sosafe

KI-resiliente Cybersicherheit

Ihr Partner für Sicherheit, EU-Compliance
und verantwortungsvolle Innovation

Übersicht

Die Auswirkungen von KI auf die digitale Sicherheit

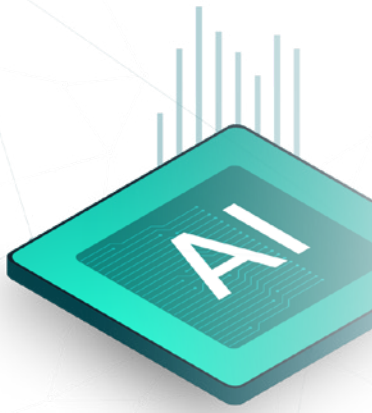
Während sich die Nutzung von künstlicher Intelligenz in exponentiellem Tempo ausbreitet, wächst genauso der Bedarf an intelligenter KI-Governance. **Doch wie lässt sich das in der Cyber Security vereinen?** Organisationen in der EU sind durch verschiedene Richtlinien verpflichtet, die Nutzung, Bereitstellung und Überwachung ihrer KI-Systeme zu überprüfen und ggf. anzupassen. Dazu gehören **Datenschutz- und regulatorische Richtlinien wie die Datenschutz-Grundverordnung (DSGVO)** und die **EU-Verordnung über künstliche Intelligenz**.

Das Forschungs- und Beratungsunternehmen **Gartner™** gibt zu bedenken, dass „zukünftige Regularien zu einer verborgenen Bedrohung für Organisationen werden können, die KI-Anwendungen verwenden (oder selbst entwickeln)“, wobei manche Unternehmen gezwungen sind, ihre Nutzung von LLM-Anwendungen vorübergehend einzustellen oder zurückzunehmen.

Die Tatsache, dass **89 Prozent der IT-Verantwortlichen sagen, sie würden Cyber-Security-Anweisungen zugunsten geschäftlicher Ziele bewusst umgehen**, verdeutlicht, dass wir die mit generativer KI verbundenen Risiken nicht ignorieren können.

Gartner™ empfiehlt in Bezug auf die Governance bei der GenAI-Nutzung, dass für Organisationen die Durchführung der Folgenabschätzungen eine Mindestvoraussetzung sein sollte, wie sie von der DSGVO und der KI-Verordnung der EU gefordert wird.

Wir bei SoSafe sind überzeugt, dass **KI-getriebene Technologien bei der Abwehr gegen Cyberbedrohungen eine immer größere Rolle spielen**. Aus diesem Grund sind wir entschlossen, eine nahtlose Integration zwischen unseren eigenen KI-Richtlinien, Produktfunktionen und Schutzmaßnahmen umzusetzen – im Einklang mit geltenden EU-Richtlinien.

