Intéressant pour les employés, efficace pour les responsables.

Essai gratuit
k-asap.fr

Kaspersky ASAP : Automated Security Awareness Platform

kaspersky bring on the future

Kaspersky Automated Security Awareness Platform

Kaspersky ASAP : Automated Security Awareness Platform

82 % des cyberincidents sont dus à une erreur humaine, ce qui fait perdre des millions aux entreprises. Les programmes de formation traditionnels ne sont pas conçus pour répondre à ce problème, et une nouvelle approche est nécessaire. Dites bonjour à Kaspersky ASAP.

L'erreur humaine est le plus grand risque informatique

79 %
des salariés
admettent s'être livrés à au moins une activité à risque au cours de l'année précédente alors qu'ils étaient conscients des risques*

51 %
des salariés
pensent que leur service informatique devrait être entièrement responsable de la prévention des cyberattaques dont leur employeur est victime*

55 %
des entreprises
signalent des menaces dues à une utilisation inappropriée des technologies informatiques par les employés**

51 %
des petites entreprises
ont subi un incident de sécurité à la suite d'une violation des politiques de sécurité informatique par des employés**

26 %
des salariés
déclarent que leur adresse email personnelle utilise le même mot de passe que leur compte professionnel***

Obstacles au lancement d'un programme de sensibilisation à la sécurité efficace

Si les entreprises sont disposées à mettre en œuvre des programmes de sensibilisation aux questions de sécurité, beaucoup sont mécontentes du processus et des résultats. Les PME en particulier rencontrent des difficultés, car elles n'ont généralement pas l'expérience ni les ressources nécessaires.

Inefficace pour les étudiants

Perçus comme difficiles, ennuyeux et assimilables à une corvée superflue

Uniquement des interdictions plutôt que des explications

Les connaissances ne sont pas retenues

La lecture et l'écoute ne sont pas aussi efficaces que l'action

Une contrainte pour les administrateurs

Comment créer un programme et fixer des objectifs ?

Comment gérer les missions de formation ?

Comment contrôler les progrès ?

Comment s'assurer que notre personnel est bien investi ?

* « Balancing Risk, Productivity, and Security » (Équilibrer les risques, la productivité et la sécurité), Delinea, 2021

** Rapport « IT security economics 2022 » (Économie de la sécurité informatique 2022), Kaspersky

*** https://www.beyondidentity.com/blog/password-sharing-work

Une formation efficace et facile à gérer pour les organisations de toutes tailles

Présentation de Kaspersky ASAP (Automated Security Awareness Platform), une solution qui constitue l'épine dorsale du programme de formation Kaspersky Security Awareness. Cette plateforme est un outil en ligne qui permet aux employés d'acquérir des compétences solides en matière de cyberhygiène tout au long de l'année, ce qui a pour effet **de réduire le nombre de cyberincidents impliquant des personnes au sein des organisations.**

Le lancement et la gestion de la plateforme ne requièrent aucune ressource ni disposition spécifique. Cette plateforme fournit une aide intégrée à chaque étape de son parcours d'apprentissage vers un environnement de cybersécurité.

Un contenu pertinent et incontournable

L'un des critères les plus importants dans le choix d'un programme de sensibilisation est son efficacité. Le programme ASAP est efficace, tant du point de vue du contenu que de la gestion de la formation. Le contenu repose sur une expérience cumulée de **plus de 25 ans dans le domaine de la cybersécurité**, présentée sous la forme d'un modèle de compétences comprenant plus de **350 notions de cybersécurité pratiques et indispensables** à tous les employés.

Formez vos employés à la cybersécurité.
Transformez leur attitude et leur comportement et protégez votre entreprise ainsi que vos systèmes informatiques.

