



Comment construire une cybersécurité résiliente à l'ère de l'IA ?

Gestion de la sécurité, conformité aux normes européennes et innovation responsable

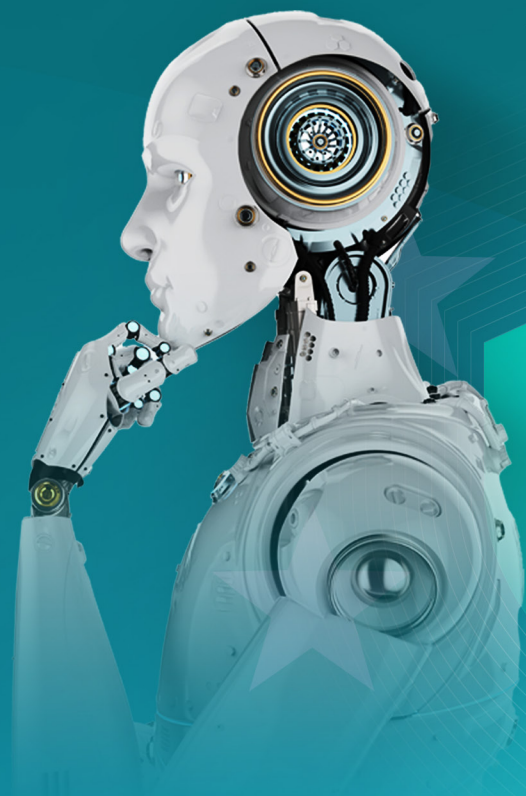


Tableau de bord

Comment l'intelligence artificielle redéfinit-elle la sécurité numérique ?	3
Les arguments en faveur de l'IA dans le domaine de la sensibilisation et de la formation à la sécurité	4
L'IA responsable et le cadre éthique défini par SoSafe	6
Confidentialité et mesures de sécurité	6
Le Règlement européen sur l'intelligence artificielle	8
Gouvernance des données et règlement général de protection des données (RGPD)	10
Garde-fous en matière d'IA	12
Le portefeuille de produits IA de SoSafe	13
Découvrez toutes les possibilités de l'IA	15
Références	15

Comment l'intelligence artificielle redéfinit-elle la sécurité numérique ?

Avec l'adoption de plus en plus généralisée de l'IA, le besoin d'une gouvernance mieux pensée se fait cruellement sentir. **Qu'en est-il exactement dans le secteur de la cybersécurité ?**

Les lois qui régissent la confidentialité des données au sein de l'Union européenne, notamment le **Règlement général sur la protection des données (RGPD)** et le **Règlement européen sur l'intelligence artificielle**, exigent des entités qu'elles repensent l'usage qu'elles font des systèmes d'IA, la façon dont elles les déploient et dont elles les contrôlent.

Le cabinet de recherche et de conseil **Gartner™** avertit que « les réglementations qui seront adoptées prochainement constituent une menace latente pour les entreprises qui utilisent (et développent) des applications d'IA ». Certaines sociétés risquent, en effet, de devoir faire marche arrière, voire cesser d'utiliser les grands modèles de langage.

Lorsqu'on sait que **89 % des responsables de la technologie en entreprise se disent prêts à contourner les directives en matière de cybersécurité si elles les empêchent d'atteindre les objectifs de l'entreprise**, il y a de quoi s'inquiéter quant aux risques posés par les applications d'IA générative.

En matière de gouvernance, Gartner recommande aux entreprises d'exiger que toutes les IA utilisées soient soumises aux évaluations d'impact requises par la législation qui régit la confidentialité et l'intelligence artificielle : en particulier à celles préconisées par le Règlement général sur la protection des données (RGPD) et par le Règlement européen sur l'intelligence artificielle (AI Act).

Chez SoSafe, nous croyons que les technologies augmentées à l'IA peuvent jouer un **rôle essentiel dans la gestion des cybermenaces** et nous nous efforçons de les intégrer, en toute transparence, dans nos politiques, nos solutions produits et nos mesures de sécurité, afin de proposer des outils conformes à la réglementation européenne.

