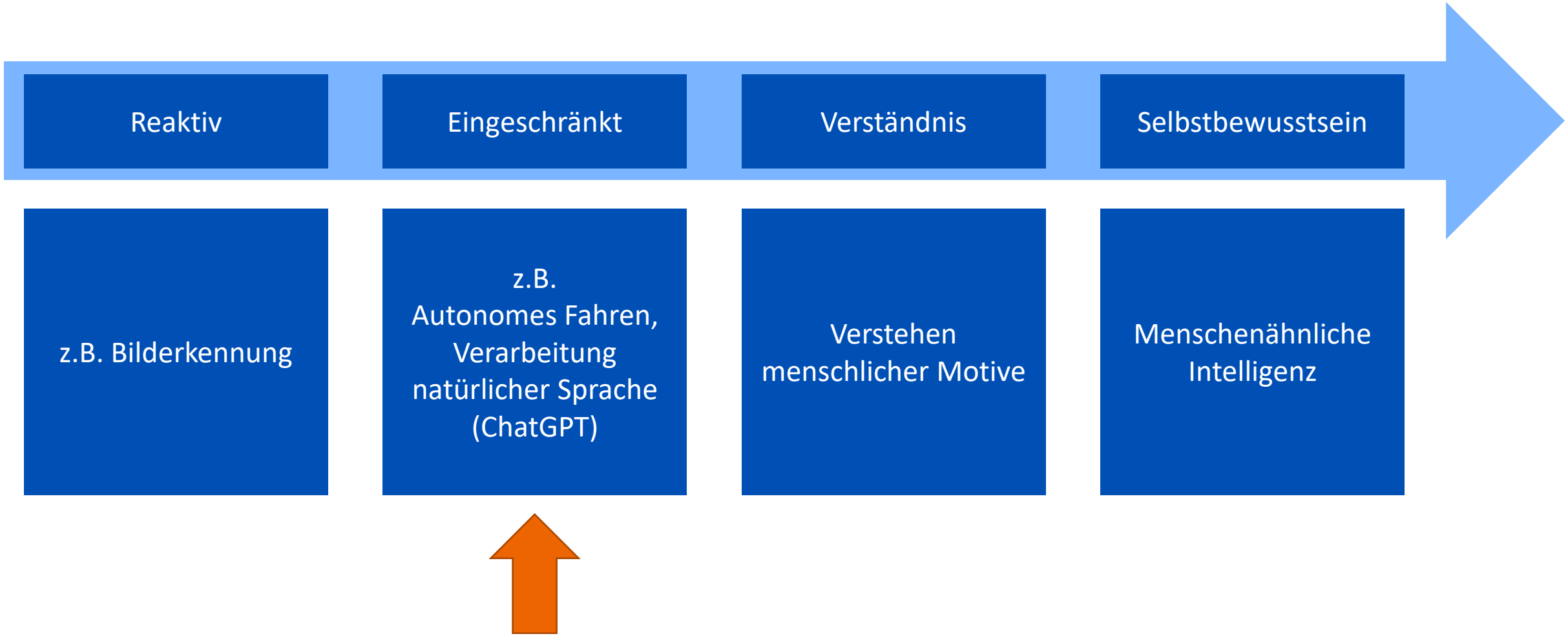
Neue Gefahren und Chancen durch KI in der Cyber Security

Michael Veit
Technology Evangelist, SOPHOS

November 2023

SOPHOS

Entwicklungsstufen von KI

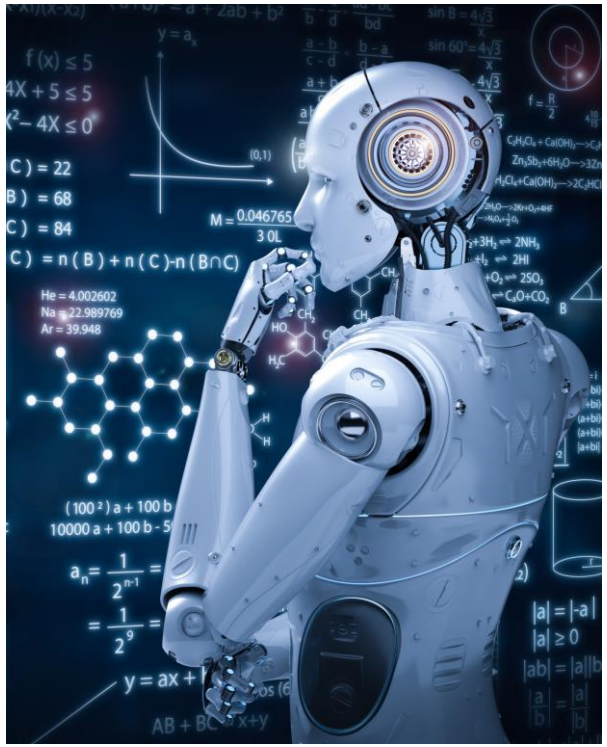


Wie funktioniert ChatGPT?

1. Statistische Analyse der Frage
   - Aufteilung in Bestandteile/Tokens
   - Identifizierung von Beziehungen zwischen Tokens
2. Traditionelle Suche
3. Generierung der Antwort

*„… Antworten auf Fragen klingen bei ChatGPT (..) oft plausibel, basieren aber letztlich **nicht auf menschlichem Verstehen**, sondern auf einer **statistischen Verteilung** über Wort-Zusammenhänge.“*
Dr. Nikolas Müller, Fraunhofer AISEC

⇨ Statistik



manager magazin

Abonnement | Anmelden

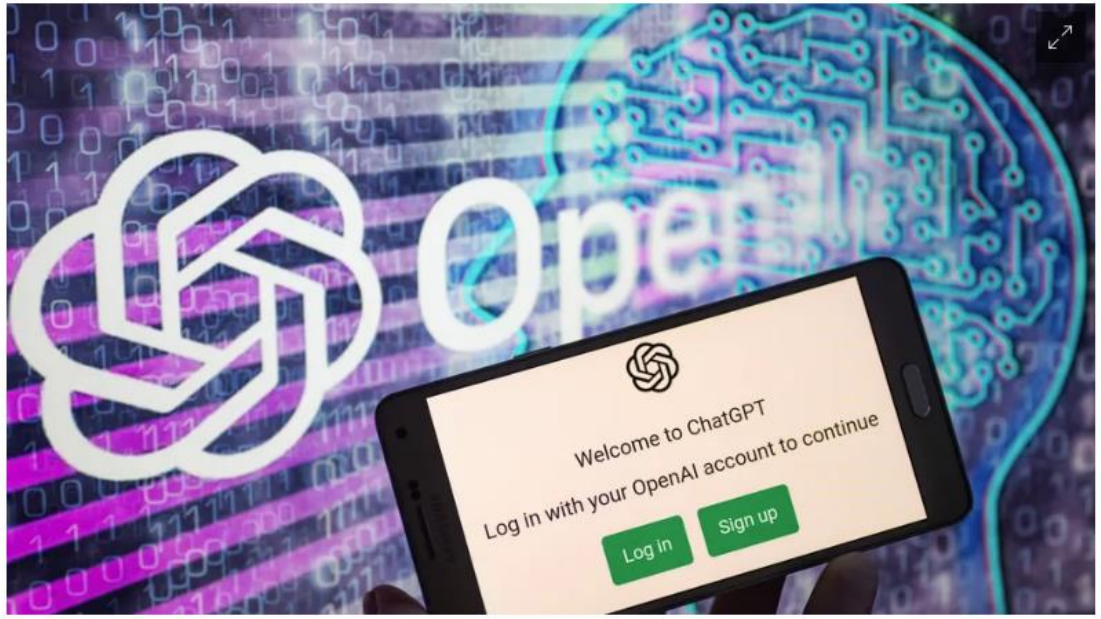
Menü | Unternehmen > Tech > Microsoft > ChatGPT: Microsoft will offenbar zehn Milliarden Dollar in OpenAI investieren