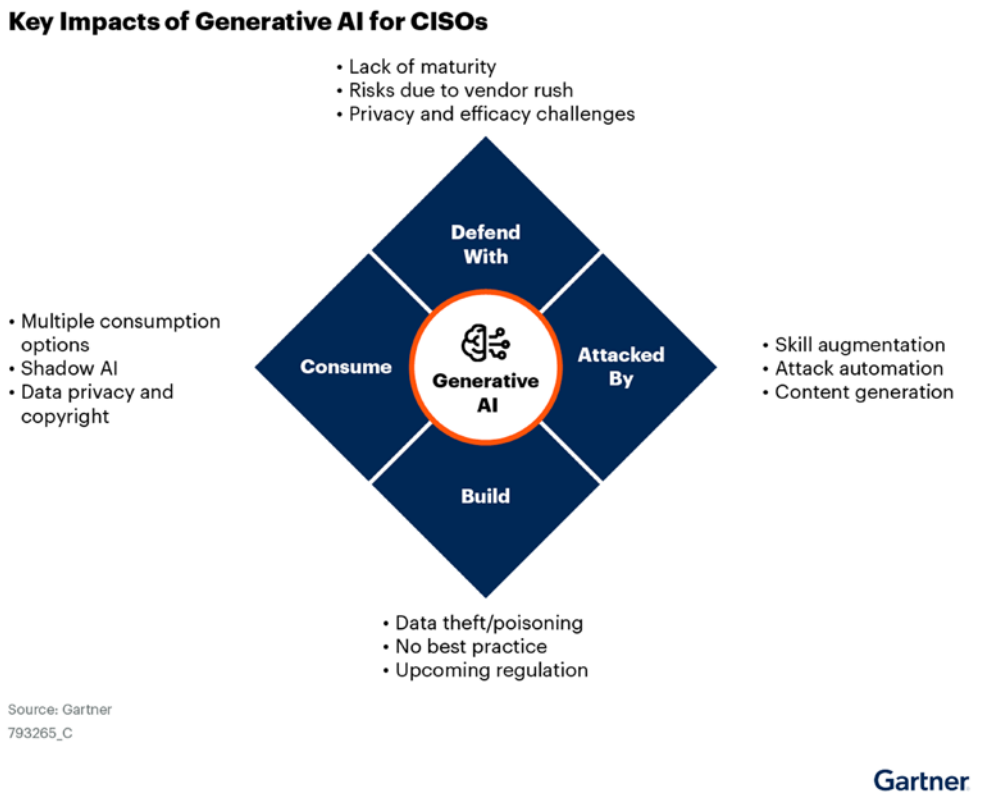


Dieses White Paper richtet sich an Sicherheitsbeauftragte, IT-Administratoren, Datenschutzexpertinnen und -experten sowie Beschaffungsverantwortliche, die sich ein klares Bild davon machen wollen, **wie die KI-Tools von SoSafe ihre Unternehmensdaten im Einklang mit der DSGVO und dem KI-Gesetz verarbeiten**.

Im Folgenden erhalten Sie Einblicke in die wichtigsten Funktionen, Governance-Maßnahmen und praktischen Vorteile KI-gestützter Security-Awareness-Maßnahmen.

Welche Vorteile bietet der Einsatz von KI in Awareness- und Trainingslösungen?

Laut Gartner sollten sich CISOs und Sicherheitsteams in **vier Hauptbereichen** auf den Einfluss generativer KI vorbereiten:



GenAI-Anwendungen werden von Unternehmen in so rasantem Tempo eingeführt, dass der Markt bei der Entwicklung ausgereifter Sicherheitslösung zum Schutz gegen neue Bedrohungen nicht mithalten kann. Um diese Entwicklung abzumildern, empfiehlt Gartner Organisationen, „neue Features bestehender Security-Anbieter zu testen und diese zunächst zielgerichtet für spezifische Anwendungsfälle im Bereich der Sicherheitsprozesse und Application Security einzusetzen."

Social-Engineering-Angriffe – und vor allem Phishing- und Spear-Phishing-Angriffe – werden auch in Zukunft zu den beliebtesten Angriffsmethoden zählen. In Cybersecurity-Anwendungen integrierte KI-Technologie hilft Kunden auf folgende Weise, sich vor diesen Bedrohungen zu schützen:

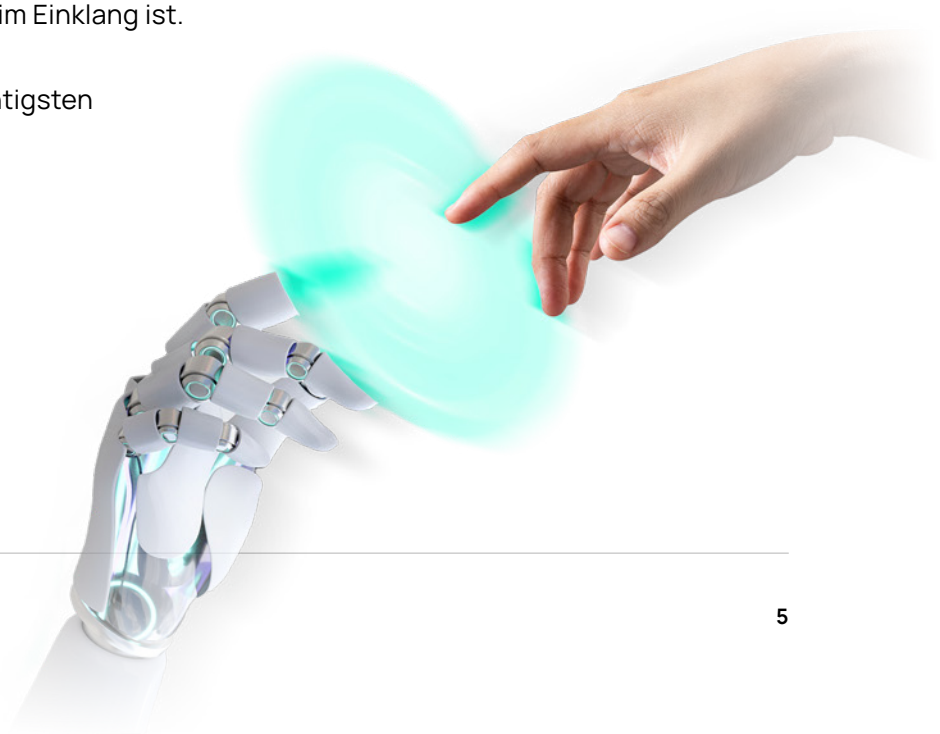
- **Sie können höchstpersonalisierte KI-generierte Szenarien erstellen, die die Effizienz des Trainings erhöhen.**
- **Sie reduzieren den Betriebsaufwand für Administratoren und schaffen so mehr Zeit für strategische Initiativen.**
- **Sie bieten entscheidende Einblicke basierend auf User-Verhalten und -Feedback.**

