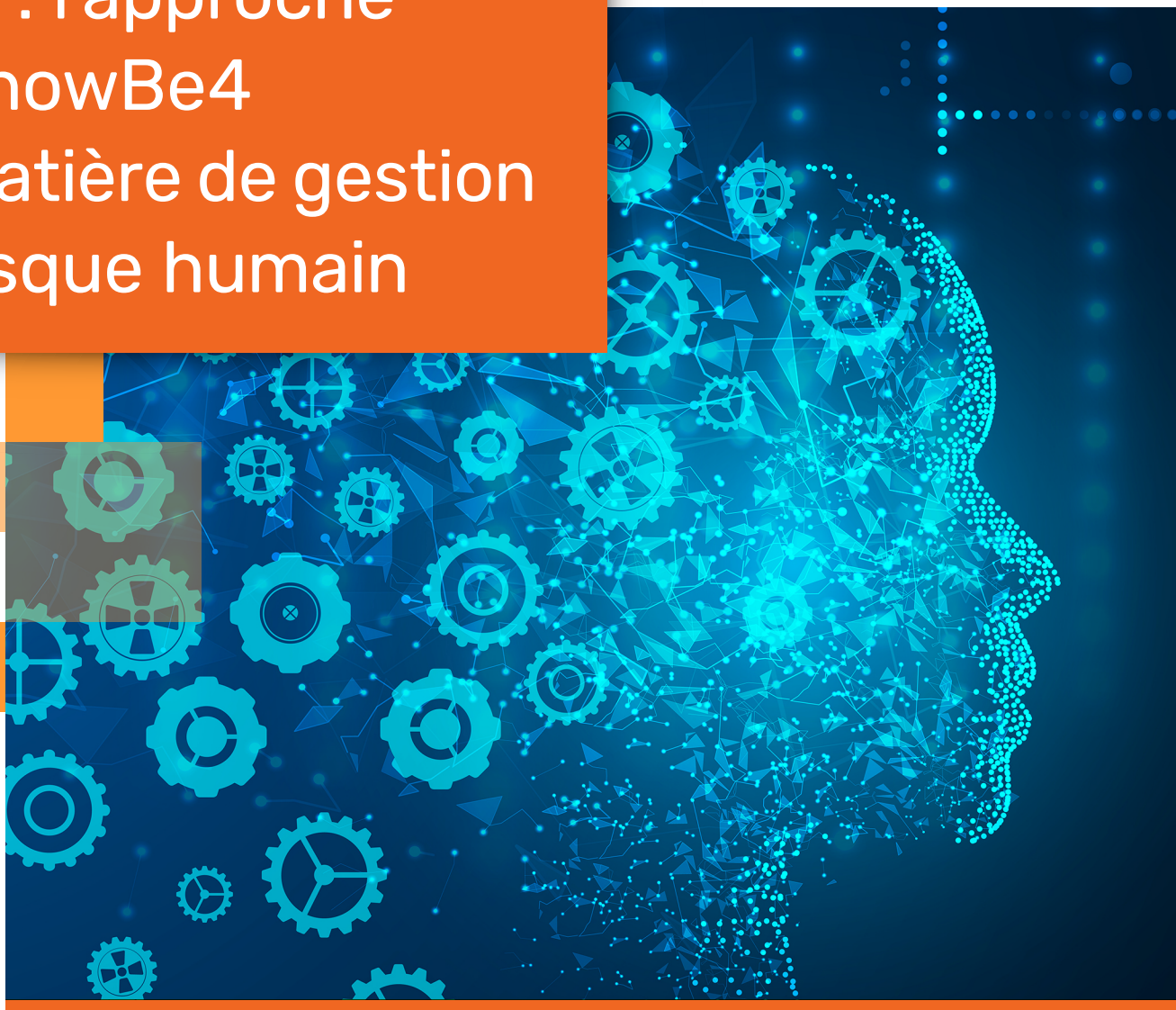
KnowBe4

Découvrez AIDA : l'approche de KnowBe4 en matière de gestion du risque humain



Sommaire

Introduction

La montée en puissance des cyberattaques basées sur l'IA attire l'attention de tous les professionnels de l'infosec. Selon une étude du secteur, plus de 95 % des professionnels de la cybersécurité estiment que le contenu généré par l'IA complique la détection des tentatives d'hameçonnage.

