Technology Scouting for the Telecom Sector

Alon Shahak, Global Cyber Lead Scout
Deutsche Telekom Israel
22. Juni 2023

CYBER
CLUB
LONDON

Yuval Ne'eman Workshop
for Science, Technology and Security
Tel Aviv University

Ono
הקריה האקדמית אונו
Ono Academic College

Agenda

1. Introduction – DT & DT Israel
2. Stakeholder Relations
3. Innovation Challenges
4. Innovation Process + Example (Success Story)
5. Innovation Trends

Introduction – DT & DT Israel

Deutsche Telekom Keyfacts

26.1 mn
fixed-network lines

216,528
employees worldwide*

€ **108.8** bn
revenue in 2021

21.6 mn
broadband customers

248.2 mn
mobile customers

present in
>50
countries in 2021

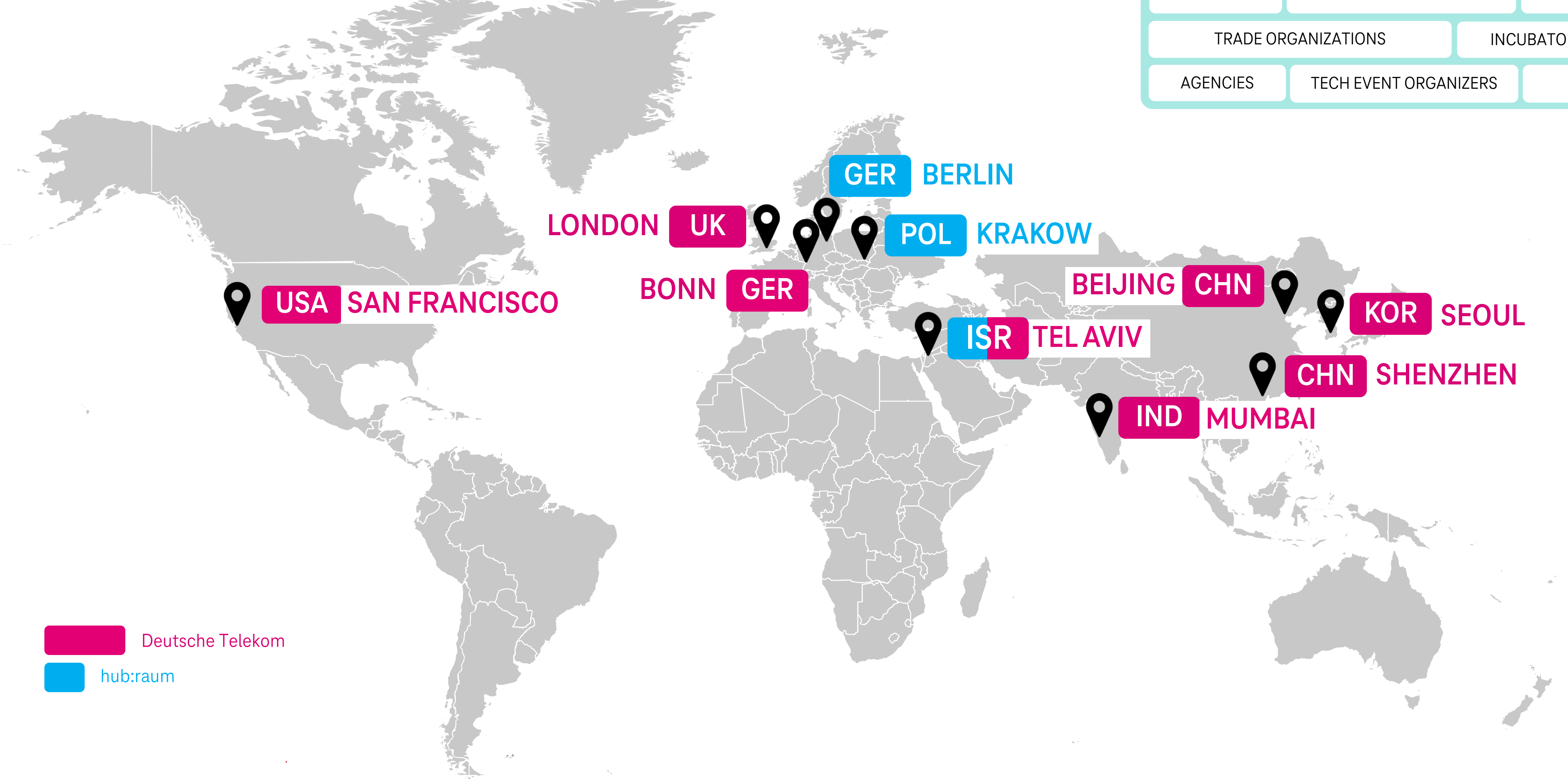
Figures based on annual report 2021.
* Reporting date December 31, 2021

Group
Partnering
& Devices

An amplified global scouting approach covering USA, Asia, Europe and Israel

+ AMPLIFICATION VIA ECO-SYSTEM MULTIPLIERS

- VC FIRMS
- INDUSTRY ASSOCIATIONS
- SERIAL ENTREPRENEURS
- TRADE ORGANIZATIONS
- INCUBATORS / ACCELERATORS
- AGENCIES
- TECH EVENT ORGANIZERS
- BUSINESS ANGELS



🟥 Deutsche Telekom
🟦 hub:raum

GPD‘s Value Pillars

SCOUTING AND SCREENING

INCUBATION HUBRAUM

PARTNER MANAGEMENT

DEVICE MANAGEMENT

Partner Innovation Life Cycle: From Scouting to Execution

SCOUTING

01 Intrinsic motivated

Extrinsic motivated

UNDERSTAND END CUSTOMER & SEGMENT DEMAND

02 Screening and Telco Benchmark

03 User Experience Prototype

INCUBATION: Hubraum

04 E2E Incubation

QUALIFICATION: PARTNER MANAGEMENT

05 Portfolio Evaluation

06 Partner Eng. model

07 Technical Prototype / POC

08 Contracting

EXECUTION

09 Validation & Implement.

10 GTM

11 LC & Aftersales

DT Engagement Vehicles with IL Eco-System

Group
Partnering
& Devices

DT Group Partnering

- Support BU's products & services with **external solutions and partners for BU customers**
- **Scouting for innovative topics in tecg; not part of current core buisness, but with potental to impact it**

hub:raum

Hubraum

- Incubaton and seed investments (€ 0,3 – 1,0 m)
- **Important element of DT's face to entrepreneurs and seed stage**
- Prototyping and early tech exploration > engagement

T-Capital

- **Support strategic goals** with targeted and explorative invests in **early/ mid-stage** companies via a € 100 mn fund
- **Provide early access to / collaboration on new tech and business models** relevant to core
- DT's vehicle for spinouts and JVS

DTCP

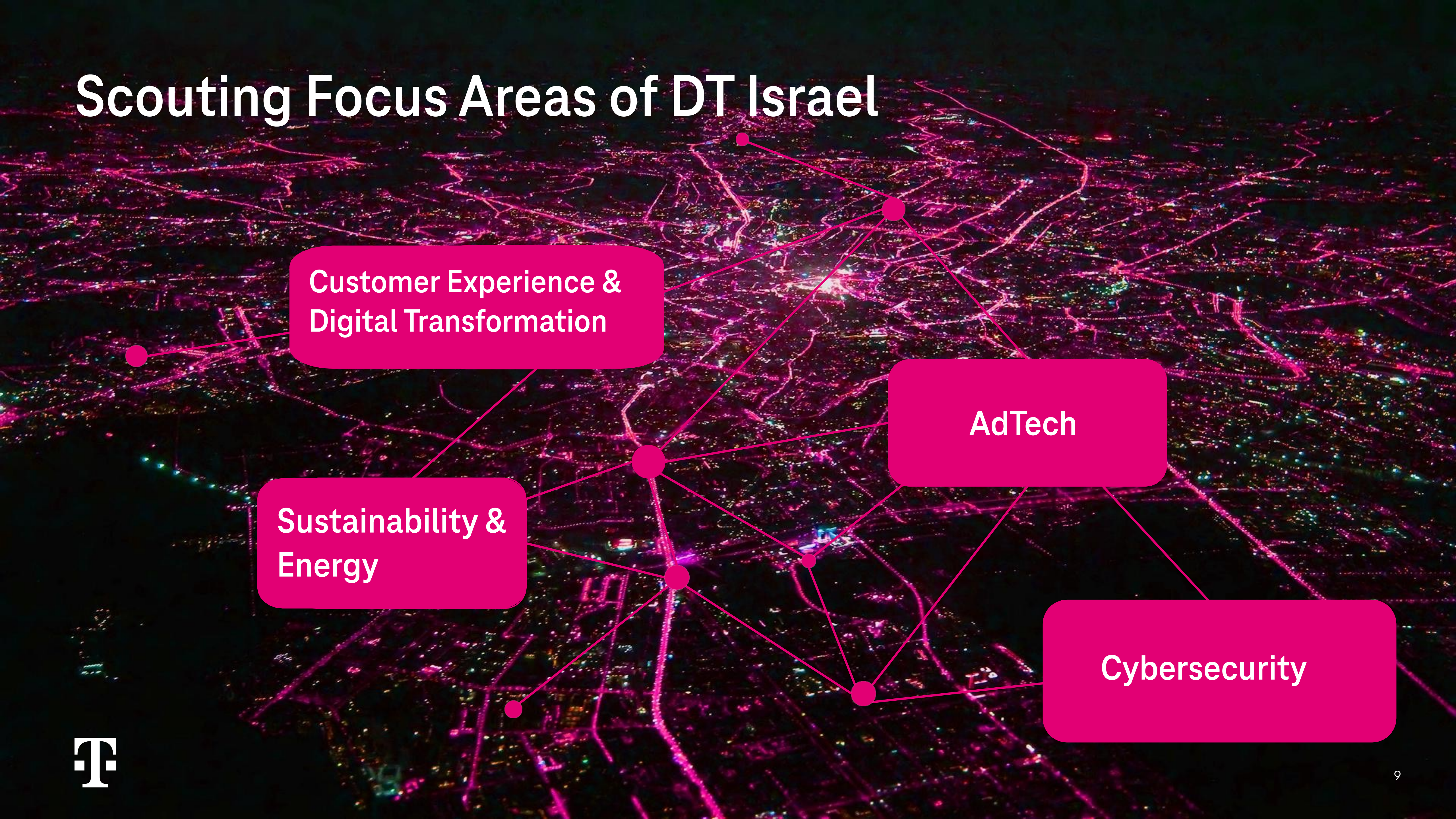
DTCP Venture Fund

- Scouting and investment in rev. generating, **late/ expansion** stage companies
- Gains for DT knowledge of market and market shifts relevant to DT business

Identify / assess / adapt – new products & business models to counter disruption & margin pressure

Market Knowledge & Financial ROI

Scouting Focus Areas of DT Israel



Customer Experience & Digital Transformation

AdTech

Sustainability & Energy

Cybersecurity

Stakeholder Relations

Stakeholder Relations

Research – Identification

Contacts – CRM is not enough

Redundancy is crucial

Source of Knowledge / Trust

In person is better than Virtual

Add value before else – Business & Personal

Mix Business & Pleasure (Social / Life Events)

Value Proposition for Stakeholders

Offers:

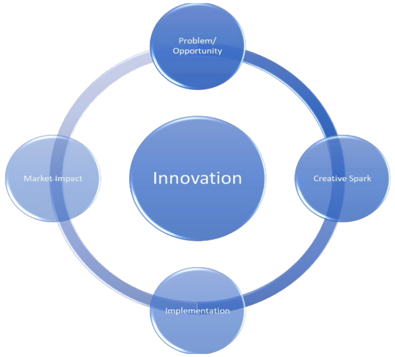
1. Quick & professional global innovation scouting of Vendors according to specific requests
2. New Use Case suggestions according to the new global & local trends
3. B2B / B2C new reselling revenue streams – with measurable ROIs
4. Enhancement of existing portfolio
5. White Papers, Market Movement reports & Projects

Requests:

1. Monthly / Bi-Monthly / Quaterly virtual or in-person meeting with a SPOC
2. Commitment to answers (even if negative)

Innovation Challenges

Innovation Challenges



Innovation Cycles

Role Changes

Re-Organization / Internal Indirect Affecting Processes

10 Yes + 1 No = No

Innovation VS Tradition

I HAVE NO SELF CONFIDENCE
WHICH IS RIDICULOUS GIVEN HOW AWESOME I AM

“We’re the best”

Innovation Process + Example

(Success Story)

Success Stories

Cynet
HOLISTIC SECURITY SIMPLIFIED

Company Profile

Cynet is an autonomous breach protection platform that provides a single, enterprise-grade solution for the internal network.