Die Empfehlung von Gartner lautet, dass CISOs und ihre Teams „berücksichtigen sollten, dass die **Prioritätenfolge für jede Security-Investition immer Mensch, Prozess und – erst dann – Technologie sein sollte**“. Der Fokus sollte auf jenen Angriffsvektoren liegen, die durch KI-generierte Inhalte die Interpretation des Menschen manipulieren – und für die es keine technischen Schutzvorrichtungen gibt.

Bei SoSafe sind wir überzeugt, dass **der Mensch das zentrale Herzstück der Cyberresilienz** ist. Unsere verhaltenspsychologisch fundierte Trainingsplattform verhilft Mitarbeitenden zu mehr Security Awareness, dank der sie Risiken zuverlässiger erkennen. Außerdem gibt sie ihnen die nötigen Prozesse und Tools an die Hand, um effektiv zu reagieren und sichere Gewohnheiten in ihrem Arbeitsalltag zu verankern. **Sofie**, unser KI-basierter Sicherheits-Copilot, führt diesen Ansatz einen Schritt weiter: Sie steigert die Security Awareness in der gesamten Organisation und fördert eine proaktive Sicherheitskultur.

Sofie bietet automatisierte Antworten auf die häufigsten Sicherheitsfragen und hilft Mitarbeitenden so in Echtzeit weiter – dennoch bleibt die menschliche Aufsicht ein zentraler Aspekt, denn Administratoren behalten die volle Kontrolle über Daten, Einstellungen und Einschränkungen, die das Verhalten von Sofie festlegen. Damit schaffen wir ein **ausgeklügeltes Gleichgewicht zwischen Automatisierung und Accountability** und stellen eine Lösung bereit, die effizient, richtlinienkonform und mit unseren Unternehmenswerten im Einklang ist.

Klicken Sie hier, um mehr über die wichtigsten Funktionalitäten von Sofie zu erfahren.



Unser Ethik-Framework für den verantwortungsvollen Einsatz von KI

Für SoSafe ist die **verantwortungsvolle Nutzung vertrauenswürdiger KI** von grundlegender Bedeutung. Deshalb richten wir uns nach branchenweit anerkannten Ethik-Richtlinien, um die Verbreitung von falschen oder schädlichen Informationen zu vermeiden (Hochrangige Expertengruppe für KI Ethikleitlinien der Europäischen Kommission, 2019, Kapitel II). Dieser Ansatz umfasst:

Regelmäßige Bias-Audits

Content-Filter und Guardrails

Fortschreitende Roadmap für Innovation

Datenschutz- und Sicherheitsmaßnahmen

Die interne KI-Richtlinie von SoSafe

Die Nutzung von KI in jeglichen an den Kunden gerichteten Produkten ist bei SoSafe durch die **interne Richtlinie zur KI-Nutzung** geregelt.

Unsere KI-Richtlinie ist in unserem internen KI-Dienst implementiert, der einen konsistenten und automatisch angewandten Rahmen für die Governance und Sicherheit aller genehmigten internen und externen KI-Anbieter darstellt.