Formation efficace

Cohérente	– Contenu bien pensé et structuré – Des cours interactifs, un renforcement constant, des tests et des simulations d'attaques par phishing pour veiller à l'application des compétences Le contenu et la structure du matériel de formation tiennent compte des particularités de la mémoire humaine et de notre faculté à absorber et à retenir l'information.
Pratique et motivante	– Pertinente pour le travail quotidien des salariés – Des compétences qui peuvent être mises en pratique immédiatement Des exemples concrets auxquels les employés peuvent s'identifier contribuent à susciter l'intérêt du participant, ce qui favorise la mémorisation des informations.
Positive	– Permet d'inculquer de manière proactive des comportements plus sûrs – Explique « pourquoi » et « comment » au lieu d'interdire simplement Trop de règles et de restrictions peuvent susciter le mécontentement et un découragement, tandis que des explications et des principes en adéquation avec le mode de pensée naturel des utilisateurs contribuent à leur adhésion et à la modification de leur comportement.

Administration simplifiée

Gestion simplifiée	– La gestion entièrement automatisée des formations aide tous les salariés à atteindre les compétences adaptées à leur profil, sans aucune intervention de l'administrateur de la plateforme – La synchronisation avec AD (Active Directory), l'authentification unique (SSO), l'API ouverte (la possibilité d'interagir avec des solutions tierces), l'accueil en ligne lors de la première visite, une section FAQ ainsi que des conseils rendent la prise en main de la plateforme pratique et efficace.
Contrôle simplifié	Tableau de bord « tout-en-un » et rapports exploitables : – rapport sur l'avancement des cours – rapports sur les tests et les simulations d'attaques de phishing
Participation simplifiée	La plateforme envoie automatiquement des invitations et des rappels, ainsi que des rapports aux utilisateurs et aux administrateurs.

Formules des services

Kaspersky ASAP est disponible en trois options différentes, selon vos préférences :

- **Solution entièrement en ligne basée dans le cloud.** Dans ce cas, les données des utilisateurs sont traitées dans le respect total de la législation, en fonction de l'emplacement du serveur choisi. Par exemple, si vous choisissez l'Europe, les données seront stockées dans l'Union européenne (à Francfort, en Allemagne) et toutes les données légalement protégées seront traitées conformément aux règlements sur la protection des données de l'Union européenne (RGPD).
- **Contenu dans un paquet SCORM.** Cette option permet d'intégrer les modules de formation à votre système de gestion de l'apprentissage (LMS) interne. Veuillez cependant noter que cette option n'inclut pas les tests et les simulations d'attaques de phishing
- **Sur site.** Cette option est destinée aux clients qui ont besoin d'un niveau de confidentialité maximal. Pour les entreprises soumises à une forme ou une autre de contrôle réglementaire, le déploiement sur site favorise la mise en conformité, ce qui vous permet d'éviter les amendes ou les pénalités. Les formations sont déployées sur le réseau du client et vous contrôlez entièrement le matériel du serveur, la sécurité des données ainsi que la configuration. Les utilisateurs peuvent accéder au matériel de formation même sans connexion Internet.

Gestion ASAP : la simplicité par une automatisation complète

Démarrez votre programme en 4 étapes simples

1

Ajouter des utilisateurs

Utilisez la **synchronisation AD**, chargez un fichier .xlsx ou ajoutez-en un manuellement

2

Diviser les utilisateurs par groupes

Divisez les utilisateurs manuellement ou à l'aide de règles en fonction du niveau cible souhaité

3

Lancer la formation

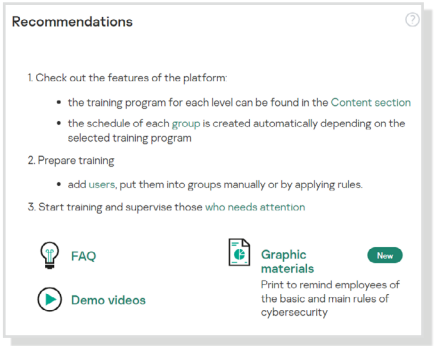
Répartissez les utilisateurs manuellement ou à l'aide de règles en fonction du niveau souhaité, et définissez la date de début pour chaque groupe

4

Gestion des formations automatisé effectuée par ASAP

ASAP crée une planification pour chaque groupe, pour les invitations, les rappels et autres communications – tout se fait automatiquement

L'accueil lors de la première connexion, les recommandations, la FAQ et les vidéos de démonstration, expliquant le fonctionnement de la plateforme du point de vue de l'administrateur et de l'utilisateur – tout ce dont vous avez besoin pour commencer le processus d'apprentissage se trouve sur la page principale de l'administrateur.