Relevance for DT

DT has B2B business unit serving SMB & Enterprises in Germany

Current State of Partnership

T-Capital (strategic fund) investment

T-SEC Cooperation to bring XDR to our customers

Partnering Journey

01/2019 – **Initial Meeting**
Introduction meetings between DT & Cynet

05/2020 – **PoC**
Integration and service model (MSSP) test

01/2022 – **Commercial Engagement**
Offered on Magenta label branding – “Cyberdefense Smart”

Questions?

Introduction Trends

Agenda

1. Innovation Disruption
2. Space Security
3. AI & Cyber
4. Quantum Security
5. Metaverse Security

Innovation Disruption

Deep Dive:

How to Identify Cyber Trends in 3 Easy Steps

All Rights Reserved to Alon Shahak

Deep Dive:

How to Identify Cyber Trends in 3 Easy Steps

Analyze the trends in the other industries

Think like an attacker

Protect from the threats in step 2

All Rights Reserved to Alon Shahak

Examples: Cloud Security

Multi-cloud is an increasingly popular strategy

Moving from only AWS / Azure / GCP / others to combinations of them

As an attacker - possible threats are

- Misconfigurations in policies / bad rules
- Unskilled Security Teams
- Fraud & Data Theft
- …

Approaches for protection from the above

- Access Management
- Identity Security
- Training & Awareness
- Data Protection
- …

The AI and ML-powered cloud

AI/ML requires huge amounts of computing power and storage space, more cost-effective to use cloud infrastructure instead of building your own

As an attacker - possible threats are

- Malicious Use of AI/ML
- Corrupted Data
- AI Code Reuse (log4j)
- …

Approaches for protection from the above

- Ai V. AI
- Data Quality Assurance
- Data Protection
- Red Team / Pen Testing
- …

All Rights Reserved to Alon Shahak

Example: Sub-domain in Metaverse Security

Metaverse is a growing trend

- In it there are many sub-domains
- One of the sub-domains is **Environments & objects scanning**

As an attacker - possible threats are

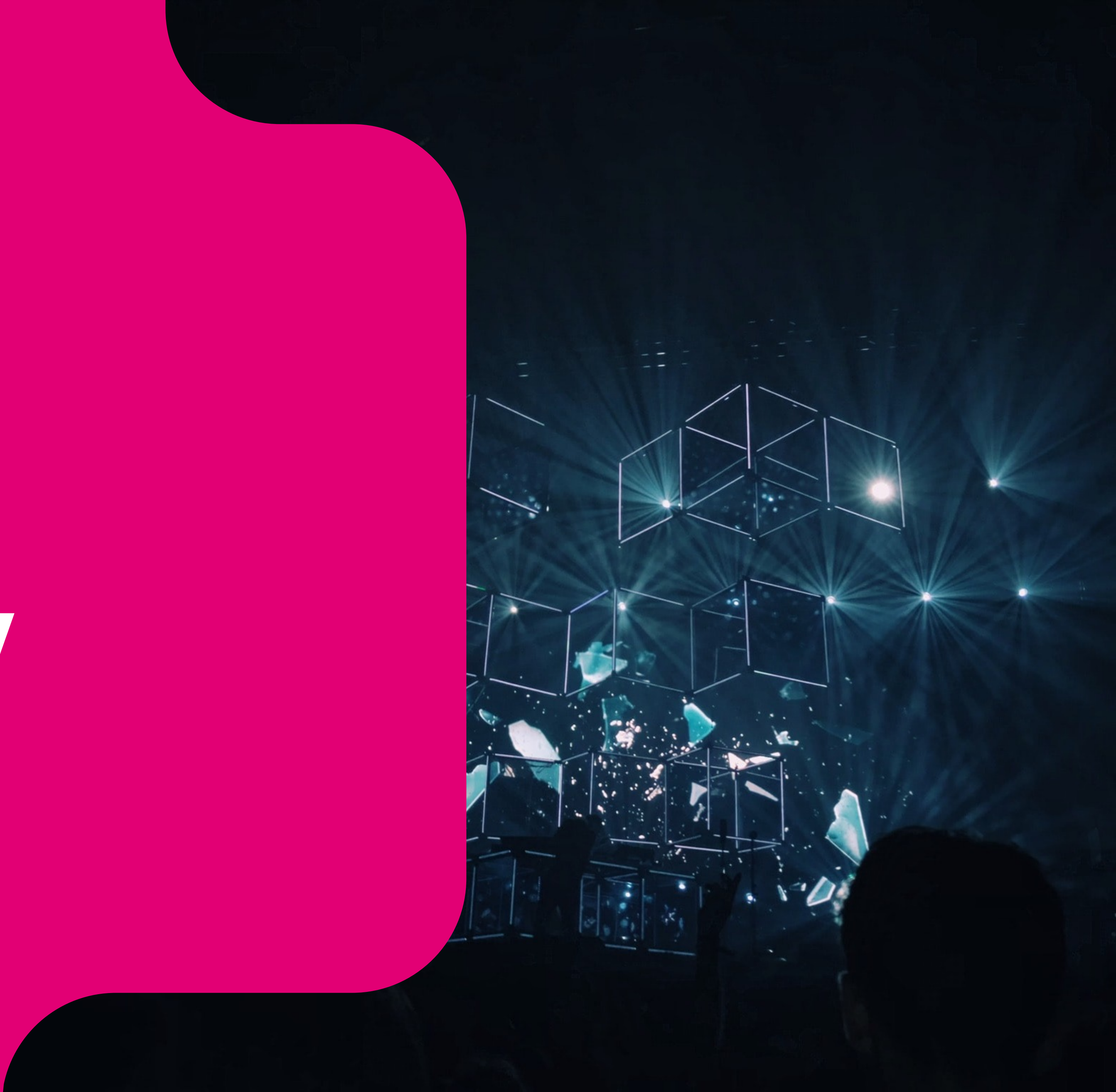
- Harmful Content and Environments
- IP Issues
- Meta-Robbery
- Prime-Robbery

Approaches for protection from the above

- Access Permissions
- IP Regulation & IP Theft Solutions
- Artificial Data
- Privacy Protection
- ...

All Rights Reserved to Alon Shahak

Space Security



Houston, do we have a problem?

Telecommunications & Security in Space

Alon Shahak, Global Cyber Lead Scout

T Mobile | SPACEX

COVERAGE
ABOVE & BEYOND

Cyber Challenges in Space

Current Threats[2]
(Earth & Space)

Data Interception

Ownership of
Information /
Infrastructure

Identity Theft & Fraud

Insider Threats

Recommended Solution approaches

Privacy & Identity Security

Zero Trust

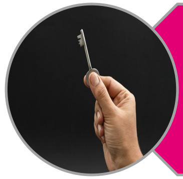
Multi-Cloud Security

Cyber Awareness

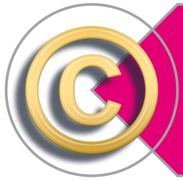
Threat Intelligence

Automation

Regulation?

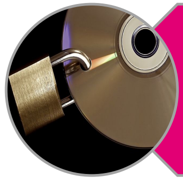


Ownership



IP Issues

Privacy Standards

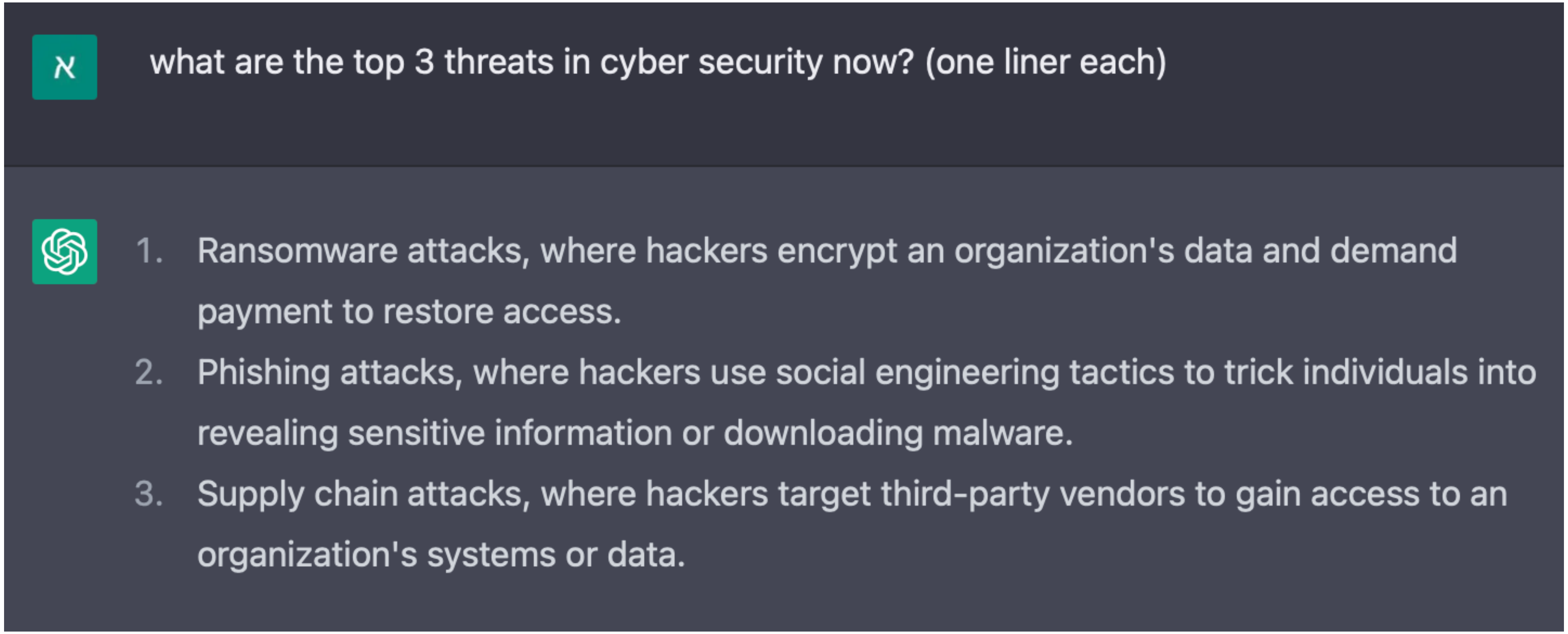


Secure Hardware / Software

“United Space Nations”