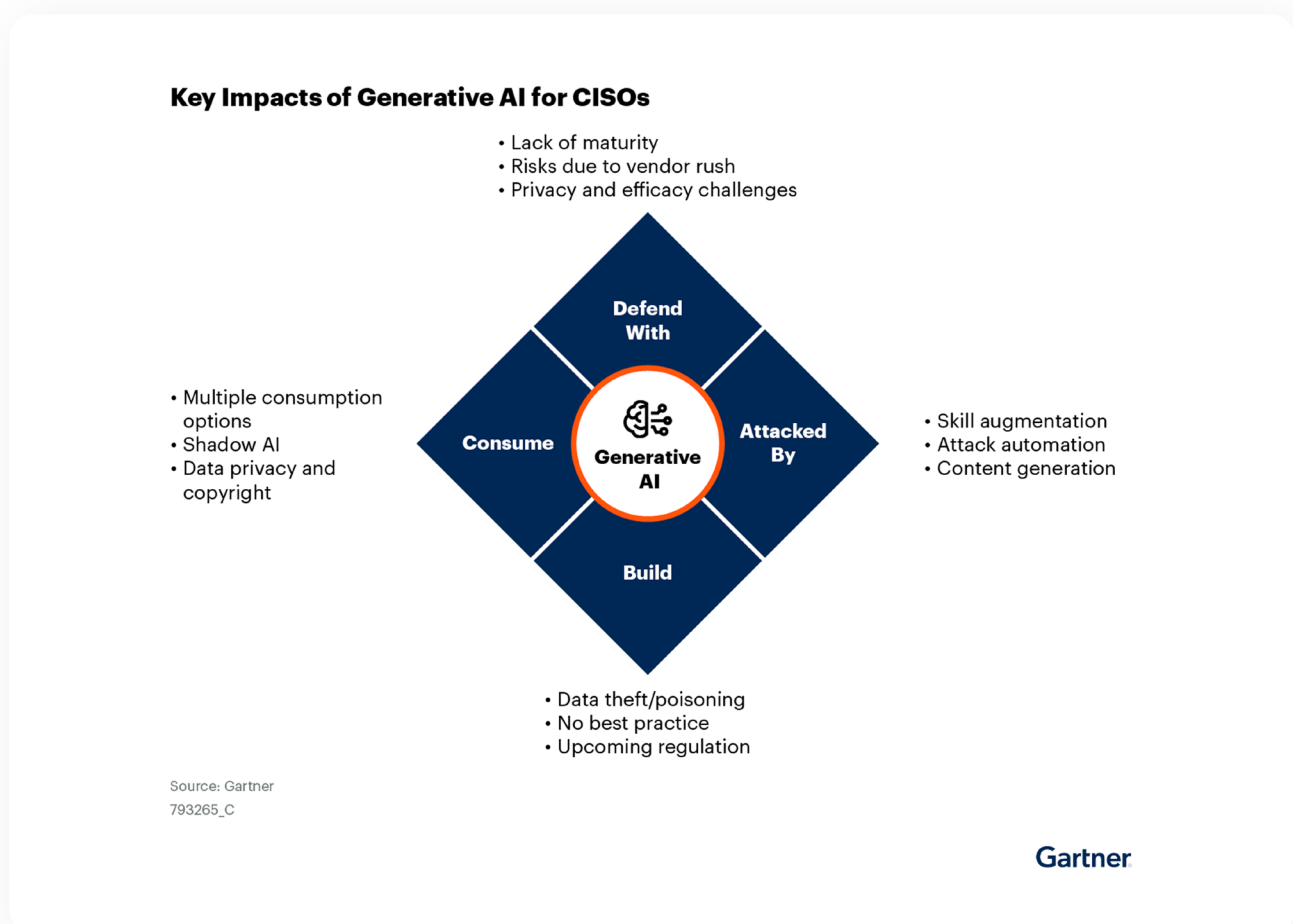
Le présent livre blanc s'adresse aux professionnels de la cybersécurité, aux administrateurs informatiques, aux experts en protection des données et aux équipes responsables des achats. Son objectif est de leur présenter en détail la **façon dont SoSafe traite les données d'entreprise dans le respect du RGPD et du Règlement sur l'IA**.

Vous découvrirez, au fil de votre lecture, les principales fonctionnalités, les mesures de gouvernance, ainsi que les avantages concrets d'une **sensibilisation à la sécurité augmentée à l'IA**.