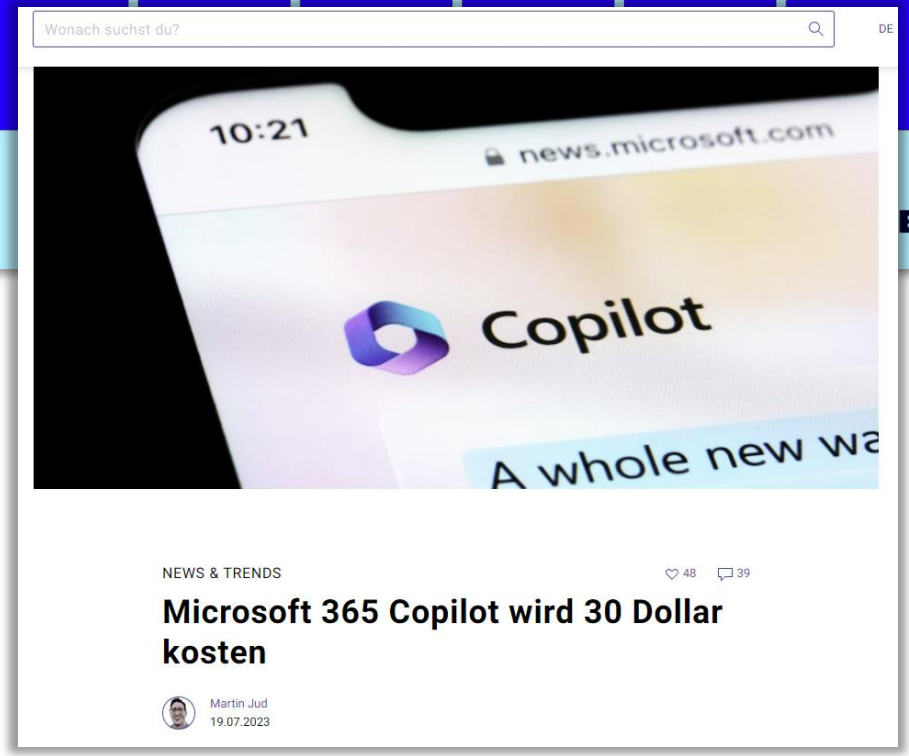
OpenAI

Microsoft will zehn Milliarden Dollar in ChatGPT-Macher investieren

Microsoft soll seit Monaten mit OpenAI über eine Beteiligung verhandeln. Offenbar will sich der Softwarekonzern knapp 50 Prozent an dem Entwickler der Chatbot-Software ChatGPT sichern und plant dazu eine milliardenschwere Investition.

