

Neue Gefahren und Chancen durch KI in der Cyber Security

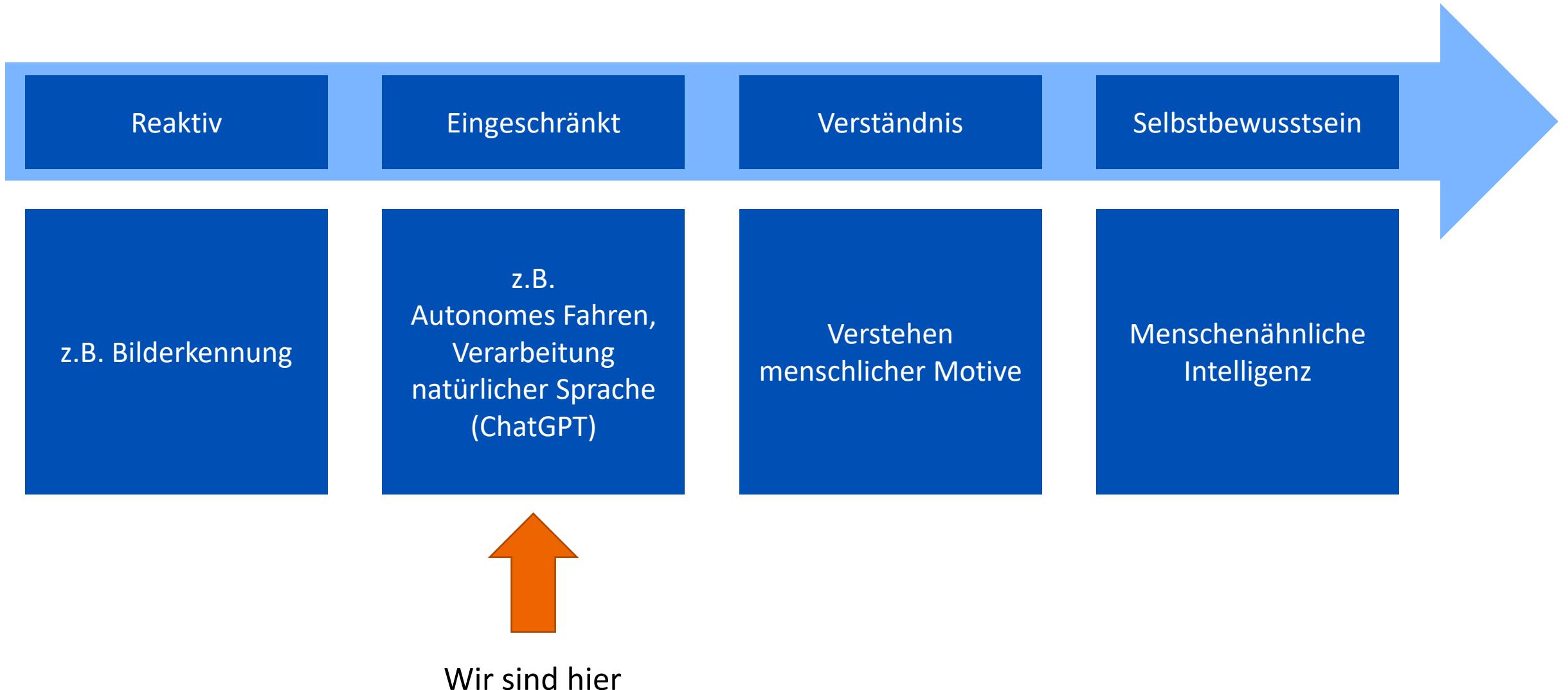
Michael Veit
Technology Evangelist, SOPHOS



November 2023

SOPHOS

Entwicklungsstufen von KI

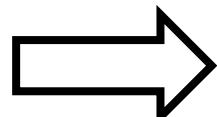


Wie funktioniert ChatGPT?

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

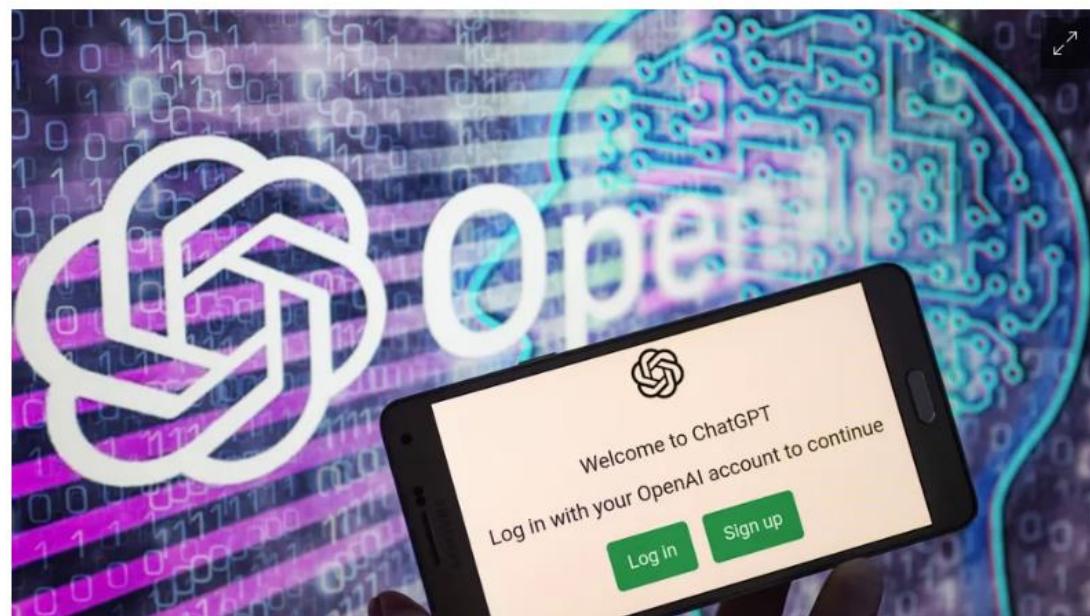


[OpenAI](#)