Les arguments en faveur de l'IA dans le domaine de la sensibilisation et de la formation à la sécurité

Selon Gartner, les RSSI et les équipes de sécurité doivent se préparer à ce que l'IA générative ait des répercussions dans **quatre domaines clés** :



Visuel provenant de Gartner en anglais à titre de référence

Les entreprises adoptent les applications d'IA générative à un rythme tel, qu'il ne permet pas au marché de concevoir des solutions suffisamment matures pour garantir leur sécurité contre les menaces émergentes. Gartner recommande de limiter les risques en « testant les nouvelles fonctionnalités proposées par les fournisseurs habituels de cybersécurité et en commençant à les utiliser sur des cas ciblés et bien circonscrits relatifs aux opérations de sécurité et à la sécurité des applications. »

Les attaques d'ingénierie sociale, notamment le phishing et le spear phishing continuent de figurer parmi les menaces les plus fréquentes et ne sont pas près de disparaître. L'intelligence artificielle peut aider nos clients à mieux maîtriser les difficultés posées par la cybersécurité. Elle peut, par exemple :

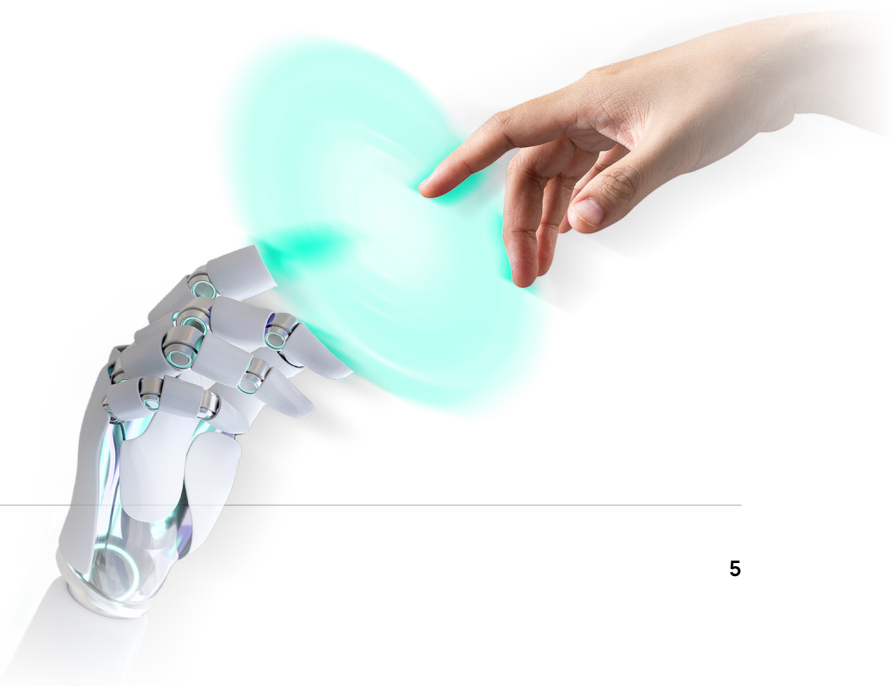
- **renforcer l'efficacité des formations en proposant des scénarios générés par l'IA et entièrement personnalisables ;**
- **réduire la charge opérationnelle qui pèse sur les administrateurs, leur permettant ainsi de libérer du temps pour des mesures stratégiques ;**
- **mettre en lumière des données essentielles, sur la base des comportements et des retours des utilisateurs.**

De manière générale, Gartner recommande aux RSSI et à leurs équipes de « respecter le bon ordre en matière d'investissements pour la sécurité : **d'abord les ressources humaines, ensuite les processus, et enfin la technologie**. Il faut cibler, avant tout, les vecteurs de menace qui sont liés à l'influence que peuvent exercer sur l'interprétation humaine, les contenus générés pour lesquels il n'existe aucun contrôle technologique. »

Chez SoSafe, nous croyons que **l'humain est la clé de la cyberrésilience**. Notre formation fondée sur les sciences comportementales sensibilise les employés pour leur apprendre à identifier les risques, à y réagir efficacement en adoptant les bons gestes et à utiliser des outils efficaces pour assurer leur sécurité au quotidien. **Sofie**, notre copilote de cybersécurité augmenté à l'IA, pousse cette approche encore plus loin en renforçant la vigilance au sein de l'entreprise et en cultivant une cybersécurité proactive.