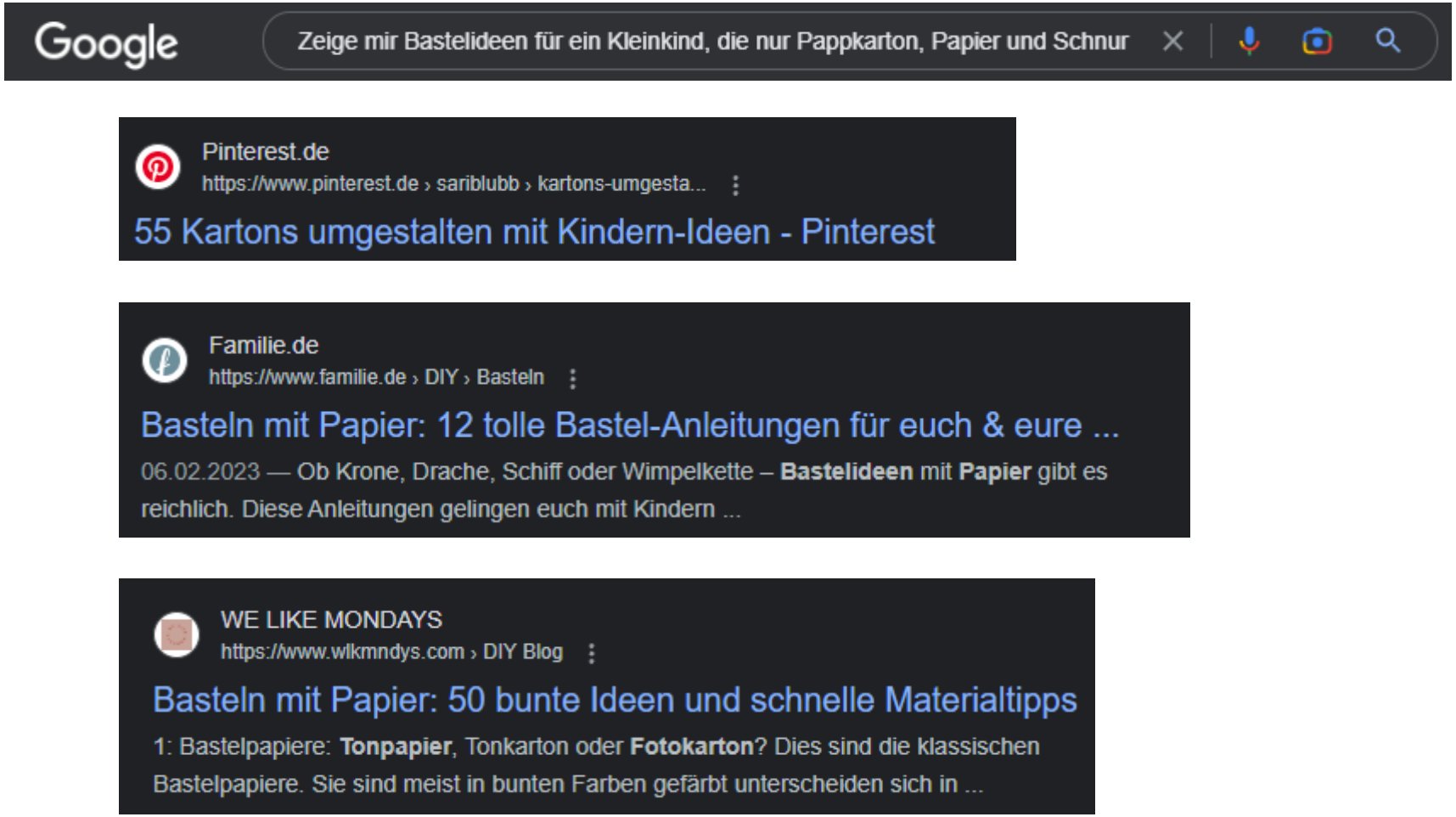
10.01.2023, 11.49 Uhr



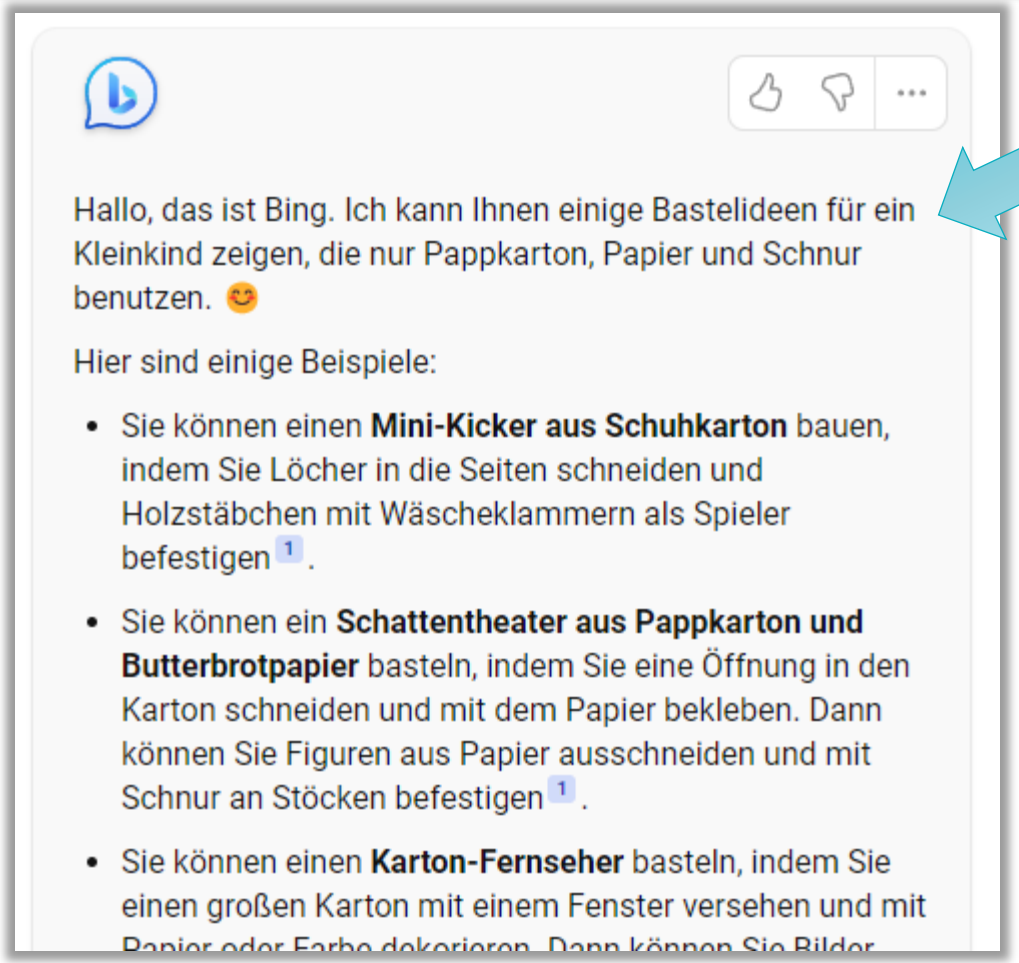


SOPHOS

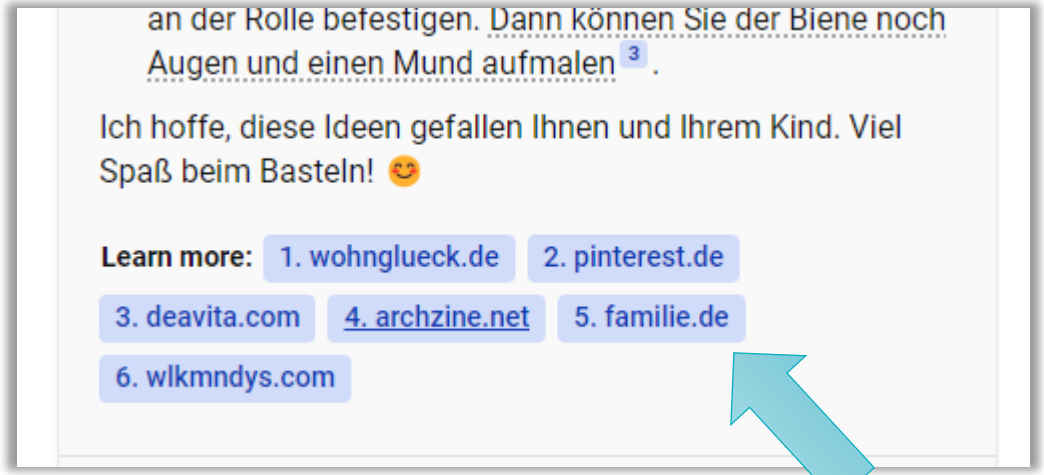
Traditionelle Google-Suche



ChatGPT4 in Bing



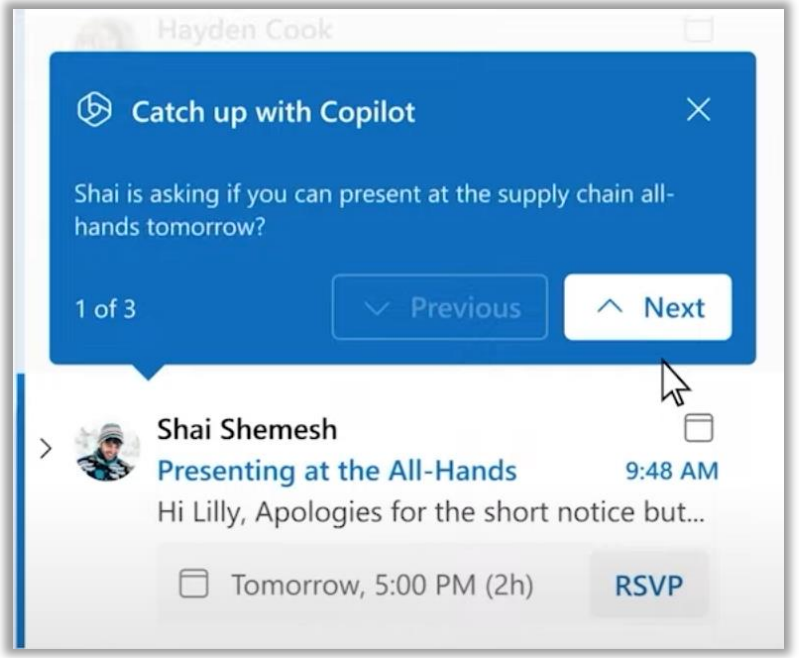
Wiederholung der Token / „was hat ChatGPT verstanden“



Gleiche Quellen wie bei Google-Suche

Wo ist ChatGPT eine Chance?