En passant entre les mains de personnes malintentionnées, cette avancée technologique a engendré une nouvelle forme d'attaques d'ingénierie sociale très convaincantes contre lesquelles les formations classiques et génériques sur la sensibilisation à la sécurité peinent à lutter.

Il est temps de combattre l'IA avec l'IA : laissez-nous vous présenter AIDA (Artificial Intelligence Defense Agents) de KnowBe4. AIDA est une suite d'agents alimentés par l'IA qui renforce votre approche de la gestion du risque humain (HRM pour « human risk management »). AIDA fait appel à diverses technologies d'IA pour créer des formations personnalisées et adaptatives destinées aux utilisateurs. Extrêmement efficaces, elles parviennent à modifier réellement leur comportement.

Dans ce livre blanc, nous verrons comment chacun des quatre premiers agents AIDA peut contribuer à améliorer votre stratégie HRM et examinerons des exemples concrets d'utilisation.

Quelques mots sur AIDA

AIDA est une suite IA native complète d'agents qui révolutionne la façon dont les organisations abordent les formations sur la sensibilisation à la sécurité. Grâce à l'IA, AIDA propose une formation hyperpersonnalisée, efficace et adaptative qui réduit les risques organisationnels et induit un changement de comportement durable.

Contrairement à d'autres produits de formation traditionnelle sur la sensibilisation à la sécurité, KnowBe4 AIDA apprend en permanence et s'adapte aux besoins uniques de votre organisation, optimisant ainsi l'impact et le retour sur investissement de vos efforts de sensibilisation à la sécurité. Par exemple, avec AIDA, le temps consacré par vos administrateurs à la création du contenu de formation passe d'une durée moyenne de sept jours à seulement quelques secondes. Votre équipe de sécurité gagne ainsi un temps plus que précieux.

Nous reviendrons plus en détail sur chacune des quatre fonctionnalités centrales d'AIDA dans la suite de ce livre blanc, mais en voici déjà un aperçu :

Agent Formation automatisée : il s'appuie sur l'IA en utilisant 316 indicateurs influençant 37 facteurs dans 7 domaines de connaissance différents afin d'analyser l'historique d'apprentissage de vos utilisateurs, le rôle associé à leur poste, leur score de risque, leurs modèles de comportement et même leurs langues, afin qu'AIDA puisse automatiquement leur attribuer le contenu le plus pertinent et le plus attrayant. Ainsi, chacun de vos utilisateurs, quel que soit son poste ou son lieu de travail, reçoit une formation adaptée à ses besoins spécifiques et à son style d'apprentissage. Cela permet d'optimiser la rétention des connaissances et l'application concrète des bonnes pratiques en matière de sécurité.

Agent Génération de modèles : grâce à l'IA générative, AIDA crée des modèles d'hameçonnage ultra-réalistes capables d'imiter les vecteurs d'attaque actuels. Les signes d'ingénierie sociale, ou signaux d'alarme, sont basés sur le cadre de mesure de la vulnérabilité à l'hameçonnage « Phish Scale Framework » du NIST.

Agent Actualisation des connaissances : AIDA propose des actualisations des connaissances à intervalles optimaux, veillant ainsi à ce que vos utilisateurs mettent vraiment les concepts de sécurité essentiels en application.

Agent Tests sur les politiques : AIDA génère des tests intelligents basés sur les politiques de sécurité et de conformité spécifiques à votre organisation. Vous avez ainsi l'assurance que vos utilisateurs ne se contentent pas d'accepter les consignes qu'ils sont censés suivre, mais qu'ils les comprennent vraiment.

