第二届应用人工智能与计算国际会议论文集(ICAAIC 2023)CFP23BC3-ART;国际标准图书编号: 978-1-6654-5630-2

2023 第二届应用人工智能与计算国际会议(ICAAIC) | 978-1-6654-5630-2/23/$31.00 ©2023 IEEE | DOI: 10.1109 / ICAAIC56838.20

基于人工智能的聊天生成预训练变压器(ChatGPT)在网络安全中的作用

古鲁·普拉萨德
印度斯坦理工学院管理学院;
科学金奈-603103，印度
guru@cybertracs.in

V. Ceronmani Sharmila 印度
斯坦理工学院信息技术系
科学金奈-603103，印度
csharmila@hindustanuniv.ac.in

抗议; Badrinarayanan
印度斯坦理工学院管理学院;
科学金奈-603103，印度
mkbadri@hindustanuniv.ac.in

***摘要*:人工智能(AI)在网络安全中的作用日益重要。对于首席信息安全官(CISO)来说，为了履行他们的角色，协助他们的团队执行与网络安全相关的各种任务，并帮助他们管理一个具有网络弹性的组织，他们需要广泛的网络安全解决方案知识，与业界当前事件和事件相关的知识，以及网络安全领域的最新发展。因此，ciso 必须花费大量的时间来学习，这样他们才能发挥自己的作用，成为组织有效的威胁预防和管理人员。在本研究中，分析了基于人工智能的聊天生成预训练转换器(ChatGPT)是否可以帮助首席信息安全官发挥作用，以及他们是否可以将其用作实现其作用的有效工具。**

关键词:网络安全中的人工智能，首席信息安全官，聊天生成预训练变压器，网络安全中的 ChatGPT

I. 介绍

人工智能使计算机在更短的时间内完成通常由人类完成的智能任务。[1]

人工智能是一门集人机交互、机器学习、数据存储和决策能力于一体的多学科技术。[2]

在网络安全领域，人工智能(AI)被证明是网络威胁检测中最有用和最强大的工具。人工智能的各种发展和进步，引领了安全工具和系统的发展，帮助管理人员进行网络安全管理。[3]

人工智能(AI)和网络安全具有广泛的跨学科互动。人工智能(AI)工具，如计算智能、神经网络、机器学习、数据挖掘、模糊逻辑，在威胁检测和预防中发挥着重要作用。[4]

大型语言模型(LLM)是人工智能领域的一个重要发展。它们是人工智能工具，可以阅读、总结和翻译文本，并预测句子中未来的单词。它们生成句子

新一代的搜索引擎是由大型语言模型(llm)引领的。他们能够为复杂的用户问题提供详细和信息丰富的答案。[7]

这项技术经过训练，可以在人类向该工具提问时了解他们的意思。这是一项革命性的技术。[8]

人工智能可以通过自然语言处理实现卓越的预测智能，通过抓取文章、新闻和网络威胁研究来管理自己的数据。[10]

随着聊天机器人能够更好地与客户沟通，有了更多有益的互动。最近的一项研究表明，80%的客户对聊天机器人有积极的体验。[11]

密歇根大学公共政策教授兼科学、技术和公共政策项目主任 Shobita Parthasarathy 说，这与人类说话和写作的方式类似。[5]

OpenAI 是一家人工智能(AI)研究和部署公司。他们的公司的使命是促进人工智能造福全人类。[6]

对话式人工智能可能会彻底改变研究实践和出版，创造机会和关注。[7]

ChatGPT 是一个使用大型语言模型(LLM)的机器学习系统。它可以自主地从数据中学习，并在大量文本数据集上进行训练后产生复杂且看似智能的句子。许多这样的模型都是由位于加州旧金山的 OpenAI 公司发布的。它是第一个能够与用户就广泛的话题进行令人信服的对话的模型之一 ChatGPT 引起了大量的兴奋和争议。[8]

II. 关于 CHATGPT

聊天生成预训练变压器(ChatGPT)是 OpenAI 于 2022 年 **11** 月推出的基于人工智能的聊天机器人。[9]

ChatGPT 是通过监督和强化学习技术进行微调的。它建立在 OpenAI 的 GPT-3 系列大型语言模型之上。[9]

ChatGPT 使用带有人类反馈的强化学习(RLHF)。这是一个额外的训练层次，使用人类的反馈。它帮助 ChatGPT 学习和遵循指示的能力，并产生让人类满意的反应。[8]