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



Google Ad Revenue (2019–2024)



Source: eMarketer



NEWS & TRENDS

Microsoft 365 Copilot wird 30 Dollar kosten

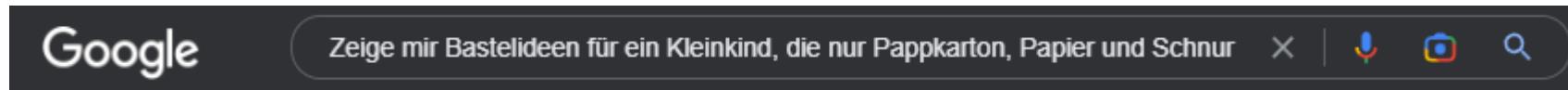
Martin Jud
19.07.2023

48

39

BERLO**SOPHOS**

Traditionelle Google-Suche



 Pinterest.de
<https://www.pinterest.de/sariblubb/kartons-umgestalten/> ::

[55 Kartons umgestalten mit Kindern-Ideen - Pinterest](#)

 Familie.de
<https://www.familie.de/Artikel/DIY/Basteln> ::

[Basteln mit Papier: 12 tolle Bastel-Anleitungen für euch & eure ...](#)

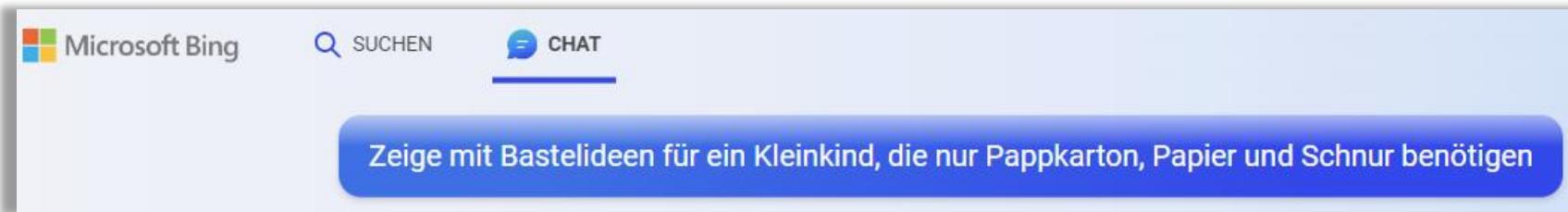
06.02.2023 — Ob Krone, Drache, Schiff oder Wimpelkette – **Bastelideen mit Papier** gibt es reichlich. Diese Anleitungen gelingen euch mit Kindern ...

 WE LIKE MONDAYS
<https://www.wlkmndys.com/Artikel/DIY-Blog> ::

[Basteln mit Papier: 50 bunte Ideen und schnelle Materialtipps](#)

1: Bastelpapiere: **Tonpapier**, Tonkarton oder **Fotokarton**? Dies sind die klassischen Bastelpapiere. Sie sind meist in bunten Farben gefärbt unterscheiden sich in ...