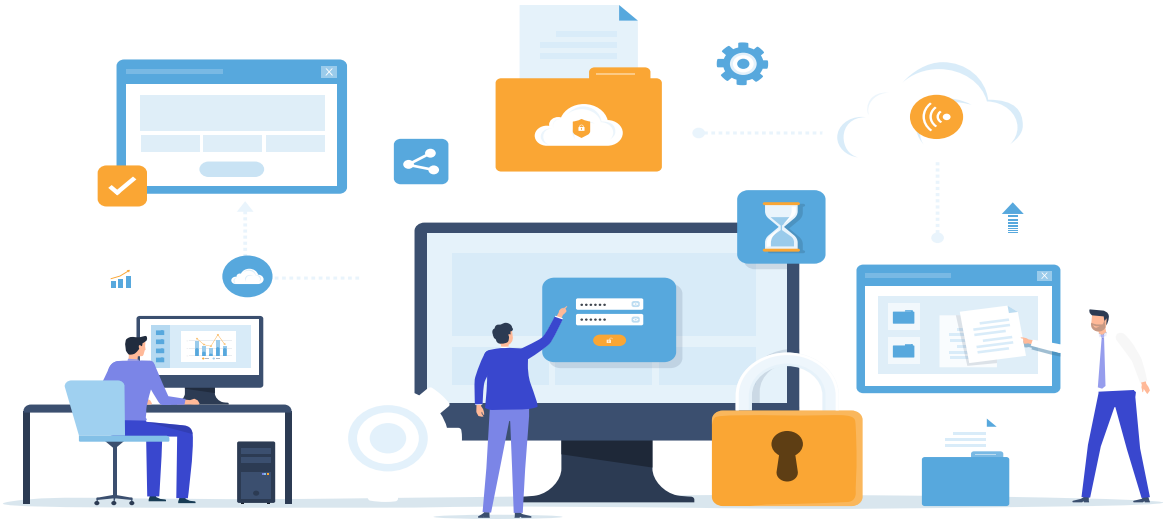
Lien avec la gestion du risque humain (HRM)

La HRM représente aujourd'hui le principal moyen de répondre au besoin permanent de forger une culture de la sécurité solide dans les organisations, quelle que soit leur taille. Cette approche ne se limite pas à dispenser une simple formation sur la sensibilisation à la sécurité à intervalles réguliers. Elle a pour objectif d'instaurer une culture de la sécurité positive en s'appuyant sur trois tactiques principales :

1. Quantifier le risque humain en détectant les comportements humains et en évaluant leurs caractéristiques
2. Utiliser ces mesures pour déployer un contenu de formation pertinent et adapté
3. Mettre en place des actualisations récurrentes des connaissances pédagogiques pour s'assurer que les utilisateurs savent comment se protéger contre les cyberrisques les plus répandus et ayant l'impact le plus important

En raison de leur caractère générique, les formations sur la sensibilisation à la sécurité disponibles sur le marché ne sont plus efficaces face à la complexité des environnements de travail actuels. Il en va de même des formations ponctuelles organisées une fois par an. De plus, l'emploi du temps des utilisateurs ayant tendance à s'alourdir, il convient d'exploiter au mieux le temps dont ils disposent pour la formation. L'adoption d'une stratégie HRM vous permet de proposer un contenu pertinent et motivant, capable de modifier les comportements des utilisateurs et de trouver un écho auprès des différents rôles et services, dans plusieurs langues. AIDA constitue l'épine dorsale de cette approche.

Nous allons maintenant nous pencher sur les quatre premières fonctionnalités d'AIDA, grâce auxquelles tout ceci est possible, avant d'évoquer les développements à venir.



Les quatre premiers agents d'AIDA

Avant de passer en revue ces quatre agents, intéressons-nous à une composante clé de KnowBe4 sur laquelle ils s'appuient : le SmartRisk Agent™ de KnowBe4. Cet instrument fournit des statistiques et des données exploitables, appelées scores de risque, pour vous aider à mieux comprendre les forces et les faiblesses de votre organisation en matière de sécurité.

SmartRisk Agent exploite les données comportementales de l'utilisateur final issues de l'ensemble des produits de KnowBe4 en vue de mesurer le cyberrisque associé aux êtres humains. Les scores de risque multidimensionnels de cet agent sont conçus de façon à faciliter la détection des problèmes potentiels aux niveaux de l'utilisateur, du groupe et de l'organisation. Vous obtiendrez des informations clés de plus en plus complètes au fur et à mesure que vous utiliserez les produits KnowBe4.

Découvrons maintenant ensemble ces quatre agents.

Agent Formation automatisée

Que fait-il ?

