Kaspersky
Security
Awareness

Gamified Assessment Tool

kaspersky.fr

kaspersky bring on the future

Kaspersky
Gamified Assessment
Tool

Gamified Assessment Tool

Kaspersky Gamified Assessment Tool (GAT) : un moyen rapide et passionnant d'évaluer les compétences des employés dans le domaine de la cybersécurité.

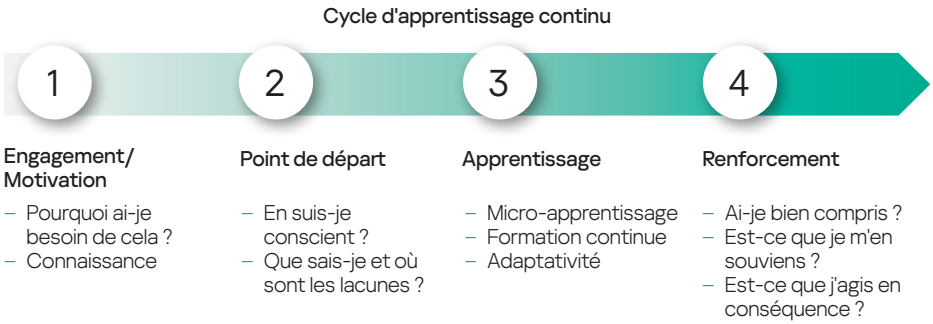
52 % des grandes entreprises et 50 % des PME ont subi un incident de cybersécurité suite à une utilisation inappropriée des ressources informatiques par les employés*

42 % des entreprises considèrent les employés comme le problème de sécurité informatique le plus préoccupant (avec l'utilisation inappropriée des ressources informatiques, la perte d'appareils appartenant à l'entreprise et le fait d'être victime d'attaques de phishing et/ou d'ingénierie sociale)*

1 195 000 $ impact financier moyen des violations de données causées par une mauvaise utilisation des ressources informatiques par les employés*

Une cybersécurité solide constitue l'un des points les plus importants, mais aussi les plus fragiles, de nombreuses entreprises aujourd'hui. Les entreprises du monde entier travaillent fort sur la cybersécurité, développant des systèmes de protection de plus en plus complexes et efficaces. Pourtant, il reste une faille dans la structure de cybersécurité de chaque entreprise qui ne peut être comblée par des mesures techniques.

Cette faille est le « facteur humain ». Le facteur humain est l'une des principales causes des incidents de cybersécurité. Il peut être difficile de changer le comportement des employés. Les utilisateurs ne cherchent pas à se familiariser avec la cybersécurité : ils sont peu motivés et ne se rendent souvent même pas compte de leurs lacunes dans ce domaine. Comment inciter les employés à se former ? Comment évaluer leur niveau actuel de connaissances en matière de cybersécurité ? L'outil Gamified Assessment Tool mesure rapidement le niveau actuel des compétences des employés en matière de cybersécurité, les incitant et les motivant à poursuivre leur apprentissage. Les départements DSI/RH peuvent comprendre la situation générale de la sensibilisation à la cybersécurité dans l'entreprise en utilisant un petit outil ludique comme étape d'introduction à un programme de formation.



Que propose l'outil Gamified Assessment Tool ?

- L'évaluation comporte trois scénarios représentant des situations familières qui font appel à des compétences particulières en matière de cybersécurité : le travail en open space, les déplacements et le travail à domicile.
- Chaque employé reçoit un scénario avec 12 situations aléatoires qui traitent de compétences particulières en matière de cybersécurité. Les employés doivent tous les passer en revue, évaluer si les actions du personnage sont risquées ou non et indiquer le niveau de confiance dans leur réponse à l'aide de jetons.
  Pour chaque réponse, l'utilisateur gagne un certain nombre de points. Lors du calcul du score final de l'utilisateur, le système prend en considération à la fois la réponse, qu'elle soit juste ou fausse, ainsi que le niveau de confiance associé.
- Pour éviter la tricherie et rendre l'évaluation plus intéressante, les types de scénarios sont fournis aux employés de façon aléatoire. Pour chaque scénario, 12 situations sont également choisies au hasard parmis les 225 scénarios de la bibliothèque, ce qui signifie que les autres utilisateurs seront évalués selon des scénarios différents.
- Une fois que les utilisateurs ont terminé toutes les zones, ils obtiennent un score global qui est une évaluation de leur niveau de sensibilisation à la cybersécurité ainsi que des commentaires sur chaque zone, accompagnés d'explications et de conseils utiles.
- Un certificat est délivré à l'issue de l'évaluation. Celui-ci peut être téléchargé et partagé.
- L'administrateur de l'évaluation reçoit un rapport de tous les utilisateurs avec les résultats détaillés sur chaque thème, y compris les scores, le nombre de bonnes réponses ainsi que le niveau de confiance. Ces commentaires clairs sur le niveau de compétence des employés en matière de cybersécurité permettent de mieux planifier et organiser les formations de sensibilisation à la sécurité.