ChatGPT4 in Bing

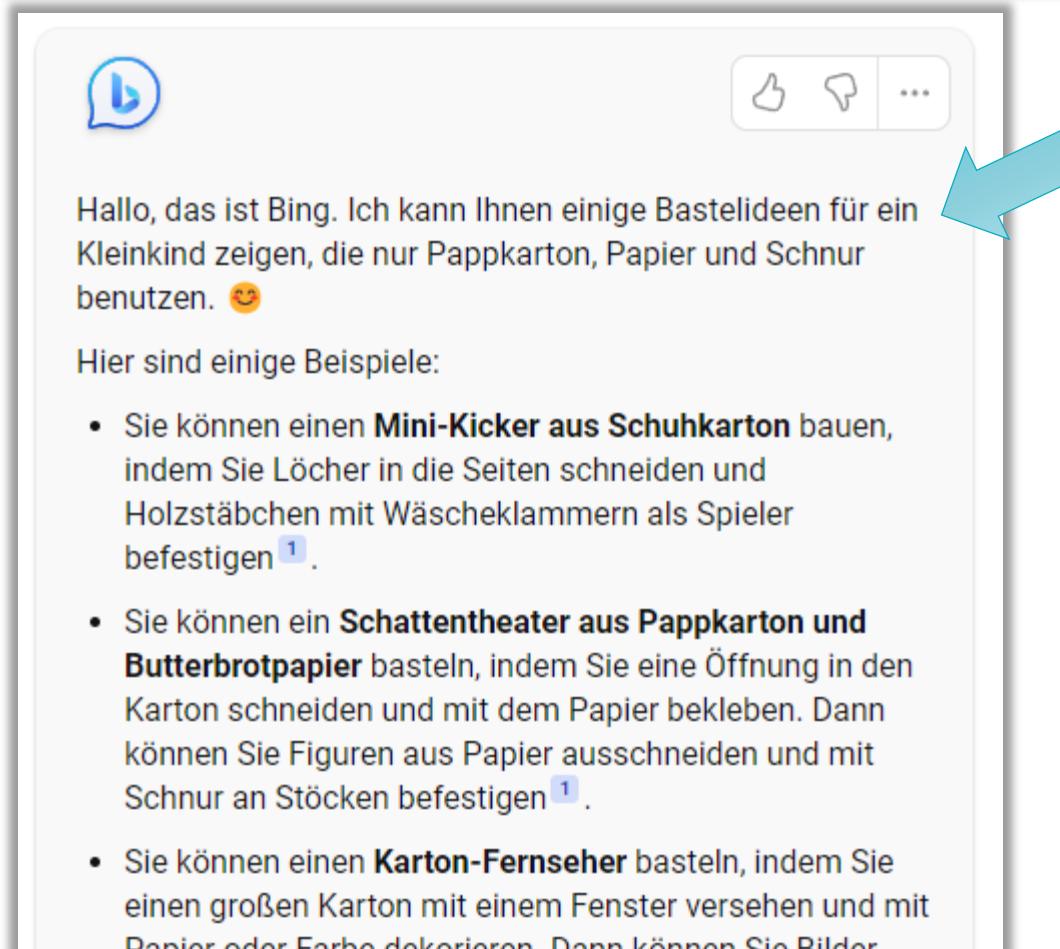


Microsoft Bing

SUCHEN

CHAT

Zeige mir Bastelideen für ein Kleinkind, die nur Pappkarton, Papier und Schnur benötigen

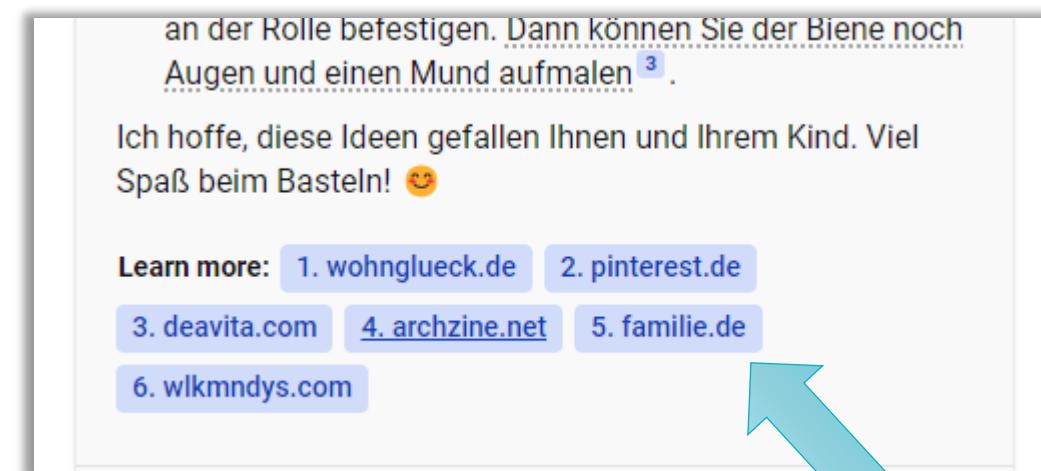


Hallo, das ist Bing. Ich kann Ihnen einige Bastelideen für ein Kleinkind zeigen, die nur Pappkarton, Papier und Schnur benutzen. 😊

Hier sind einige Beispiele:

- Sie können einen **Mini-Kicker aus Schuhkarton** bauen, indem Sie Löcher in die Seiten schneiden und Holzstäbchen mit Wäscheklammern als Spieler befestigen ¹.
- Sie können ein **Schattentheater aus Pappkarton und Butterbrotpapier** basteln, indem Sie eine Öffnung in den Karton schneiden und mit dem Papier bekleben. Dann können Sie Figuren aus Papier ausschneiden und mit Schnur an Stöcken befestigen ¹.
- Sie können einen **Karton-Fernseher** basteln, indem Sie einen großen Karton mit einem Fenster versehen und mit Papier oder Farbe dekorieren. Dann können Sie Bilder

Wiederholung der Token / „was hat ChatGPT verstanden“



an der Rolle befestigen. Dann können Sie der Biene noch Augen und einen Mund aufmalen ³.

Ich hoffe, diese Ideen gefallen Ihnen und Ihrem Kind. Viel Spaß beim Basteln! 😊

Learn more: 1. wohnglueck.de 2. pinterest.de
3. deavita.com 4. archzine.net 5. familie.de
6. wlkmndys.com