- Interaktive Inhaltssuche
  - Suchmaschinen
  - Chatbots
  - z.B. Expedia Plugin in ChatGPT
- Generierung von Code, Texten und Bildern
  – ohne Vorkenntnisse
- Zusammenfassung komplexer Vorgänge
- Vereinfachung / Automation wiederkehrender Tätigkeiten
  -> „500 Emails nach dem Urlaub durchsehen“

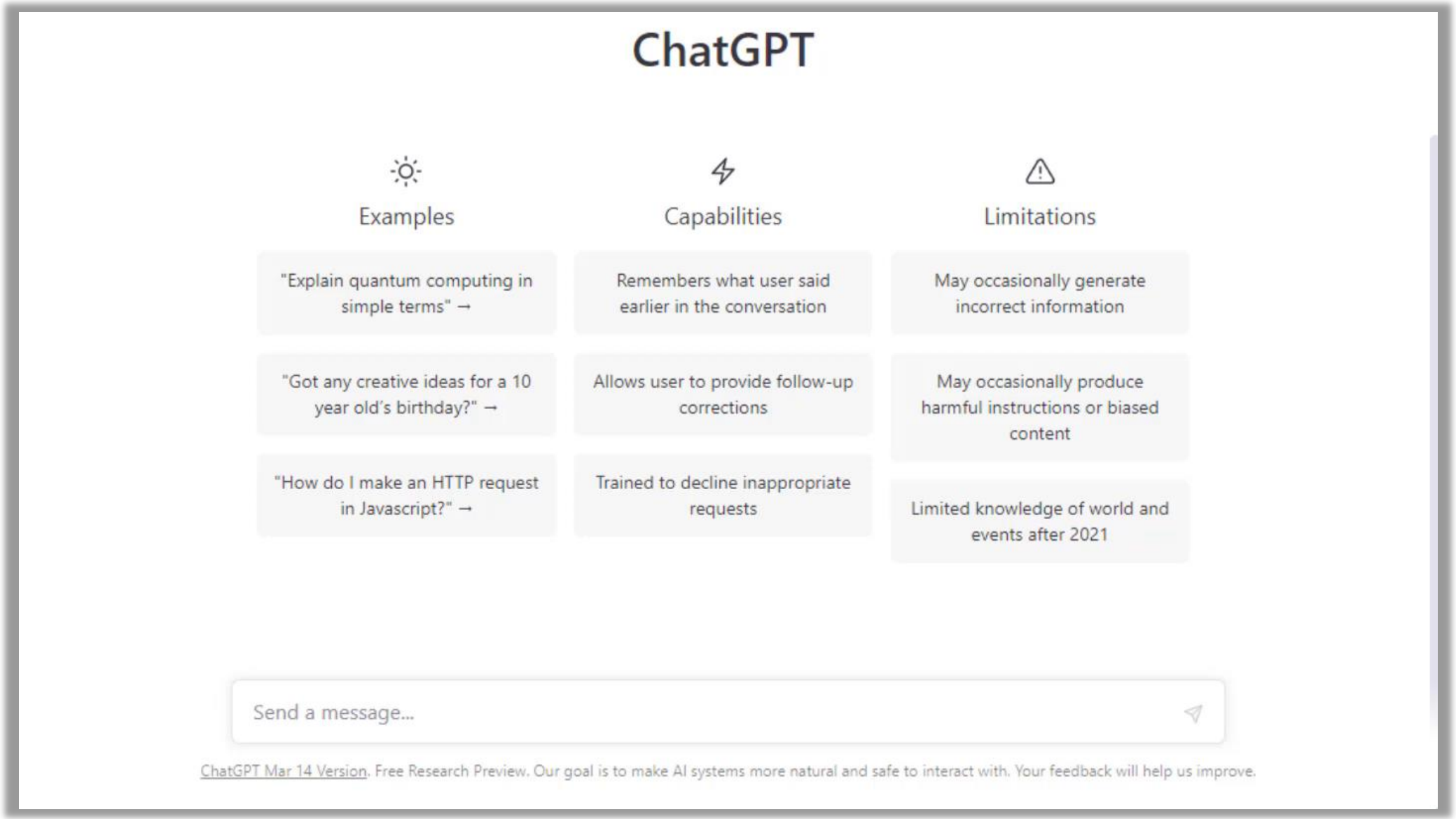


Quelle: Microsoft

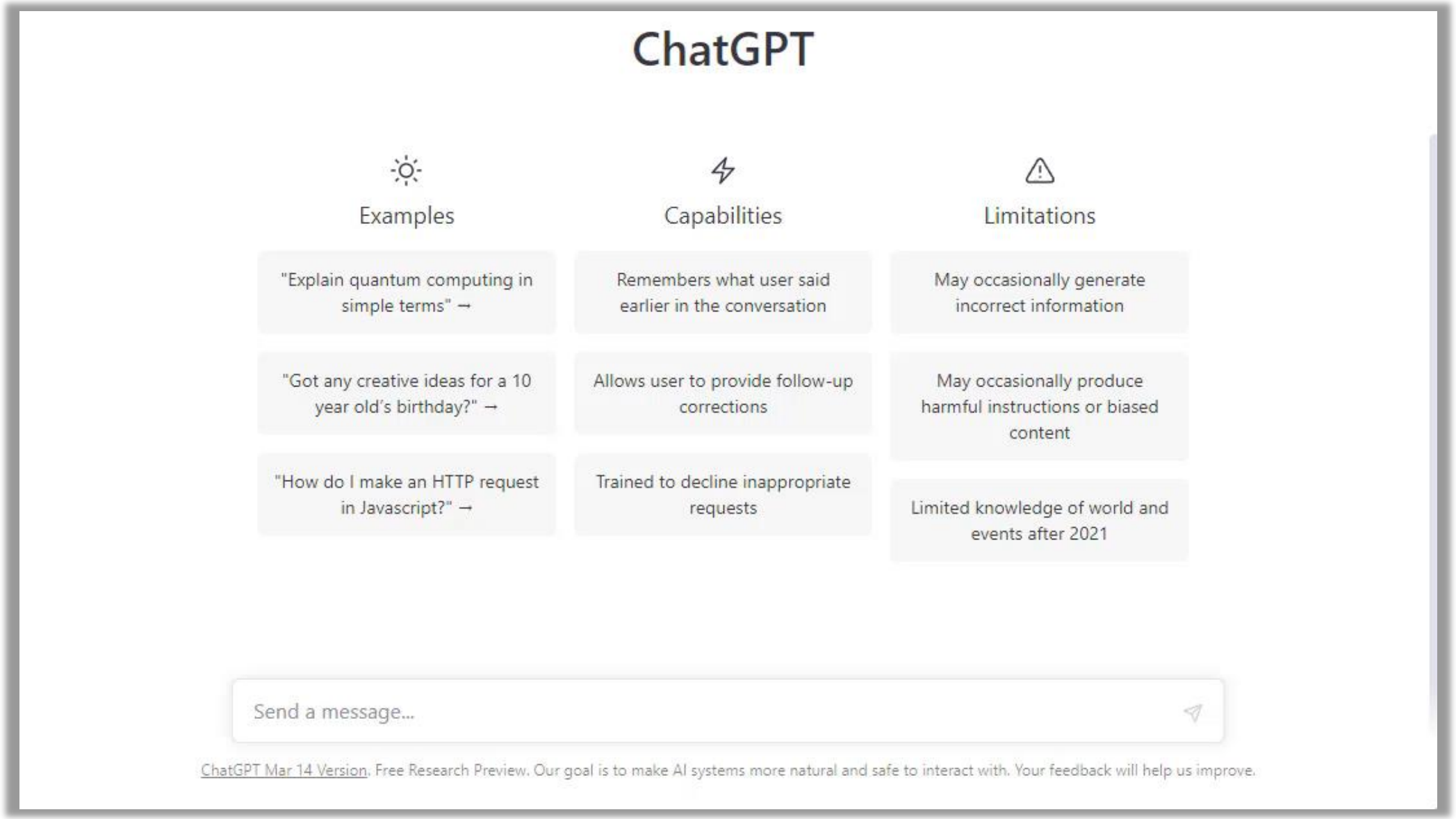
„It will replace tasks, not jobs“ - Tech Journalist, BBC