L'agent Formation automatisé analyse un nombre important de points de données, notamment les scores de risque, les résultats des tests d'hameçonnage et les préférences d'apprentissage individuelles, en vue de créer une expérience de formation personnalisée pour chaque utilisateur. Il se distingue par sa capacité à identifier les lacunes en matière de connaissances et à y remédier grâce à des modules d'apprentissage ciblés qu'il puise dans l'énorme bibliothèque de contenu ModStore de KnowBe4.

Comment l'utiliser ?

Vous devez configurer l'agent en fonction des besoins spécifiques de votre organisation, en définissant par exemple les critères d'inscription, les délais d'achèvement et les préférences de notification, le tout à partir de la console KnowBe4. Le mode test de l'agent vous permet de voir un aperçu des recommandations de formation avant leur déploiement complet et ainsi de vérifier que vous êtes satisfait des affectations automatisées.

Vous souhaitez surveiller les performances de la formation ? Vous avez accès à des statistiques de suivi telles que les taux d'achèvement des tâches et les résultats des enquêtes, qui vous permettent d'évaluer l'efficacité de votre programme de formation.

Exemples concrets

Lutte contre les vulnérabilités à l'hameçonnage : appuyez-vous sur les réponses ou les échecs des utilisateurs à des tests spécifiques de simulation d'hameçonnage et affectez automatiquement une formation qui leur enseigne les stratégies et les tactiques d'hameçonnage identifiées avant qu'ils n'y soient confrontés en situation réelle.

Accueil des nouveaux employés : évaluez le score de risque des nouveaux employés et suggérez des formations sur la sensibilisation à la sécurité adaptées à leur niveau de connaissances existant grâce à des groupes intelligents ciblés.

Agent Génération de modèles

Que fait-il ?

Le générateur de modèles d'hameçonnage produit des e-mails d'hameçonnage très convaincants, adaptés aux besoins spécifiques et au profil de risque de votre organisation, grâce à la puissance de l'IA générative intégrée. Il peut créer divers scénarios d'hameçonnage multilingues couvrant toute une gamme de niveaux de difficulté, de tons et de vecteurs d'attaque, afin que vos utilisateurs soient prêts à faire face à l'ensemble des éventuelles menaces qu'ils sont susceptibles de rencontrer en situation réelle.

Comment l'utiliser ?

Tous les ajustements relatifs notamment à la langue, aux paramètres régionaux, au ton et au vecteur d'attaque souhaité sont à votre disposition. Vous pouvez affiner le niveau de difficulté des simulations d'e-mails d'hameçonnage en sélectionnant des signes d'ingénierie sociale (SEI) spécifiques ou en choisissant un niveau de difficulté prédéfini. Une fois générés, les modèles peuvent être prévisualisés, modifiés et enregistrés afin d'être utilisés ultérieurement, ce qui vous permet de gagner un temps précieux lors de la création et de la gestion d'un programme de simulation d'hameçonnage robuste.

Exemples concrets

Simulation de compromission de la messagerie professionnelle : prenez une semaine par mois ou par trimestre pour rédiger des e-mails qui semblent provenir de votre PDG ou d'autres cadres supérieurs afin de tester spécifiquement le risque de compromission de la messagerie de l'entreprise. Exploitez les fonctionnalités d'IA générative de l'agent pour imiter le style d'écriture des cadres et solliciter un virement bancaire ou toute autre demande urgente.

Tests d'hameçonnage multilingues : rédigez et déployez rapidement des e-mails d'hameçonnage en plusieurs langues à l'intention d'un personnel international. Le générateur de modèles peut même adapter le texte de l'e-mail à une région spécifique en employant des expressions, des nuances et des styles culturels typiques.

Réponse rapide aux menaces émergentes : vous venez de repérer une toute nouvelle attaque dans le monde réel ? Il vous suffit de quelques minutes de travail aux commandes du générateur de modèles pour créer une copie simulant cette attaque par hameçonnage et préparer votre personnel à ce qui l'attend.

Agent Actualisation des connaissances

Que fait-il ?

L'agent d'actualisation des connaissances aide les utilisateurs à affûter leurs compétences en cybersécurité et à remporter des badges en répondant à des tests courts générés par l'IA, amusants et basés sur des scénarios. Les utilisateurs peuvent ainsi réviser rapidement les points clés de la formation qu'ils ont suivie récemment.