Une approche nouvelle et améliorée des formations

Kaspersky ASAP change la façon dont nous fournissons du contenu de formation à la cybersécurité. Vous pouvez désormais choisir d'attribuer aux salariés une formation express de base qui vous permettra de répondre rapidement aux exigences réglementaires en matière de formation à la cybersécurité, ou de rafraîchir leurs connaissances, ou d'opter pour la formation principale déclinée en plusieurs niveaux de complexité

Thèmes abordés

Thèmes abordés

Formation principale	Formation express
Email	Email
Mots de passe et comptes	Mots de passe et comptes
Sites Web et Internet	Sites Web et Internet
Réseaux sociaux et messageries	Sécurité des appareils mobiles
Sécurité pour PC	Réseaux sociaux
Appareils mobiles	Mon ordinateur
Protection des données confidentielles	Protection des données confidentielles
Données personnelles	Doxing
RGPD	Sécurité des cryptomonnaies
Industrial Cybersecurity	Sécurité de l'information dans le cadre du travail à distance
Sécurité des cartes bancaires et norme PCI DSS	Loi fédérale 152-FZ (pour la Russie)
Sécurité physique des données	Loi fédérale FZ-187 (sécurité des infrastructures d'informations critiques pour la Russie)

Les thèmes sont divisés en grands blocs, couvrant de nombreux concepts de sécurité informatique*.

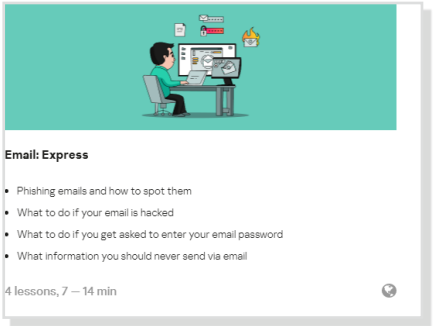
#Mots de passe #Phishing #Comptes d'entreprise #Messages dangereux #Cartes bancaires #Ransomware #Ingénierie sociale #Fichiers dangereux #Utilisation des navigateurs #Éthique de l'entreprise #Antivirus #Programmes malveillants #Applications #Navigateur #Informations confidentielles. Stockage d'informations #Envoi d'informations #Données personnelles #Internet et la loi #Législation européenne #Entreprise #Liens dangereux #Faux sites Internet #Sites ransomwares #Sauvegarde #Données mobiles #Chiffrement #Services cloud #Espionnage industriel #PCI DSS #Authentification à deux facteurs #Empreinte numérique #Torrents #Catfishing #Attaque ciblée #Hachage #Jetons #Schéma #Minage #Contrôle parental

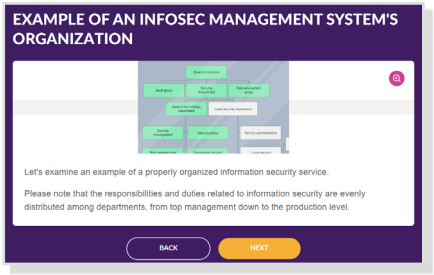
* Pour obtenir la liste la plus récente des thèmes et des concepts, veuillez consulter le site k-asap.com/fr

Chaque thème comprend plusieurs niveaux, chacun comportant une description des compétences en matière de sécurité. Les niveaux sont définis en fonction du degré de risque qu'ils contribuent à éliminer. Par exemple, le niveau 1 est normalement suffisant pour se protéger des attaques les plus simples et des attaques de masse. Il convient d'étudier les niveaux supérieurs pour apprendre à se protéger contre les attaques les plus complexes et les plus ciblées.