Grâce à l'IA, Sofie prend en charge les questions de sécurité les plus fréquentes de manière automatisée et conseille les utilisateurs en temps réel, mais il est indispensable que l'humain reste au contrôle. Pour assurer un **équilibre bien pensé entre automatisation et responsabilités**, les administrateurs gardent la main sur les données, les paramètres et les limites qui définissent le comportement de Sofie, afin d'en garantir l'efficacité, la conformité et l'adéquation aux valeurs de votre entreprise.

[Cliquez ici](#) pour en savoir plus sur les principales fonctionnalités de Sofie.



L'IA responsable et le cadre éthique défini par SoSafe

SoSafe adhère pleinement aux **principes de l'IA responsable**, et respecte les lignes directrices du secteur en matière d'éthique sur ce sujet, afin de limiter les biais et les résultats préjudiciables (Groupe d'experts de haut niveau de la Commission européenne sur l'intelligence artificielle 2019, chapitre II). Cette approche prévoit :

des audits réguliers portant sur les biais

des filtres de contenu et des systèmes de prévention

une feuille de route évolutive pour l'innovation

Confidentialité et mesures de sécurité

La politique de SoSafe en matière d'IA

SoSafe a adopté une **politique** générale qui limite **l'utilisation de l'IA** dans les produits destinés aux clients.

Très concrètement, elle est appliquée dans le cadre de notre service d'IA interne qui soumet tous les fournisseurs d'IA, qu'ils soient internes ou externes, à une gouvernance et à un dispositif de sécurité automatisés.



Chez SoSafe, la politique qui régit l'utilisation de l'IA en interne exige que les produits ayant recours à cette technologie comportent la mention suivante :



Les données utilisateurs sont susceptibles d'être communiquées à un grand modèle de langage (LMM) approuvé ou à un autre moteur d'analyse augmenté à l'IA lorsque la fonctionnalité du produit est assurée ou améliorée en arrière-plan par l'utilisation de cette technologie. Cette transmission est soumise à une gouvernance appropriée. À cette fin, SoSafe met à la disposition de l'utilisateur, dans ce produit, un service d'IA destiné à un usage interne.

Une mention claire figurant dans le produit ou la documentation du produit indique que la fonctionnalité du produit est assurée ou améliorée en arrière-plan par l'utilisation d'une IA. Lorsque le cas de figure le permet, les administrateurs du client pourront s'opposer à l'utilisation de cet outil.

S'il s'avère nécessaire de communiquer les données de l'utilisateur à un grand modèle de langage ou à un outil d'analyse augmenté à l'IA, ce transfert ne porte que sur le minimum d'informations requis pour le bon fonctionnement du service (nous n'adoptons pas une approche de type « partager toutes les données non restreintes sans raison précise »). SoSafe ne communique les données utilisateurs qu'à des modèles qui lui sont dédiés, dans le cadre d'une gouvernance juridique et d'une sécurité adaptées et conformément au RGPD.

SoSafe ne communique jamais de données utilisateurs à un public non autorisé ni à des modèles privés. Elle ne permet pas non plus l'utilisation des données utilisateurs pour l'entraînement de modèles autres que ceux spécifiques à SoSafe.

Groupe de travail sur l'IA

Chez SoSafe, l'usage de l'IA est défini par un groupe de travail officiel composé du Directeur du service IA, du RSSI, du Directeur juridique, ainsi que d'un représentant de la direction, membre du conseil stratégique du PDG.

Ce groupe a pour mission de rassembler l'expertise disponible en interne en matière d'utilisation pratique de l'IA, de sécurité et de confidentialité, afin d'assurer une gouvernance efficace sur les questions relatives à l'IA chez SoSafe.

Les décisions que le groupe de travail sur l'IA ne s'estime pas en mesure de prendre en assumant l'entière responsabilité sont transférées au Comité de sécurité et à l'équipe dirigeante dans le cadre de notre système de management de la sécurité conformément à la norme ISO 27001. À ce titre, les enregistrements sont soumis à un audit externe.

Le Règlement européen sur l'intelligence artificielle

Le Règlement européen sur l'intelligence artificielle est entré en vigueur le 1^{er} août 2024. Son objectif est de poser un cadre pour la gestion des systèmes d'IA sur la base des risques. Il met l'accent sur **la transparence, la responsabilité et la sécurité** afin de garantir que les solutions augmentées à l'IA n'enfreignent pas les droits fondamentaux ou ne comportent pas de risques inconsiderés pour les utilisateurs.