Comment l'utiliser ?

Vous devez activer et configurer cette fonctionnalité dans l'onglet Formation à AIDA ou lors de la création d'une nouvelle campagne de formation. Vous pouvez y définir des paramètres tels que l'intervalle de temps entre l'achèvement de la formation et la mise à disposition d'une actualisation des connaissances. Une fois cette fonctionnalité activée, les utilisateurs peuvent accéder à leurs actualisations de connaissances via leur Learner Experience, ce qui favorise la participation à cet élément récurrent de leur processus d'apprentissage.

Exemples concrets

Renforcement de la sensibilisation à l'hameçonnage : les actualisations de connaissances générées par l'IA et basées sur des scénarios peuvent être utilisées dans le cadre d'une formation de remise à niveau dispensée après qu'un utilisateur a cliqué sur un e-mail d'hameçonnage simulé, afin d'étayer la formation initiale. Ce renforcement continu permet de maintenir un bon niveau de vigilance face à l'évolution des tactiques d'hameçonnage.

Rétention du contenu de la formation sur la conformité : en proposant des actualisations régulières et ciblées sur des thèmes clés de la conformité, les organisations soumises à des exigences réglementaires particulières peuvent faire preuve d'une diligence constante en ce qui concerne le maintien d'une culture appropriée de la conformité, et ainsi réduire leurs lacunes et améliorer les résultats des audits.

Agent Tests sur les politiques

Que fait-il ?

Cet agent alimenté par l'IA génère automatiquement des questionnaires basés sur les politiques spécifiques de votre organisation afin de garantir que les employés ne se contentent pas de lire les informations critiques, mais les comprennent et les assimilent.

Comment l'utiliser ?

Dans votre console KnowBe4, vous commencez par ajouter la politique de votre organisation sous forme de fichier PDF. Une fois cela fait, vous pouvez modifier et gérer les questions du test sur la politique, puis créer une campagne de formation en vue d'assigner la politique à vos utilisateurs. Lorsqu'une politique est assignée à une campagne, vous pouvez suivre la progression et les confirmations d'acceptation de vos utilisateurs.

Exemples concrets

Accueil des nouveaux employés : grâce à des questionnaires sur mesure, vous vous assurez que les nouveaux employés prennent connaissance des politiques et les comprennent. Cela peut servir de référence mesurable dans le cadre de leur formation initiale à la conformité et réduire le risque de violation des politiques due à une mauvaise compréhension.

Examen annuel des politiques : rationalisez votre processus de révision annuelle des politiques en utilisant l'agent Tests sur les politiques pour générer rapidement des questionnaires actualisés qui reflètent toutes les modifications apportées aux consignes et aux règles de l'entreprise. Les campagnes de formation basées sur les politiques contribueront à assurer la rétention des connaissances et fourniront aux administrateurs des mesures claires concernant la compréhension des politiques dans l'ensemble de l'entreprise, ce qui permettra d'identifier les domaines susceptibles de nécessiter une formation supplémentaire ou des éclaircissements.

Perspectives

Les fonctionnalités de ces quatre agents vont s'améliorer de manière significative au fur et à mesure de leur fonctionnement en synergie selon un modèle d'orchestration alimenté par l'IA qui utilise une approche constamment active basée sur les objectifs, visant à réduire au minimum le risque humain au sein de votre organisation.

Mais ce n'est là qu'un début. Voici les prochains éléments qui viendront les compléter :

- **Agent d'orchestration :** cet agent alimenté par l'IA fera office d'administrateur de la formation sur la sensibilisation à la sécurité, en gérant les simulations d'hameçonnage, leur diffusion et la création de rapports.
- **Agent axé sur les objectifs :** cet agent optimisera le ciblage, les vecteurs d'attaque et la fréquence des formations afin de réduire au maximum le risque humain au sein de votre organisation.
- **Agent de défense adaptatif :** en tenant compte des horaires de travail et des menaces actuelles, cet agent programmera la formation aux moments les moins perturbants et adaptera le contenu afin de faire face aux risques émergents.
- **Agent d'évaluation de la formation sur la sensibilisation à la sécurité :** cet agent mettra en place des évaluations personnalisées de la formation sur la sensibilisation à la sécurité en s'appuyant sur les politiques et les procédures spécifiques de votre organisation.

