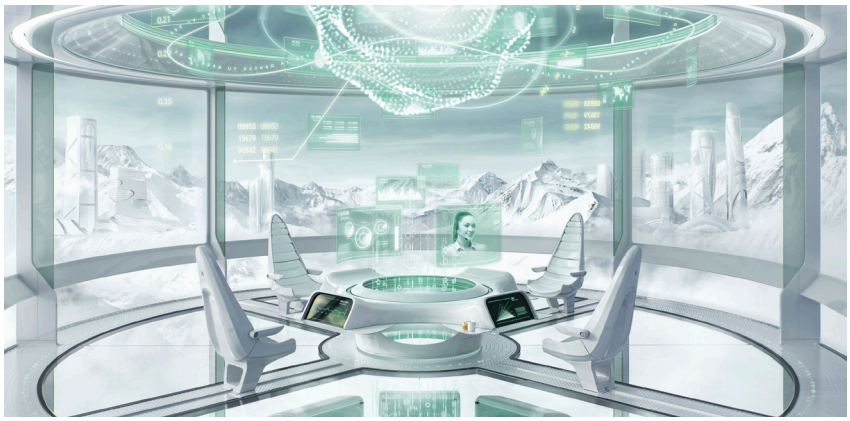
kaspersky

Dépliant du fabricant
Kaspersky / ASAP



Formation à la sécurité pour tous

La formation automatisée Security Awareness depuis le cloud sensibilise les collaborateurs à la cybersécurité

Kaspersky ASAP: les points forts

- Formation automatisée de sensibilisation à la sécurité
- E-mails automatiques de motivation et d'invitation avec recommandations individuelles
- Formation ciblée, basée sur les rôles
- Des exemples pratiques permettant d'acquérir des compétences immédiatement applicables
- Centré sur le mode de pensée naturel et la mémoire humaine
- Apprentissage continu, étape par étape
- Solution en mode cloud: évolutive de la PME à l'entreprise mondiale
- Gestion automatisée de la formation

Kaspersky a été fondé à Moscou en 1997. Aujourd'hui, le spécialiste de la sécurité est présent dans 200 pays, emploie plus de 4000 spécialistes hautement qualifiés et est considéré comme l'un des principaux fournisseurs de solutions de sécurité. Les technologies Kaspersky protègent environ 400 millions d'utilisateurs dans le monde et sont utilisées par plus de 270 000 entreprises et organisations. Les solutions et services de cybersécurité de Kaspersky englobent des services managés dans le cloud et des solutions sur site notamment Endpoint Security, Hybrid Cloud Security et Enterprise Security de nouvelle génération, y compris les solutions de sécurisation de l'IoT et des applications industrielles. La plateforme Kaspersky Automated Security Awareness Platform (ASAP) propose une formation en ligne automatisée mais personnalisée sur la sécurité, en fonction des rôles et des compétences de chaque collaborateur. Des exemples pratiques et des simulations enseignent des compétences qui peuvent être directement mises en œuvre dans la vie quotidienne. Les divers sujets abordés comprennent la gestion des comptes, les mots de passe, les appareils mobiles et les données confidentielles, la sécurité des e-mails, y compris la sensibilisation au phishing et le comportement sur les réseaux sociaux. ASAP offre également une gestion automatisée de la formation, de l'e-mail d'invitation jusqu'à l'évaluation de la réussite de l'apprentissage, et convient en tant que solution cloud évolutive pour toutes les tailles d'entreprise.

Plus d'informations sur les produits Kaspersky

BOLL
IT Security Distribution

Formation à la cybersécurité à la fois automatisée et individuelle

Plus de 80 % des cyberincidents sont dus à une erreur humaine et coûtent des millions aux entreprises. Cependant, les programmes de formation classiques visant à prévenir ces problèmes ne sont pas assez efficaces et ne conduisent pas aux comportements requis. La plateforme Kaspersky Automated Security Awareness permet de former tous les collaborateurs afin qu'ils acquièrent les connaissances nécessaires pour faire face à la situation.

Les obstacles à une formation de cybersécurité réussie

Les entreprises voient les avantages des programmes de sensibilisation à la sécurité, mais elles ne sont souvent pas satisfaites du processus et des résultats. Les PME sont confrontées à des défis particuliers dans ce domaine, car elles manquent généralement d'expérience et de ressources. L'effort requis pour créer et gérer des programmes de formation est immense, l'accent est souvent mis sur les interdictions plutôt que sur les solutions, et la formation est perçue comme compliquée, ennuyeuse et non pertinente. Par conséquent, on ne se souvient pas de ce que l'on a appris.