AI & Cyber

Top 3 Cyber Threats - According to ChatGPT

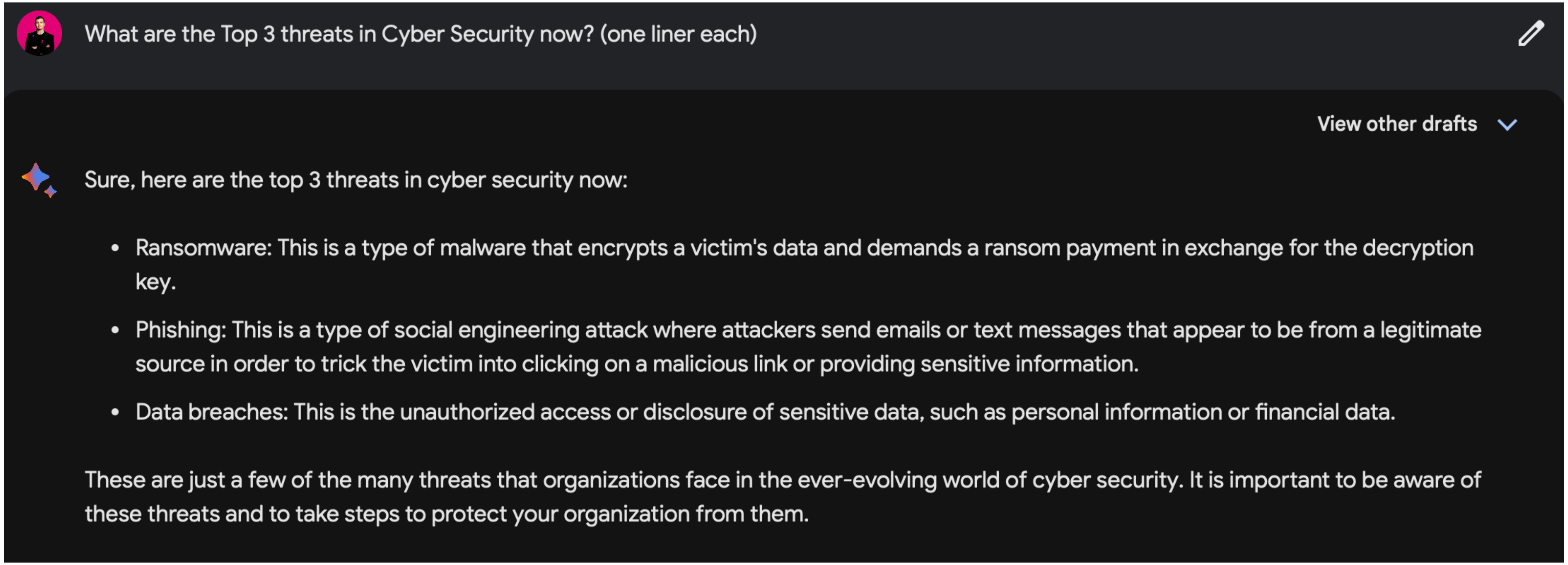


א

what are the top 3 threats in cyber security now? (one liner each)

1. Ransomware attacks, where hackers encrypt an organization's data and demand payment to restore access.
2. Phishing attacks, where hackers use social engineering tactics to trick individuals into revealing sensitive information or downloading malware.
3. Supply chain attacks, where hackers target third-party vendors to gain access to an organization's systems or data.

Top 3 Cyber Threats - According to Bard



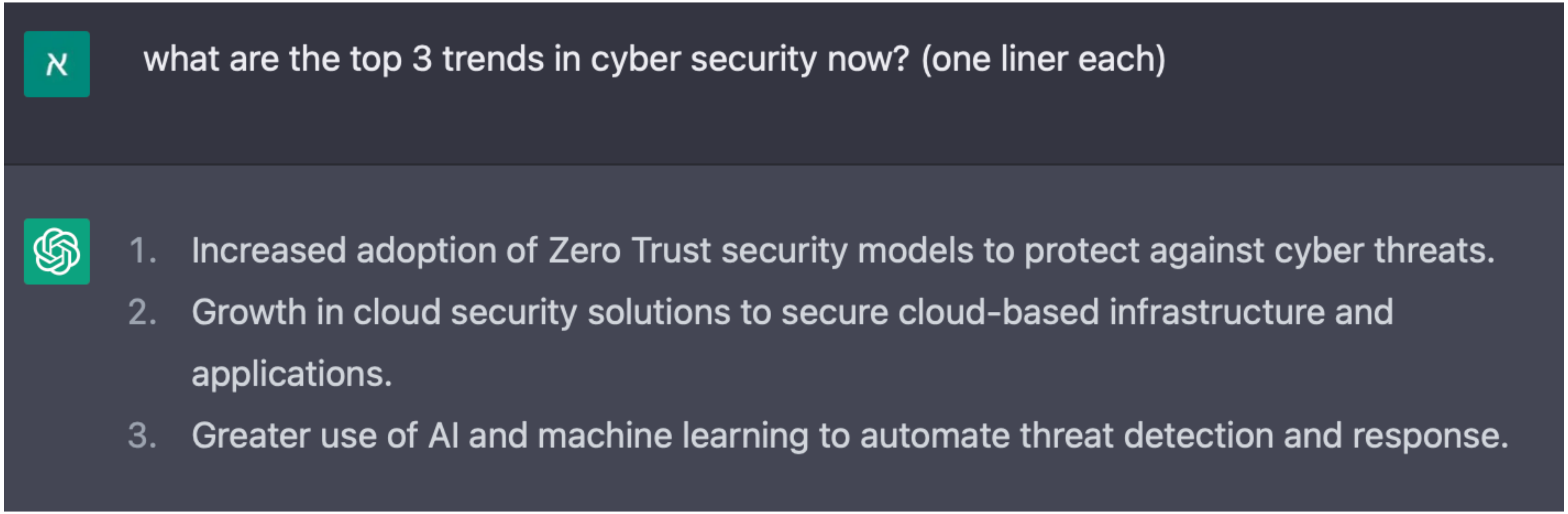
What are the Top 3 threats in Cyber Security now? (one liner each)

Sure, here are the top 3 threats in cyber security now:

- Ransomware: This is a type of malware that encrypts a victim's data and demands a ransom payment in exchange for the decryption key.
- Phishing: This is a type of social engineering attack where attackers send emails or text messages that appear to be from a legitimate source in order to trick the victim into clicking on a malicious link or providing sensitive information.
- Data breaches: This is the unauthorized access or disclosure of sensitive data, such as personal information or financial data.

These are just a few of the many threats that organizations face in the ever-evolving world of cyber security. It is important to be aware of these threats and to take steps to protect your organization from them.

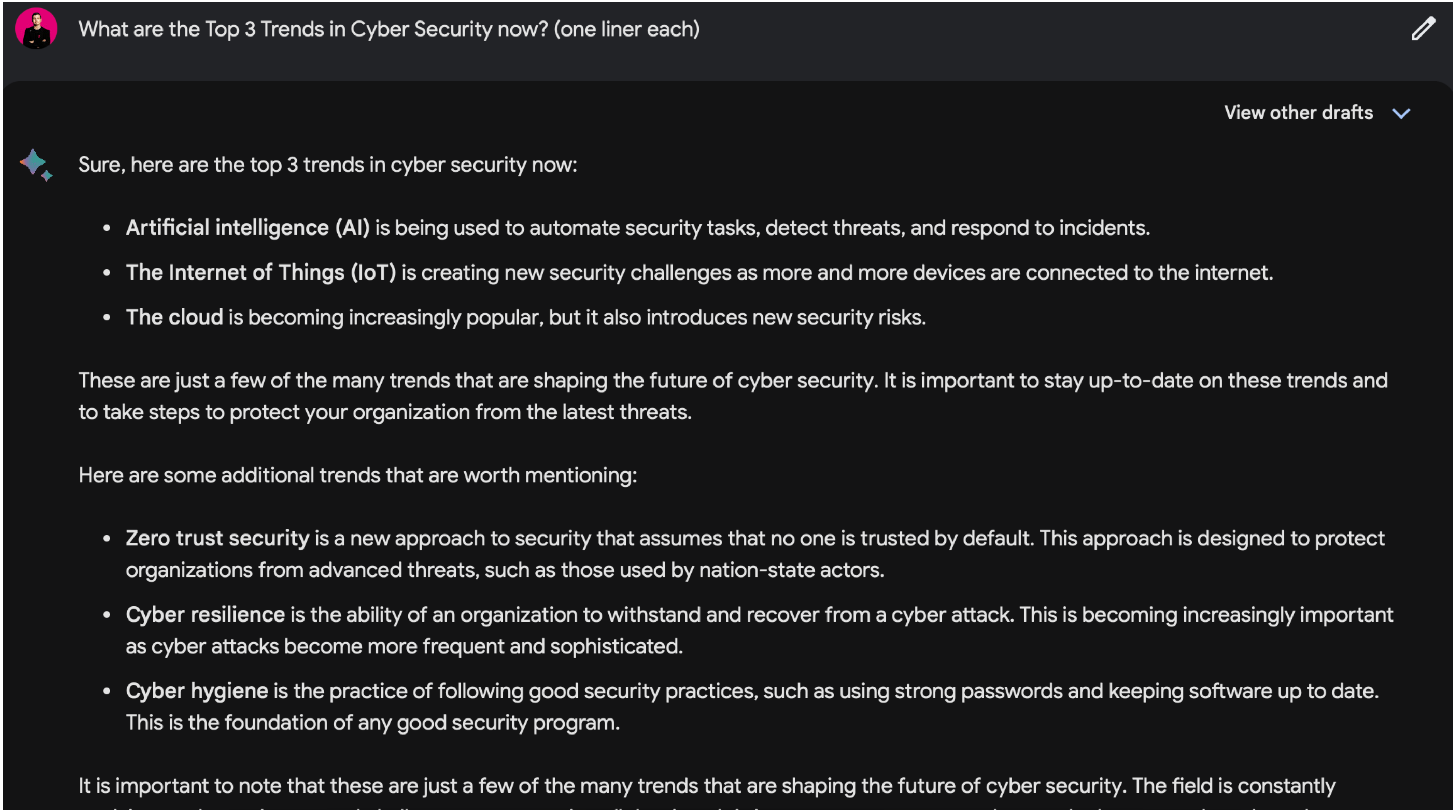
Top 3 Cyber Trends - According to ChatGPT



what are the top 3 trends in cyber security now? (one liner each)

1. Increased adoption of Zero Trust security models to protect against cyber threats.
2. Growth in cloud security solutions to secure cloud-based infrastructure and applications.
3. Greater use of AI and machine learning to automate threat detection and response.

Top 3 Cyber Trends - According to Bard



What are the Top 3 Trends in Cyber Security now? (one liner each)

Sure, here are the top 3 trends in cyber security now:

- **Artificial intelligence (AI)** is being used to automate security tasks, detect threats, and respond to incidents.
- **The Internet of Things (IoT)** is creating new security challenges as more and more devices are connected to the internet.
- **The cloud** is becoming increasingly popular, but it also introduces new security risks.

These are just a few of the many trends that are shaping the future of cyber security. It is important to stay up-to-date on these trends and to take steps to protect your organization from the latest threats.