* Rapport : « IT security economics in 2019 » (Économie de la sécurité informatique 2019), Kaspersky

Domaines de sécurité couverts par l'outil Gamified Assessment Tool :

- Mots de passe et comptes
- Email
- Navigation sur Internet
- Réseaux sociaux et messageries instantanées
- Protection PC
- Appareils mobiles

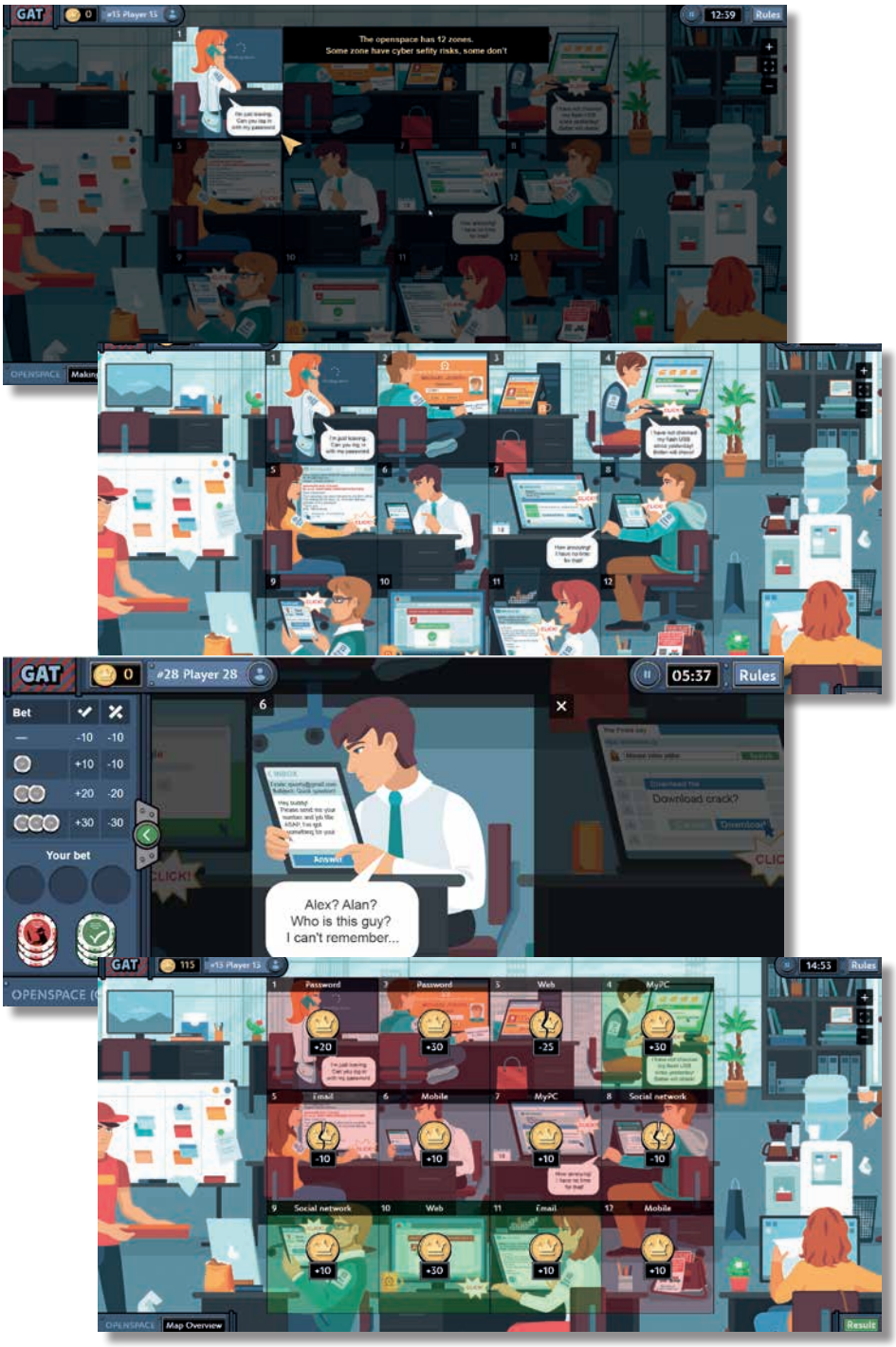
Processus d'apprentissage

Une brève description des règles est fournie au début de l'évaluation.