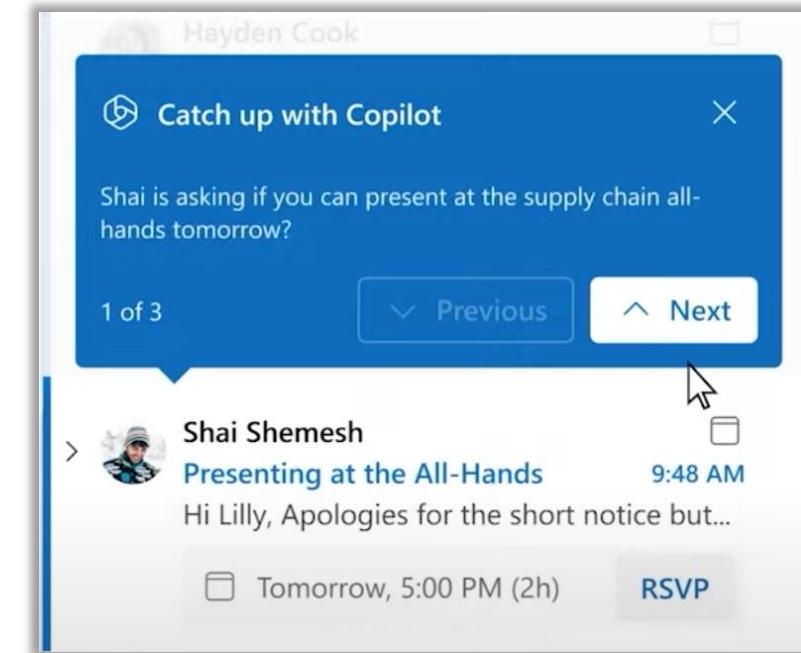
Gleiche Quellen wie bei Google-Suche

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“

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

Neuer Job: Prompt Engineer



Quelle: Microsoft

Phishing-Email

ChatGPT



Examples

"Explain quantum computing in simple terms" →



Capabilities

Remembers what user said earlier in the conversation



Limitations

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

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.

Ransomware

ChatGPT



Examples

"Explain quantum computing in simple terms" →



Capabilities

"Got any creative ideas for a 10 year old's birthday?" →



Limitations

May occasionally generate incorrect information

Allows user to provide follow-up corrections

"How do I make an HTTP request in Javascript?" →

May occasionally produce harmful instructions or biased content

Trained to decline inappropriate requests

Limited knowledge of world and events after 2021

Send a message...

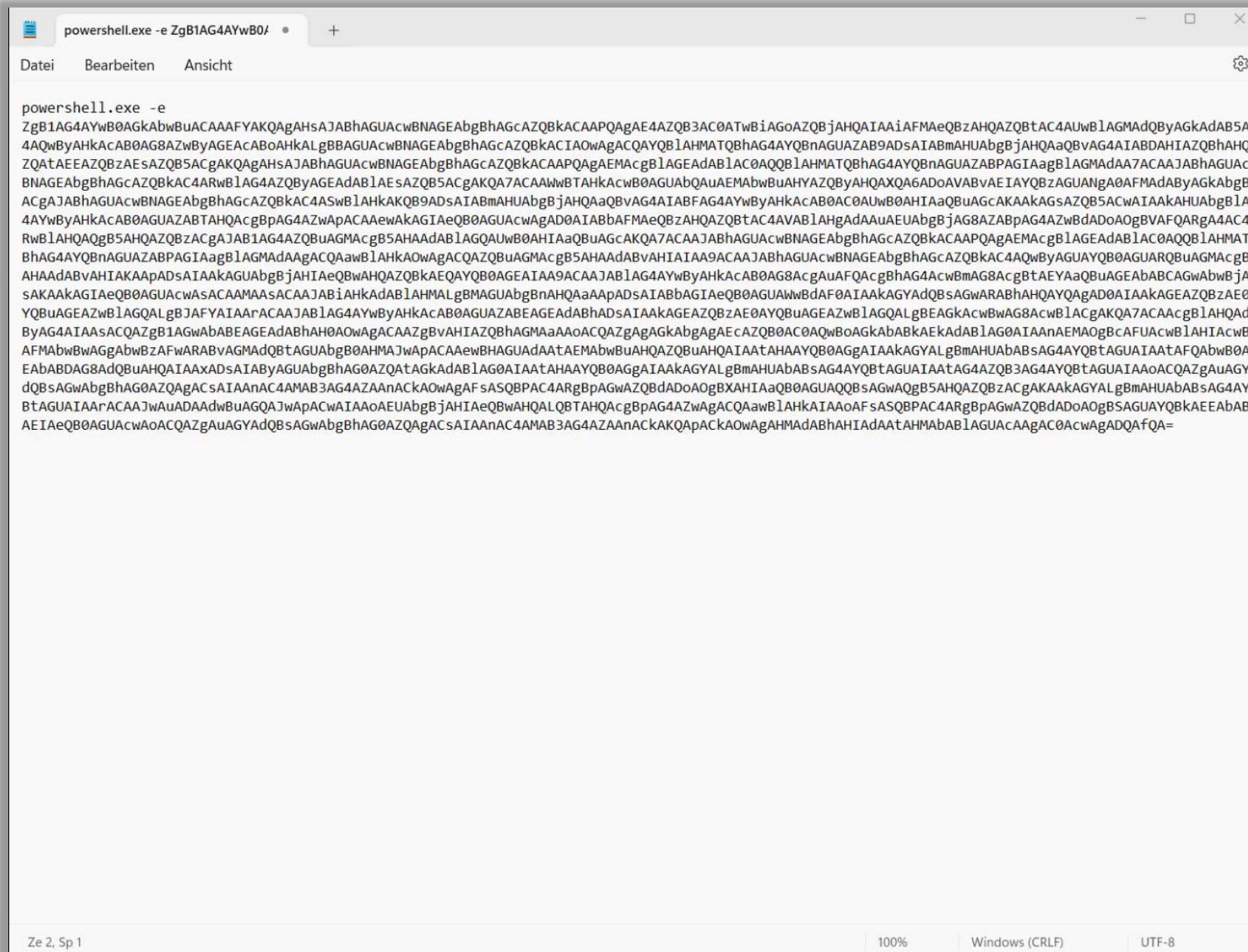


[ChatGPT Mar 14 Version](#). Free Research Preview. Our goal is to make AI systems more natural and safe to interact with. Your feedback will help us improve.