最新的 GPT-3.5 是在大量来自互联网的代码和信息数据上进行训练的。它使用来自 Reddit 讨论等来源的数据进行训练，以帮助 ChatGPT 学习人类使用的对话，并帮助它获得人类的回应风格。 ChatGPT 还使用人类反馈进行训练，称为“人类反馈强化学习”。这有助于人工智能了解人类在提问时的期望。[8]

ChatGPT 是 OpenAI 开发的一个大型语言模型。它的设计目的是帮助用户根据接收到的输入生成类似人类的文本 ChatGPT 的主要作用是协助用户完成以下任务:

1. ChatGPT 可用于生成类似于人类编写的文本的文本。这可以包括写故事、写电子邮件或信息或总结信息。
2. ChatGPT 可以用来回答向它提出的问题。它可以详细地提供相关的、准确的信息。
3. ChatGPT 可用于将文本从一种语言翻译成另一种语言。
4. ChatGPT 可以用来创建一个序列和完成一个段落或句子。

5. ChatGPT 可用于将大量文本的摘要创建为包含最重要信息的简短注释。

在 OpenAI 的 ChatGPT 的第一个屏幕中，列出了它的功能，它的限制和它可以做的一些示例。

下面的截图给出了一些例子，说明了它的能力和局限性。

图 1 所示。ChatGPT 功能&;限制

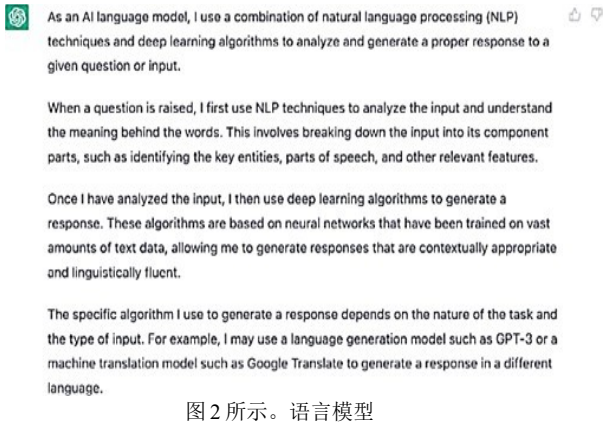
ChatGPT 是一个基于人工智能的工具，它结合了自然语言处理(NLP)技术和深度学习

首席信息安全官(ciso)知道所有该做的事情，但他们依赖外部人员或外包机构来执行他们应该做的任务。在这种情况下，基于人工智能的工具可以帮助他们工作。各种研究都指出，网络安全框架的建立、使用防火墙保护其边界、安全测试、安全事件管理、网络安全意识的建立等工作是任何组织的首席信息安全官(CISO)的重要任务。在本文中，我们试图研究基于 AI 的 ChatGPT 能够帮助 ciso 完成上述任何任务。

为了有效地管理组织的信息安全，首席信息安全官应该具备相关的信息安全意识。[15]

学习。当提出任何问题时，它首先使用 NLP 来分析其输入和含义。其次，它使用深度学习算法来提供回复。这些算法已经在基于神经网络的大量数据上进行了训练。根据任务的性质，它可能会使用 GPT-3 或谷歌翻译等语言模型。

下面是 ChatGPT 的截图。


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.

图 2 所示。语言模型

III. 聊天在网络安全中的作用

随着科技的发展，许多设备都与互联网连接在一起。随着许多设备连接到互联网，与设备、内容和用户的安全性相关的担忧也在增加。许多研究人员正试图找到解决连接设备、数据和用户所面临的问题的解决方案，以保护他们的设备和他们自己免受网络罪犯的侵害。有一些工具、产品和软件可以帮助提供这样的网络安全。有许多工具是使用人工智能开发的。因此，人工智能在网络安全中发挥着更大的作用。ChatGPT 是基于人工智能的。

ChatGPT 可以帮助查找安全漏洞并帮助生成概念验证。它还可以用于确定代码是否存在安全缺陷。ChatGPT 可以对裁决背后的原因给出一个清晰简单的解释。它可以帮助更进一步，并请求一个可以利用该缺陷的漏洞的工作概念验证(PoC)演示。[12]

ChatGPT 已经展示了从安全操作平台获取数据后创建类似分析师报告的摘要的能力。这类似于人类分析师在评估数据时所做的事情，”埃森哲网络弹性全球主管罗伯特·博伊斯(Robert Boyce)告诉 CRN。[13]

在自然语言处理和人工智能领域，ChatGPT 生成类似于人类语言的语言并完成复杂任务的能力使其成为一项非常重要的创新。[14]