En 10 minutes, les employés doivent évaluer les actions des personnages dans 12 situations liées à la cybersécurité représentées dans le scénario. Ils doivent décider si les actions du personnage sont risquées ou non et exprimer le niveau de confiance de leur réponse. Il est possible de mettre les jeux en pause. Si vous devez effectuer une autre tâche, n'oubliez pas de mettre le jeu en pause (le bouton de pause se trouve dans le coin supérieur droit, près du chronomètre).

Les utilisateurs placent des jetons verts s'ils pensent que la situation est sûre, ou des jetons rouges s'ils pensent qu'elle est dangereuse. Le nombre de jetons indique leur degré de confiance dans leur réponse.

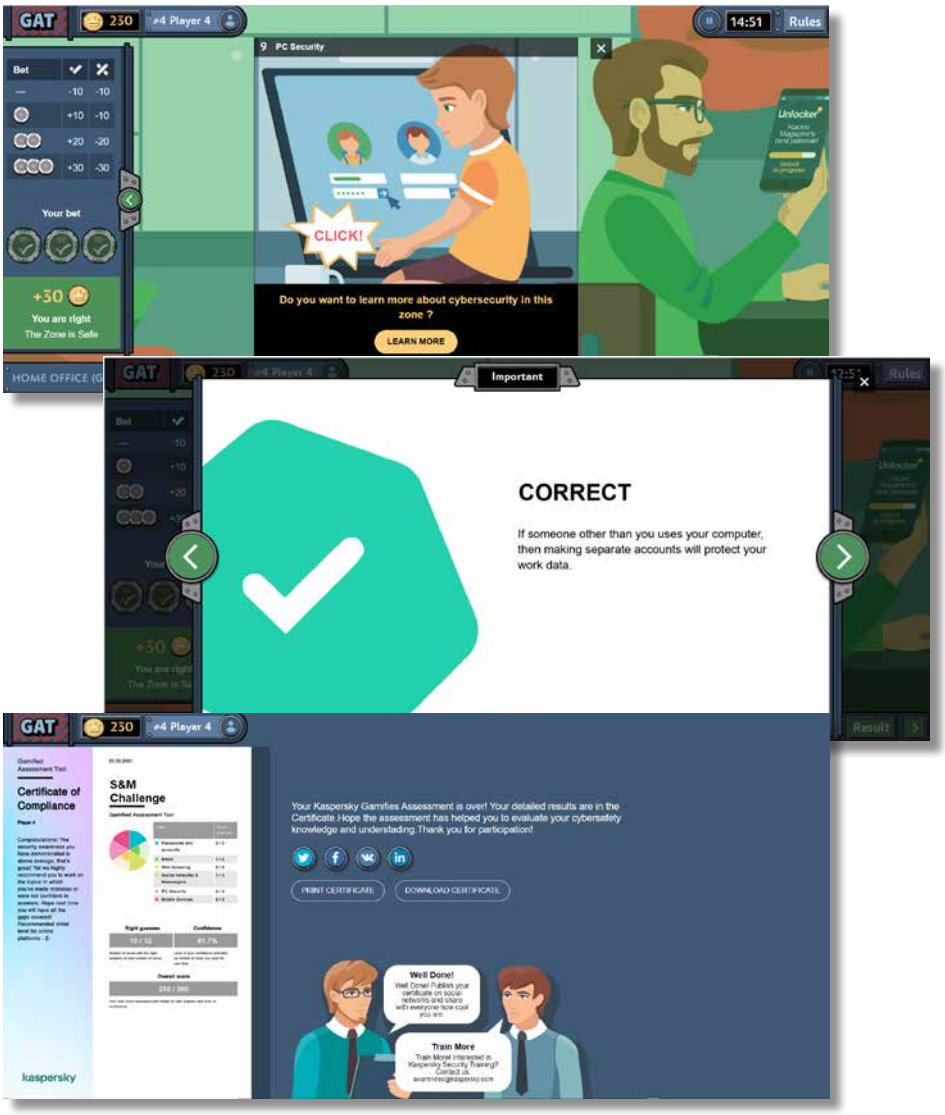
Une fois le jeu terminé, les utilisateurs obtiennent leur score global, qui est une évaluation de leur niveau de sensibilisation à la cybersécurité.



Il est possible d'analyser chaque situation.