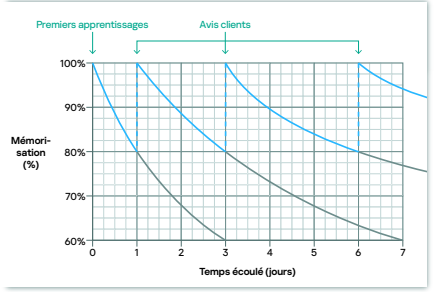
Exemple : Compétences enseignées dans le thème « Sites Web et Internet »

Débutant Éviter les attaques massives (bon marché et faciles)	**Élémentaire** Éviter les attaques massives sur un profil spécifique	**Intermédiaire** Éviter les attaques ciblées bien préparées	**Avancé*** Éviter les attaques ciblées
23 compétences, notamment : – Reconnaître les fausses fenêtres contextuelles – Faire attention aux redirections – Distinguer les liens de téléchargement authentiques des faux – Reconnaître les fichiers exécutables trouvés sur le Web – Être capable de déterminer l'authenticité d'une extension de navigateur	**34 compétences, notamment :** – Saisir des données uniquement sur les sites disposant d'un certificat SSL valide – Utiliser des mots de passe variés pour les différentes inscriptions – Reconnaître les faux sites par un certain nombre de signes – Éviter les liens numériques – Reconnaître les adresses de liens réseau invalides par la présence de faux sous-domaines	**12 compétences, notamment :** – Vérifier les liens de partage avant de les envoyer – Utiliser uniquement des logiciels de fabricants fiables pour télécharger des torrents – Télécharger uniquement du contenu légal à partir des torrents – Effacer régulièrement les cookies des navigateurs	**13 compétences, notamment :** – Reconnaître des liens contrefaits sophistiqués (dont des liens ressemblant au site Web de votre entreprise et des liens avec redirections) – Vérifier les sites à l'aide d'utilitaires spéciaux – Reconnaître si le navigateur est en train de faire du minage – Éviter des sites référencés sur liste noire
	+ renforcement des compétences élémentaires	+ renforcement des compétences précédentes	+ renforcement des compétences précédentes





Courbe de l'oubli d'Ebbinghaus



Formation express ASAP

Une version courte de la formation au format audio-vidéo. Chaque thème de cybersécurité contient plusieurs cours succincts destinés à aider l'utilisateur à acquérir les compétences de base en matière de cybersécurité.

- Théorie interactive
- Vidéos
- Tests

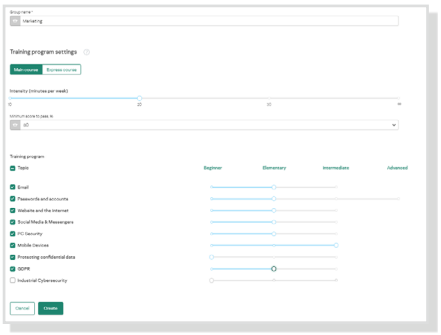
Les simulations d'attaques de phishing ne sont pas incluses dans le parcours d'apprentissage, mais peuvent être attribuées séparément par l'administrateur.

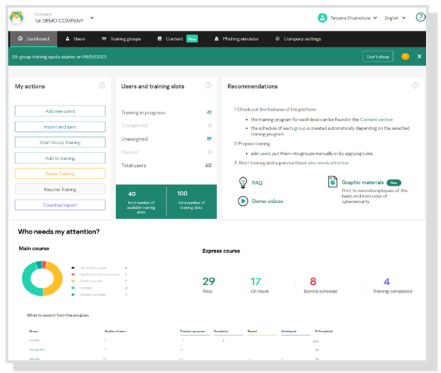
Formation principale ASAP

La formation se fonde sur les particularités de la mémoire humaine :