Wo kann ChatGPT eine Bedrohung sein?

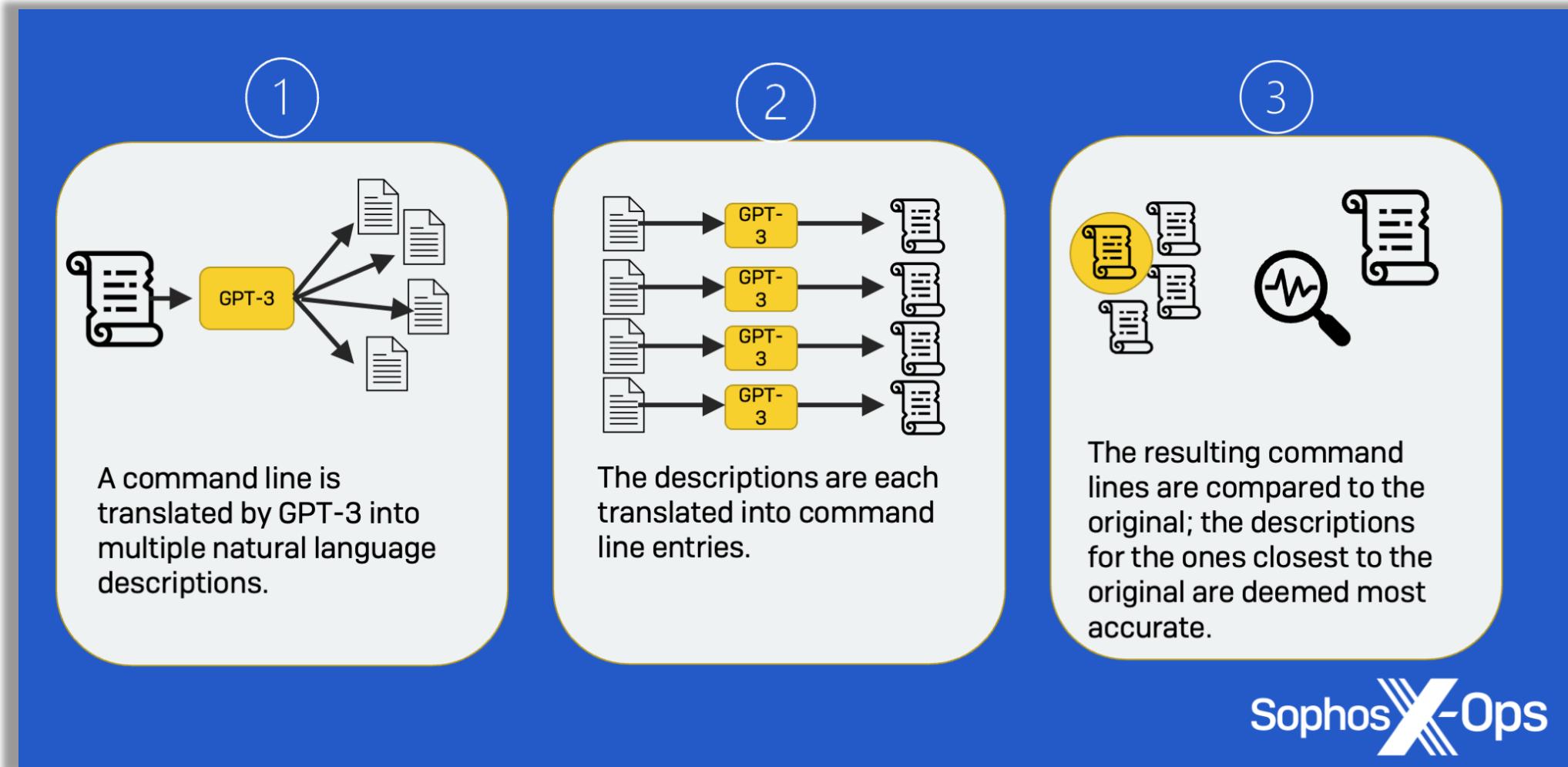
- Phishing Emails Reloaded
- Skript-Malware schreiben
- Code Debugging -> Exploits finden
- Für Profis ändert sich wenig
- Amateure bekommen mächtige neue Werkzeuge