La conformité chez SoSafe

SoSafe se conforme au Règlement européen sur l'intelligence artificielle sur les points suivants :

Approche fondée sur les risques

- **Usage à risque minimal** : Les fonctionnalités d'IA de SoSafe ciblent avant tout les tâches de communication et de formation. Elles n'effectuent aucune des activités classées comme « à fort risque » dans le Règlement européen sur l'intelligence artificielle.
- **Limites imposées** : Dans la mesure du possible, les restrictions posées à l'utilisation des fonctions d'IA sont maintenues à un niveau système dans le service d'IA interne fourni aux développeurs de SoSafe.

Transparence

- **Notification utilisateur** : Conformément aux dispositions légales qui exigent que les systèmes d'IA portent une mention claire indiquant la technologie utilisée, les utilisateurs sont dûment informés lorsqu'ils interagissent avec des fonctionnalités augmentées à l'IA.
- **Politique de retrait du consentement** : Une mention informe les administrateurs des fonctionnalités de produit augmentées à l'IA et de la possibilité de retirer leur consentement.

Test et validation

- **Assurance qualité (QA)** : Chaque nouvelle version d'une fonctionnalité est soumise à un contrôle qualité minutieux et à une procédure d'évaluation de la sécurité. Ces vérifications visent à identifier les éventuels biais, contenus malveillants et hallucinations et à garantir la conformité aux normes de sécurité obligatoires.

Surveillance humaine

- **Contrôle stratifié** : Une approche à deux niveaux garantit des interactions sécurisées, précises et de grande qualité avec l'IA :
 - **Niveau 1**: La curation par l'administrateur définit la portée des données auxquelles Sofie peut accéder, afin de limiter les références non pertinentes ou incorrectes.
 - **Niveau 2**: Les garde-fous mis en place par SoSafe ajoutent une surveillance supplémentaire, non perceptible par le client. Elle permet de détecter, de restreindre et de corriger les résultats indésirables.

Alphabétisation en matière d'IA

- **Formation axée sur l'IA** : Les développeurs et l'équipe de SoSafe suivent une formation adaptée à leur fonction dans l'entreprise.
- **Service interne d'IA** : Les services d'IA orientés produits sont soumis à une gouvernance technique qui assure l'application des règles, ainsi qu'à un dispositif de contrôle qui limite encore davantage les préjudices que le personnel de SoSafe est susceptible de causer, volontairement ou involontairement, en utilisant l'IA de manière inappropriée.

Gouvernance de l'IA

- **Accréditation** : L'utilisation de l'IA est totalement intégrée dans nos processus de gouvernance selon la norme ISO 27001. En outre, SoSafe se conforme aux pratiques en matière d'IA recommandées par la norme ISO/CEI 42001.
- **Évaluation formelle** : Les activités liées à l'IA telles que le traitement de données, la mise à jour du modèle et les répercussions éventuelles sur la prise de décision sont soumises à une évaluation des risques.
- **Documentation** : Nous documentons les contrôles requis pour sécuriser les données traitées par l'IA, suivre les risques éventuels en matière de conformité et de sécurité et maintenir une surveillance claire sur le fonctionnement des systèmes d'IA.

Gouvernance des données et règlement général de protection des données (RGPD)

Le RGPD est une **loi détaillée qui régit la confidentialité au sein de l'Union européenne**. Adoptée le 14 avril 2016 par l'Union européenne pour une entrée en vigueur le 25 mai 2018, elle a pour mission de protéger les données personnelles des personnes et leurs droits en matière de confidentialité.

SoSafe et le RGPD

Pour assurer sa conformité avec le RGPD et les principes sous-jacents du Règlement européen sur l'intelligence artificielle, SoSafe a pris des mesures strictes de gouvernance, incluant le chiffrement des données, le contrôle des accès et la séparation des données physiques et virtuelles.