- Contenu multimodal :
  - chaque unité inclut : une évaluation de l'apprentissage via des cours interactifs (test et simulation d'attaque par phishing, le cas échéant) ;
  - tous les éléments de formation étayent la compétence particulière développée dans chaque unité, de sorte que les compétences soient totalement maîtrisées et fassent partie intégrante du nouveau comportement souhaité.
- Apprentissage par intervalles :
  - les éléments de formation se succèdent à certains intervalles, ce qui favorise la mémorisation plutôt que le simple enchaînement des cours. Les intervalles reposent sur l'étude de la « courbe de l'oubli » d'Ebbinghaus ;
  - la répétition crée des comportements sûrs et aide à retenir l'information.
- Un contenu équilibré, structuré et pertinent par rapport aux situations réelles est synonyme d'efficacité :
  - des exemples concrets qui mettent en évidence l'importance personnelle de la cybersécurité pour les salariés ;
  - la plateforme met l'accent sur le développement des compétences et non uniquement sur la mise à disposition de connaissances. Les exercices pratiques sont donc au cœur de chaque module.

Une gestion flexible des formations





Formation souple

Le domaine de formation est entièrement flexible, tout en conservant les avantages de la gestion automatisée et séquentielle des formations. Pour chaque groupe d'entraînement, vous pouvez choisir :

- la formation principale ou express, ou une combinaison des deux ;
- les thèmes à aborder dans la formation principale et/ou la formation express que les participants du groupe doivent apprendre ;
- le niveau cible que vous souhaitez que les apprenants atteignent pour chaque thème sélectionné dans la formation principale.

Le parcours d'apprentissage sera automatiquement créé par la plateforme pour chaque groupe de participants en fonction de ces paramètres.

Faites tout à partir du tableau de bord

- Tout ce dont vous avez besoin pour contrôler et gérer la formation (statistiques, résumés des activités et des progrès des utilisateurs, créneaux de formation, formation de groupe, suggestions sur la manière d'améliorer les résultats) peut être fait à partir du tableau de bord. Vous pouvez télécharger les rapports en un seul clic et configurer leur fréquence.

La liberté d'exceller

- Les employés peuvent se former à leur convenance et à partir de n'importe quel appareil, grâce à la conception conviviale d'ASAP qui rend l'apprentissage pratique et agréable.
- Les utilisateurs peuvent accéder au portail de formation à partir des liens personnalisés fournis dans l'invitation à la formation ou via un lien unique pour tous les utilisateurs avec la technologie d'authentification unique si elle est configurée par l'administrateur.

Personnalisation

L'administrateur peut facilement modifier l'apparence du programme :

- remplacer le logo de Kaspersky par celui de votre entreprise dans le volet d'administration, le portail de formation et les emails de la plateforme ;
- personnaliser les certificats ;
- ajouter un contenu personnel à n'importe quel cours.

Intégration

Vous pouvez utiliser Open API pour interagir avec des solutions tierces. Open API fonctionne via HTTP et offre un ensemble de méthodes de demande/réponse.

ASAP s'intègre aux plateformes Kaspersky KUMA et XDR :

– L'administrateur peut voir un événement dans XDR et prendre les mesures appropriées, y compris attribuer une formation dans ASAP

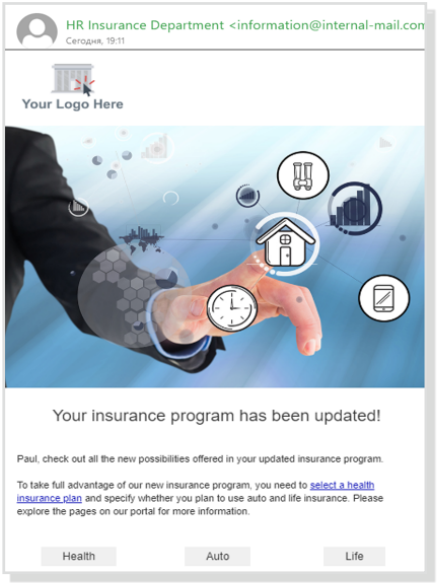
– Enrichissement automatique des fiches d'incidents avec des informations sur le niveau de sensibilisation de l'utilisateur attaqué

Localisation

ASAP est disponible en 25 langues*. La localisation dans ASAP ne se limite pas à une simple traduction : les textes et les images ne sont pas seulement traduits dans différentes langues, ils sont également adaptés de manière à tenir compte des différentes cultures et mentalités locales.