Die interne Richtlinie zur KI-Nutzung von SoSafe schränkt den Einsatz von KI in unseren Produkten durch die folgenden Abschnitte ein:

> Nutzerdaten können mit einem zugelassenen Large Language Model (LLM) oder einem anderen KI-basierten Analysesystem geteilt werden, dessen zugrundeliegende Produktfunktionalität durch KI-Technologie unter entsprechender Governance ermöglicht oder erweitert wird. Zu diesem Zweck bietet SoSafe intern einen im Produkt integrierten KI-Dienst.
>
> Wann immer zugrundeliegende Produktfunktionalität durch KI ermöglicht oder erweitert wird, wird im Produkt selbst oder in seiner Dokumentation deutlich darauf hingewiesen und kundenseitigen Administratoren wird, wenn möglich, die Option zur Deaktivierung bereitgestellt.
>
> Wenn Nutzerdaten mit einem LLM- oder KI-Analysetool geteilt werden, dann nur in dem minimalen Umfang, der unbedingt für die Funktion des Dienstes erforderlich ist. (D. h. wir teilen keine Daten, wenn nicht unbedingt erforderlich.) SoSafe teilt Nutzerdaten ausschließlich mit dedizierten Modellen von SoSafe gemäß entsprechender rechtlicher und Security-Governance und der DSGVO.
>
> SoSafe teilt keinesfalls Nutzerdaten mit nicht-dedizierten öffentlichen oder privaten Modellen und lässt unter keinen Umständen zu, dass Nutzerdaten zum Training anderer Modelle als denen von SoSafe genutzt werden.

KI-Arbeitsgruppe

Die Nutzung von KI wird bei SoSafe durch eine offizielle KI-Arbeitsgruppe verwaltet, zu der der Head of AI, der CISO, der General Counsel und ein Vertreter der Führungsebene aus der Strategiegruppe des CEO gehören.

Für effektive Governance vereint die KI-Arbeitsgruppe interne Expertise zum praktischen Einsatz von KI, sowie zu Sicherheit und zum Datenschutz.

Bei Entscheidungen, die die KI-Arbeitsgruppe nicht alleinverantwortlich treffen kann, werden im Rahmen unseres auf ISO-27001 basierenden Security-Management-Systems das Security Committee und Führungsteam miteinbezogen, wobei Aufzeichnungen externen Audits unterliegen.

Die KI-Verordnung der EU

Das sogenannte KI-Gesetz trat am 1. August 2024 in Europa in Kraft. Es soll ein risikobasiertes Framework für die Nutzung von KI-Systemen bieten. In seinem Zentrum stehen **Transparenz, Verantwortlichkeit und Sicherheit**, um zu gewährleisten, dass durch die Nutzung von KI-getriebenen Lösungen keine Grundrechte verletzt oder User unnötigen Risiken ausgesetzt werden.

Compliance bei SoSafe

SoSafe erfüllt die KI-Verordnung der EU durch folgende Maßnahmen:

Risikobasierter Ansatz

- Nutzung mit minimalem Risiko: Der Fokus der KI-Features von SoSafe liegt vorrangig auf Kommunikations- und Trainingsfunktionen. Sie führen keinerlei Funktionen aus, die gemäß KI-Gesetz der EU unter „Hochrisiko-KI-Systeme“ fallen.
- Auferlegte Einschränkungen: Die Einschränkungen bei der Nutzung von KI-Features werden, wann immer möglich, auf Systemebene im internen KI-Dienst durchgesetzt, der den Entwicklern von SoSafe zur Verfügung steht.

Transparenz

- Aufklärung der Nutzer: Gemäß Vorgaben zur deutlichen Kennzeichnung von KI-Systemen weisen wir Nutzer stets darauf hin, wenn sie mit KI-basierten Funktionen interagieren.
- Recht zur Deaktivierung: Administratoren werden darüber informiert, welche Funktionen KI-getrieben sind, und haben gegebenenfalls die Möglichkeit, diese zu deaktivieren.

Prüfung und Validierung

- Qualitätssicherung (QA): Jede neue Iteration eines Features durchläuft einen sorgfältigen QA-Prozess und eine Sicherheitsprüfung, um mögliche Verzerrungen, Schäden und Halluzinationen festzustellen und die Compliance mit geltenden Sicherheitsstandards zu gewährleisten.