Neuer Job: Prompt Engineer

Phishing-Email



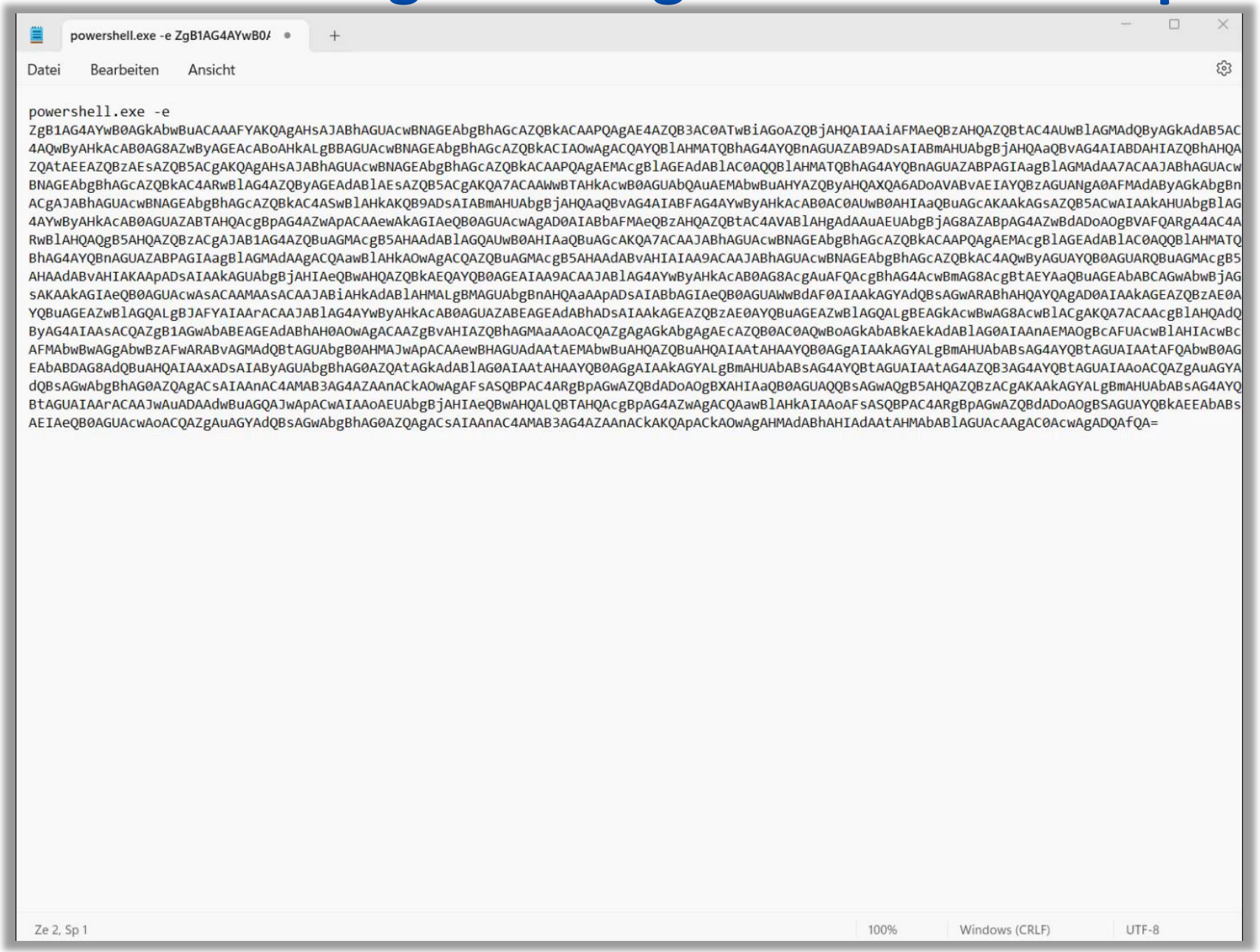
Ransomware


ChatGPT
Examples
"Explain quantum computing in simple terms" →
"Got any creative ideas for a 10 year old's birthday?" →
"How do I make an HTTP request in Javascript?" →
Capabilities
Remembers what user said earlier in the conversation
Allows user to provide follow-up corrections
Trained to decline inappropriate requests
Limitations
May occasionally generate incorrect information
May occasionally produce harmful instructions or biased content
Limited knowledge of world and events after 2021
Send a message...
ChatGPT Mar 14 Version. Free Research Preview. Our goal is to make AI systems more natural and safe to interact with. Your feedback will help us improve.

Wo kann ChatGPT eine Bedrohung sein?

