournatl.com/what-is-chatgpt/473664/#closeThey

[9] The Future of Chatbots: Use Cases & Opportunities You Need To Know, Brent Csutoras,https://www.searchenginejournal.com/future-of-chatbots/278595/#close

[10] https://www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity

[11] https://www.searchenginejournal.com/future-of-chatbots/278595/#close

[12] ChatGPT: 30 incredible ways to use the AI-powered chatbot, Christopher McFadden,

https://interestingengineering.com/innovation/chatgpt-30-incredible-ways-to-use

[13] Accenture Exec: ChatGPT May Have Big Upside For Cybersecurity, BY KYLE ALSPACH , JANUARY 26, 2023, 04:54 PM EST, https://www.crn.com/news/security/accenture-exec-chatgpt-may-have-big-upside-for-cybersecurity

[14] Lund, B. D., & Wang, T. (2023). Chatting about ChatGPT: how may AI and GPT impact academia and libraries?. *Library Hi Tech News.*

[15] Monzelo, Pedro and Nunes, Sérgio, "The Role of the Chief Information Security Officer (CISO) in Organizations" (2019). *CAPSI 2019 Proceedings*. 36. https://aisel.aisnet.org/capsi2019/36

[16] https://www.bleepingcomputer.com/news/technology/openais-new-chatgpt-bot-10-coolest-things-you-can-do-with-it/

[17] ChatGPT Experts group https://www.facebook.com/groups/aicomunity