Conclusion

AIDA n'est pas qu'un simple pas de plus dans l'approche HRM de KnowBe4 : c'est un véritable bond en avant, axé sur une suite d'agents IA native qui révolutionnent votre façon d'aborder la HRM. AIDA donne à votre organisation les moyens de garder une longueur d'avance en vous protégeant contre les menaces de l'IA, à l'aide de l'IA.

Voici les avantages qu'AIDA vous apporte, à vous et à votre organisation :

- Alignée sur l'outil « Phish Scale Framework » du NIST américain (National Institute of Standards and Technology), la suite AIDA met en phase votre formation sur la sensibilisation à la sécurité avec les initiatives globales de sécurité de votre organisation.
- Le temps consacré par vos administrateurs à la création du contenu de formation passe d'une durée moyenne de 7 jours à seulement quelques secondes. AIDA libère ainsi un temps plus que précieux pour votre équipe de sécurité.
- Vous améliorez les relations entre votre équipe de sécurité et les autres services en alignant les utilisateurs sur les objectifs de sécurité, de quoi renforcer la culture de la sécurité de votre organisation.
- La gestion active et efficace du risque humain vous permet d'allouer une partie de votre budget de sécurité à d'autres initiatives clés.
- Vous optimisez la valeur de l'ensemble de vos technologies de sécurité existantes grâce à une intégration aisée d'AIDA.

KnowBe4 est le seul fournisseur qui couvre entièrement la sensibilisation, le comportement et la culture de la sécurité, permettant ainsi aux organisations de traiter l'aspect humain de la cybersécurité. KnowBe4 a pour objectif d'aider les organisations à mettre en place une culture de la sécurité solide, en adoptant une approche axée sur les données pour gérer le risque humain.

Voir AIDA en action

Ressources supplémentaires

Test de sécurité gratuit relatif à l'hameçonnage
Découvrez le pourcentage de Phish-prone de vos employés, en profitant de votre test de sécurité gratuit relatif à l'hameçonnage.

Programme automatisé de sensibilisation à la sécurité gratuit
Créez un programme de sensibilisation à la sécurité, personnalisé pour votre organisation.

Outil Phish Alert Button gratuit
Un seul clic suffit désormais à vos employés pour signaler les attaques par hameçonnage de manière sécurisée.

Outil Email Exposure Check (EEC) gratuit
Identifiez avant les pirates les adresses e-mail à risque de vos utilisateurs.

Outil Domain Spoof Test gratuit
Déterminez si les pirates peuvent usurper une adresse e-mail de votre domaine.

À propos de KnowBe4

KnowBe4 offre à votre personnel les moyens de prendre au quotidien des décisions plus éclairées en matière de sécurité. Des dizaines de milliers d'organisations dans le monde font confiance à la plateforme KnowBe4 pour renforcer leur culture de la sécurité et réduire le risque humain. KnowBe4 crée une couche dite « humaine » de défense afin que les organisations puissent renforcer les comportements des utilisateurs en les sensibilisant à la sécurité de façon inédite, et en les formant à la conformité.

Le déploiement de KnowBe4 rend les utilisateurs vigilants et attentifs aux dommages causés par l'hameçonnage, les rançongiciels et les autres menaces découlant de l'ingénierie sociale. La plateforme comprend une suite complète de programmes de sensibilisation et de formation à la conformité, un coaching des utilisateurs en temps réel, une simulation d'ingénierie sociale optimisée par l'IA et une défense anti-hameçonnage basée sur des actions collaboratives.

Offrant du contenu en plus de 35 langues, KnowBe4 fournit la plus grande bibliothèque au monde, toujours actualisée avec du contenu engageant vous permettant de renforcer votre pare-feu humain.

Pour en savoir plus, consultez la page www.KnowBe4.com

KnowBe4

KnowBe4 NL, BV | Central Park, Stadsplateau 27-29, 3521 AZ Utrecht, Pays-Bas |
Tél. : +31 (0)30 7996074 | www.KnowBe4.com | E-mail : Sales@KnowBe4.com

08F01K01