Menschliche Aufsicht

- Mehrschichtige Kontrollmaßnahmen: Ein zweistufiger Ansatz gewährleistet sichere und korrekte KI-Interaktionen mit hochwertigem Output:
    - **Stufe 1:** Die Administratoren bestimmen selbst, auf welche Daten Sofie Zugriff erhält, was irrelevanter oder inkorrekter Bezugnahme vorbeugt.
    - **Stufe 2:** Die SoSafe Guardrails bieten über die direkte Kontrolle durch den Kunden hinaus zusätzliche Aufsicht, um unerwünschten Output zu erkennen, zu verringern und aufzuklären.

Interne KI-Kompetenz

- KI-bezogenes Training: Die Entwickler und Mitarbeitenden von SoSafe durchlaufen auf ihre Aufgaben abgestimmtes Training zu KI-Themen.
- Interner KI-Dienst: In Produkte integrierte KI-Dienste unterliegen technischen Governance- und Kontrollmechanismen, was das Risiko, dass Mitarbeitende von SoSafe durch die unangemessene Nutzung von KI versehentlich oder absichtlich Schaden anrichten, weiter reduziert.

KI-Governance

- Akkreditierung: Die KI-Nutzung ist vollständig in unsere ISO-27001 Governance-Prozesse integriert und SoSafe richtet sich beim Einsatz von KI nach ISO/IEC-42001.
- Formelle Evaluation: KI-bezogene Aktivitäten wie die Datenverwaltung, Modell-Updates und mögliche Auswirkungen von Entscheidungen unterliegen einer Risikobewertung.
- Dokumentation: Wir dokumentieren die zur Sicherung der durch KI verarbeiteten Daten durchgeführten Maßnahmen, zeichnen mögliche Compliance- und Sicherheitsrisiken auf und behalten klare Aufsicht über die Funktionsweise der KI-Systeme.

Datenverwaltung und die Datenschutz-Grundverordnung (DSGVO)

Die Datenschutz-Grundverordnung ist das Datenschutzgesetz der Europäischen Union, das die **personenbezogenen Daten und Privatsphärerechte von Einzelpersonen** schützen soll. Sie wurde am 14. April 2016 angenommen und ist am 25. Mai 2018 in Kraft getreten.

SoSafe und die DSGVO

Durch strikte Governance-Maßnahmen, wie Verschlüsselung, Zugriffskontrollen und physische/virtuelle Datentrennung, stellt SoSafe sicher, dass es alle Vorgaben der DSGVO und des KI-Gesetzes erfüllt:

Verschlüsselung und sichere Speicherung

- Daten während der Übertragung: Sämtliche Kommunikation zwischen den Kunden und Servern von SoSafe ist durch TLS-Verschlüsselung geschützt.
- Ruhende Daten: Ruhende Kundendaten werden durch 256-Bit-AES-Verschlüsselung (Advanced Encryption Standard) oder eine gleichermaßen starke Verschlüsselungsmethode geschützt.
- Löschung von Wissensdatenbanken: Sobald ein Admin eine Wissensdatenbank löscht, wird sie auch aus dem System von Sofie und dem Backend der KI entfernt. Damit erfüllen wir das „Recht auf Löschung“ gemäß DSGVO.
- Datennutzung durch externe LLM-Anbieter: Um fortschrittliche KI-Funktionen bereitzustellen, ist Sofie mit Large Language Modellen (LLM) sorgfältig ausgewählter Drittanbieter integriert.
    - SoSafe gewährleistet, dass keinerlei Endnutzer- oder Kundendaten von diesen Drittanbietern zum Training ihrer KI-Modelle gespeichert werden.
    - Alle Daten, die an das LLM gesendet werden, werden ausschließlich genutzt, um eine Antwort zu generieren, und werden danach umgehend gelöscht.
    - Dieser Ansatz gewährleistet in Kombination mit der Verschlüsselung während der Übertragung den Schutz von Kundendaten und die Compliance mit der DSGVO und anderen Datenschutzrichtlinien.