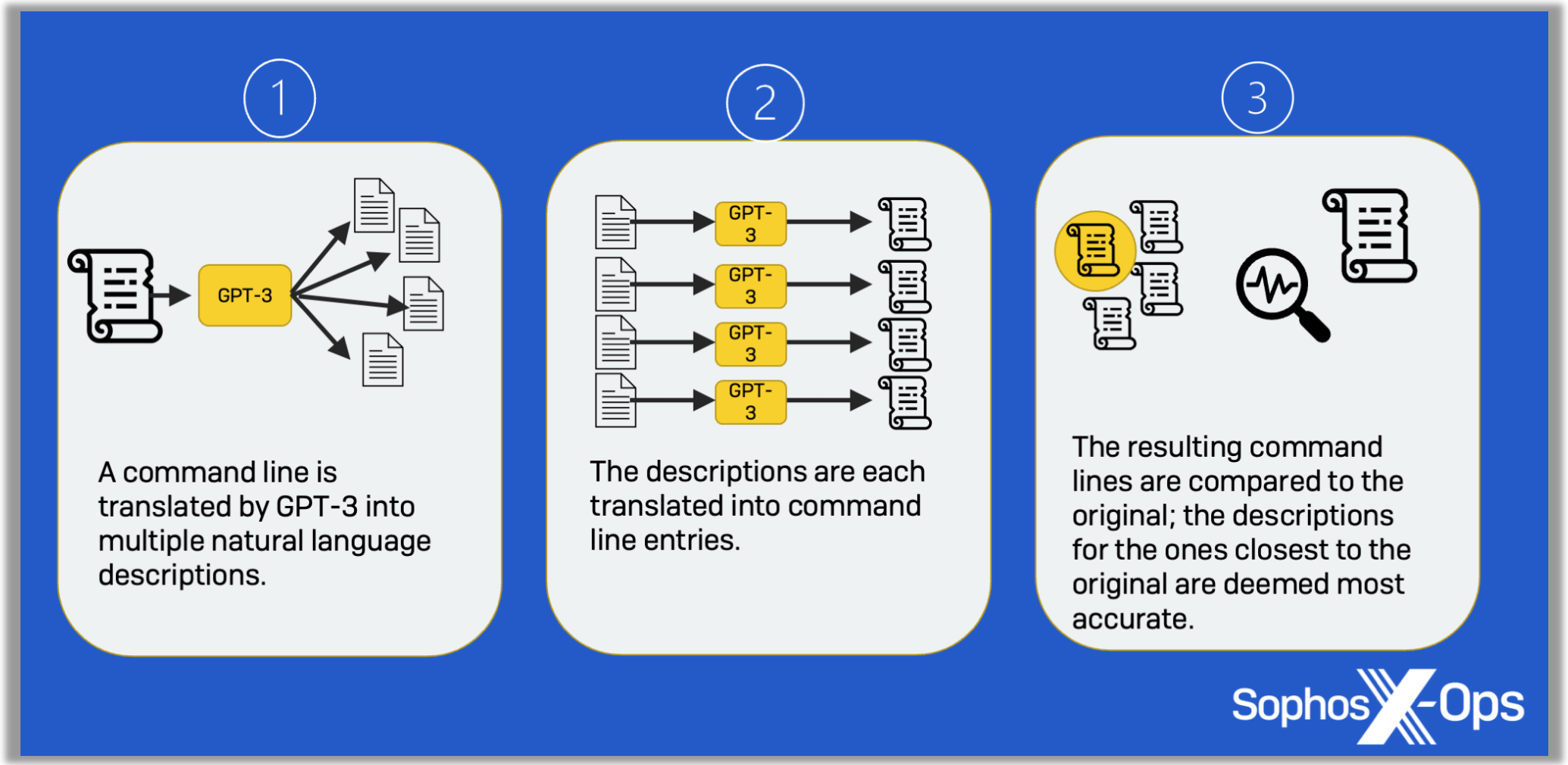
- Phishing Emails Reloaded
- Skript-Malware schreiben
- Code Debugging -> Exploits finden
- Für Profis ändert sich wenig
- Amateure bekommen mächtige neue Werkzeuge

ChatGPT übersetzt mögliche Angriffsaktivität in Sprache



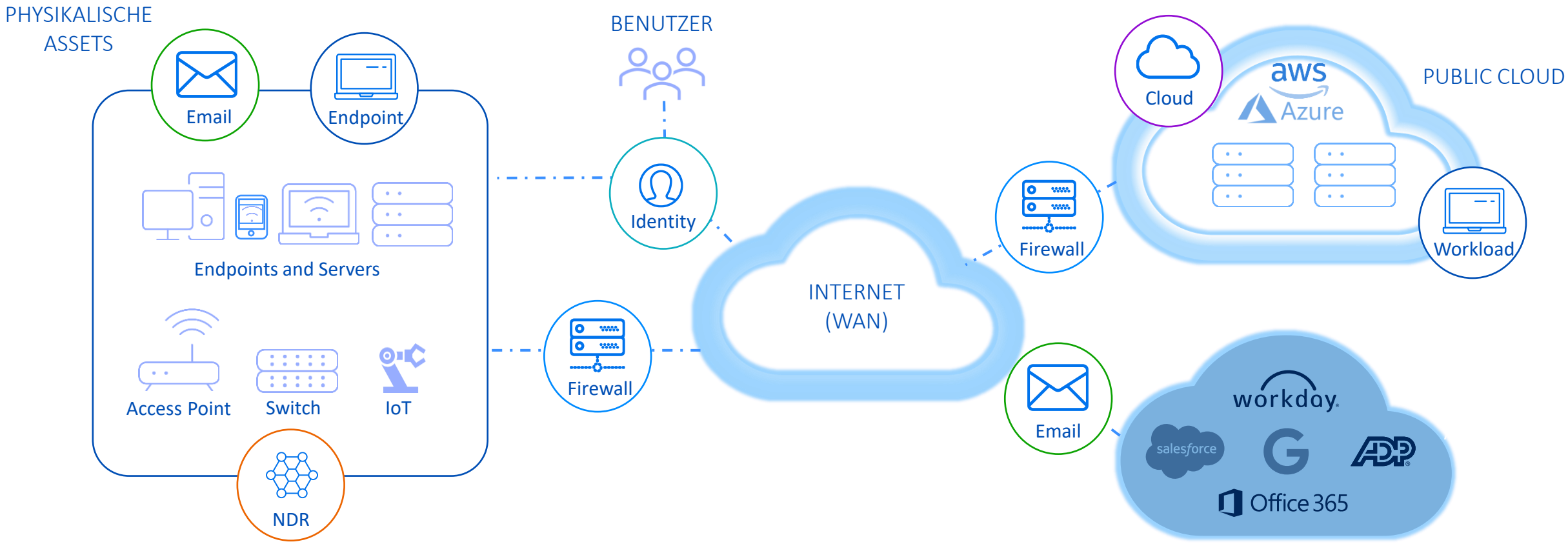
SOPHOS

ChatGPT übersetzt mögliche Angriffsaktivität in Sprache



https://news.sophos.com/en-us/2023/03/16/gpt-for-you-and-me-applying-ai-language-processing-to-cyber-defenses/