Et de recevoir des commentaires sur chaque zone, avec des explications et des conseils.

Un certificat contenant une liste de recommandations sur les aspects de la cybersécurité qui nécessitent une attention particulière et des améliorations, ainsi que des conseils sur la façon de renforcer la sensibilisation à la sécurité, sera disponible à l'issue de l'évaluation. Celui-ci peut être téléchargé et partagé.



Recommandations techniques

Système d'exploitation :
Windows 7, 10 ;
Mac : Sierra, High Sierra, Mojave, Catalina ;
Ubuntu 18.04.
Nous vous recommandons vivement d'utiliser les navigateurs suivants :
Firefox 70 et versions ultérieures ;
Chrome 80 et versions ultérieures ;
Safari 11 et versions ultérieures.
En tant que solution cloud, GAT ne nécessite qu'un navigateur sur un ordinateur de bureau ou une tablette avec une résolution d'au moins 1024 x 768.

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 en cybersécurité qui est au cœur de nos produits

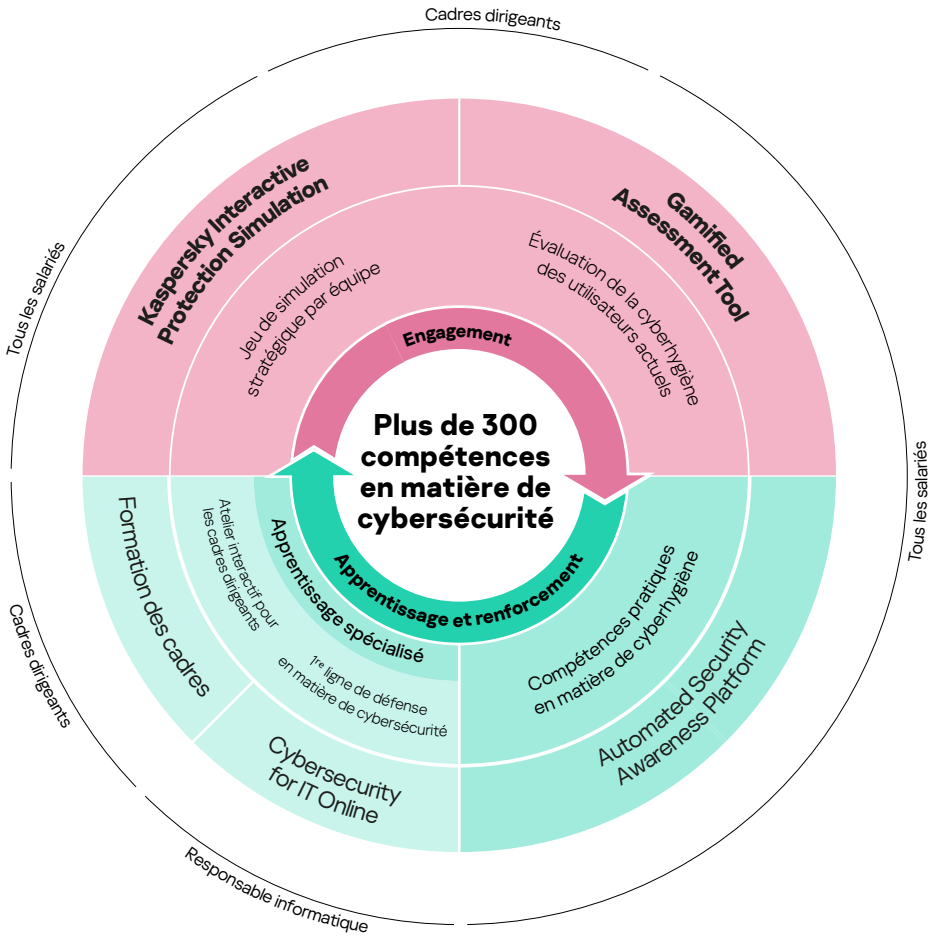
Des formations qui modifient le comportement des employés à chaque niveau de votre organisation
Notre formation ludique stimule l'intérêt et la motivation grâce au divertissement éducatif, tandis que les plateformes d'apprentissage permettent d'internaliser les compétences en matière de cybersécurité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

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 cybercomportement 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.fr
Solutions de cybersécurité pour les entreprises : https://www.kaspersky.fr/enterprise-security
Kaspersky Security Awareness : https://www.kaspersky.fr/enterprise-security/security-awareness
Actualités dédiées à la sécurité informatique : https://www.kaspersky.fr/blog/category/business/

www.kaspersky.fr

kaspersky bring on the future