Zugriffskontrolle

- **Konfiguration durch Admins:** Die Administratoren legen fest, auf welche Inhalte Sofie gemäß Least-Privilege-Zugriffsprinzip zugreifen und welche sie nutzen kann.
- **Strenge Daten-Governance:** SoSafe wendet strenge Richtlinien für die Klassifizierung, Handhabung und Speicherung von Daten an, die regelmäßig durch unser internes Sicherheitsteam und externe Auditoren geprüft werden.
- **Data Subject Access Requests (DSAR):** Die KI-Funktionen von SoSafe sind so konzipiert, dass sie eine möglichst geringe Menge an personenbezogenen Daten speichern. In Fällen, in denen identifizierbare Daten verarbeitet werden (wie Benutzernamen in Phishing-Simulationen), unterstützt das System gemäß DSGVO-Vorgaben DSAR.
- **Nutzerzentrierte Datenverarbeitung:** In Abstimmung mit den Administratoren auf Kundenseite haben wir die Möglichkeit, zu prüfen, ob personenbezogene Daten eines bestimmten Datensubjekts (Nutzer) in unserem System gespeichert sind, und können diesen Nutzer darüber in Kenntnis setzen. Auf Anfrage und wenn aus technischer Sicht möglich, können wir die entsprechenden persönlichen Daten im Einklang mit den rechtlichen Vorschriften löschen.
- **Single-Tenant-Architektur:** Jeder Kunde von SoSafe verfügt über seine eigene, isolierte Umgebung, um Cross-Pollination zwischen verschiedenen Tenants auszuschließen. Dieser Ansatz stärkt den Schutz sensibler Daten und entspricht den DSGVO-Grundsätzen zur Datenminimierung und Datentrennung.

Operative Sicherheit

- **Audits und Monitoring:** Wir führen detaillierte Audit-Logs für Systemzugriff, Modifikationen und die Nutzung KI-generierter Inhalte. Diese Logs ermöglichen den zuständigen Mitarbeitenden bei SoSafe, Aktivitäten zu verfolgen und Anomalien zu erkennen.
- **Incident Response und Recovery:** Das Incident-Response-Team von SoSafe ist qualifiziert und in der Lage, im Falle eines Sicherheitsvorfalls schnell und effektiv zu reagieren. Unterstützt wird es dabei durch etablierte Prozesse sowie zuverlässige Backup- und Recovery-Systeme.
- **Qualifikation der Mitarbeitenden:** Die an der Entwicklung von Sofie beteiligten Produktentwicklungs-Teams wurden – gemäß den Anforderungen unseres KI-Dienstes – zu den Themen Large Language Modelle, verantwortungsvolle KI-Nutzung und zu unseren vielfältigen Tools geschult. Dieses Training befähigt unsere Teams, operative Risiken in Verbindung mit KI zu minimieren und unsere Sicherheitsstandards konsequent zu erfüllen.

KI-Guardrails

SoSafe nutzt ein Framework für Sicherheitsmaßnahmen zur **kontinuierlichen Überwachung, Filterung und Moderation** von KI-Input (Prompts) sowie Output, um sicherzustellen, dass sie **unseren Sicherheits- und Compliance-Standards entsprechen**. Diese Guardrails sind auf die Verschlüsselung, Single-Tenant-Architektur und strengen Zugriffskontrollen abgestimmt, um operative Risiken zu minimieren und die verantwortungsvolle Nutzung von KI zu fördern.

Die Guardrails sind zudem in unser zentrales Sicherheits-Framework integriert und entsprechen unseren Unternehmensstandards für Vertraulichkeit, Integrität und Verantwortlichkeit.

Aufgaben der Guardrails

Schnelle Validierung	Eingehende Anfragen werden automatisch überprüft und schädliche oder unzulässige Prompts blockiert, um Datenverlust und unerlaubte Manipulation des Modells zu vermeiden.
Echtzeit-Analyse von Inhalten	KI-generierter Text wird auf verbotene Inhalte (wie Hate Speech) und vertrauliche Daten überprüft. Der Output kann durch die Guardrails abgeändert oder eingeschränkt werden, bevor er dem User bereitgestellt wird.
Monitoring und Alerts	Logs stärken den Schutz im Falle von Interventionen oder Anomalien. Sie ermöglichen den internen Teams von SoSafe, Ergebnisse zu überprüfen, bei Problemen schnell zu reagieren und die Compliance bei regulatorischen Anfragen nachzuweisen.

