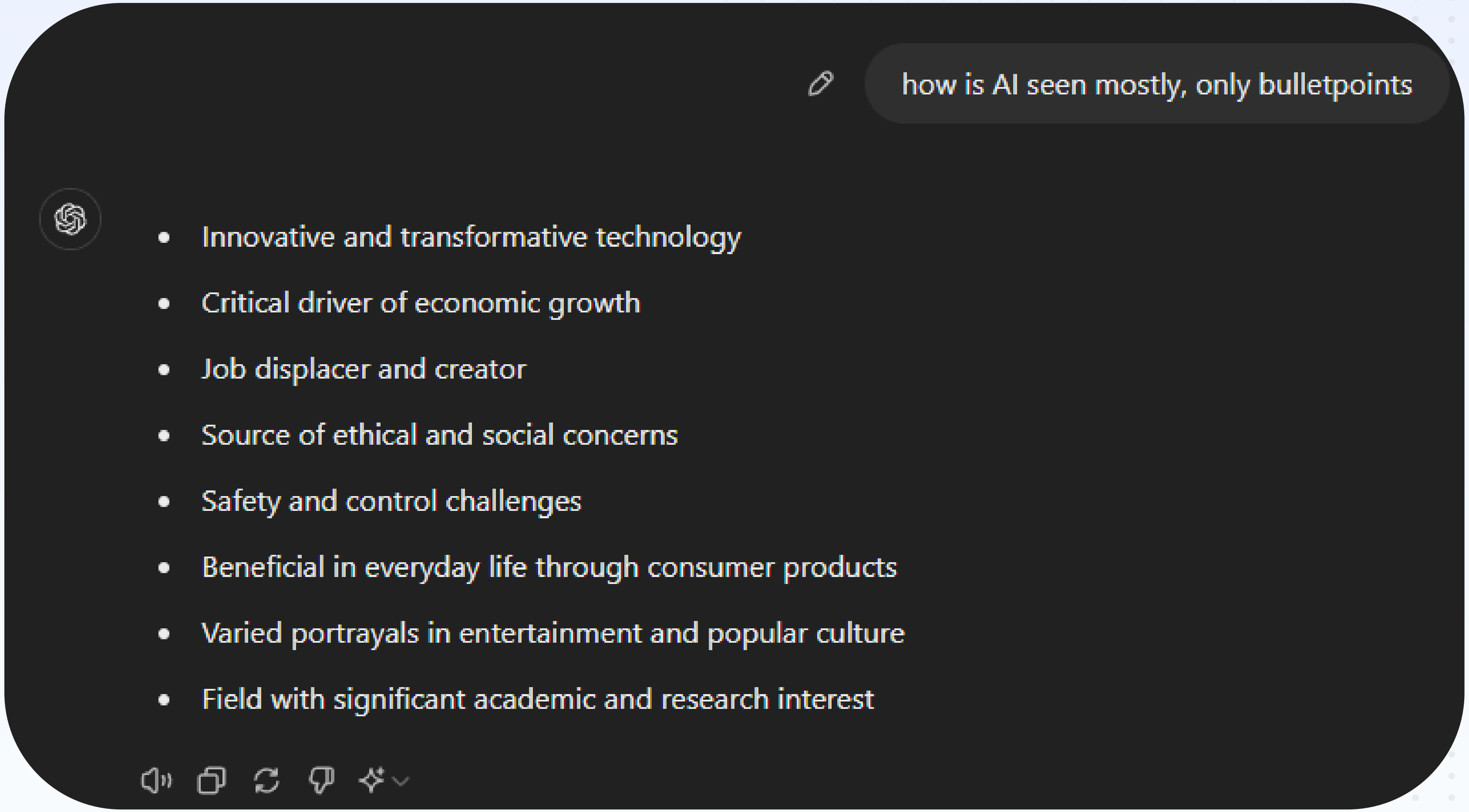
# Deutsche TELEKOM Security

## How AI Affects Cyber Security

# How AI is seen mostly



how is AI seen mostly, only bulletpoints

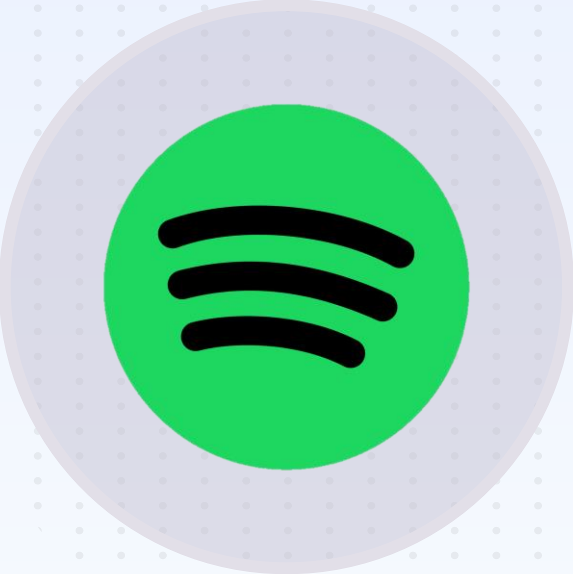
- Innovative and transformative technology
- Critical driver of economic growth
- Job displacer and creator
- Source of ethical and social concerns
- Safety and control challenges
- Beneficial in everyday life through consumer products
- Varied portrayals in entertainment and popular culture
- Field with significant academic and research interest

# Is AI really new?

✓ Fancy? - YES ✗ New? NO! =)