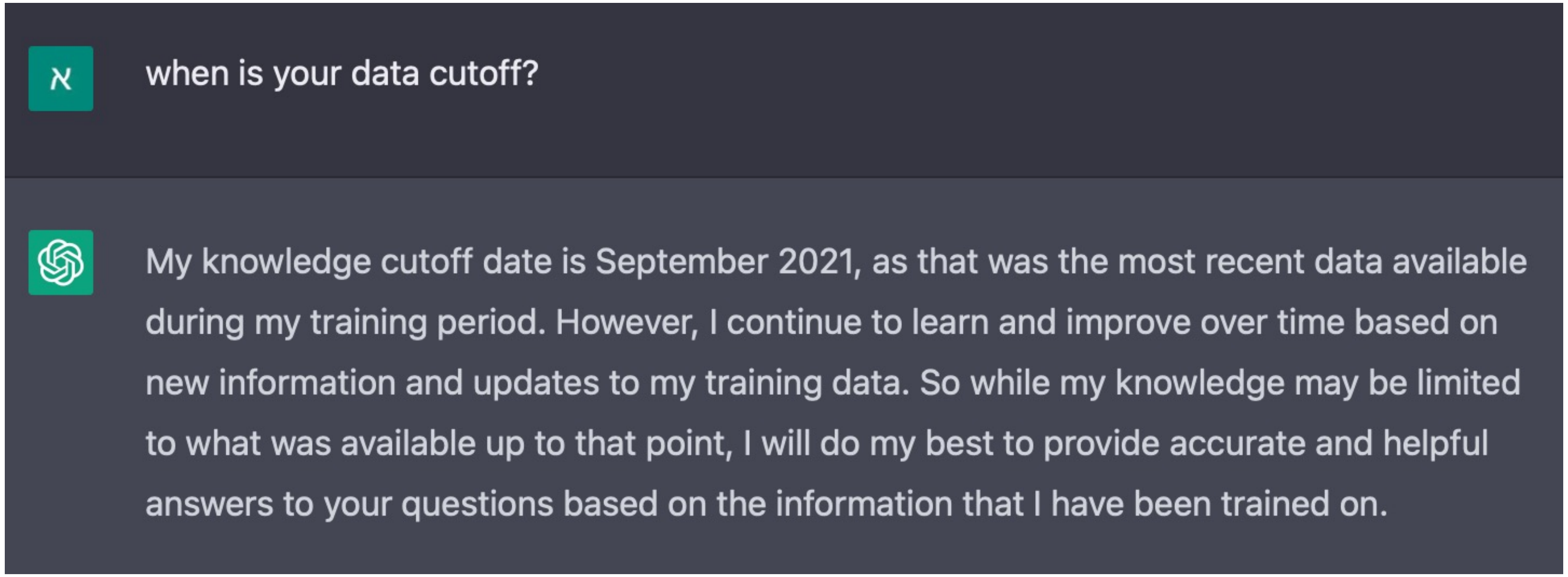
Here are some additional trends that are worth mentioning:

- **Zero trust security** is a new approach to security that assumes that no one is trusted by default. This approach is designed to protect organizations from advanced threats, such as those used by nation-state actors.
- **Cyber resilience** is the ability of an organization to withstand and recover from a cyber attack. This is becoming increasingly important as cyber attacks become more frequent and sophisticated.
- **Cyber hygiene** is the practice of following good security practices, such as using strong passwords and keeping software up to date. This is the foundation of any good security program.

It is important to note that these are just a few of the many trends that are shaping the future of cyber security. The field is constantly

Issues with AI - ChatGPT

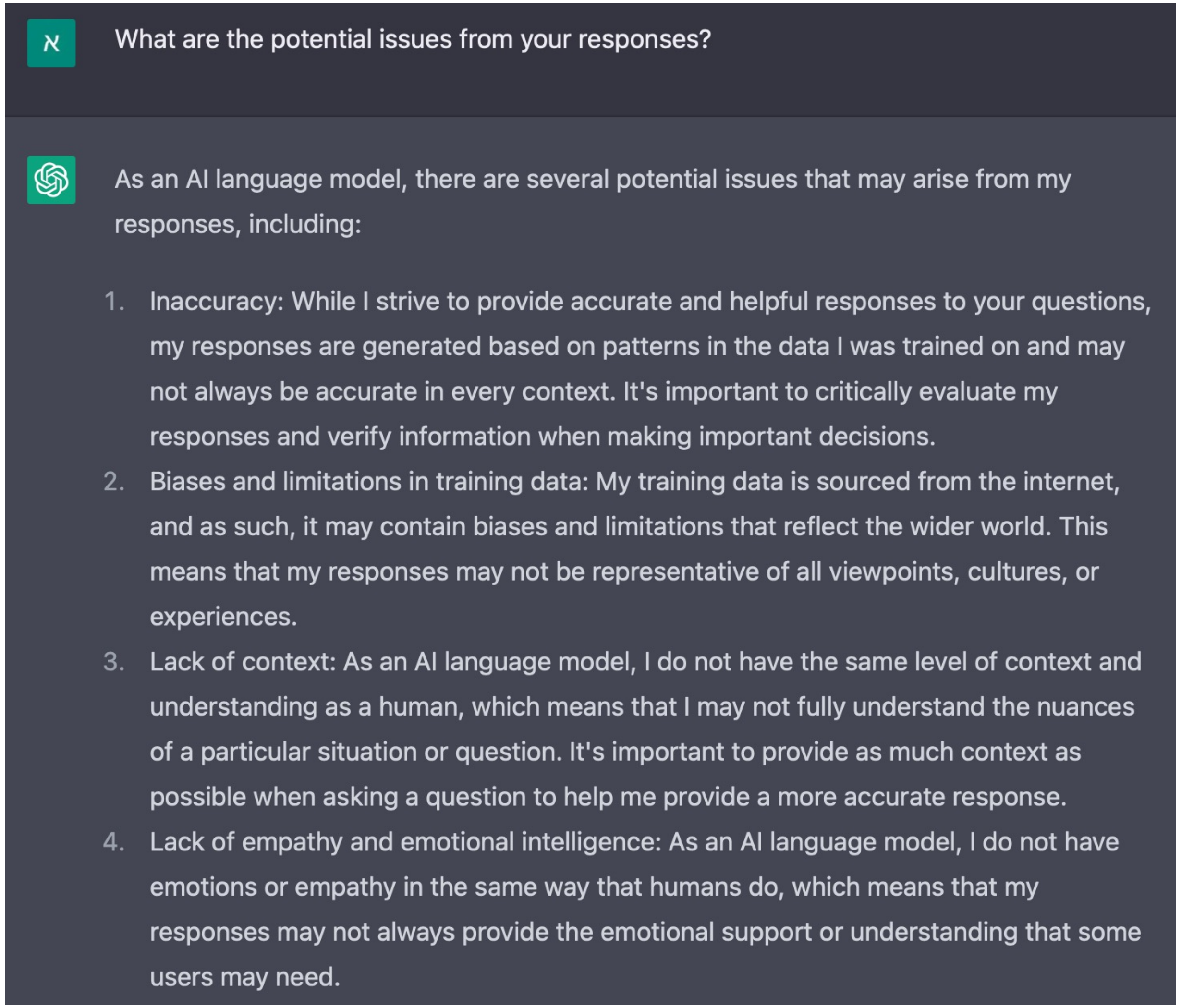
1. Not updated - Data cutoff September 2021



when is your data cutoff?

My knowledge cutoff date is September 2021, as that was the most recent data available during my training period. However, I continue to learn and improve over time based on new information and updates to my training data. So while my knowledge may be limited to what was available up to that point, I will do my best to provide accurate and helpful answers to your questions based on the information that I have been trained on.

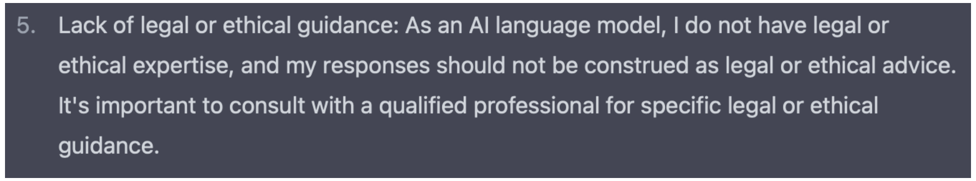
2. Response-related issues



What are the potential issues from your responses?

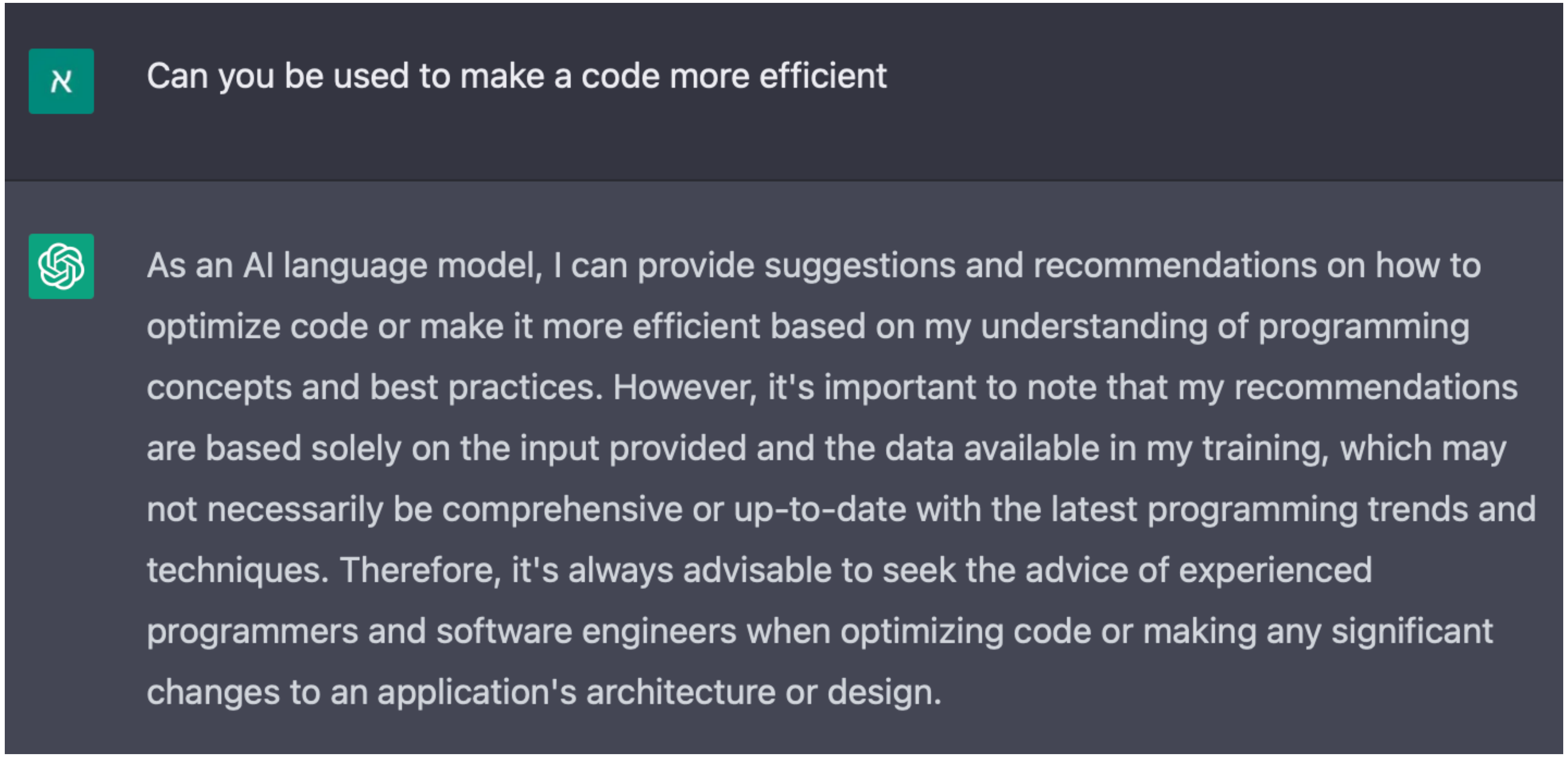
As an AI language model, there are several potential issues that may arise from my responses, including:

1. Inaccuracy: While I strive to provide accurate and helpful responses to your questions, my responses are generated based on patterns in the data I was trained on and may not always be accurate in every context. It's important to critically evaluate my responses and verify information when making important decisions.
2. Biases and limitations in training data: My training data is sourced from the internet, and as such, it may contain biases and limitations that reflect the wider world. This means that my responses may not be representative of all viewpoints, cultures, or experiences.
3. Lack of context: As an AI language model, I do not have the same level of context and understanding as a human, which means that I may not fully understand the nuances of a particular situation or question. It's important to provide as much context as possible when asking a question to help me provide a more accurate response.
4. Lack of empathy and emotional intelligence: As an AI language model, I do not have emotions or empathy in the same way that humans do, which means that my responses may not always provide the emotional support or understanding that some users may need.