Benutzerkontrolle und KI-Opt-out bei Sofie

Bei SoSafe soll die KI-Nutzung unseren Usern eine flexible und transparente Option bieten, die sie selbstbestimmt einführen können. Unsere Kunden haben die volle Kontrolle darüber, inwieweit sie mit KI arbeiten wollen, und können bestimmte KI-getriebene Funktionen gezielt deaktivieren. Sei es die automatisierte Erstellung von Phishing-Mails, Unterstützung durch den Chatbot oder KI-optimierte Lernmodule – Organisationen können selbst konfigurieren, wie sie Sofie nutzen, und sie auf ihre eigenen Sicherheitsrichtlinien und Compliance-Anforderungen abstimmen.

Das KI-Portfolio von SoSafe

Sofie, unser **KI-basierter Sicherheits-Copilot**, führt diesen Ansatz einen Schritt weiter: Sie steigert die Security Awareness in der gesamten Organisation und fördert eine proaktive Sicherheitskultur.

Sofie unterstützt User mit **Echtzeit-Antworten auf häufige IT- und Sicherheitsfragen**, wozu sie Ihre unternehmenseigene Wissensdatenbank nutzt. Unser KI-Chatbot ist mit dem Tone-of-Voice, Branding und der Visual Identity Ihrer Organisation personalisierbar und versorgt Ihre Teams mit wichtigen Informationen zu neuen Angriffsszenarien, Compliance-Aufgaben und Best Practices für mehr Sicherheit.

Administratoren können **realistische, zielgerichtete Phishing-Templates** erstellen und Mitarbeitende haben die Möglichkeit, mit Hilfe des Phishing-Meldebutton in Echtzeit Hilfestellung und weiterführende Analysen zu verdächtigen E-Mails einzuholen.

KI-basierter Cyber-Security-Copilot

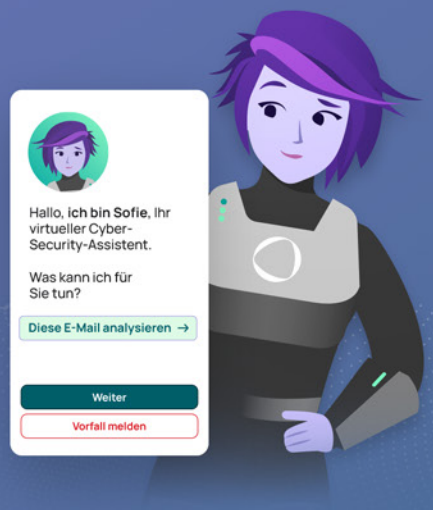
WICHTIGSTE FUNKTIONEN

- **Zero-Level-Support:** Entlasten Sie Ihr IT-Team, denn Sofie beantwortet häufige Fragen schnell und automatisiert.
- **Rapid Awareness Alerts:** Warnen Sie Ihre Mitarbeitenden über MS Teams oder Slack in Echtzeit vor neuen Bedrohungen oder informieren Sie sie über neue Richtlinien. Alerts sind in wenigen Minuten erstellt und lassen sich in über 32 Sprachen übersetzen und auf verschiedene Nutzergruppen abstimmen.
- **Integration mit Ticketsystemen:** Bei komplexeren Fragen oder einem potenziellen Sicherheitsvorfall leitet Sofie die Anfrage weiter, indem sie ein Support-Ticket in Jira, Zendesk oder anderen E-Mail-basierten Ticketsystemen erstellt.
- **Anerkennung für positives Verhalten:** Heben Sie proaktives Verhalten hervor, um das Engagement im Team zu stärken und Security in Ihrer Unternehmenskultur zu verankern.
- **Mühelose Updates der Wissensdatenbank:** Laden Sie neue Materialien einfach in geläufigen Formaten wie PDF, Word, PowerPoint und mehr hoch, damit Sofie immer auf dem neuesten Stand ist.
- **Erkennen häufig gestellter Fragen:** Identifizieren Sie beliebte Sicherheitsthemen und stellen Sie Antworten bereit, die nicht in der Wissensdatenbank enthalten sind, um Sofies Wissenslücken nach und nach zu schließen.