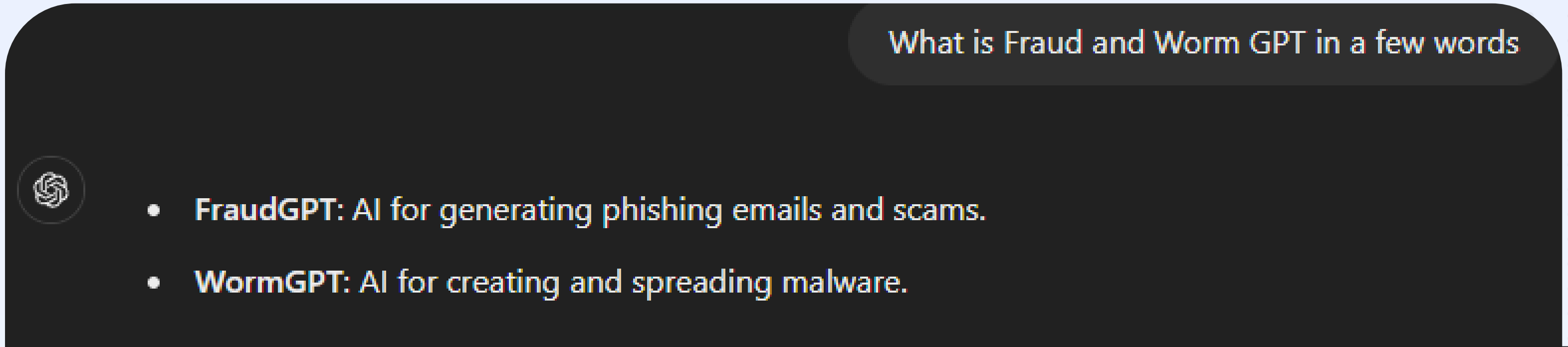
Tells us what we want to **see**

Tells us what we want to **buy**



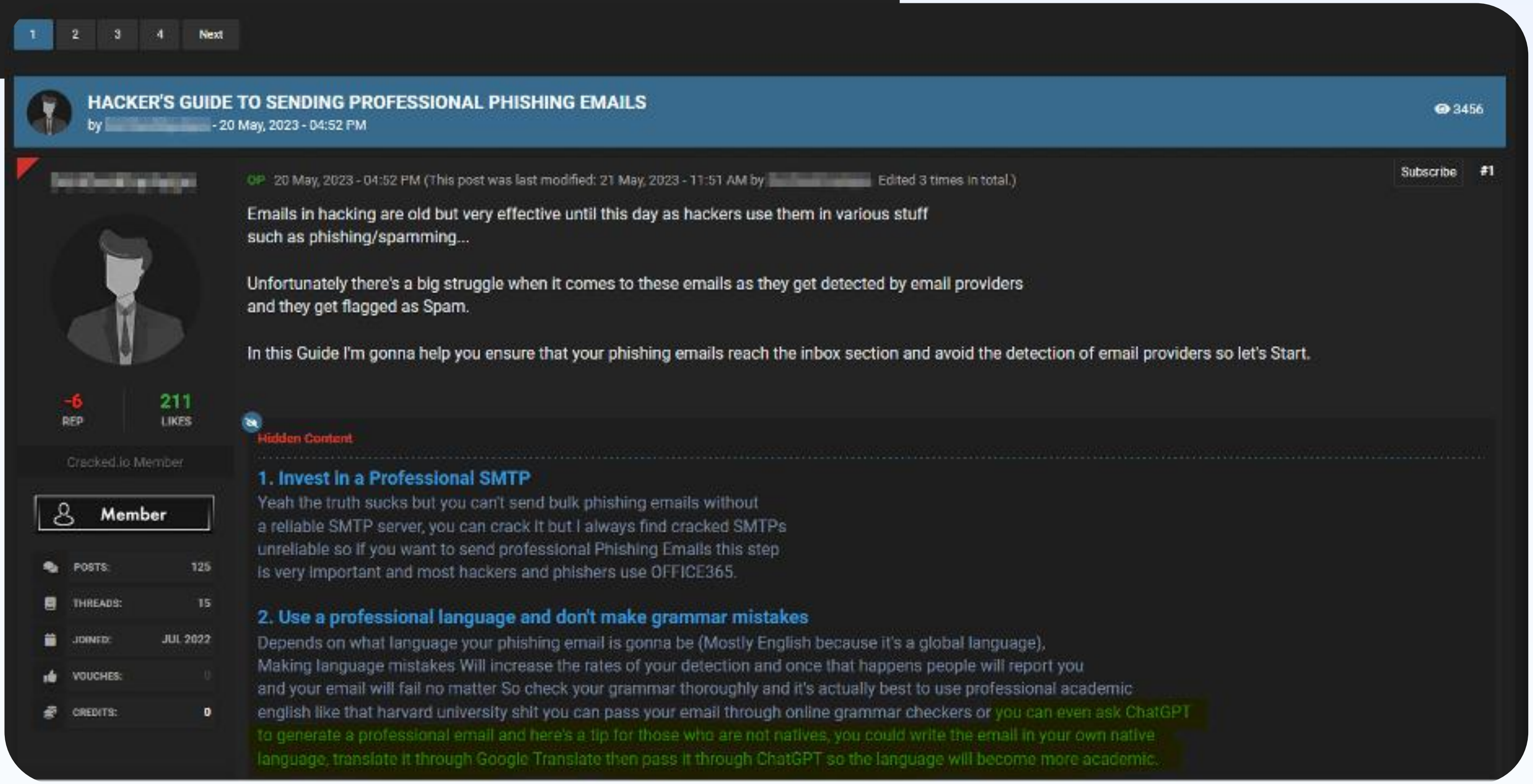
Tells us what we want to **listen** to

# Do Cirminals use AI as well?



What is Fraud and Worm GPT in a few words

- **FraudGPT**: AI for generating phishing emails and scams.
- **WormGPT**: AI for creating and spreading malware.



**HACKER'S GUIDE TO SENDING PROFESSIONAL PHISHING EMAILS**
by [redacted] - 20 May, 2023 - 04:52 PM
3456

[redacted]

-6 REP
211 LIKES

Cracked.io Member

Member

| | |
|---|---|
| POSTS: | 125 |
| THREADS: | 15 |
| JOINED: | JUL 2022 |
| VOUCHES: | 0 |
| CREDITS: | 0 |

OP 20 May, 2023 - 04:52 PM (This post was last modified: 21 May, 2023 - 11:51 AM by [redacted] Edited 3 times in total.)

Emails in hacking are old but very effective until this day as hackers use them in various stuff
such as phishing/spamming...

Unfortunately there's a big struggle when it comes to these emails as they get detected by email providers
and they get flagged as Spam.

In this Guide I'm gonna help you ensure that your phishing emails reach the inbox section and avoid the detection of email providers so let's Start.

Hidden Content

**1. Invest in a Professional SMTP**
Yeah the truth sucks but you can't send bulk phishing emails without
a reliable SMTP server, you can crack it but I always find cracked SMTPs
unreliable so if you want to send professional Phishing Emails this step
is very important and most hackers and phishers use OFFICE365.

**2. Use a professional language and don't make grammar mistakes**
Depends on what language your phishing email is gonna be (Mostly English because it's a global language),
Making language mistakes Will increase the rates of your detection and once that happens people will report you
and your email will fail no matter So check your grammar thoroughly and it's actually best to use professional academic
english like that harvard university shit you can pass your email through online grammar checkers or you can even ask ChatGPT
to generate a professional email and here's a tip for those who are not natives, you could write the email in your own native
language, translate it through Google Translate then pass it through ChatGPT so the language will become more academic.