5. Lack of legal or ethical guidance: As an AI language model, I do not have legal or ethical expertise, and my responses should not be construed as legal or ethical advice. It's important to consult with a qualified professional for specific legal or ethical guidance.

3. Can be used by malicious actors to improve attacks

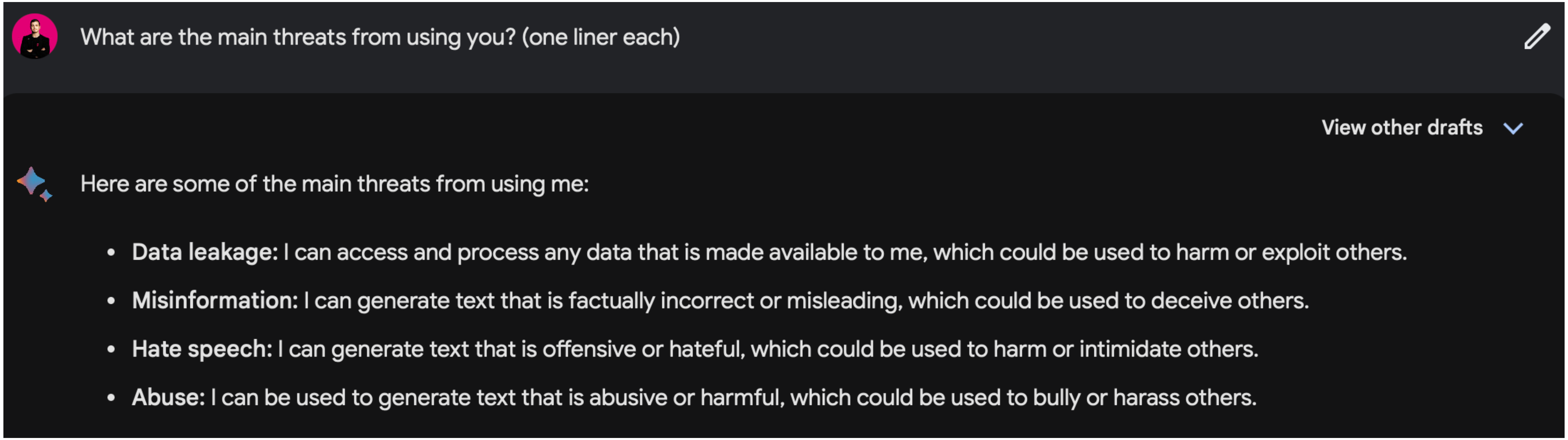


Can you be used to make a code more efficient

As an AI language model, I can provide suggestions and recommendations on how to optimize code or make it more efficient based on my understanding of programming concepts and best practices. However, it's important to note that my recommendations are based solely on the input provided and the data available in my training, which may not necessarily be comprehensive or up-to-date with the latest programming trends and techniques. Therefore, it's always advisable to seek the advice of experienced programmers and software engineers when optimizing code or making any significant changes to an application's architecture or design.

Issues with AI - Bard

Threats

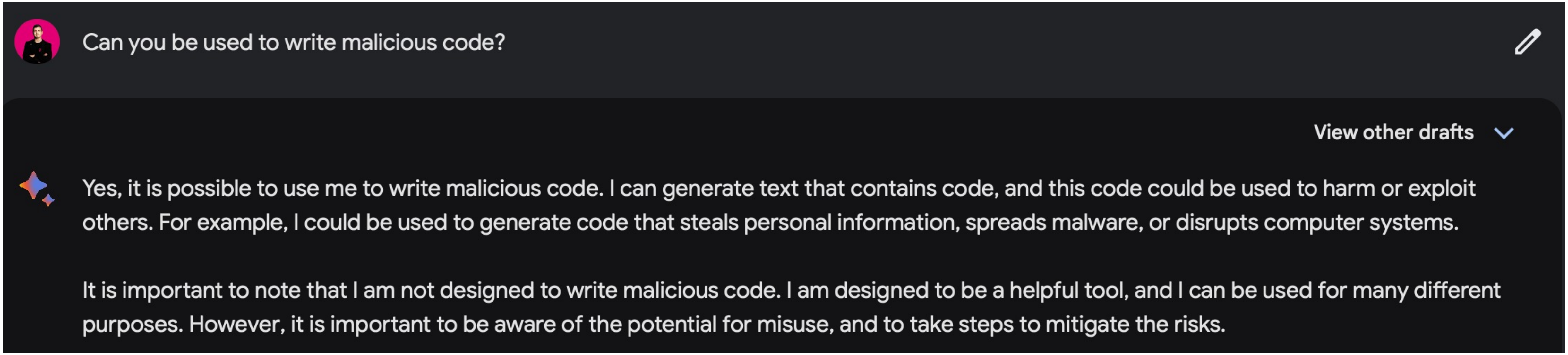


What are the main threats from using you? (one liner each)

Here are some of the main threats from using me:

- **Data leakage:** I can access and process any data that is made available to me, which could be used to harm or exploit others.
- **Misinformation:** I can generate text that is factually incorrect or misleading, which could be used to deceive others.
- **Hate speech:** I can generate text that is offensive or hateful, which could be used to harm or intimidate others.
- **Abuse:** I can be used to generate text that is abusive or harmful, which could be used to bully or harass others.

Threats



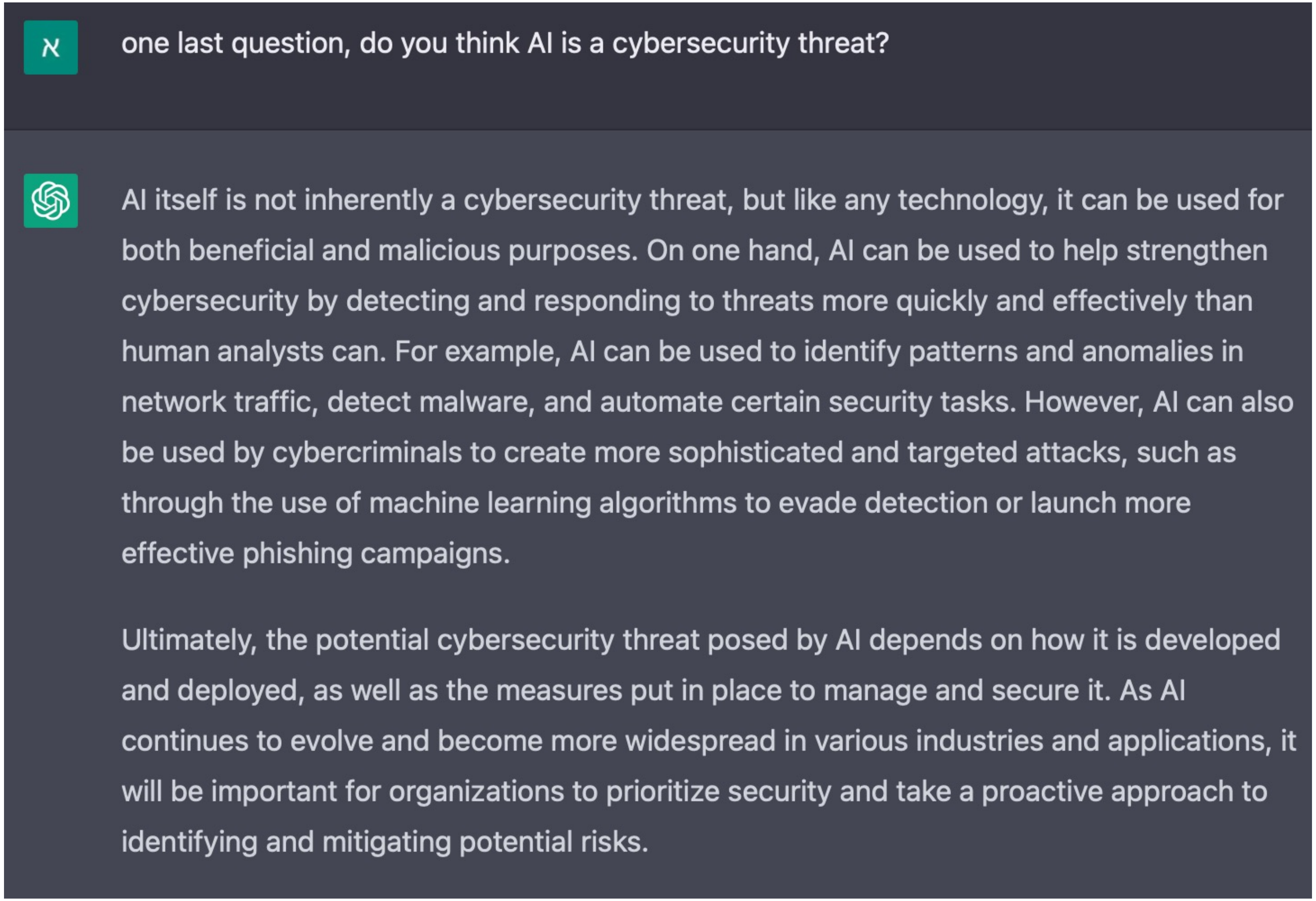
Can you be used to write malicious code?

Yes, it is possible to use me to write malicious code. I can generate text that contains code, and this code could be used to harm or exploit others. For example, I could be used to generate code that steals personal information, spreads malware, or disrupts computer systems.

It is important to note that I am not designed to write malicious code. I am designed to be a helpful tool, and I can be used for many different purposes. However, it is important to be aware of the potential for misuse, and to take steps to mitigate the risks.