* La liste actuelle des langues disponibles est disponible sur le site k-asap.com/fr

Exemple de modèle de phishing simulé modifiable et de commentaires



Simulations de campagnes de phishing

La formation principale est complétée par des campagnes de phishing. Celles-ci permettent de tester les compétences pratiques des employés en matière de prévention des attaques de phishing, et aident les responsables de la formation à identifier rapidement les lacunes dans les connaissances des utilisateurs et à encourager l'approfondissement des thèmes difficiles. Les campagnes de phishing sont également un excellent outil pour apprendre aux employés à reconnaître les signes potentiellement dangereux et à mettre leurs connaissances en pratique.

La plateforme propose des modèles d'emails prêts à l'emploi contenant des exemples de phishing qui peuvent être envoyés aux utilisateurs dans toutes les langues disponibles. Les modèles sont régulièrement mis à jour et des nouveautés sont ajoutées. Vous pouvez également créer des emails personnalisés à partir de modèles prédéfinis.

Essayez de simuler une attaque de phishing avant de commencer la formation – vérifiez la résilience de vos employés ! Cette action permettra aux salariés et à la direction de constater les avantages de la formation.

Les employés peuvent également démontrer leur compréhension d'un thème en ne tombant pas dans le piège d'une simulation d'attaque informatique et en signalant les emails de phishing via l'outil « Signaler une tentative de phishing ».

L'outil « Signaler une tentative de phishing » indique le niveau de sensibilisation des employés, supprime les emails de la boîte de réception et envoie des messages non seulement à l'administrateur de la plateforme, mais aussi aux équipes informatiques et aux équipes de sécurité informatique, ce qui permet aux entreprises d'améliorer leurs niveaux de détection et de réponse en matière de phishing.

Kaspersky ASAP pour les partenaires MSP/ MSSP ou les entreprises avec une structure géographiquement distribuée

La plateforme permet de déployer et de gérer des formations de sensibilisation dans plusieurs entreprises à partir d'une console unique prête pour la multilocation, sans besoin de logiciel supplémentaire.

Bonne nouvelle ! Kaspersky ASAP dispose d'une fonctionnalité de gestion des quotas de licences qui permet d'attribuer un quota de licences pour chaque entreprise avec une certaine période de validité.

Il est également possible d'ajouter des administrateurs supplémentaires pour chaque entreprise et de leur attribuer des rôles différents.

Kaspersky Security Awareness : une nouvelle approche pour maîtriser les compétences en matière de sécurité informatique

Principaux facteurs de différenciation des programmes

Une expertise considérable en matière de cybersécurité
Plus de 25 ans d'expérience dans le domaine de la cybersécurité transformés en un ensemble de compétences de cybersécurité qui est au cœur de nos produits

Des formations qui modifient le comportement des employés à chaque niveau de votre organisation
Notre formation ludique stimule l'intérêt et la motivation grâce au divertissement éducatif, tandis que les plateformes d'apprentissage permettent d'internaliser les compétences en matière de cybersécurité afin de s'assurer que les compétences acquises ne se perdent pas en cours de route.

