

Sofie

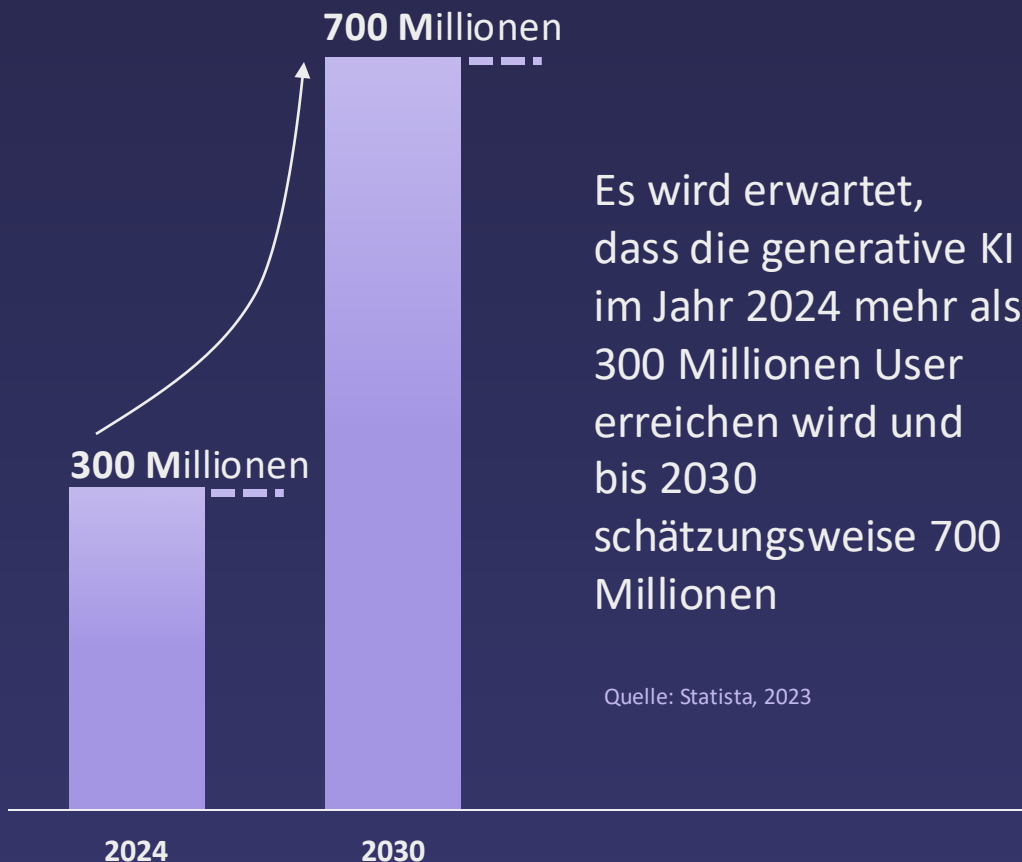
Level Zero Support

KI-gestützte sofortige
Sicherheitsunterstützung, wann
immer Sie sie brauchen



KI HAT LETZTES JAHR ALLES VERÄNDERT

Generative KI ist hier um Unternehmen zu verändern



“

Jüngsten Studien zufolge könnte generative KI in den 63 von uns analysierten Anwendungsfällen jährlich das Äquivalent von **2,6 Billionen bis 4,4 Billionen Dollar** einbringen - zum Vergleich: Das gesamte BIP des Vereinigten Königreichs lag 2021 bei 3,1 Billionen Dollar.

[McKinsey and Company, The Economic Potential of Generative AI, Juni 2023](#)

Herausforderung für Sicherheitsteams im Jahr 2024: Personalmangel & Burnout

3.9
mil.

unbesetzte Stellen im Bereich
Cybersicherheit weltweit

59%

der Unternehmen haben einen
Mangel an
Cybersicherheitspersonal

66%

der Fachkräfte für
Cybersicherheit leiden unter
erheblichem Arbeitsstress

“

Die größte Herausforderung in der
Cybersicherheitsbranche ist derzeit
Burnout: Es gibt zu viele Daten, zu
viele Vorfälle und zu wenig Zeit.