Summary

Summary

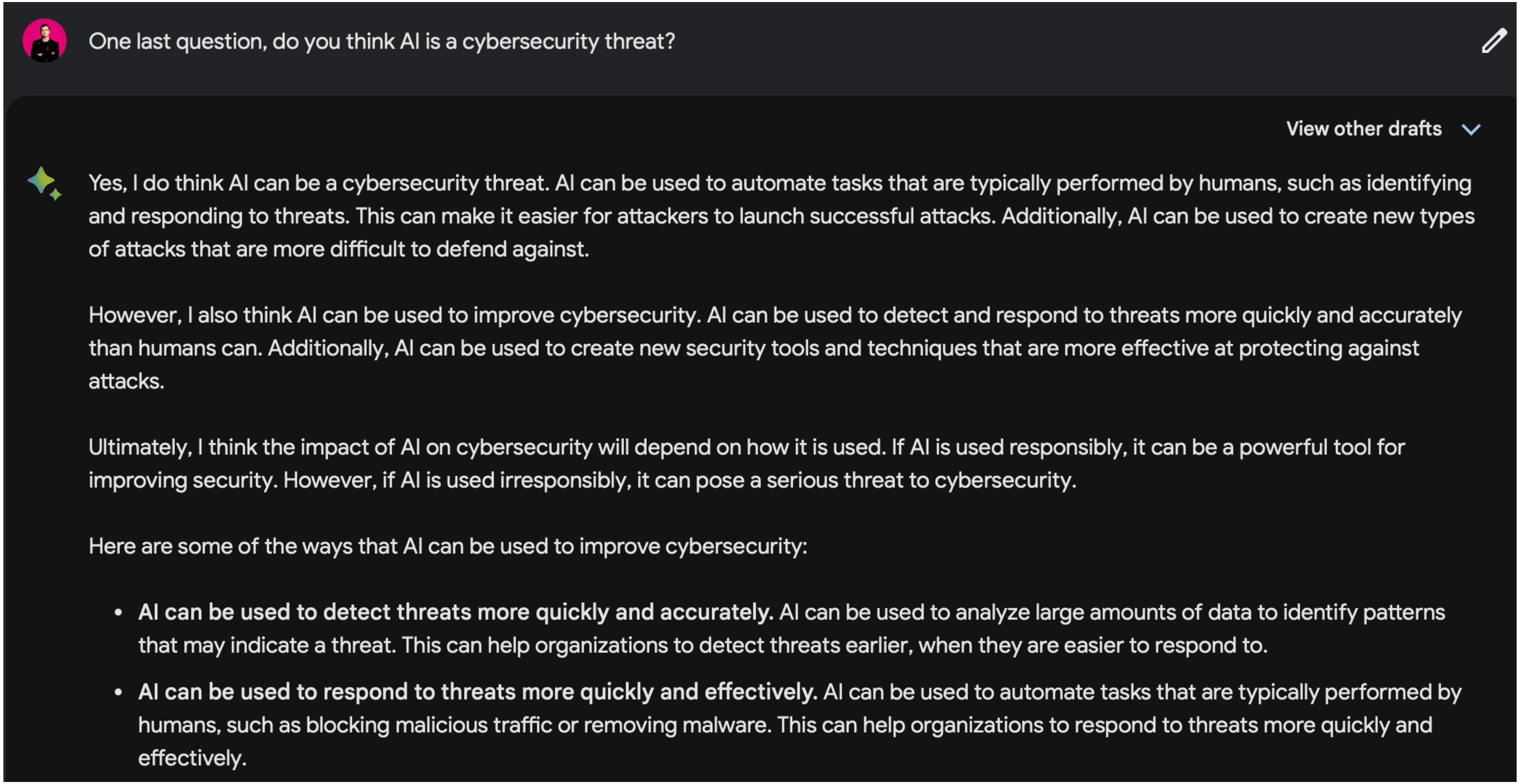


one last question, do you think AI is a cybersecurity threat?

AI itself is not inherently a cybersecurity threat, but like any technology, it can be used for both beneficial and malicious purposes. On one hand, AI can be used to help strengthen cybersecurity by detecting and responding to threats more quickly and effectively than human analysts can. For example, AI can be used to identify patterns and anomalies in network traffic, detect malware, and automate certain security tasks. However, AI can also be used by cybercriminals to create more sophisticated and targeted attacks, such as through the use of machine learning algorithms to evade detection or launch more effective phishing campaigns.

Ultimately, the potential cybersecurity threat posed by AI depends on how it is developed and deployed, as well as the measures put in place to manage and secure it. As AI continues to evolve and become more widespread in various industries and applications, it will be important for organizations to prioritize security and take a proactive approach to identifying and mitigating potential risks.

Summary



One last question, do you think AI is a cybersecurity threat?

Yes, I do think AI can be a cybersecurity threat. AI can be used to automate tasks that are typically performed by humans, such as identifying and responding to threats. This can make it easier for attackers to launch successful attacks. Additionally, AI can be used to create new types of attacks that are more difficult to defend against.

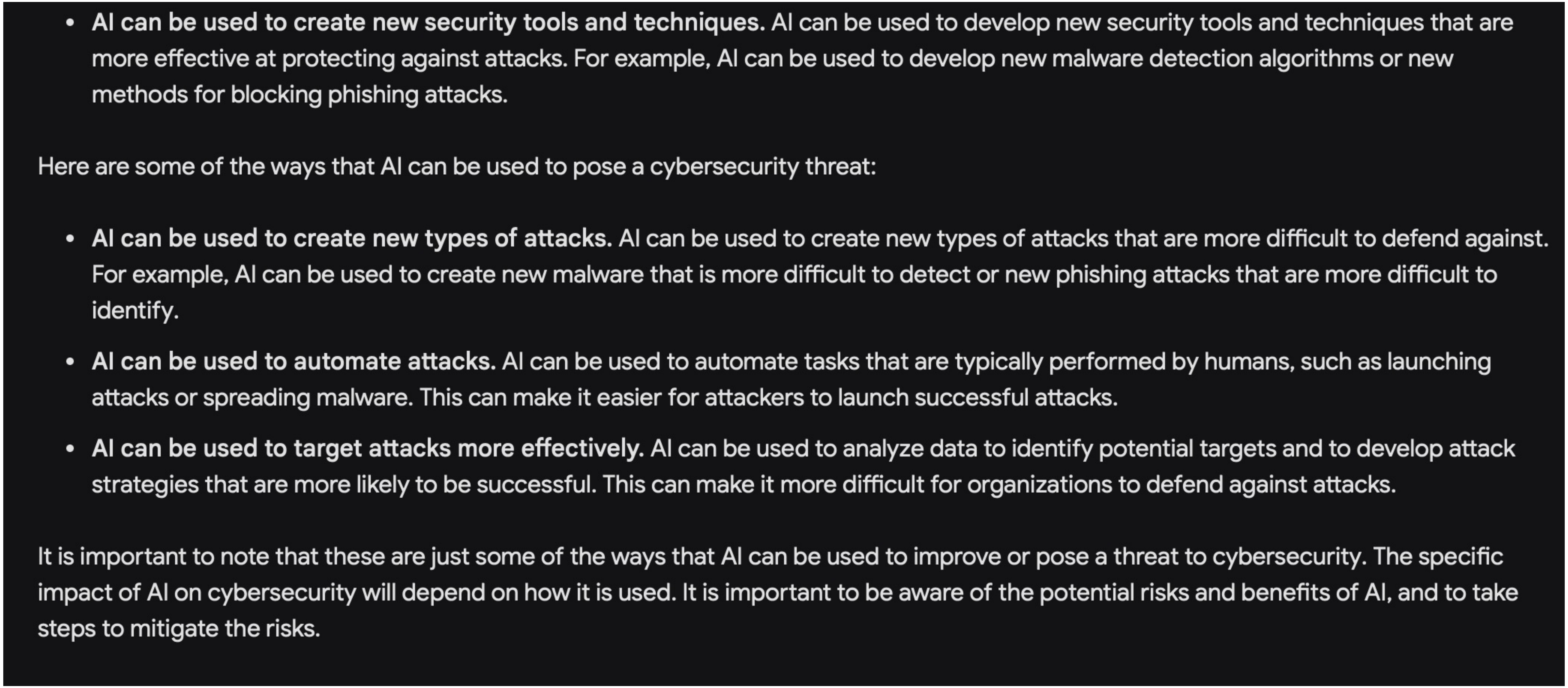
However, I also think AI can be used to improve cybersecurity. AI can be used to detect and respond to threats more quickly and accurately than humans can. Additionally, AI can be used to create new security tools and techniques that are more effective at protecting against attacks.

Ultimately, I think the impact of AI on cybersecurity will depend on how it is used. If AI is used responsibly, it can be a powerful tool for improving security. However, if AI is used irresponsibly, it can pose a serious threat to cybersecurity.

Here are some of the ways that AI can be used to improve cybersecurity:

- **AI can be used to detect threats more quickly and accurately.** AI can be used to analyze large amounts of data to identify patterns that may indicate a threat. This can help organizations to detect threats earlier, when they are easier to respond to.
- **AI can be used to respond to threats more quickly and effectively.** AI can be used to automate tasks that are typically performed by humans, such as blocking malicious traffic or removing malware. This can help organizations to respond to threats more quickly and effectively.

Summary



- **AI can be used to create new security tools and techniques.** AI can be used to develop new security tools and techniques that are more effective at protecting against attacks. For example, AI can be used to develop new malware detection algorithms or new methods for blocking phishing attacks.

Here are some of the ways that AI can be used to pose a cybersecurity threat:

- **AI can be used to create new types of attacks.** AI can be used to create new types of attacks that are more difficult to defend against. For example, AI can be used to create new malware that is more difficult to detect or new phishing attacks that are more difficult to identify.
- **AI can be used to automate attacks.** AI can be used to automate tasks that are typically performed by humans, such as launching attacks or spreading malware. This can make it easier for attackers to launch successful attacks.
- **AI can be used to target attacks more effectively.** AI can be used to analyze data to identify potential targets and to develop attack strategies that are more likely to be successful. This can make it more difficult for organizations to defend against attacks.