Gestion efficace et simplifiée de la sensibilisation à la sécurité

La plateforme Automated Security Awareness Platform (ASAP) est l'élément central du portfolio de la formation de la sensibilisation à la sécurité de Kaspersky. Cette plateforme est un outil en ligne permettant aux collaborateurs de promouvoir des connaissances complètes et pratiques en matière de cybersécurité. La mise en œuvre et la gestion de la plateforme ne requièrent aucune ressource ou préparation particulière. Cette plateforme fournit à l'entreprise une aide intégrée à chaque étape de son parcours vers un environnement de cybersécurité d'entreprise sûr.

L'un des critères déterminants dans le choix d'un programme de sensibilisation est son efficacité. Avec ASAP, l'efficacité est intrinsèque au contenu et à la gestion de la formation. Le contenu de la plateforme est basé sur un modèle de compétences composé de 350 compétences pratiques et essentielles en matière de cybersécurité, que tous les collaborateurs doivent acquérir.

Sans ces compétences, les collaborateurs peuvent faire courir des risques à l'entreprise par leur mauvaise conduite ou leur négligence.

Formation efficace

Cohérente

- Un contenu bien pensé et structuré
- Des leçons interactives, consolidation continue des connaissances, tests, simulation d'attaques de phishing pour l'application pratique des connaissances
- Les documents de formation et leur structure sont présentés conformément aux particularités de la mémoire humaine, autrement dit, à notre capacité à assimiler et à retenir l'information.

Pratique et motivante

- Pertinence dans le travail quotidien des collaborateurs
- Compétences directement applicables
- Exemples concrets de situations aux quelles les collaborateurs peuvent s'identifier encouragent la participation et le rappel de ce qui a été appris.

Facile à mettre en œuvre

- La gestion entièrement automatisée des formations aide tous les collaborateurs à atteindre les compétences en matière de sécurité adapté es à leur profil de risque, sans aucune intervention de l'administrateur de la plateforme
- Facile à utiliser
- Tableau de bord «tout-en-un» et rap ports exploitables
- Concept attrayant
- Les invitations et des e-mails de motivation, ainsi que des rapports hebdomadaires destinés aux administrateurs et aux utilisateurs, sont envoyés auto matiquement par la plateforme.

Contenus équilibrés et structurés et référence pratique

Les concepts de formation d'ASAP sont basés sur une méthodologie qui tient compte des collaborateurs et de leur capacité à absorber les informations. Les contenus comprennent de nombreux exemples concrets, des tâches basées sur la simulation, des exercices et des cas qui renforcent l'importance de la cybersécurité pour tous les collaborateurs. La plateforme favorise les compétences plutôt que la simple communication de connaissances. Des exercices pratiques et des tâches pertinentes pour les employés sont au centre des différents modules.
Les modules contiennent différentes combinaisons de tâches pour maintenir l'intérêt des utilisateurs et les motiver à acquérir un comportement sûr. Le style visuel et les textes sont non seulement traduits dans différentes langues, mais également adaptés à la culture et aux conditions locales respectives. Kaspersky ASAP est disponible en français, arabe, néerlandais, anglais, allemand, italien, portugais, russe et espagnol.

Thèmes de formation

- Mots de passe et comptes
- E-mail
- Surfer sur Internet
- Réseaux sociaux et messageries instantanées
- Sécurité pour PC
- Appareils mobiles
- Données confidentielles
- RGPD/DSGVO

Chaque thème comprend plusieurs niveaux, chacun comportant une description des compétences en matière de sécurité. Les niveaux sont définis selon les degrés de risque qu'ils visent à éliminer: le niveau 1 est généralement suffisant pour éviter les attaques les plus courantes et massives, alors que pour une protection contre les attaques plus sophistiquées et ciblées, il convient d'étudier les niveaux suivants.