T SECURITY

# AI in Infosec

# From detection to Prevention: The Evolution of AI in Security

**Artificial intelligence (AI)** plays an increasingly important role in IT security.
The development in this area can be roughly divided into **three phases:**

## Detection of attacks and anomalies

AI-based systems analyze large amounts of data to identify patterns that could indicate an attack

## Automation of security tasks

AI Systems automate tasks such as analyzing logs, searching for vulnerabilities and responding to incidents

## Prevention and reduction of attacks

AI systems can proactively identify and remediate vulnerabilities before they can be exploited

SECURITY

Source: IBM, Cost of a Data Breach Report 2023

# How AI could be used in Info Sec

AI – Offensive use

AI – Defensive use

Securing AI

# AI – Offensive use

## Penetration testing, Red Teaming, etc.

- Automatic inofmration gathering
- Analyze data and determine different courses of action for attack phases
- Cost and time efficieny
- Reporting incorporating threat intelligence and past knowledge for actionable insights

## Adversaries

### Highly skilled

Optimal AI use for advanced cyber operations, including sophisticated malware generation against networks.

### Skilled

Significant AI-driven capability boost in reconnaissance, social engineering, and exfiltration, likely spreading AI tools to less experienced cyber attacks

### Low-skilled

Reduced entry barriers for efficient and scalable access operations, leading to a rise in successful compromises of devices and accounts

Source: Kaspersky 2024, ERMprotect; National Cyber Security Centre 2024

# AI – Deffensive use

## Lowering the bar

- Smart, adaptive automation tools provide timely advice on newly discovered conficugration issues
- Automatically adjust settings as needed
- AI and ML ensure consistency with manual processes and updates
- Supports in logging acativites and data mining as well as data analysis

## Improving the tech

- Cyber attacks often build on past behaviours, frameworks, and codes
- Machinge learning leverages past attacks to identify new threats
- ML helps highlight commonalities and spot attacks more effectively
- ML facilitaes prediction of new threats, reducing lag time
- Immediate grouping and analysis of attack

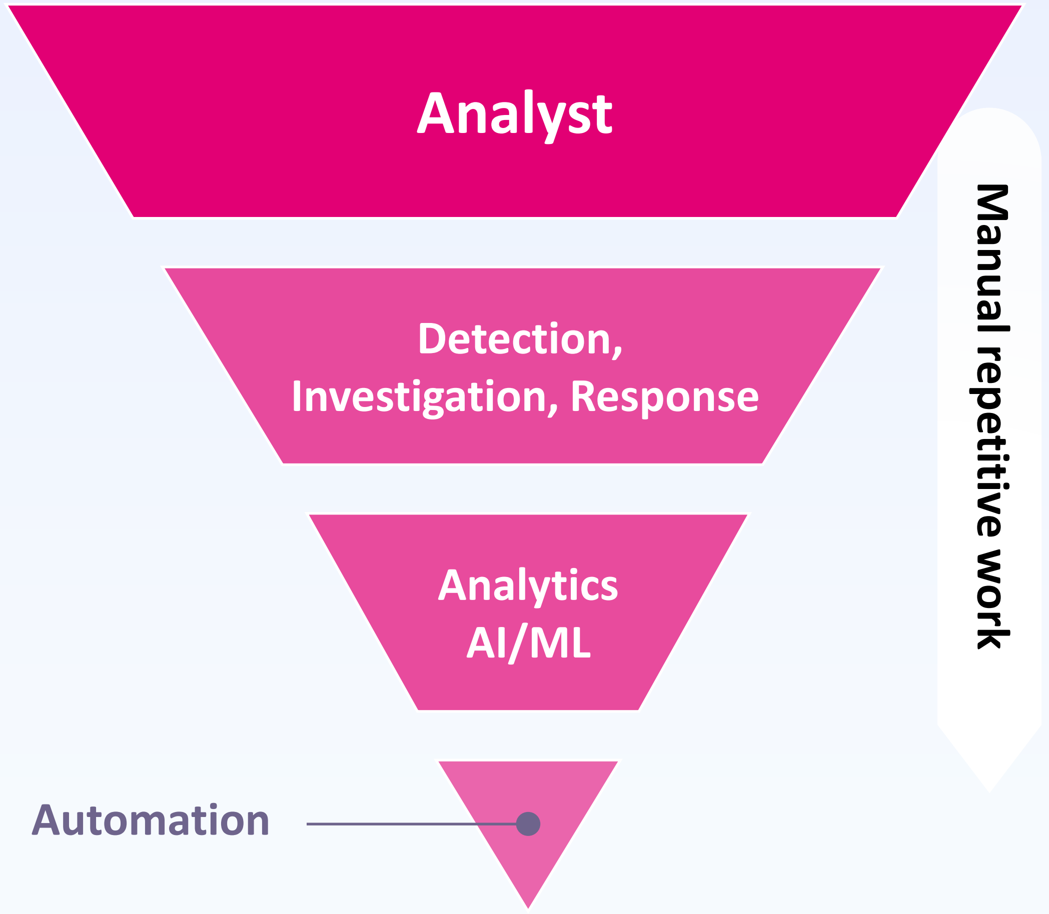
Source: Kaspersky 2024, ERMprotect; National Cyber Security Centre 2024