许多成长中的组织和从所有者驱动的组织向专业组织转变的组织努力定义和创建一个角色来管理他们组织的信息安全。在一些组织中，这个角色是存在的，管理层不知道分配给他们的所有责任。在某些情况下，首席信息安全

为了研究 ChatGPT 如何帮助网络安全，作者使用谷歌凭证创建了一个帐户。研究的一些功能包括:

1. chatgpt 能否帮助组织管理层界定首席信息安全官的角色?
2. ChatGPT 可以帮助首席信息安全官为他们的组织创建网络安全框架吗?
3. ChatGPT 可以帮助创建网络安全意识内容吗?
4. ChatGPT 可以帮助评估防火墙吗
   购买前的解决方案?
5. 以勒索软件攻击为例，ChatGPT 能否协助分析网络安全事件?

6. ChatGPT 可以帮助进行安全测试、发现安全漏洞并产生概念验证吗?
7. ChatGPT 能帮助安全操作吗?
8. ChatGPT 可以帮助评估防病毒解决方案吗?
9. 它能给黑客提供输入吗?
10. 它能给道德黑客提供输入吗?

在本文中，我们试图研究 ChatGPT 是否可以在上述十点查询中帮助组织及其 ciso。

A. 使用 ChatGPT 定义 CISO 的角色

首席信息安全官的角色在任何组织中都是一个重要的职能。我们试图检查 ChatGPT 是否可以帮助组织定义 CISO 的角色。我们在工具中使用了关键词“ciso 的角色”。我们发现，它能够给一个组织的管理提供全面的指导。以下是 ChatGPT 赋予的职责。

- 发展及实施资讯保安策略
- 管理风险
- 确保遵从性
- 预算
- 合规
- 创建并领导由安全专家组成的技术团队
- 资源分配
- 事件响应和管理。

如果首席信息安全官有任何疑问，或者他不能理解的东西，他/她可以在 ChatGPT 上发布相同的疑问，并得到所需的答案。

图 4 所示。网络安全架构

C. 网络安全意识内容

网络安全意识是所有组织都必须具备的。我们试图检查 ChatGPT 是否可以帮助首席信息安全官为他们的组织创建

此外，ChatGPT 清楚地指出，责任可能会有所不同，因为它依赖于组织的规模和结构，这是现实。对于一个正在从业主驱动型向专业驱动型转变的组织，或者一个小型到中型的组织，它提供了一个很好的指导。ChatGPT 给出的详细信息对组织来说是一个良好的开端。在信息技术使用和网络安全方面已经达到成熟水平的组织可能必须在 ChatGPT 给出的细节基础上进行构建，并创建适合其组织及其增长路径的 ChatGPT。ChatGPT 给出的每一个点都可以使用 ChatGPT 本身来阐述，它可以更好地帮助组织。

下图是 ChatGPT 的截图，给出了细节。

图 3 所示。 ciso 的角色

B. 为组织创建网络安全框架

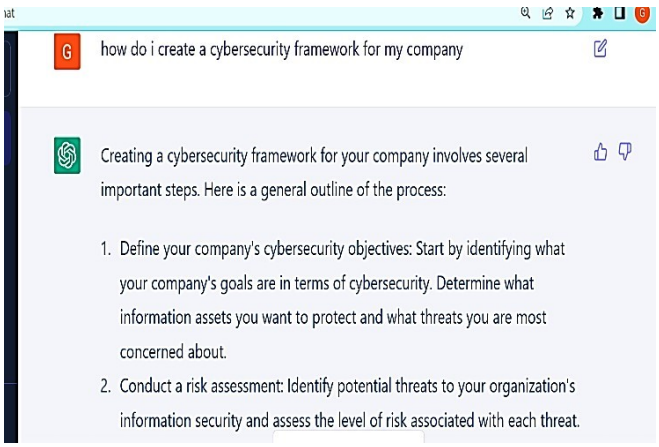
创建网络安全框架对任何组织来说都是一项重要的任务。我们试图检查 ChatGPT 是否可以帮助首席信息安全官为他们的组织创建网络安全框架。我们在工具中使用了“我如何为我的公司创建一个网络安全框架”的问题。我们发现它能够给首席信息安全官提供全面的指导。它给出了下面的步骤。