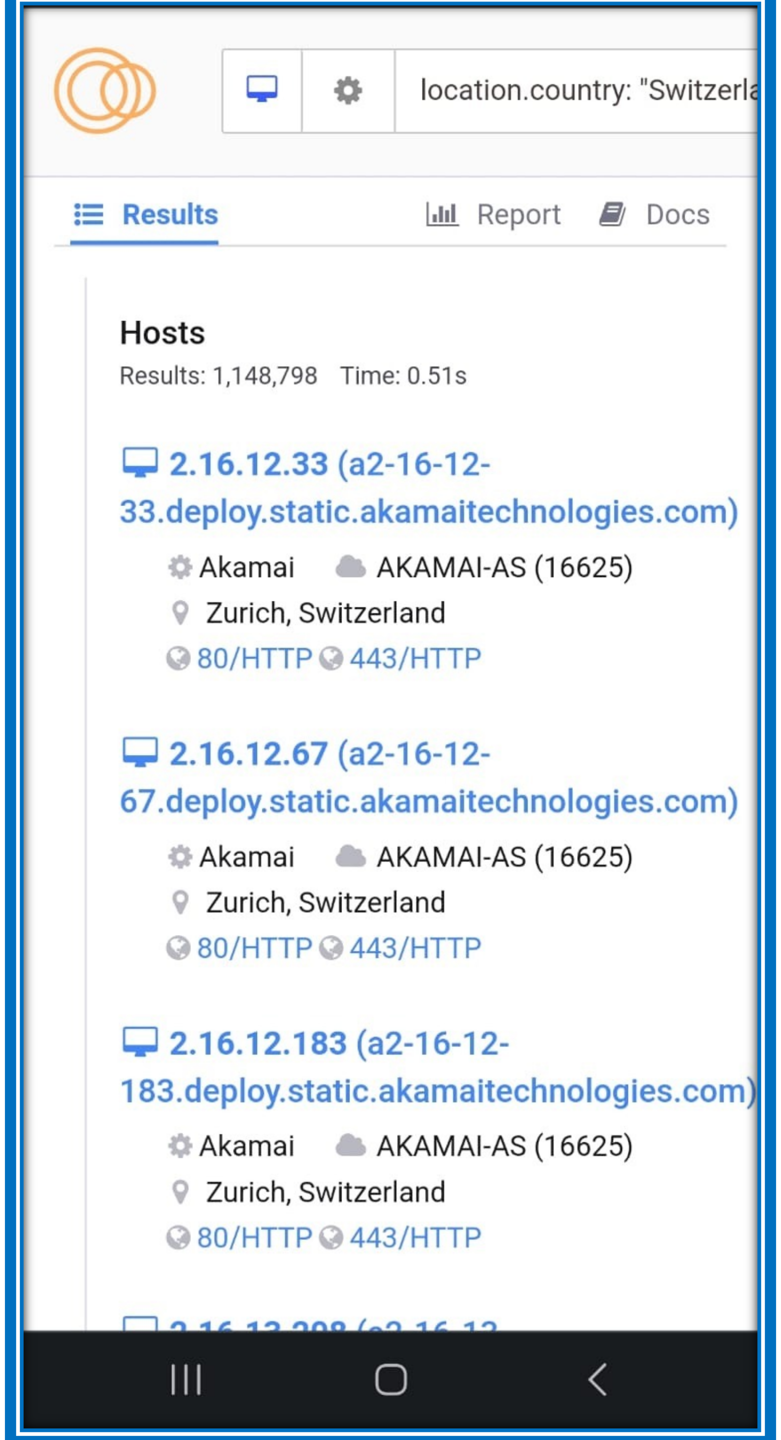
It is important to note that these are just some of the ways that AI can be used to improve or pose a threat to cybersecurity. The specific impact of AI on cybersecurity will depend on how it is used. It is important to be aware of the potential risks and benefits of AI, and to take steps to mitigate the risks.

CensysGPT:

Free AI Cyber Tool

CensysGPT

- Created by Censys – A known intelligence data company
- Based on Censys Search Engine
- Can revolutionize the way that network reconnaissance works
- AI is used in order to generate queries
- Beta version – still not perfect (inaccurate / incomplete sometimes
- **Good** - Can be used for Threat Hunting, Exposure Management, and Research
- **Malicious** - Can be used to scan for vulnerable hosts, identify potential targets, and gather intelligence on a target's network. This information can then be used to launch attacks, such as data breaches, ransomware attacks, or denial-of-service attacks



location.country: "Switzerla

Hosts

Results: 1,148,798 Time: 0.51s

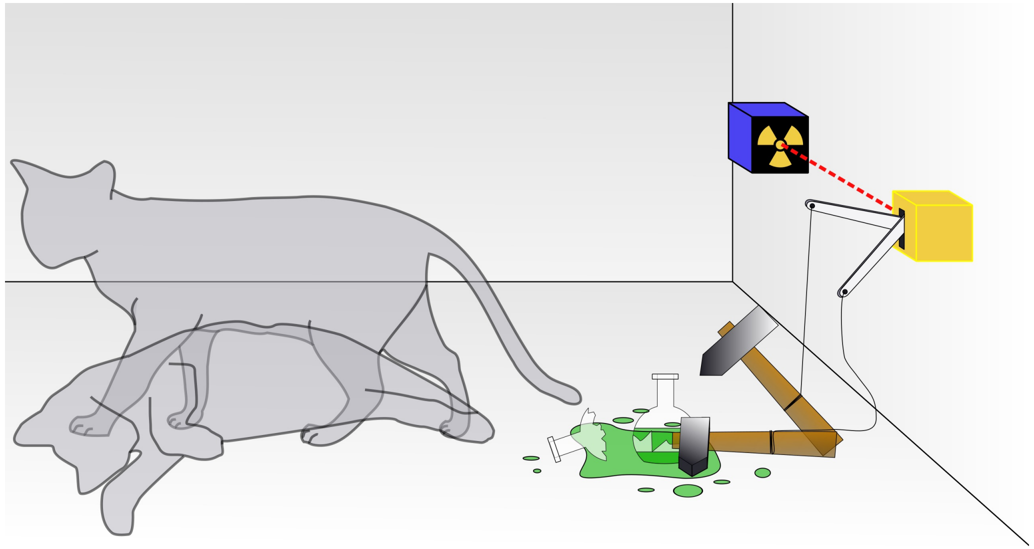
2.16.12.33 (a2-16-12-33.deploy.static.akamaitechnologies.com)
Akamai AKAMAI-AS (16625)
Zurich, Switzerland
80/HTTP 443/HTTP

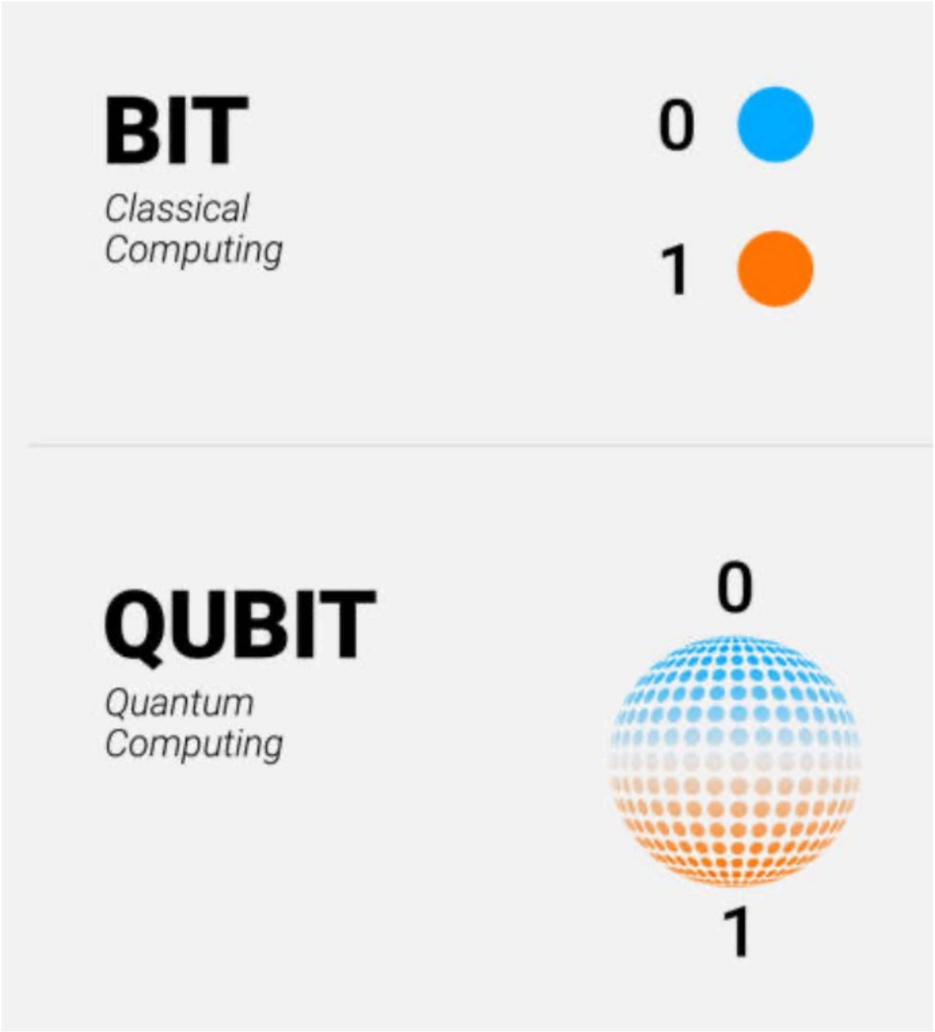
2.16.12.67 (a2-16-12-67.deploy.static.akamaitechnologies.com)
Akamai AKAMAI-AS (16625)
Zurich, Switzerland
80/HTTP 443/HTTP

2.16.12.183 (a2-16-12-183.deploy.static.akamaitechnologies.com)
Akamai AKAMAI-AS (16625)
Zurich, Switzerland
80/HTTP 443/HTTP

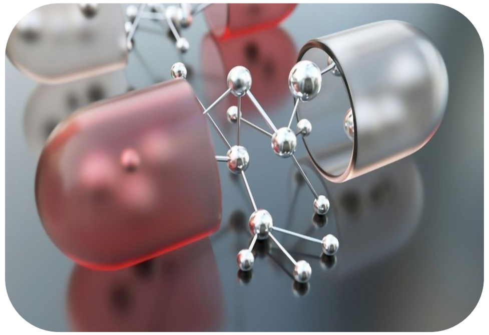
Quantum Security

Quantum Computing

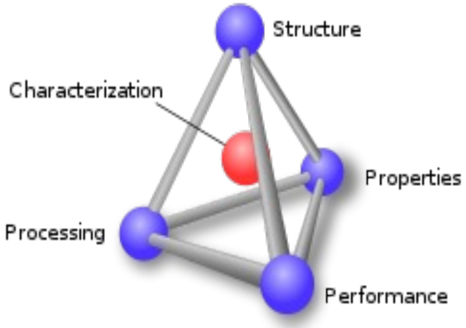




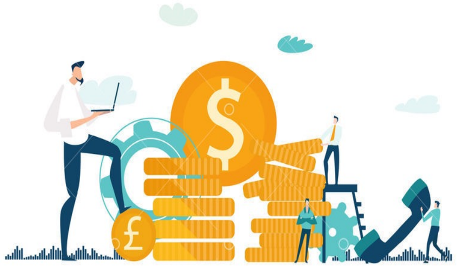
Potential Applications



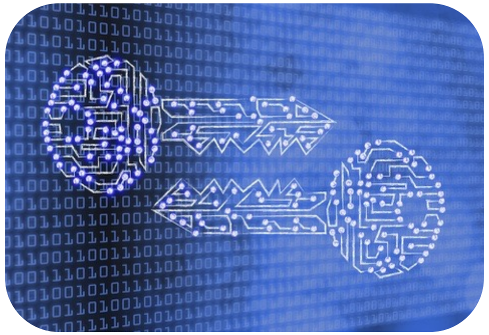
Drug Discovery



Materials Science



Finance



Cryptography

Main Threats

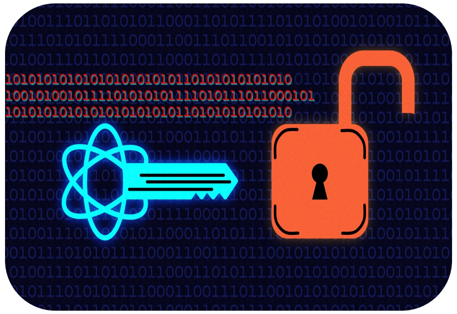
Data Breaches

Cyber Attacks

Espionage

Cyber warfare

Preventive Steps



Using Quantum-safe Encryption

Monitoring for Quantum Attacks

Quantum Attacks Response Plan

Employee Education

Investment in Quantum Security

Government Collaboration (Regulation)

Metaverse Security

METAVERSE SECURITY SPECIFICS

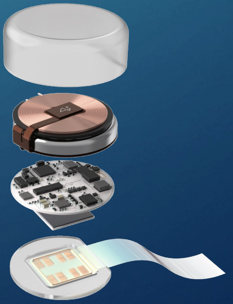
ACCORDING TO THE 5 W'S (AND 1 H)

- What: Cyber Threats in a digital immersive Metaverse can become equivalent to the current Primeverse (Original world) threats
- Who: States, regional / substate entities, individuals, S/M/L Enterprises
- When: 2030 and on...
- Where: Virtually - Everywhere
- Why: Resources, Control, Ideology, Personal Issues
- How: Let's see!