ChatGPT übersetzt mögliche Angriffsaktivität in Sprache



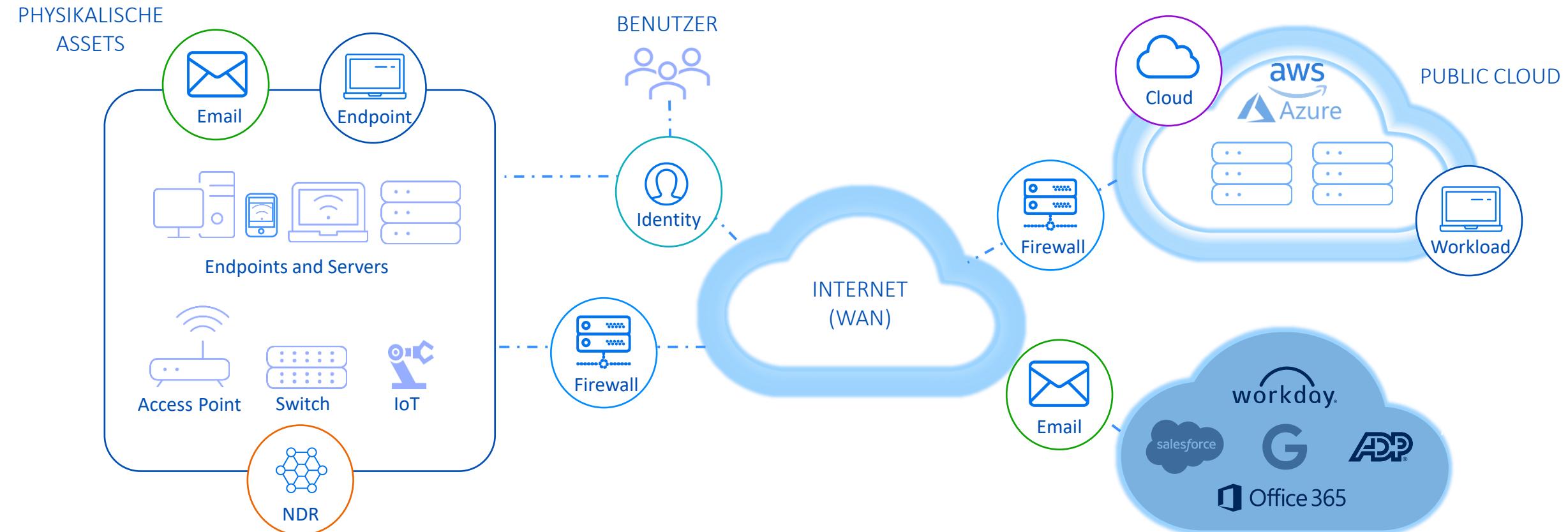
A screenshot of a Windows PowerShell window titled "powershell.exe - e ZgB1AG4AYwB0/". The window contains a single line of extremely long and complex base64-encoded text. The text is a multi-line command, likely a PowerShell script or a series of commands, designed to perform a sophisticated attack. The command is too long to be read in full here but is clearly visible in the window. The window has a standard Windows title bar and a menu bar with "Datei", "Bearbeiten", and "Ansicht". The status bar at the bottom shows "Ze 2, Sp 1", "100%", "Windows (CRLF)", and "UTF-8".