Chiffrement et stockage sécurisé

- **Données en transit** : Toutes les communications entre les clients SoSafe et les serveurs sont protégées par cryptage TLS.
- **Données au repos** : Au repos, les données du client sont cryptées par Advanced Encryption Standard de 256 bits (AES 256) ou par une clé solide équivalente.
- **Suppression du fichier de connaissances** : Si un administrateur supprime un fichier de connaissances, il est immédiatement effacé du système de Sofie, ainsi que du backend de l'IA afin de garantir le respect du « droit à l'effacement ».
- **Utilisation des données par les grands modèles de langage de fournisseurs tiers** :
Pour offrir des fonctionnalités d'IA sophistiquées, Sofie a recours à de grands modèles de langage (LLM) conçus par des sous-traitants triés sur le volet.
 - SoSafe veille à ce qu'aucune donnée sur les utilisateurs finaux ou sur les clients ne soit conservée par ces fournisseurs externes à des fins d'entraînement du modèle.
 - Toutes les données envoyées au LLM sont traitées aux seules fins de générer une réponse, après quoi elles sont immédiatement supprimées.
 - Cette approche, associée au protocole de chiffrement en transit, protège les données clients et garantit la conformité au RGPD, ainsi qu'aux autres réglementations en matière de confidentialité.

Contrôle des accès

- **Configuration par l'administrateur** : Les administrateurs gèrent les contenus auxquels Sofie a accès et ceux que l'outil peut utiliser, en respectant le principe du moindre privilège.
- **Gouvernance stricte des données** : SoSafe applique des politiques strictes en matière de classification, de traitement et de stockage des données. Celles-ci sont régulièrement révisées par notre équipe de sécurité interne et des auditeurs externes.
- **Demande d'accès de la personne concernée (DSAR)** : Les solutions d'IA utilisées par SoSafe sont conçues pour limiter la collecte de données personnelles. Lorsque des informations permettant d'identifier la personne sont susceptibles d'être traitées (p. ex. les noms d'utilisateurs utilisés pour les simulations de phishing), le système envoie une DSAR, conformément aux exigences du RGPD.
- **Traitement des données axé sur l'utilisateur** : En collaboration avec les administrateurs du client, nous pouvons vérifier si notre système contient des données personnelles associées à un utilisateur spécifique et en informer ce dernier. Sur demande, et dans la limite de ce qui est techniquement faisable, nous pouvons supprimer lesdites données personnelles dans le respect des obligations légales.
- **Architecture single-tenant** : Tout environnement client chez SoSafe est rigoureusement séparé pour garantir qu'il n'y a aucun croisement de données entre les différents clients. Cette approche, qui permet de protéger les informations sensibles, est en accord avec les exigences du RGPD en matière de minimisation et de séparation des données.

Sécurité opérationnelle

- **Audit et suivi** : Nous tenons à jour des journaux d'audits détaillés sur les accès au système, les modifications et l'utilisation de contenu généré par IA. Ces informations permettent aux employés de SoSafe qui y sont autorisés de suivre l'activité et de détecter d'éventuelles anomalies.
- **Intervention en cas d'incident et restauration** : Chez SoSafe, l'équipe responsable des interventions en cas d'incident est formée et équipée pour réagir rapidement aux éventuels incidents de sécurité. De solides procédures, des backups et des systèmes de restauration ont été mis en place à cet effet.
- **Équipe entraînée** : Les équipes de développement produit qui travaillent sur Sofie ont été formées à la bonne utilisation des grands modèles de langage, aux procédures responsables en matière d'IA et aux divers outils répondant aux critères imposés par notre service d'IA. Grâce à cette formation, nos équipes sont bien équipées pour limiter les risques opérationnels liés à l'IA, sans jamais déroger à nos exigences en matière de sécurité.

Garde-fous en matière d'IA

SoSafe a mis en place un cadre « garde-fou » dont la raison d'être est de **suivre en continu, de filtrer et de modérer** qui sont faites à l'IA (prompts) ainsi que les résultats obtenus, afin de veiller à ce qu'ils **respectent nos critères de sécurité et de conformité**. Ces dispositifs de protection s'ajoutent au chiffrement, à l'architecture single-tenant et aux contrôles stricts des accès pour limiter les risques opérationnels et favoriser une utilisation responsable de l'IA.

Ils sont intégrés dans le cadre global de gestion de la sécurité et respectent les normes de l'entreprise en matière de confidentialité, d'intégrité et de responsabilisation.

Fonctions « garde-fous » :

Validation des prompts

Analyse automatiquement les prompts pour bloquer les demandes malveillantes ou interdites afin de prévenir toute fuite de données ou manipulation illicite du modèle.