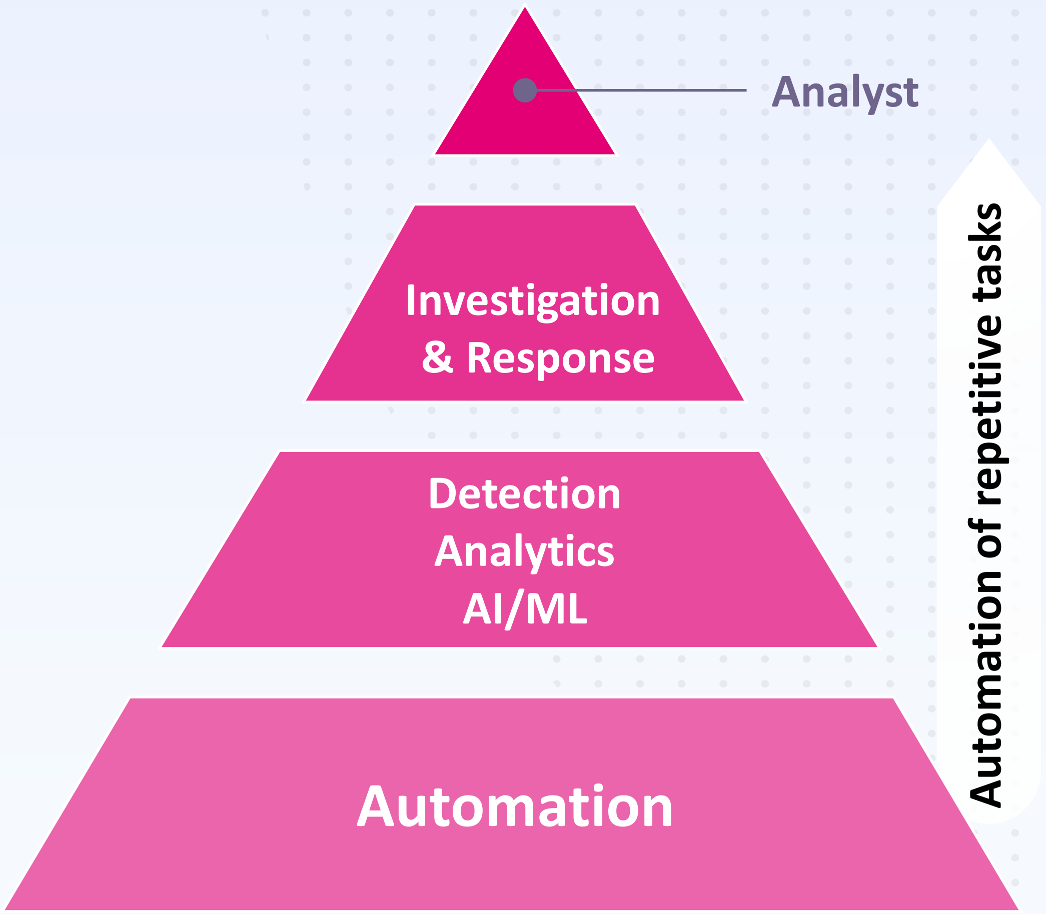
# Secure AI Usage

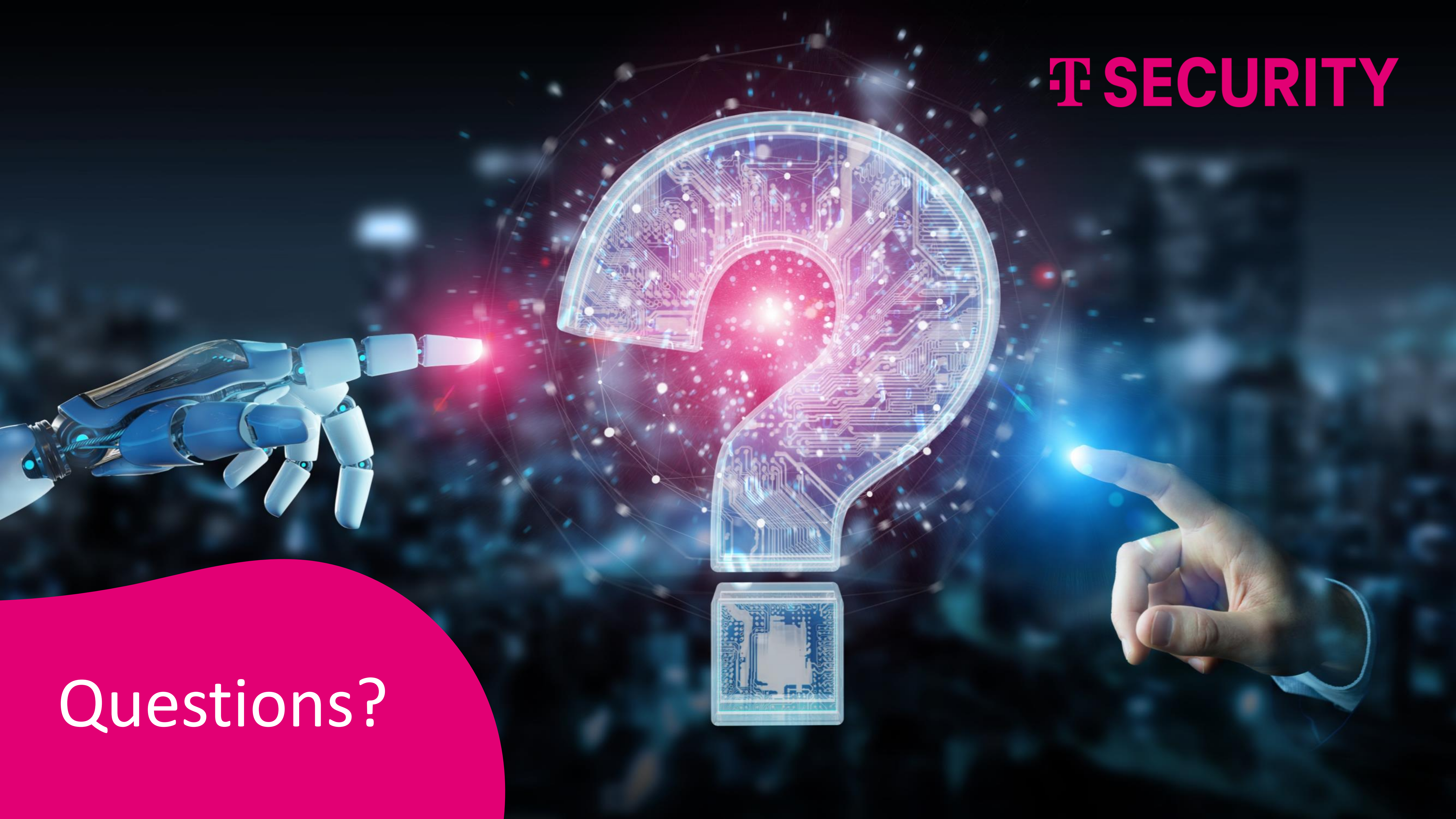
| Description | Security – Stakeholders should consider… |
|---|---|
| **Application** | • Aditional attack vectors – as AI is accessabel via different endpoints<br>• Additional security risks accosiated with AI-application<br>• Possibility of data breaches and privacy violations |
| **Prompt** | • Prompt injections (models are instructed to deliver false or bad responses)<br>• Manipulation of prompts might lead to unauthorized access to content |
| **Foundation model** | • Monitor foundational model behavior and outputst → Identify anomalies , attacks, or deviations from expected performance<br>• Provide support for private models or sandboxes → Ensure isolation and privacy of sensitive information<br>• Implement model-level filters to Safeguard data, reduce bias<br>• Enhance overall integrity of model outputs |
| **Application** | • Ensure appropriate use of sensitive/proprietary data<br>• Maintain direct control over handlung this data handling<br>• Tailor incident response plans (specifically data brech incidents)<br>• And outline clear, effective procedures to ensure timely and efficient response |
| **Humans aspect** | • Humans play a crucial role as they play a part in many aspects mentioned above<br>• Employees must be trained to minimize risk of sensitive data loss through careless prompts |

Source: Accenture 2023

# Example: SOC Workflow now and then







# Questions?

# Let‘s connect!

**Siegfried Schauer**
ziggy@telekom.com