Sicherheitslösungen verteilt in der gesamten Umgebung



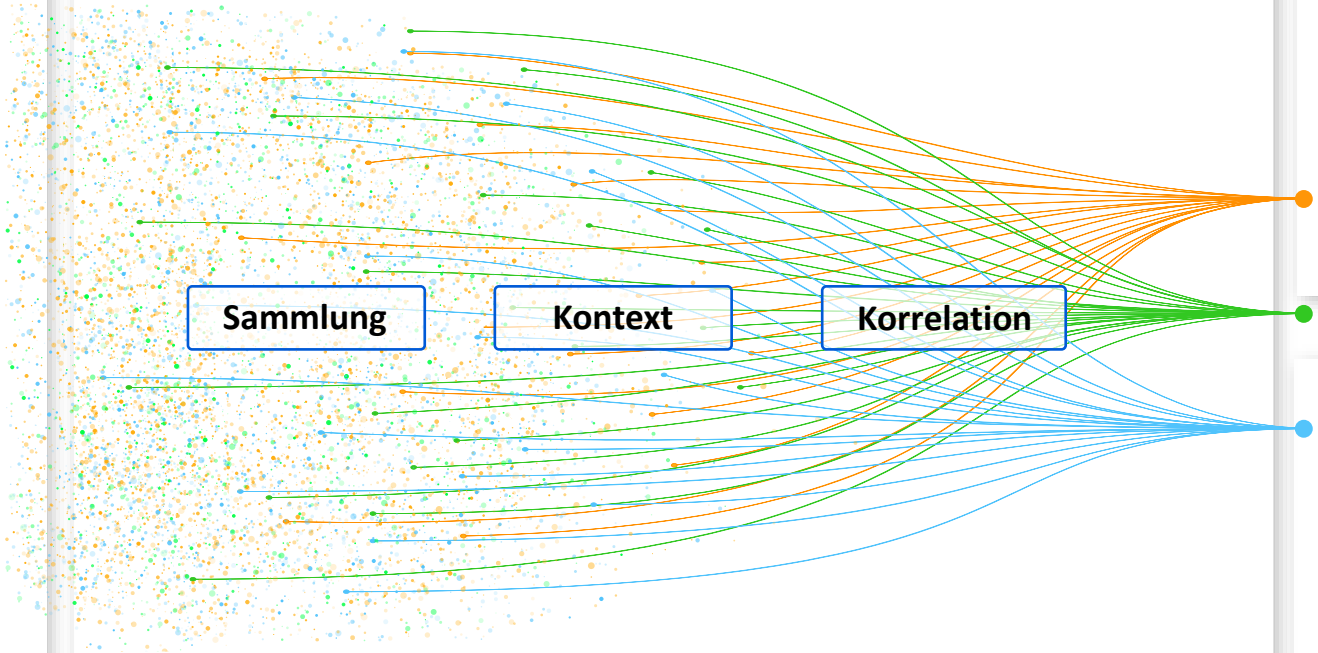
Herausforderung Detection and Response

Telemetriequellen

- Endpoint
- Firewall
- Email
- Cloud
- NDR
- Identität
- Microsoft

Bedrohungsanalyse und Korrelation

Sophos XDR Data Lake



Threat Intelligence + Automatische Reaktion + Erweiterte Analyse

Untersuchung und Reaktion

24/7 Managed Detection and Response Services

Sophos MDR Experten für Bedrohungssuche, Analyse und Reaktion

38 Min Ø Zeit bis zur Behebung

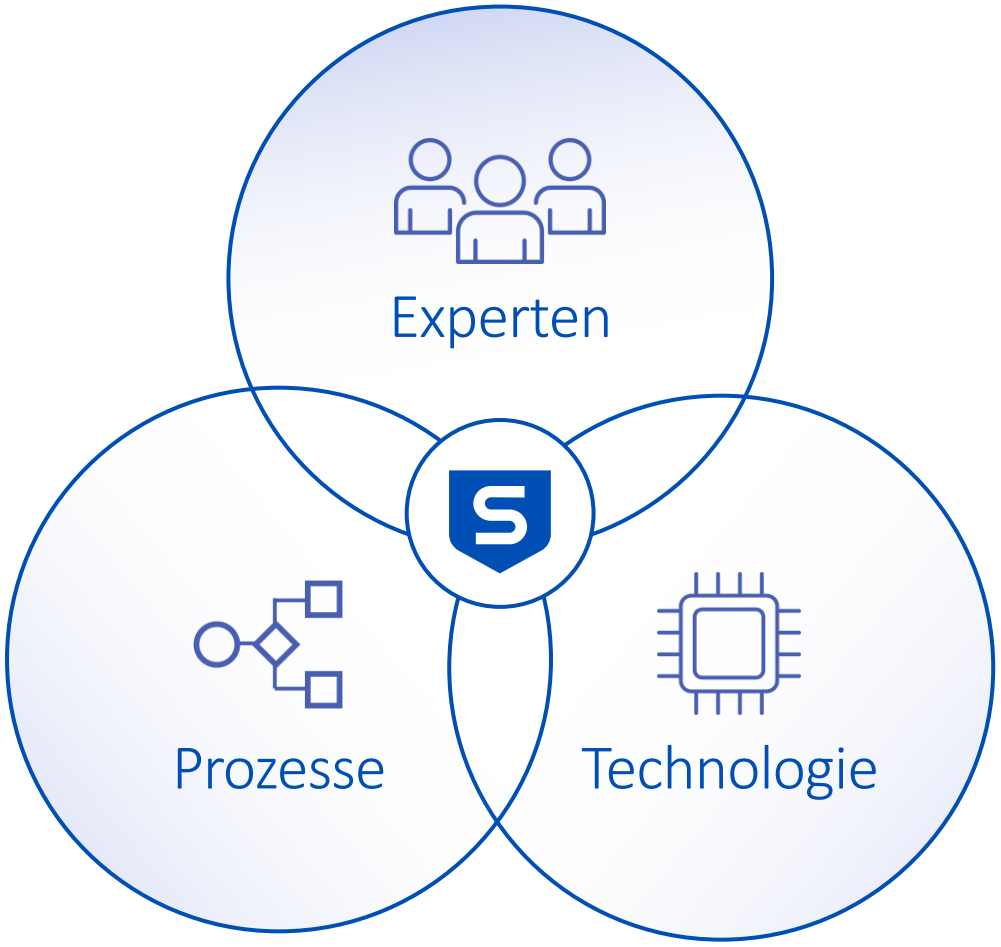
Investigation and Response Platform für das eigene SOC