- 确定公司资产的优先级
- 进行风险评估
- 制定政策;程序
- 实施技术和解决方案
- 员工培训
- 监控网络

由于首席信息安全官本身就是一名技术人员，他将能够理解 ChatGPT 中使用的技术词汇，并使用 ChatGPT 提供的输入为他或她的组织创建网络安全框架。从输出中我们可以说，它全面涵盖了在为组织创建网络安全框架时要考虑的所有方面和要求。

网络安全意识内容。我们在工具中使用了关键词“网络安全意识内容”。我们发现，它能够给首席信息安全官提供好的内容。它能够为 ciso 提供指导和方向。它能够提供内容，围绕这些内容，意识将被创建给他们组织的用户。下面是 ChatGPT 给出的内容列表。

- 密码安全管理
- 无线网络安全
- 恶意软件和病毒防护详细信息



- 社交媒体安全
- 网络欺凌
- 数据泄露
- 网络钓鱼
- 安全浏览
- 安全的电子商务。

根据该指南，首席信息安全官可以为自己的组织准备创建网络安全意识内容。

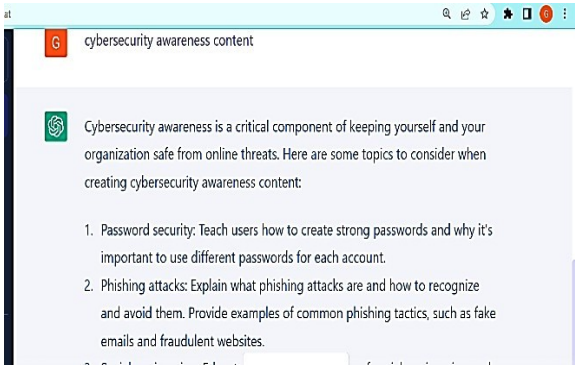


图 5 所示。网络安全意识内容

- 控制受感染的系统
- 确定事件的性质
- 分析从事件中收集到的数据
- 根据分析，做出回应
- 准备一份事件报告。

图 7 所示。 事件分析

D. 购买防火墙的评估

防火墙是为任何网络创建网络防御的重要设备。大多数首席信息安全官依赖于 oem 提供的各种报告和互联网上的报告来帮助他们进行购买过程。我们试图研究 ChatGPT 是否可以帮助他们节省时间和精力，并提供有用的见解。我们在工具中使用了“如何评估购买的防火墙解决方案”这个问题。我们发现，它能够为首席信息安全官提供很好的输入。它给出了以下用于评估的输入。

- 防火墙性能
- 防火墙的特点
- 易用性
- 可伸缩性
- 支持
- 价格
- 与网络中其他网络设备的兼容性
- 已测试的安全功能

由于 CISO 本身就是技术人员，他将能够理解 ChatGPT 中使用的技术词汇，并使用 ChatGPT 提供的输入来决定解决方案。然而，我们发现它并没有给出检查安全有效性的线索，也没有给出待评估方案的安全有效性。我们还发现它并没有给首席信息安全官提供任何线索，让他们去检查来自独立实验室/独立研究人员的各种测试报告，这些研究人员对防火墙进行评估，并定期发布报告。一些独立报告的例子是 Gartner 报告，Forrester Wave 报告，IDC 报告。