ChatGPT übersetzt mögliche Angriffsaktivität in Sprache

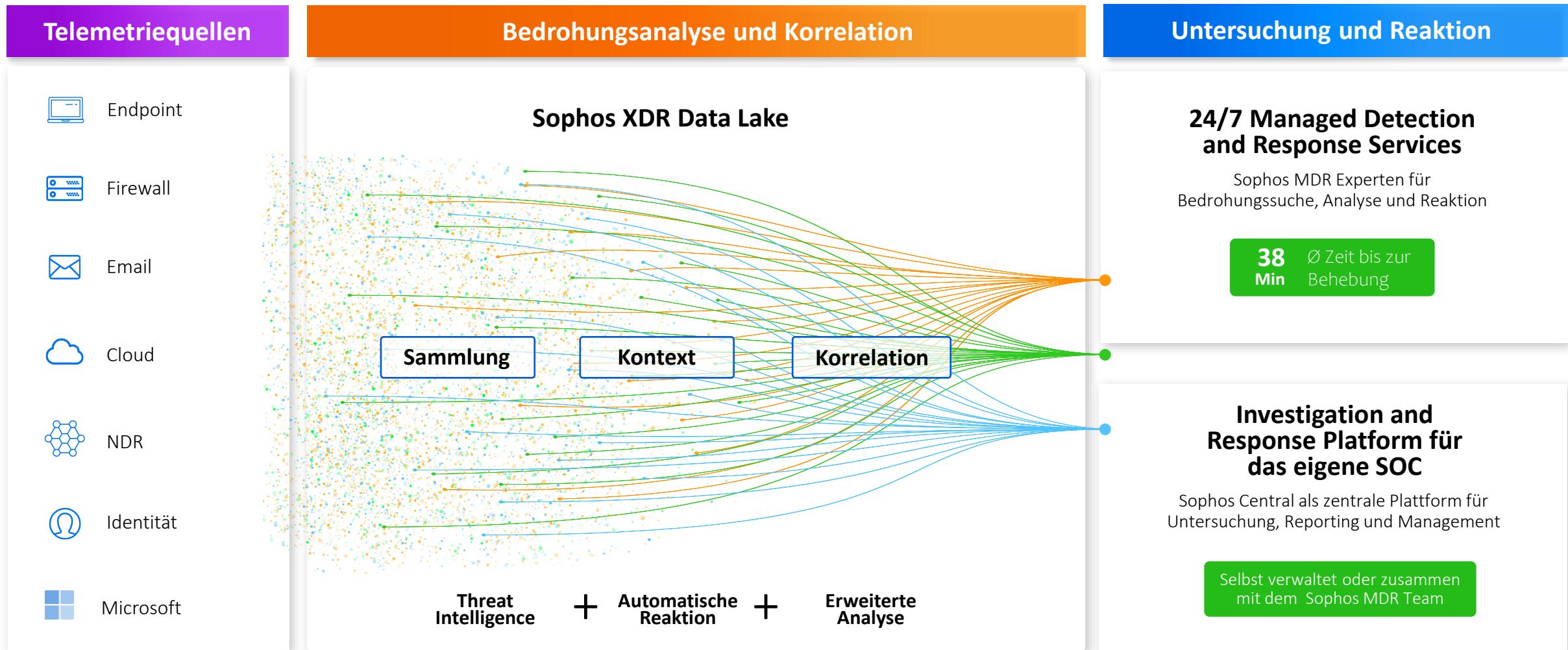


Sophos X-Ops

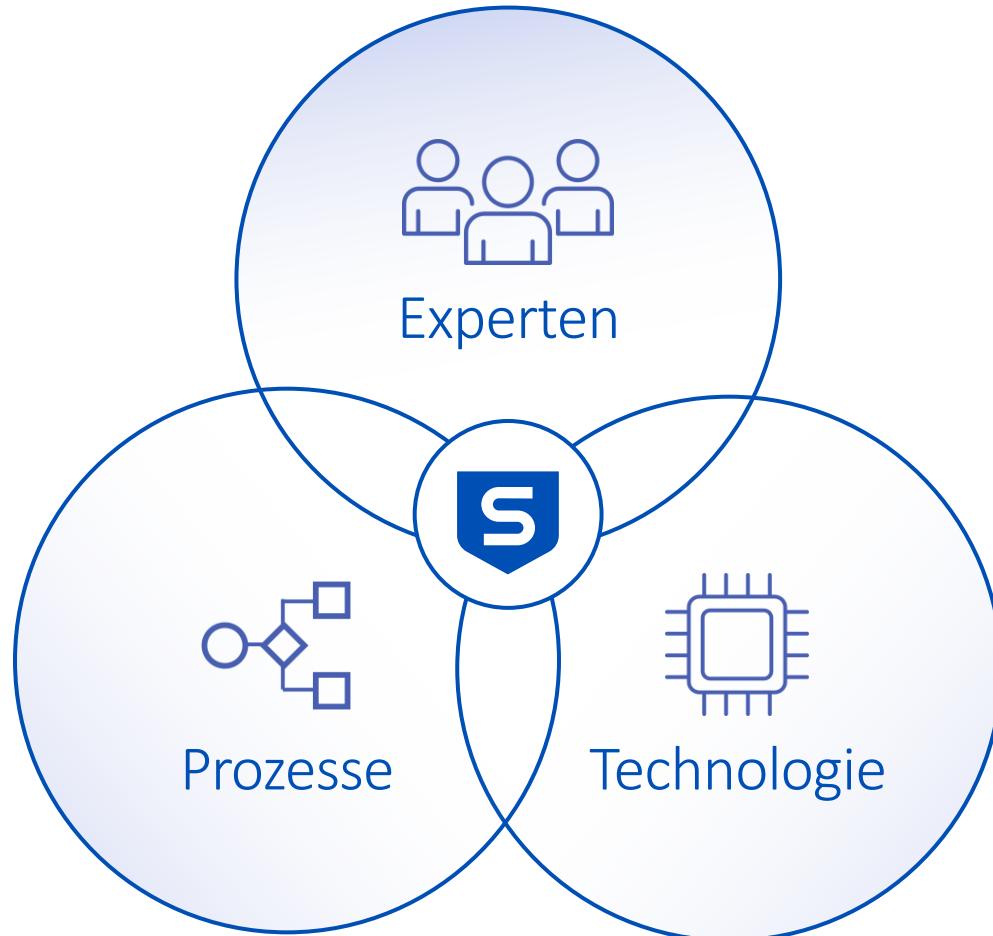
Sicherheitslösungen verteilt in der gesamten Umgebung