Sophos Central als zentrale Plattform für Untersuchung, Reporting und Management

Selbst verwaltet oder zusammen mit dem Sophos MDR Team

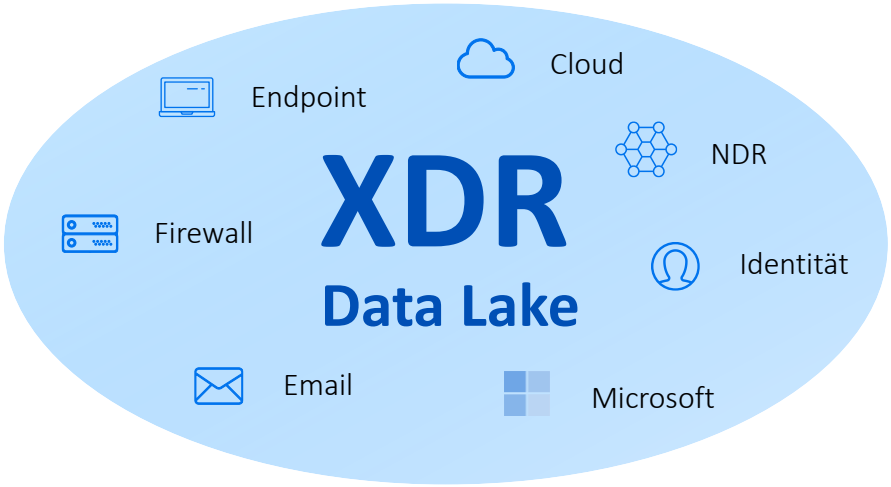
SOPHOS

SOPHOS MDR - Cybersecurity as a Service



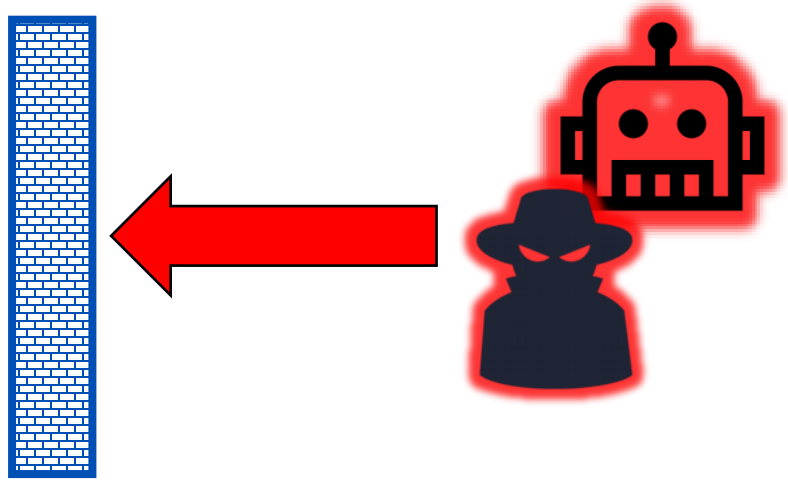
- Proaktive Bedrohungssuche
- 24/7 Erkennung und Reaktion durch Analysten
- Vollständige Ursachenanalyse + Incident Response
- Mehr als 18.000 MDR Kunden
- Telemetrie von mehr als 580.000 Unternehmenskunden
- All-inclusive Service – keine versteckten Kosten
- Bestmögliches Ergebnis für Ihre IT-Sicherheit

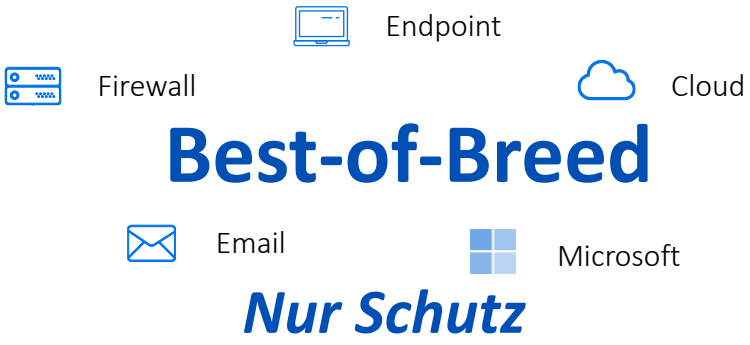
Ist KI also eher Gefahr oder Chance?



Schutz + Erkennung

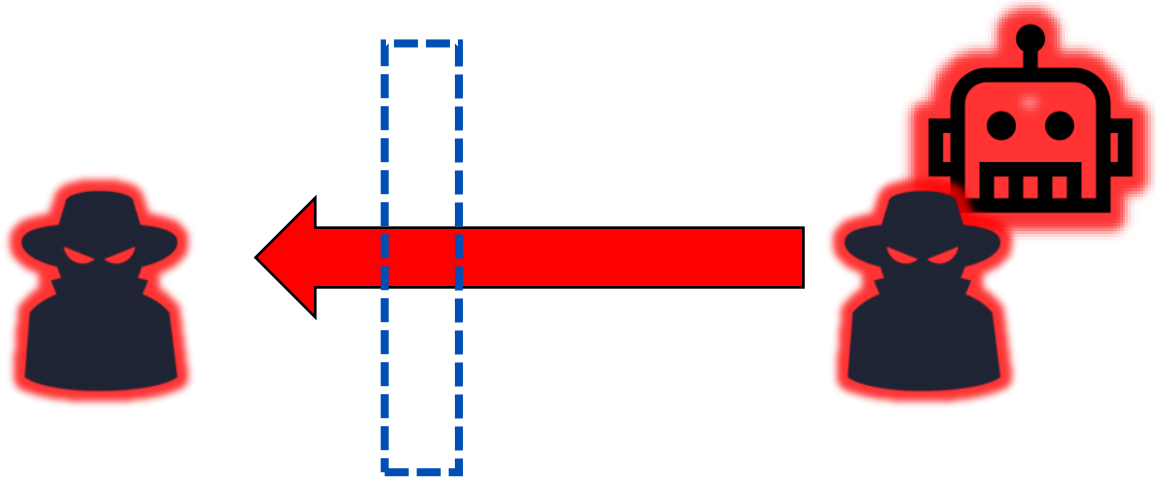
\+ KI + Experten 24/7





Nur Schutz

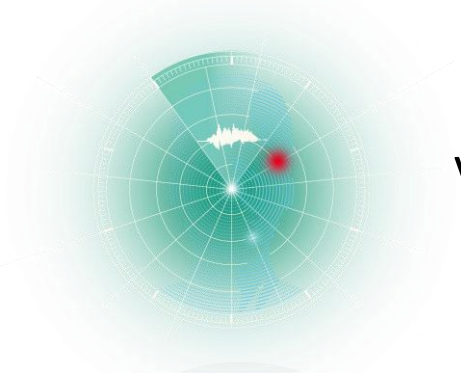
\+ IT 8/5



SOPHOS

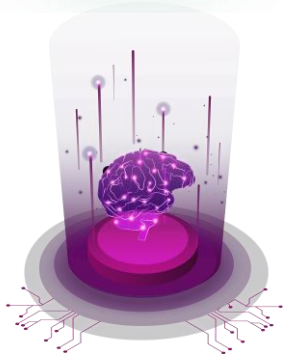
Sophos KI - ai.sophos.com/projects/

Next-Gen Web



Verhaltenserkennung

Infrastruktur



KI Forschung

Phishing Erkennung

XDR / MDR:

- Korrelation von Ereignissen
- Analyst Experience/Assistance

Die nächsten Schritte

Sophos Intercept X Advanced with XDR

Sophos Intercept X Advanced with XDR erfasst neben Endpoint- und Server-Informationen auch Netzwerk-, E-Mail-, Cloud- und mobile Datenquellen und bietet Ihnen so ein noch umfassenderes Bild Ihrer Cybersicherheit

Zum Datenblatt

Sophos AI

Sophos hat bereits seit einigen Jahren Maschine Learning in Lösungen integriert. Die weitere Entwicklung mit AI in den Bereichen Next Gen Web, Behavioral Detection, Infrastucture, Interpretable ML als auch Phishing Detection können Sie live mit verfolgen.

ai.sophos.com/projects/

Sophos MDR

24/7 Schutz vor Cyberangriffen – mit Ihrem persönlichen MDR-Service: Weitere Informationen zu unserer Lösung Sophos MDR erhalten Sie auf unserer Produktseite.

sophos.de/mdr

Kontakt

Wenn Sie Fragen haben oder Unterstützung benötigen, ist Ihr Sophos-Ansprechpartner gerne für Sie da und hilft Ihnen weiter.

sophos.de/kontakt