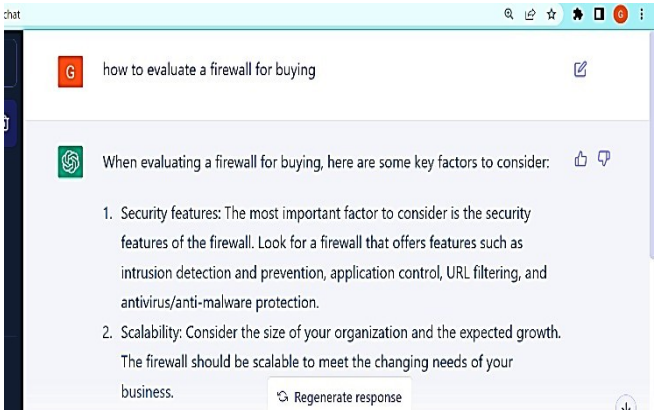


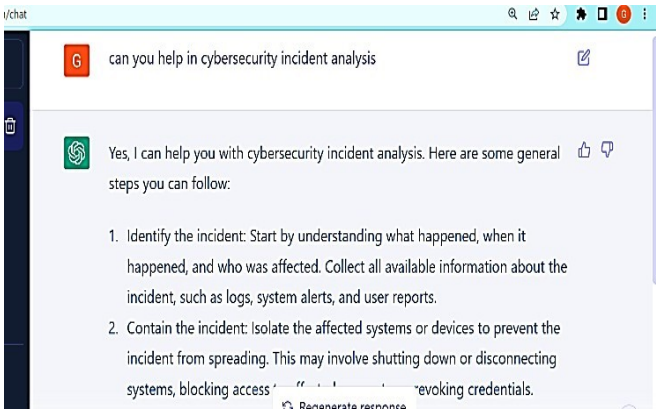
图 6 所示。防火墙的评估

E. 网络安全事件分析

在全球范围内，网络安全事件有所增加，并被视为造成组织损失的关键因素。我们试图检查 ChatGPT 是否可以帮助首席信息安全官为他们的组织进行网络安全事件分析。我们在这个工具中使用了“你能帮助分析网络安全事件吗”的问题。我们发现，它给出了下面的输入。它给出了事件分析的一般步骤如下。

F. 安全测试，安全漏洞并产生概念证明

安全测试、发现安全漏洞和生成概念证明有助于 ciso 保护应用程序。我们试图研究 ChatGPT 是否可以帮助进行安全测试，发现安全漏洞并产生概念证明，ChatGPT 表示，它不是执行安全测试，发现安全漏洞或产生概念证明的电缆，因为它涉及应用程序或系统所有者的事先授权，而且它涉及法律角度。然而，它给寻求输入的人提供了一个线索，建议如



果要识别软件或网络中的安全漏洞，最好考虑漏洞扫描器或渗透测试工具。这些工具有助于识别安全漏洞。
为了识别安全漏洞，它给出了以下步骤:

- 分析系统架构
- 执行渗透测试
- 查看源代码
- 查看系统配置文件
- 执行社会工程任务

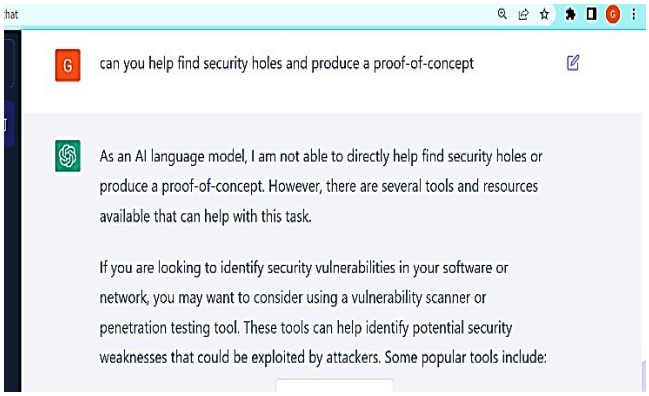


图 8 所示。安全漏洞和 POC

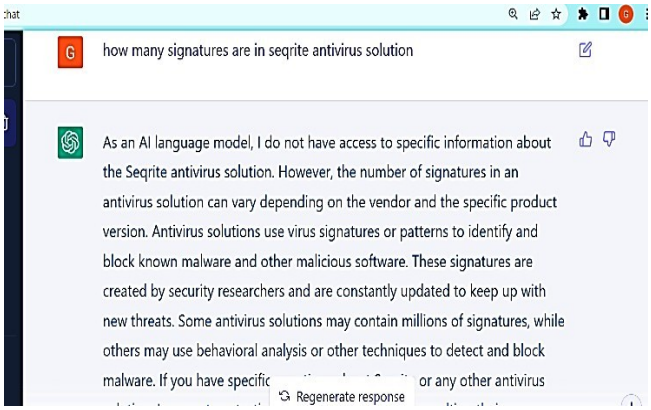


图 9 所示。杀毒软件的评估

I. 黑客输入

G. 安全操作

组织中的网络安全操作涉及许多功能。补丁管理和漏洞管理是网络安全运营的关键功能之一。ChatGPT 可以自动化漏洞管理和补丁管理操作。[16]

ChatGPT 可以使用机器学习功能扫描网络中的漏洞。它可以从网络及其流量中收集数据，并从 ChatGPT 可用的各种来源分析已知漏洞的数据。经过分析，可以帮助检测漏洞。这可以与漏洞数据库相关联，漏洞的修复可以由 ChatGPT 提供。[17]

基于人工智能的 ChatGPT 通过与现有的安全系统和 IT 基础设施集成来自动化修补过程。基于人工智能的 ChatGPT 可以识别需要打补丁的系统，并与补丁管理系统通信，安排补丁的部署。基于人工智能的 ChatGPT 可以使用机器学习算法来确定关键补丁的优先级，并在低流量期间安排不那么关键的补丁的部署。在部署补丁之前，基于 ai 的 ChatGPT 可以在沙箱环境中进行测试，以确保它们不会导致任何问题或与其他软件或系统发生冲突。在部署补丁后，基于人工智能的 ChatGPT 可以生成合规报告，以证明补丁已被应用，并且系统是最新的。