Stéphane Duguin

CEO von CyberPeace
Institute

Kann KI dem Mangel und dem Burnout von Sicherheitsfachleuten entgegenwirken?

“

76%

der Contact Center- und IT-
Führungskräfte sagen, dass
konversationelle KI/Chatbot-
Funktionen die
Unternehmenskommunikation
revolutionieren werden

8x8 State of Conversational AI Report



Sofie Level Zero Support: Die erste Anlaufstelle für Sicherheitsfragen

Namen und Avatar individuell anpassen!

Tonfall festlegen!



✓ Ein KI-gestütztes Dialogerlebnis

✓ Spart Zeit bei Zero-Level-Kundensupportfragen

Ein Mitarbeitender hat
eine Frage zur IT-
Sicherheit



Sofie ist 24/7 auf Teams
verfügbar



Sofie ermittelt die Antwort mit einer Mischung aus LLM-
und Firmenwissen

Sofie antwortet in einem
natürlichen,
dialogorientierten Ton



Wenn menschliche IT-Unterstützung
benötigt wird, wird die Frage als Ticket
weitergeleitet.

Warum Sofie 2.0

- ✓ **Verkürzt die Zeit bis zur Lösung:**
Sofie automatisiert Antworten auf häufig gestellte Anfragen
- ✓ **Spart Zeit für strategische Projekte:** Ihre Sicherheitsfachleute können sich auf das konzentrieren, was wirklich wichtig ist
- ✓ **Verbesserte Sicherheitskultur:**
Aufklärung und Einbindung der Mitarbeitenden
- ✓ **Passt sich an Ihr Unternehmen an:** Training auf Grundlage Ihrer eigenen Wissensbasis
- ✓ **Passt sich an Ihre Marke an:**
Ändern Sie Name, Avatar und Tonfall
- ✓ **Für Unternehmen, die Datenschutz priorisieren:**
Datenhandhabung und -verarbeitung entsprechen den höchsten Standards



Was können User Sofie fragen?

Ich habe möglicherweise auf eine Phishing-E-Mail geklickt. Hilfe.

Mein Firmentelefon wurde gestohlen. Was soll ich tun?

Darf ich ChatGPT für die Arbeit nutzen?

Ich habe versehentlich einige sensible Informationen weitergegeben. Was nun?

Kann ich Programm X auf meinen Computer herunterladen?

Wie kann ich mich von zu Hause aus mit meinem VPN verbinden?

Ich benötige Zugriffsrechte auf einen Ordner im Netzwerk.

Meine Antiviren-Software zeigt eine Warnmeldung an. Was kann ich tun?

Hilfe, ich habe mein Passwort vergessen!



Beispiel: Firmentelefon verloren

- User meldet Sofie den Verlust des Telefons und fragt, was zu tun ist
- User entscheidet sich, ein Support-Ticket zu eröffnen

The screenshot shows a chat interface with a dark background. At the top right, the time is 1:51 PM. A user message in a dark bubble asks: "My company-issued phone was lost/stolen. What should I do to ensure our data is protected?". Below this, a system message from "Sofie - Neptune powered" at 1:52 PM provides a list of eight immediate actions to protect data. The actions are: 1. Report the Loss, 2. Remote Wipe, 3. Change Passwords, 4. Monitor Accounts, 5. Revoke Access, 6. Notify Your Carrier, 7. File a Police Report, and 8. Review and Update Security Policies. A reminder follows: "Remember, swift action is essential to minimize the risk of data exposure." with a red star icon. At the bottom right, the time is 1:53 PM. A user message in a dark bubble asks: "Can you create a support ticket for that?". Below this, a system message from "Sofie - Neptune powered" at 1:54 PM confirms the ticket creation and asks for a satisfaction rating from 1 to 5 stars, with a star icon.