Débutant: éviter les attaques massives

3 compétences, notamment:

- Configurer le PC (mises à jour, antivirus)
- Ignorer les sites Web malveillants évidents (ceux qui demandent de mettre à jour le logiciel, d'optimiser les performances du PC,d'envoyer des SMS, d'installer des lecteurs, etc.)
- Ne jamais ouvrir les exécutab les depuis des sites Web

Elémentaire: éviter les attaques massives sur un profil spécifique

20 compétences, notamment:

- S'inscrire/se connecter uniquement sur les sites de confiance
- Eviter les liens numériques
- Saisir des informations sensibles sur des sites de confiance uniquement
- Reconnaître les signes d'un site Web malveillant

Intermédiaire: éviter les attaques ciblées bien préparées

14 compétences, notamment :

- Reconnaître des liens contrefaits
- Reconnaître des fichiers et téléchargements malveillants
- Reconnaître des logiciels malveillants

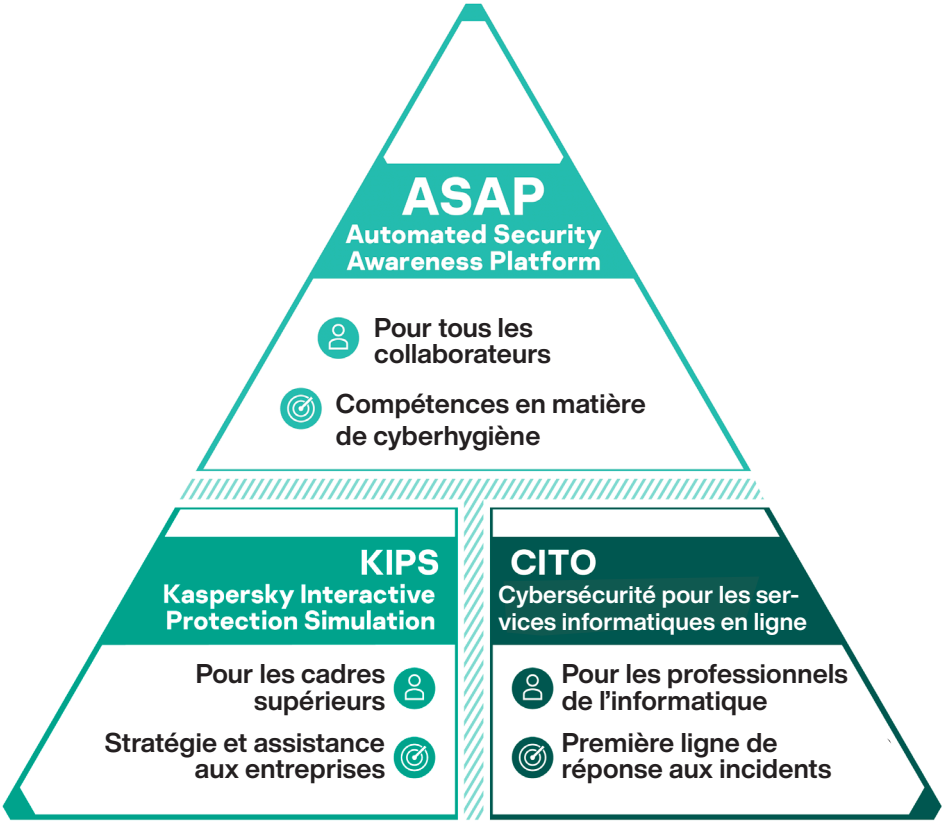
Avancé: éviter les attaques ciblées

13 compétences, notamment:

- Reconnaître des liens contrefaits sophistiqués (dont des liens ressemblant au site Web de l'entreprise et des liens avec redirections)
- Eviter des sites référencés sur liste noire
- Déconnexion après avoir terminé de travail
- Configuration avancée du PC (désactiver Java, Ad-block, Noscript, etc.)

Formats de formation spécifiques pour les différents niveaux organisationnels

Kaspersky ASAP propose des formats de formation spécifiques pour les différents niveaux organisationnels. Dans sa fonctionnalité de base, la plateforme de formation ASAP sensibilise l'ensemble du personnel aux différents aspects de la cybersécurité. La direction reçoit des informations supplémentaires sur la stratégie et le support de gestion sous le nom de KIPS (Kaspersky Interactive Protection Simulation). Et avec CITO (Cybersecurity for IT Online), les professionnels de l'informatique peuvent bénéficier d'un savoir-faire en matière de contre-mesures en cas d'incidents de sécurité.



BOLL Engineering SA . En Budron H15 / CH-1052 Le Mont-sur-Lausanne / Telefon +41 21 533 01 60 / contact@boll.ch
BOLL Engineering AG . Jurastrasse 58 / CH-5430 Wettingen / Telefon +41 56 437 60 60 / info@boll.ch / www.boll.ch
BOLL Europe GmbH . Ringstrasse 3 / DE-89081 Ulm / Telefon +49 731 85074823 / jwa@boll-europe.com / www.boll-europe.com