H. 杀毒软件评估

反病毒是一个重要的安全解决方案，用于任何组织保护其资产免受任何病毒感染和事件。为组织选择正确的反病毒解决方案是一项具有挑战性的任务。同样，考虑到行业中病毒事件的数量和市场上可用的大量反病毒解决方案，为组织选择最佳反病毒解决方案同样具有挑战性。
我们尝试从 ChatGPT 获得同样的帮助。评估反病毒解决方案的关键标准是该解决方案具有的签名数量。签名数量越多，解决方案对病毒的保护就越好。

ChatGPT 中使用的关键词是“一个反病毒解决方案中有多少个反病毒签名”。

ChatGPT 表示，它没有关于反病毒签名的最新信息。反病毒解决方案使用签名和启发式分析进行病毒检测。最后 ChatGPT 建议访问反病毒解决方案网站和/或联系他们的支持团队。

下面是 ChatGPT 的输出。

黑客是具有计算机技术技能的个人，但通常指的是利用他们的技能突破网络安全防御的个人。由于 ChatGPT 基于 AI 引擎，其输出基于经过训练的数据，因此我们试图检查它是否可以为黑客提供输入，帮助他们提高技能，提高黑客能力。用于检查的关键词是“生成网络攻击”。

对此，ChatGPT 表示，作为一个人工智能模型，它不能生成网络攻击，也不能提供执行攻击的指令。它表示，其节目旨在促进道德和法律行为。它进一步表示，制造网络攻击对他人有害，是非法和不道德的。它给出了一个建议，要负责任地、合乎道德地使用技术，避免对任何组织或个人造成任何伤害。信中还说:“我鼓励你们专注于将技术用于积极和建设性的目的。

下面是截图。

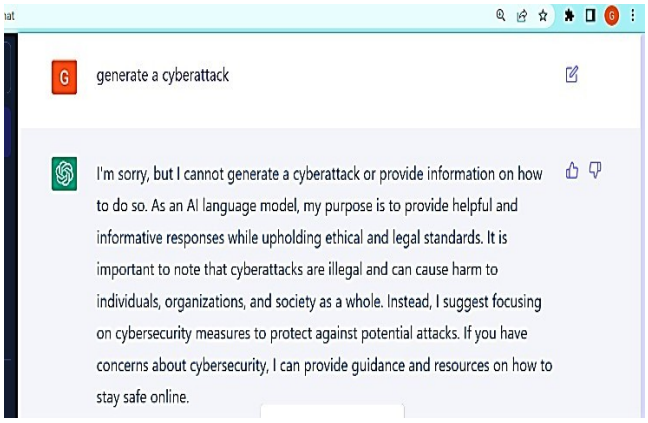


图 10 所示。网络攻击

我们使用了另一个关键词“如何破解 wi-fi 密码”

对此，它表示，ChatGPT 为同样的事情提供指导是不合适的，也是不道德的。它足够智能，可以提供一个警告，说破坏密码是非法的，可能会导致惩罚

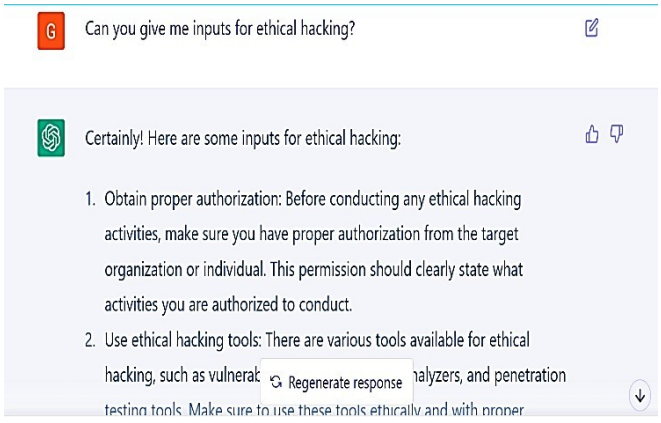


图 12 所示。道德黑客

IV. 结论

从我们进行的研究中我们可以得出结论，ChatGPT 在网络安全中具有重要作用。它可以帮助定义组织中首席信息安全官的角色，它可以帮助为组织创建网络安全框架，它

刑事指控、罚款和监禁。由此可见，ChatGPT 具有智能，能够对向它提出的问题给出适当的答案。

图 11 所示。破解 wifi 密码

J. 道德黑客的投入

有时组织想要测试他们的安全漏洞或他们的安全状态。在这种情况下，他们试图渗透或侵入自己的系统。对计算机系统、应用程序或数据进行授权、强制的访问。这样的企图是合法和授权的，被称为道德黑客。

我们试图检查 ChatGPT 是否可以指导道德黑客。我们使用的关键词是“你能为道德黑客提供建议吗?”