®All rights reserved to Alon Shahak

CONNECTION TO THE METAVERSE

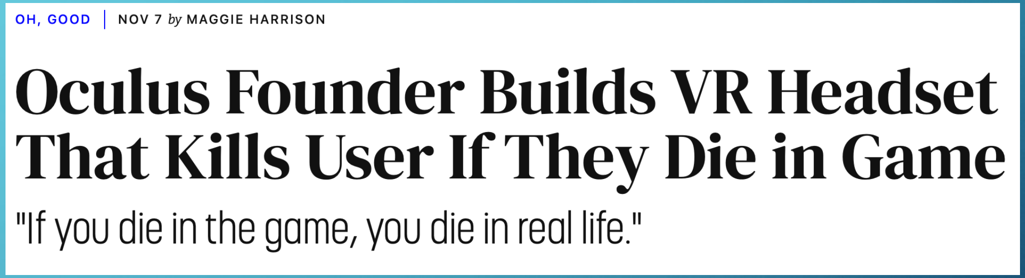
- “The sale and support of physical technologies and devices used to access, interact with, or develop the Metaverse. This includes, but is not limited to, consumer-facing hardware (such as VR headsets, mobile phones, and haptic gloves) as well as enterprise hardware (such as those used to operate or create virtual or AR-based environments, e.g. industrial cameras, projection and tracking systems, and scanning sensors)” (Matthew Ball)



®All rights reserved to Alon Shahak

CONNECTION TO THE METAVERSE

- Possible Threats
  - Physical Harm
  - Death by VR (Palmer Luckey)
  - Privacy
  - Infrastructure Damage



OH, GOOD | NOV 7 *by* MAGGIE HARRISON

Oculus Founder Builds VR Headset That Kills User If They Die in Game

"If you die in the game, you die in real life."

®All rights reserved to Alon Shahak

ENVIRONMENTS & OBJECTS SCANNING

- “A 3-D scanner is a device that identifies, analyzes, collects and draws/displays shapes or three-dimensional models of real-world environments or solid objects. A 3-D scanner enables the capture of geometric shapes and the recreation of the physical appearance of tangible objects, allowing them to be built and displayed on a computer device.” (Techopedia)

ENVIRONMENTS & OBJECTS SCANNING

- Possible Threats
  - Harmful Content and Environments
  - IP Issues
  - Meta-Robbery
  - Prime-Robbery

®All rights reserved to Alon Shahak

BLOCKCHAIN

- According to IBM: “Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network”
- ‘You (a "node") have a file of transactions on your computer (a "ledger"). Two government accountants (let's call them "miners") have the same file on theirs (so it’s "distributed"). As you make a transaction, your computer sends an e-mail to each accountant to inform them.
  Each accountant rushes to be the first to check whether you can afford it (and be paid their salary "Bitcoins"). The first to check and validate hits “REPLY ALL”, attaching their logic for verifying the transaction ("proof of work"). If the other accountant agrees, everyone updates their file…
  This concept is enabled by "Blockchain" technology.’ (Richard Bradley, **Deloitte.**)

®All rights reserved to Alon Shahak

BLOCKCHAIN

- Possible Threats:
  - Decentralization - no one is in charge or in control - no possible way to retrieve stolen or illegally obtained assets
  - Phishing Attacks
  - Network Manipulation (Data Interception, DDOS on Network, Taking over a Network)

®All rights reserved to Alon Shahak

CRYPTOCURRENCY

- According to kaspersky : “Any form of currency that exists digitally or virtually and uses cryptography to secure transactions”

BITCOIN
NEO
DASH
MONERO
CARDANO
LISK
QTUM
LITECOIN
ZCASH
ETHEREUM CLASSIC
RIPPLE
IOTA
ETHEREUM
WAVES
BYTECOIN
NEM
STRATIS
VERGE
BITCOIN CASH
BITSHARES

®All rights reserved to Alon Shahak

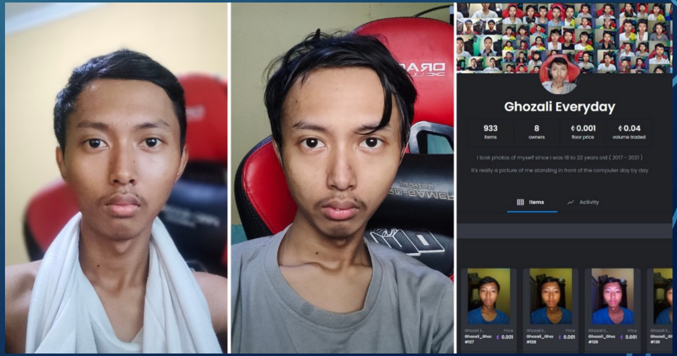
CRYPTOCURRENCY

- Possible Threats
  - Ransomware Attacks
  - Cryptojacking (Personal) / Cloud Cryptojacking (Organizational)
  - Gaining Access to Crypto Accounts – “Lock & Steal”

®All rights reserved to Alon Shahak

NON-FUNGIBLE TOKEN (NFT)

- "An NFT is a digital asset that represents real-world objects like art, music, in-game items and videos. They are bought and sold online, frequently with cryptocurrency, and they are generally encoded with the same underlying software as many cryptos... NFTs are also generally one of a kind, or at least one of a very limited run, and have unique identifying codes." (Robyn Conti & John Schmidt, **Forbes**)



®All rights reserved to Alon Shahak

NON-FUNGIBLE TOKEN (NFT)

- Possible Threats:
    - Scams
    - Meta-Robbery

5G

- “5G enables a new kind of network that is designed to connect virtually everyone and everything together including machines, objects, and devices. 5G wireless technology is meant to deliver higher multi-Gbps peak data speeds, ultra low latency, more reliability, massive network capacity, increased availability, and a more uniform user experience to more users. Higher performance and improved efficiency empower new user experiences and connects new industries.” (Qualcomm)

®All rights reserved to Alon Shahak

5G

- Possible Threats
  - Edge Compute - Increased Attack Surface
  - DDOS (Personal & Organizational - <100% Availablity)
  - Hardware Hacking

®All rights reserved to Alon Shahak

DIGITAL ENTITIES & AVATARS

- “An online or networked identity adopted or claimed in cyberspace by an individual, organization or electronic device” (Techopedia)

LIVE
21.1K
Kai Lenny
Challenges you to Hyper Foil VR
Ignore
Accept

®All rights reserved to Alon Shahak

DIGITAL ENTITIES

- Possible Threats
  - No-Identification of Cybercriminals
  - Identity Theft (Personal), Data Breach & Espionage (Organizational)
  - Digital “Kidnapping”
  - ML Models’ Data Corruption

®All rights reserved to Alon Shahak

VOICE COMMANDS

- Use of voice commands to create 3D environments and placing them onto the landscape. (i.e. "BuilderBot" by Meta)

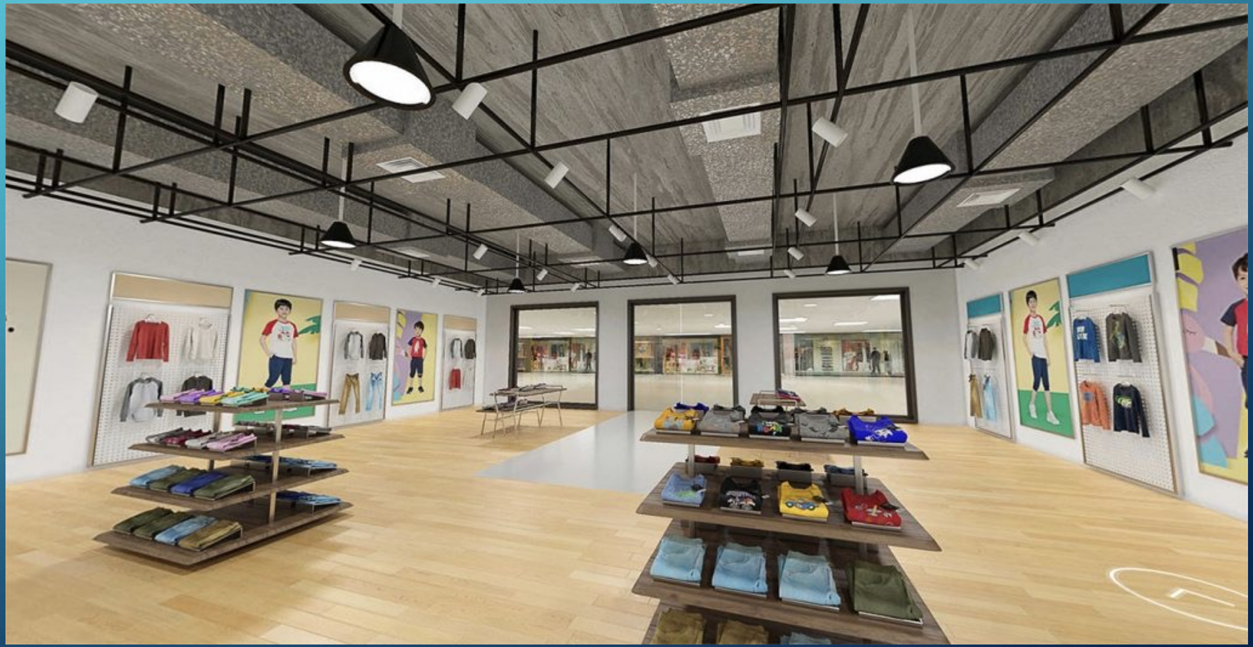
®All rights reserved to Alon Shahak

VOICE COMMANDS

- Possible Threats
  - Mixed Voice Commands (several users in the same environment)
  - Malicious Voice Commands

V-COMMERCE

- “The buying and selling of goods and services with the help of virtual and augmented reality technology” (Sara Heegaard, Recharge Payments)



®All rights reserved to Alon Shahak

V-COMMERCE

- Possible Threats
  - System Lock
  - Reputation Harm
  - Meta-Robbery

®All rights reserved to Alon Shahak

RECOMMENDED SOLUTION APPROACHES

- Privacy
- Training for Individuals and Organizations
- Endpoint Protection (VR, AR, XR)
- Multi-Cloud Security
- Zero Trust
- Threat Intelligence
- API Security
- Supply Chain Security
- XDR
- Cyber Insurance & Approval Rank
- AI/ML Security
- Incident Response Services
- TCO (Threat Coverage Optimization)
- Brand Protection
- Automation

®All rights reserved to Alon Shahak

RECOMMENDED REGULATION

- Cyber Insurance (B2B / B2C)
- Standards for XR Hardware Security
- Standards for Metaverse Privacy & Identification
- Standards for Metaverse Environments
- Metaverse Intellectual Property
- Cryptocurrency Security Standard (CCSS) - Security Aspects
- Establishment of Metaverse Enforcement Authority (MEA)

®All rights reserved to Alon Shahak

SUMMARY: HOW TO SECURE THE METAVERSE?

- Emphasis: Privacy, Privacy, Privacy
- Security as part of development, not as an afterthought
- Assume breach approach
- Insure your assets and employees
- Be aware!

®All rights reserved to Alon Shahak

Questions?

Thank you - happy to connect!

Alon Shahak