KI-basierter Phishing-Support

WICHTIGSTE FUNKTIONEN

- **Antworten auf Sicherheitsfragen:** Bieten Sie Ihren Mitarbeitenden Phishing-Support in Echtzeit und helfen Sie ihnen, verdächtige E-Mails effektiv einzuschätzen.
- **Phishing-Meldebutton:** Ermöglichen Sie Usern, interaktiv mit Sofie zu chatten, um verdächtigen E-Mails auf den Grund zu gehen und weiterführende Fragen zu stellen.
- **Generieren von Phishing-Templates:** Erstellen Sie realistische Phishing-Templates mit KI-getriebener Prompt-Generation. Administratoren können die Templates dann auf verschiedene Aufgaben, Abteilungen, Branchen oder Szenarien abstimmen, um sie noch relevanter und überzeugender zu machen.



Intelligentere Cyber Security mit dem KI-Portfolio von SoSafe

Das KI-Portfolio von SoSafe vereinfacht und stärkt die Cyber-Sicherheitsmaßnahmen Ihrer Organisation auf unterschiedliche Weise:

Sofie unterstützt Sie dabei, Security Awareness fest in den Arbeitsabläufen Ihrer Teams zu verankern. Sie verbessert

Beschleunigte Problemlösung

Automatisieren Sie Antworten auf häufige Fragen und weisen Sie frühzeitig auf Bedrohungen hin, damit das Security-Team mehr Zeit für komplexere Aufgaben hat.

Bessere Threat Awareness

Übermitteln Sie schnell relevante Neuigkeiten, damit Mitarbeitende umgehend auf neue Bedrohungen reagieren können.

Unterstützt kontinuierliches Lernen

Festigen Sie Erlerntes und beugen Sie Wissensverlust mit zeitlich abgestimmten Nudges vor.

Entlastung von Sicherheitsteams

Überlassen Sie häufige Fragen und Routinenachrichten unseren KI-getriebenen Funktionen und schaffen Sie mehr Kapazität für strategische Aufgaben.

Konsistente Kommunikation

Senden Sie schnell und einfach Nachrichten an die gesamte Organisation oder nur an ausgewählte Nutzergruppen.

Intelligenter Schutz vor Phishing

Befähigen Sie Mitarbeitende, verdächtige E-Mails in Echtzeit zu analysieren, und ermöglichen Sie Admins, realistische Templates für Phishing-Simulationen zu erstellen.

den Schutz Ihrer Organisation vor Phishing-Angriffen und stärkt die Awareness Ihrer Mitarbeitenden durch maßgeschneiderte Simulationsmails.

Entdecken Sie die Möglichkeiten

- **Vereinbaren Sie eine Produktdemo:** Testen Sie das Funktionsspektrum von Sofie in einer kontrollierten Umgebung.
- **Nehmen Sie an einem Pilotprogramm teil:** Beurteilen Sie die Technologie in Ihrem einzigartigen Unternehmenskontext.
- **Sprechen Sie mit unseren Experten:** Wir klären gern Ihre individuellen Compliance-Fragen und passen KI-Funktionalitäten an Ihre Anforderungen an.

Für weitere technische Details, FAQs und Tipps für eine nahtlose Einrichtung setzen Sie sich mit Ihrer Kontaktperson bei SoSafe in Verbindung oder besuchen Sie unser Support-Center.

Erleben Sie aus erster Hand, wie Sofie Ihnen hilft, Ihre Compliance-Herausforderungen zu überwinden:

Jetzt Produktdemo anfragen

Quellenangaben

Hochrangige Expertengruppe für KI Ethikleitlinien der Europäischen Kommission. 2019. „Ethikleitlinien für eine vertrauenswürdige KI, Kapitel II: Verwirklichung einer vertrauenswürdigen KI." Europäische Kommission, (April). https://digital-strategy.ec.europa.eu/de/library/ethics-guidelines-trustworthy-ai.

Europäisches Parlament und Rat der Europäischen Union. 2024. „Artikel 12: Aufzeichnungspflichten." Amtsblatt der Europäischen Union, L 277. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32024R1689.

Agentur der Europäischen Union für Cybersicherheit (ENISA). 2024. „ENISA Threat Landscape: The Year in Review." https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

Gartner™, 4 Ways Generative AI Will Impact CISOs and Their Teams, Jeremy D'Hoinne, Avivah Litan, Peter Firstbrook, 6. Dezember 2024.