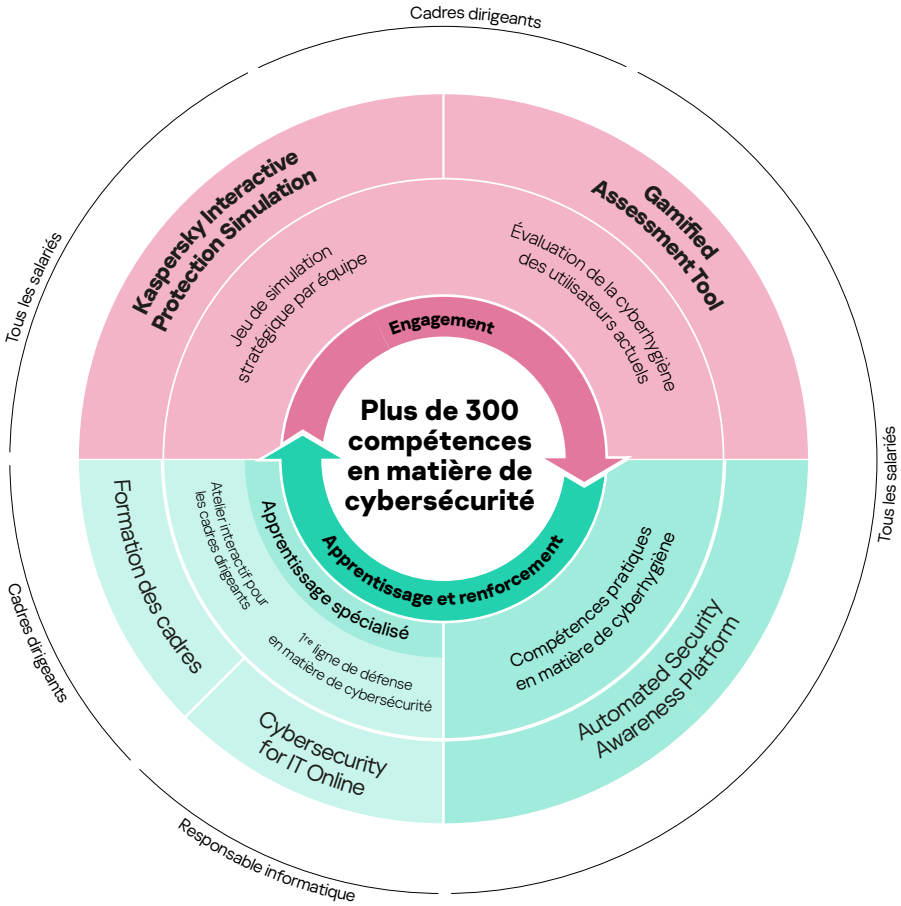
ASAP est un produit phare du portfolio de sensibilisation à la sécurité de Kaspersky.

Une solution de formation flexible accessible à tous

Kaspersky Security Awareness connaît un succès international de longue date. Utilisée par des entreprises de toutes tailles pour **former plus d'un million d'employés dans plus de 75 pays**, cette solution fait appel à plus de 25 ans d'expertise de Kaspersky en matière de cybersécurité ainsi qu'à une vaste expérience dans le domaine des formations pour adultes.

Le portfolio propose une gamme d'options de formation attrayantes qui sensibilisent vos employés à la cybersécurité à tous les niveaux, leur donnant ainsi les outils nécessaires pour jouer leur rôle dans la cybersécurité globale de votre organisation.

Étant donné que les changements durables de comportement prennent du temps, notre approche consiste à mettre en place un cycle d'apprentissage continu qui englobe différents modules. L'apprentissage par le jeu engage les cadres supérieurs, les transformant en partisans des initiatives de cybersécurité et de l'instauration d'une culture de cyber-comportement sûr. La ludification du processus d'évaluation permet d'identifier les lacunes dans les connaissances des employés et de les motiver à poursuivre leur apprentissage, tandis que les plateformes en ligne et les simulations leur permettent d'acquérir de solides compétences.



Kaspersky ASAP essai gratuit : k-asap.com/fr
Solutions de cybersécurité pour les entreprises : www.kaspersky.fr/enterprise-security
Kaspersky Security Awareness :
www.kaspersky.fr/enterprise-security/security-awareness
Actualités dédiées à la sécurité informatique : business.kaspersky.fr

www.kaspersky.fr

kaspersky bring on the future