1:51 PM

My company-issued phone was lost/stolen. What should I do to ensure our data is protected?

Sofie - Neptune powered 1:52 PM

If your company-issued phone has been lost or stolen, you should take the following immediate actions to protect your data:

1. **Report the Loss:** Contact your IT department or security team immediately to report the lost or stolen device.
2. **Remote Wipe:** If available, use the company's mobile device management (MDM) system or a similar service to remotely lock and wipe the device to prevent unauthorized access to company data.
3. **Change Passwords:** Change passwords for any work-related accounts or services that were accessible from the device.
4. **Monitor Accounts:** Keep an eye on company accounts for any unusual activity that may indicate unauthorized access.
5. **Revoke Access:** Have IT revoke the device's access to corporate networks and services to prevent any potential data breaches.
6. **Notify Your Carrier:** Inform your mobile carrier about the theft so they can disable the device and prevent unauthorized use of the service.
7. **File a Police Report:** In cases of theft, file a report with the local police. This may assist in recovering the device and is often required for insurance claims.
8. **Review and Update Security Policies:** Your IT department may review and update security policies to prevent similar incidents and improve response in the future.

Remember, swift action is essential to minimize the risk of data exposure. 🌟

1:53 PM

Can you create a support ticket for that?

Sofie - Neptune powered 1:54 PM

Your support request has been successfully created and sent to the support team. 🌟

Could you please rate your satisfaction with the support you received on a scale of 1 to 5 stars? Additionally, if you have any further comments or feedback, feel free to provide them. This helps us to improve our service! 🌟

Beispiel: Firmentelefon verloren

- Support-Ticket wird per E-Mail an das IT-Team gesendet
- Support-Ticket enthält eine Zusammenfassung des Gesprächs

The screenshot shows an email interface with a dark header. At the top, it says 'Unverified' next to a question mark icon, followed by the subject line '[Sofie - Zero Level Support] My company phone got stolen in the bus, what do I need to do?'. On the right of the header are icons for a moon, a smiley face, a speech bubble, and a checkmark, along with navigation arrows. Below the header, the sender is 'SoSafe <noreply@sosafe.de>' with a green checkmark next to 'To:'. The date 'Today at 11:42' is on the far right. The main body of the email has a white background with a light blue border. It features the 'sosafe' logo at the top center, followed by the title 'Ticket Handover'. The text begins with 'Hello,' and then states 'an employee of your company has escalated a ticket to you via Sofie - Zero Level Support. Please take care of the following:'. Below this, there are four sections: 'User Query:' with the text 'My company phone got stolen in the bus, what do I need to do?'; 'Bot Response:' with a detailed list of five steps (Report the Theft, Lock the Phone, Change Passwords, Inform Your Carrier, File a Police Report); 'User Contact Info:' with the email 'sosafedev.runme.0.all@previews.emailonacid.com'; and 'Escalation Reason:' with the text 'To ensure that the company's security team handles the theft and data protection properly.' Finally, a 'Conversation Summary:' section provides a brief overview of the incident and the request for support.

[Sofie - Zero Level Support] My company phone got stolen in the bus, what do I need to do?

Unverified

SoSafe <noreply@sosafe.de>

To: ✓

Today at 11:42

sosafe

Ticket Handover

Hello,

an employee of your company has escalated a ticket to you via Sofie - Zero Level Support. Please take care of the following:

User Query: My company phone got stolen in the bus, what do I need to do?

Bot Response: Here are the steps to take immediately: 1. Report the Theft: Notify your company's IT department or security team right away. 2. Lock the Phone: Use remote management tools (like Find My iPhone or Android Device Manager) to lock your phone and possibly wipe the data. 3. Change Passwords: Change passwords for accounts accessed through your phone, especially work-related ones. 4. Inform Your Carrier: Contact your mobile carrier to report the theft and suspend your service to prevent unauthorized use. 5. File a Police Report: Report the theft to the local police. This is important for insurance and for any further action that might be needed.