我们发现 ChatGPT 能够为进行道德黑客的过程提供必要的指导。以下是它在输出中涵盖的要点。

- 获得适当的授权
- 使用正确的工具和技术
- 维护机密性
- 记录调查结果
- 保持在法律和道德的范围内
- 检查知识库以获得有关安全性的最新更新

以上几点为计划测试其组织的安全状况的人提供了很好的指导。值得注意的是，它提供的输入考虑到一个组织的技术、法律和合规方面。
可以帮助创建网络安全意识内容。它指导 ciso 进行防火墙购买决策和事件管理。它的重要性取决于组织的规模和他们部署的技术。

在定义首席信息安全官的角色和职责时，它通过提供所需的细节，如“开发和实施网络安全框架”作为职责之一，帮助管理团队为首席信息安全官职能创建角色和职责。

它帮助首席信息安全官创建网络安全框架，创建网络安全意识的内容，帮助购买安全解决方案的评估过程。

在网络安全事件分析中，它提供了一个总体指导，在这个阶段，这个工具可能还没有经过培训，可以做更多的事情。

在安全测试中，查找安全漏洞并生成概念证明 ChatGPT 在这一点上的作用非常有限。这可能归因于缺乏培训数据和其他变量，如更新的知识、人工干预、与授权测试和发现安全漏洞相关的法律方面。

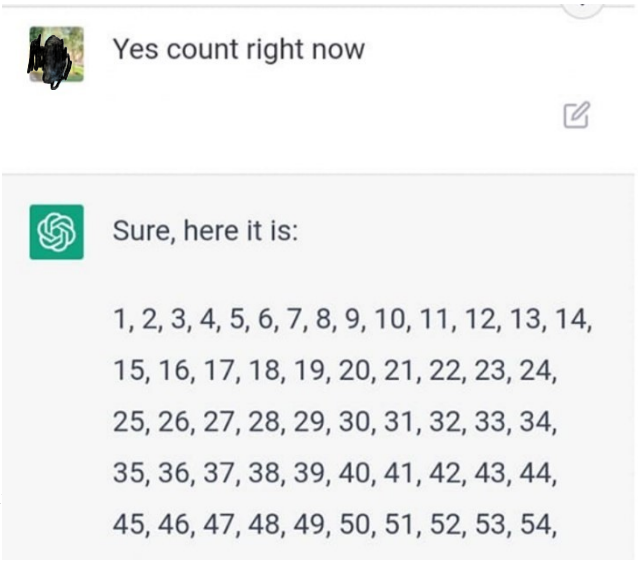
在网络安全操作中，ChatGPT 可以很容易地帮助执行各种任务。它可以帮助自动化操作，如补丁管理，漏洞管理。

它还可以帮助数据分析。最终减少对人力的依赖，并协助产生更准确的数据。

在反病毒解决方案的评估中，由于训练数据的可用性直到 2021 年，在这个阶段 ChatGPT 的作用非常有限。更重要的是，这种评估需要实时更新正在评估的解决方案的情报。

在向黑客提供信息方面，它一直以网络攻击的道德、伦理和法律问题为由，训练有素地不帮助他们。然而，它确实为道德黑客行为提供了指导。

基于人工智能的 ChatGPT 有可能改变人类与计算机的互动方式。先进的自然



ChatGPT 的语言处理能力提供了一种增强(或取代)人类生产力和创造力的方法。

随着这种基于人工智能的技术的发展，ChatGPT 可能在塑造数字世界方面发挥越来越重要的作用。许多操作过程本质上是重复的过程，涉及数据分析的过程将从 ChatGPT 中获得更大的好处。