Analyse du contenu en temps réel

Passe en revue le texte généré par l'IA pour s'assurer qu'elle ne contient pas de contenu interdit (p. ex., langage à caractère haineux) ni de données confidentielles. Elle peut alors modifier ou restreindre les résultats avant qu'ils ne soient présentés aux utilisateurs.

Suivi et alertes

Tient un journal des interventions « garde-fous » et des anomalies pour que les équipes internes de SoSafe puissent auditer les résultats, traiter rapidement les problèmes et conserver des preuves de conformité en cas de demande émanant des autorités de réglementation.

Contrôle de l'utilisateur et retrait du consentement à l'utilisation de l'IA avec Sofie

Chez SoSafe, le recours à l'IA reste un processus flexible et transparent, sous le contrôle de l'utilisateur. Les clients conservent la maîtrise totale des interactions avec l'IA et peuvent refuser l'utilisation de certaines fonctionnalités augmentées à l'IA. Qu'il s'agisse de la génération automatisée des modèles de phishing, du chatbot d'assistance utilisateur ou des modules d'apprentissage augmentés à l'IA, les entreprises ont la possibilité de configurer l'utilisation de Sofie en fonction de leurs politiques de sécurité et de leurs besoins en matière de conformité.

Le portefeuille de produits IA de SoSafe

Sofie est le **copilote de cybersécurité augmenté à l'IA** développé par SoSafe. Il est conçu pour renforcer la sensibilisation à la sécurité au sein de l'entreprise. Intégrée dans des outils de bureau comme Microsoft Teams ou Slack, Sofie génère de courts messages ciblés qui rappellent les points vus en formation, diffuse des notifications en temps réel et incite à adopter les bons gestes en matière de sécurité.

Sur un **mode conversationnel**, Sofie délivre des **conseils instantanés** sur des questions informatiques fréquentes et des problèmes liés à la sécurité en puisant dans la base de connaissances de votre entreprise. Totalement personnalisable, Sofie peut informer vos équipes sur l'évolution des menaces, les obligations de conformité et les bonnes pratiques en matière de sécurité en reprenant le ton de voix, la charte graphique et l'identité visuelle de votre entreprise.

Les administrateurs peuvent générer des **modèles de simulation de phishing ciblés et réalistes**, tandis que le personnel a la possibilité de **chatter en temps réel**, via le bouton d'alerte phishing, pour obtenir des conseils lorsqu'il est confronté à des e-mails suspects ou demander une analyse approfondie.

FONCTIONNALITÉS CLÉS

Copilote de cybersécurité augmenté à l'IA

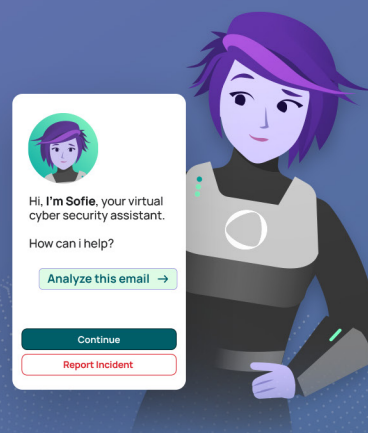
- **Support virtuel préalable** : allège la charge qui pèse sur le service informatique en répondant rapidement aux questions les plus fréquemment posées.
- **Alertes de sensibilisation rapide** : envoie des notifications au personnel via Microsoft Teams ou Slack pour les informer de nouvelles menaces ou de mises à jour des politiques. Les alertes peuvent être générées en quelques minutes, traduites dans plus de 32 langues et adaptées sur mesure aux différents groupes d'utilisateurs.
- **Intégration des tickets d'assistance** : si Sofie n'est pas en mesure de résoudre un problème ou détecte un incident potentiel, elle peut faire remonter la situation au service concerné, en créant un ticket d'assistance dans Jira, Zendesk ou d'autres systèmes de gestion des tickets par e-mails.
- **Système de récompense pour les bons gestes** : met en lumière les comportements proactifs des employés, pour les encourager dans leur engagement et favoriser une culture d'entreprise axée sur la sécurité.
- **Simplification des mises à jour de la base de connaissances** : télécharge les nouveaux éléments dans les formats les plus courants, comme PDF, Word, PowerPoint, et plus encore, pour tenir les connaissances de Sofie à jour.
- **Met en lumière les questions les plus fréquemment posées** : fait remonter les sujets d'actualité et identifie les réponses qui ne figurent pas dans les fichiers de connaissances existants, de manière à repérer les lacunes de Sofie.