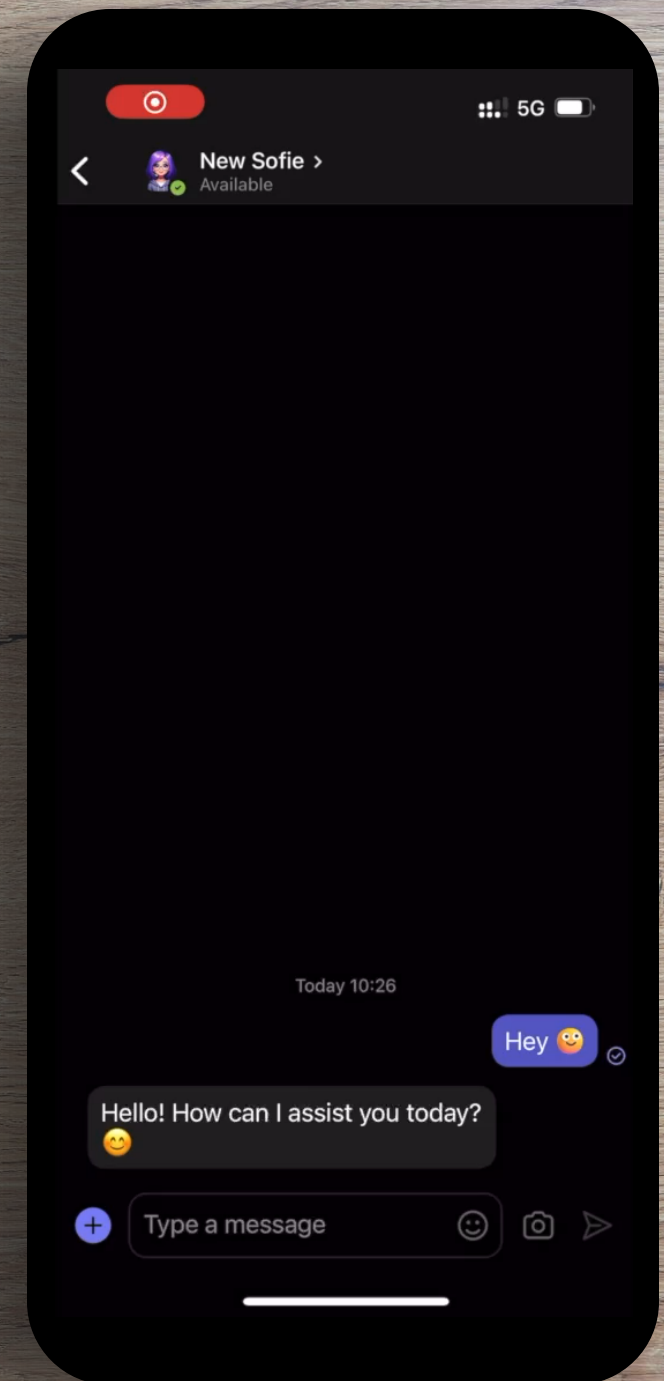
User Contact Info: sosafedev.runme.0.all@previews.emailonacid.com

Escalation Reason: To ensure that the company's security team handles the theft and data protection properly.

Conversation Summary: Petra reported her company phone was stolen and asked for the next steps. Provided instructions to secure data and requested a support ticket for further assistance.

SOFIE KONVERSATIONELLE KI

User hat sensible Informationen mit einer verdächtigen Person geteilt!



Amateurs hack systems, professionals hack people.

Bruce Schneier

Expert in Cryptography
and Computer Security
Harvard University



SoSafe GmbH
Lichtstrasse 25a,
50825 Cologne

sosafe-awareness.com
info@sosafe.de



THE
EUROPAS