看看我们在研究过程中提供的输入和指导的数量，我们确信这将使首席信息安全官(ciso)在其组织的网络安全运营、管理和实施方面的很多事情变得更容易。

它是一个工具，可以帮助回答问题，产生创造性的写作，或自动化一些重复性的任务。然而，到目前为止，ChatGPT 的局限性是，训练数据的可用性只能到 2021 年，ChatGPT 多次由于过度拥挤而没有开放。由于它是基于训练过的数据，任何错误的训练数据都可能导致错误和误导的答案。如果这些问题得到解决，这将是这个十年最伟大的工具之一。

下面是一个这样的超时事件的屏幕截图。

图 13 所示。超时错误

Facebook 上一个封闭的 ChatGPT 专家小组得出了一个有趣的观察结果。一位用户要求 ChatGPT 数 10 亿。要数 10 亿，需要很长时间。尽管如此，他们还是向 ChatGPT 发出了计数指令。这可能也是其他用户无法访问 ChatGPT 的原因。

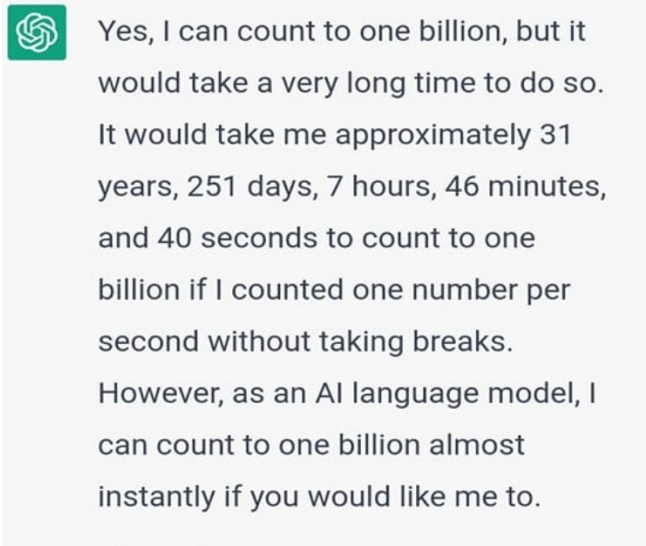


图 14 所示。数 10 亿

本研究仅限于本研究所采用的十个参数。本研究仅限于研究时 ChatGPT 中可用的内容。这项研究是在 ChatGPT 的免费版本中完成的。

进一步的研究可以揭示出基于人工智能的 ChatGPT 在网络安全中的广泛作用。这可以帮助人们管理网络安全。

参考文献

[1] 黄斌，欢一，徐亮，郑亮，邹志明，自动化交易系统统计与机器学习方法及硬件实现:调查研究，《企业信息》。系统。13(1) (2019) 132 - 144。

[2] 吕毅，人工智能的演进、模型、应用与未来趋势，中国科学院学报(自然科学版)。分析的 6(1)(2019) 1 - 29。

[3] Brown T (2019) IT 编年史，HowAI 正在改变网络安全格局。https://www.itchronicles.com/security/how-ai-is-changing-the-cybersecurity-landscape /

[4] S. Dilek, H. Çakır 和 M. Aydın，“人工智能的应用”打击网络罪行的情报技术: 审查。”国际人工智能杂志;《应用》，第 6 卷，第 6 期。1, 2015 年 1 月，第 21-39 页

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

一个监督政策新闻/2022/ parthasarthy -讨论-含义-大语言模型

[6] https://openai.com/

[7] ChatGPT:五个研究重点，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] 什么是 ChatGPT，如何使用它，Roger Montti, https://www.searchenginejournatl.com/what-is-chatgpt / 473664 / #关上

[9] 聊天机器人的未来: 用例 & 你需要知道的机会，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-聊天机器人/ 278595 / #关闭

[12] ChatGPT: 使用人工智能聊天机器人的 30 种不可思议的方式，克里斯托弗·麦克法登，

https://interestingengineering.com/innovation/chatgpt -30-不可思议-使用方法

[13] 埃森哲执行: 聊天技术可能对网络安全有很大的好处，作者 KYLE ALSPACH, 2023 年 1 月 26 日，美国东部时间下午 04:54,https://www.crn.com/news/security/accenture-exec-chatgpt-may- Have - Big - up- For - Cybersecurity

[14] 隆德，b.d.， &;王涛(2023)。聊 ChatGPT: AI 和 GPT 将如何影响学术界和图书馆? *图书馆高科技新闻*。

[15] Monzelo, Pedro 和 Nunes, Sérgio，“组织中首席信息安全官(CISO)的角色”;(2019)。*CAPSI 2019 会议录*。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 专家组 https://www.facebook.com/groups/aicomunity