FONCTIONNALITÉS CLÉS

Assistance de gestion du phishing augmentée à l'IA

- **Conseils pour la gestion du phishing augmentée à l'IA** : prodigue des conseils en temps réel aux utilisateurs pour les aider à gérer les tentatives de phishing et des informations pour évaluer, sans hésitation, les e-mails suspects.
- **Bouton d'alerte phishing** : permet aux utilisateurs d'interagir avec Sofie pour analyser plus en profondeur certains e-mails et poser des questions de suivi.
- **Génération de modèles de phishing** : crée des modèles d'e-mails de phishing réalistes ainsi que des notifications générées par IA. Les administrateurs peuvent adapter les modèles à certains rôles, certains services ou certains secteurs, ou inventer des scénarios pour augmenter la pertinence et la crédibilité de la campagne.



Une cybersécurité plus intelligente grâce au portefeuille de produits IA de SoSafe

Le portefeuille de produits IA de SoSafe simplifie la cybersécurité et la renforce à différents niveaux dans l'entreprise :

Permet une résolution plus rapide des incidents

Répond automatiquement aux questions fréquentes et signale les problèmes en amont pour permettre aux équipes de sécurité de se concentrer sur les tâches plus complexes.

Améliore la sensibilisation aux menaces

Envoie des informations utiles, au bon moment, pour aider le personnel à réagir rapidement aux nouveaux risques.

Favorise la formation continue

Envoie des notifications au bon moment pour consolider les acquis dans la durée et éviter la déperdition des connaissances.

Allège la charge qui pèse sur les équipes de sécurité

Gère les demandes courantes et les communications de routine, afin de dégager plus de temps pour les priorités stratégiques.

Assure une communication cohérente

Permet d'envoyer facilement des messages sur mesure à toute l'entreprise ou à certains groupes d'employés, au moment le plus favorable.

Permet des simulations de phishing et une stratégie de défense plus intelligentes

Apprend au personnel à évaluer des e-mails suspects en s'aidant des conseils prodigués en temps réel par l'IA, et offre aux administrateurs la possibilité de créer des modèles de simulations de phishing réalistes.

Sofie aide les entreprises à intégrer la sécurité dans leur flux de travail quotidien, pour que la vigilance devienne un réflexe professionnel dans toutes les équipes. Les conseils de gestion du phishing prodigués par l'IA et les simulations qu'elle permet de générer renforcent la sensibilisation des employés, sans empiéter sur leurs tâches quotidiennes.

Découvrez toutes les possibilités de l'IA

- **Demandez une démo** : Testez les fonctionnalités de Sofie dans un environnement contrôlé.
- **Lancez un programme pilote** : Évaluez cette technologie dans le contexte propre à votre entreprise.
- **Consultez nos experts** : Échangeons ensemble sur les questions de conformité qui vous concerne et définissons un mode d'utilisation de l'IA qui corresponde à vos besoins.

Pour consulter nos FAQ et obtenir plus de détails techniques ou de conseils sur les bonnes pratiques en matière de déploiement, n'hésitez pas à contacter votre représentant SoSafe ou à consulter notre portail d'aide en ligne.

Découvrez comment Sofie résout vos problèmes de conformité en temps réel.

Demandez une démo dès aujourd'hui.

Références

Groupe d'experts de haut niveau de la Commission européenne sur l'intelligence artificielle. 2019. « Lignes directrices en matière d'éthique pour une IA digne de confiance, chapitre II : Parvenir à une IA digne de confiance. » Commission européenne, (avril).
<https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.

Parlement européen et Conseil de l'Union européenne. 2024. « Article 12 : Enregistrement. » Journal officiel de l'Union européenne, no L 277.
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>.

European Union Agency for Cybersecurity (ENISA). 2024. « ENISA Threat Landscape : The Year in Review. (en anglais) <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 décembre 2024.

Gartner est une marque déposée et une marque de service de Gartner, Inc et/ou de ses filiales aux États-Unis et à l'international. Elle est mentionnée dans le présent document avec l'autorisation des propriétaires. Tous droits réservés.