Herausforderung Detection and Response

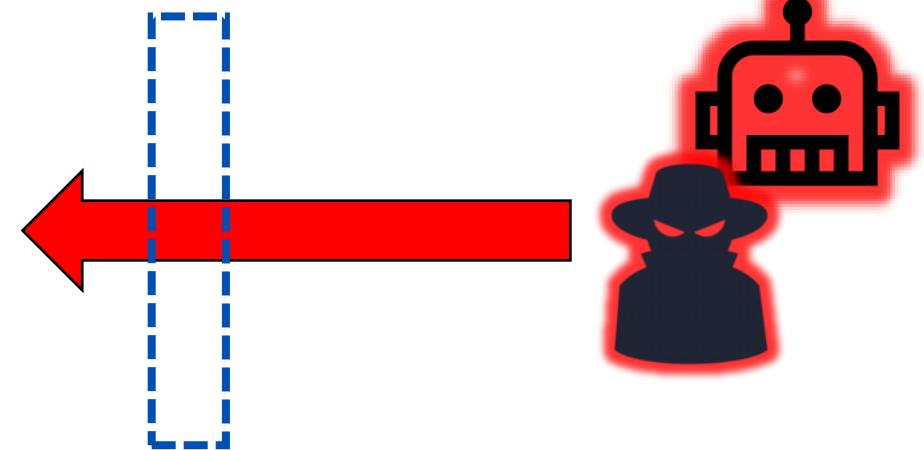
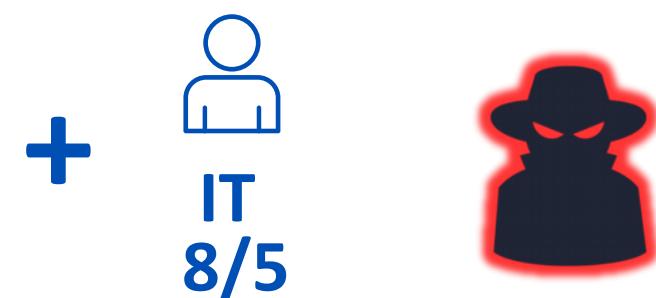
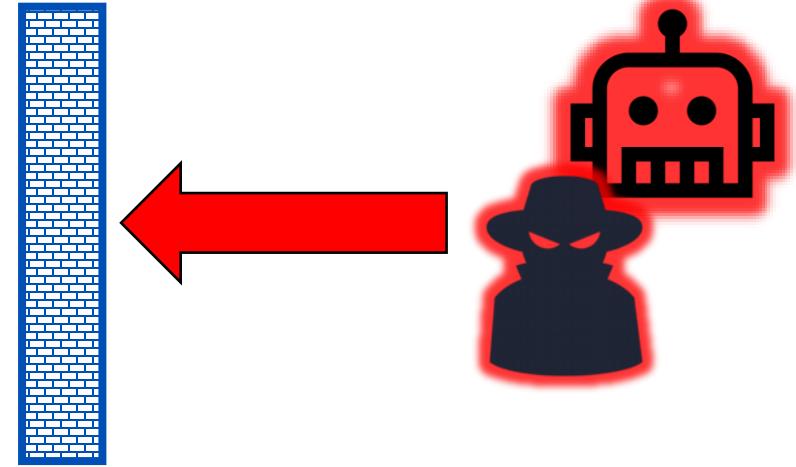
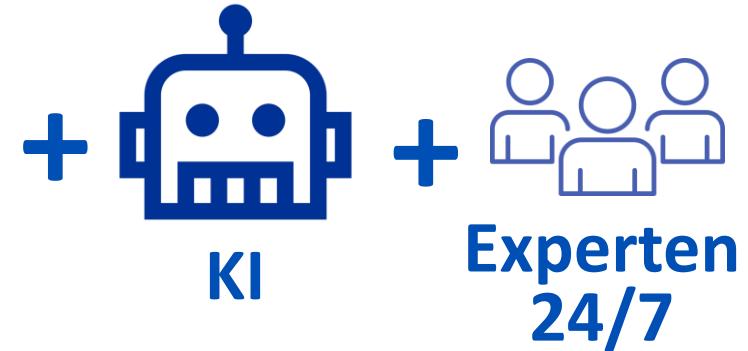
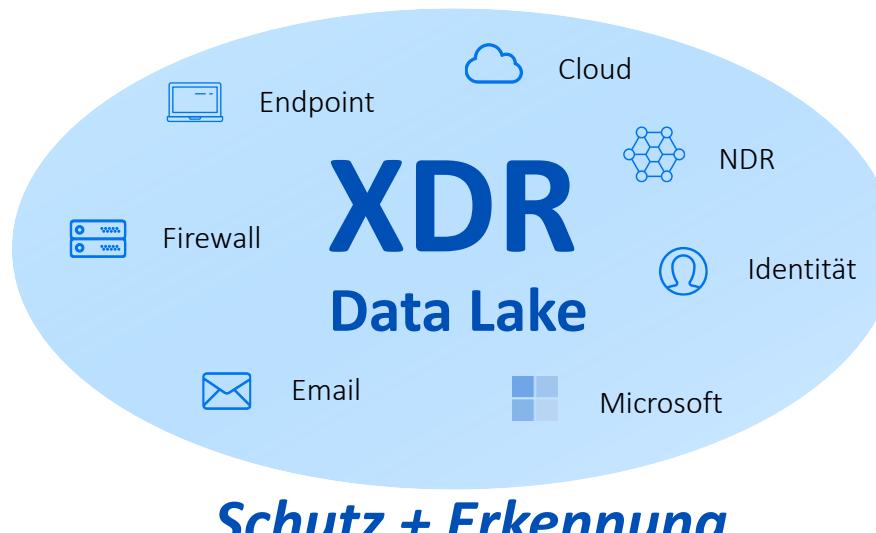


SOPHOS MDR - Cybersecurity as a Service



- ✓ **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?



Sophos KI - ai.sophos.com/projects/



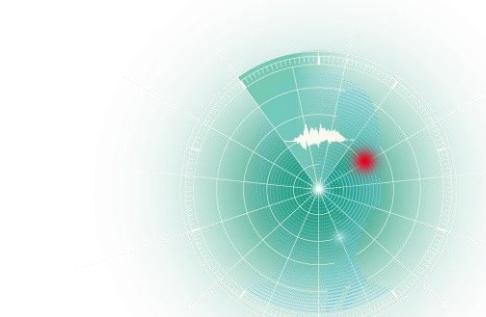
Next-Gen Web



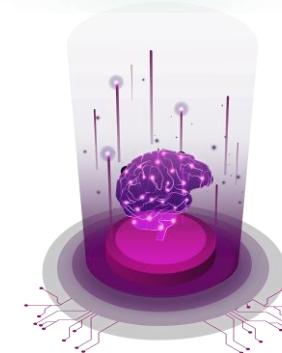
Infrastruktur



Phishing Erkennung



Verhaltenserkennung



KI Forschung



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 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



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, Infrastructure, Interpretable ML als auch Phishing Detection können Sie live mit verfolgen.

ai.sophos.com/projects/



Kontakt

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

sophos.de/kontakt