Kaspersky Interactive Protection Simulation

Sensibilisez les cadres supérieurs et les décideurs à la cybersécurité

kaspersky bring on the future

Plus d'informations sur
kaspersky.com/awareness

Kaspersky Interactive Protection Simulation

Le problème du « facteur humain »

L'une des plus grandes difficultés en matière de cybersécurité auxquelles sont confrontées les entreprises aujourd'hui consiste à concilier les différents points de vue et priorités des dirigeants. Cette diversité peut en effet entraîner une prise de décisions de type « Triangle des Bermudes » dès qu'il s'agit de la sécurité :

- Les entreprises considèrent que les mesures de sécurité
- sont contraires à leurs objectifs commerciaux (moins cher/plus rapide/meilleur).
- Les responsables de la sécurité informatique peuvent avoir le sentiment que l'infrastructure de cybersécurité et les investissements y afférents ne sont pas de leur ressort.
- Les responsables de la maîtrise des coûts peuvent ne pas voir le lien entre les dépenses de cybersécurité et les revenus ni comprendre en quoi celles-ci représentent des économies plus que des coûts.

L'efficacité de la cybersécurité repose sur une compréhension mutuelle et une collaboration entre ces trois catégories de responsables. Cependant, les méthodes de sensibilisation traditionnelles (conférences, exercices rouges/bleus) présentent des lacunes. Elles sont souvent interminables, trop techniques, incompatibles avec les emplois du temps chargés des responsables et dépourvues d'un « langage commun ».

La cyber-immunité d'une entreprise commence par ses cadres dirigeants

Pour de nombreuses entreprises, il est aujourd'hui prioritaire de veiller à la durabilité de leur infrastructure informatique. Toutefois, la gestion des questions de cybersécurité relève généralement de la responsabilité du personnel chargé des technologies informatiques et de la sécurité informatique, ce qui peut créer une culture fragmentée du comportement en matière de cybersécurité au sein de l'entreprise. Les chefs d'entreprise se concentrent principalement sur les ventes, l'expérience client, les risques et les coûts, et négligent souvent la cybersécurité dans la poursuite de leurs objectifs. Cependant, sans le soutien du conseil d'administration, qui donnerait l'exemple, la création d'une culture unifiée de la cybersécurité peut s'avérer impossible.

76 % des PDG reconnaissent contourner les protocoles de sécurité pour gagner du temps, sacrifiant au passage la sécurité au profit de la rapidité*.

62 % des responsables admettent qu'une mauvaise communication concernant la sécurité informatique au sein de leur organisation a été à l'origine d'au moins un incident de cybersécurité**.

51 % des professionnels de la sécurité de l'information estiment qu'il est très difficile de négocier une augmentation du budget consacré à la sécurité informatique. Toutefois, ils sont sur la même longueur d'onde lorsqu'il s'agit de mettre en place des stratégies de communication viables.

La majorité des cadres **(56 %) et des informaticiens (48 %)** s'accordent à dire que la méthode la plus efficace pour encourager une meilleure communication sur les questions liées à la sécurité informatique consiste à fournir des exemples concrets**.

Aide proposée par Kaspersky Security Awareness

Kaspersky Security Awareness est une solution éprouvée, efficace et performante qui a fait ses preuves dans le monde entier. 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'expérience de Kaspersky en matière de cybersécurité et à la vaste expérience de la Kaspersky Academy dans la formation des adultes.

Le portfolio est composé de produits de formation intéressants 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.

Chaque produit du portefeuille joue un rôle particulier dans le cycle d'apprentissage global et est également disponible de façon indépendante.

Un jeu d'entreprise stratégique sur la cybersécurité pour les dirigeants

Kaspersky Interactive Protection Simulation (KIPS) est un jeu simulation en équipes, de mises en situation tirées de situations réelles, qui met en évidence le lien entre l'efficacité d'une entreprise et sa cybersécurité.

Les participants sont placés dans un environnement d'entreprise simulé en tant que membres de l'équipe de sécurité informatique, où ils sont confrontés à une série de cyber-menaces inattendues alors qu'ils doivent veiller au bon fonctionnement de l'entreprise et à la réalisation de son chiffre d'affaires.

Ils doivent élaborer une stratégie de cyber-défense en choisissant parmi les meilleurs contrôles proactifs et réactifs mis à leur disposition. Chaque choix qu'ils font modifie la façon dont le scénario se déroule et, en fin de compte, influe sur le montant des recettes de l'entreprise.

En équilibrant les priorités en matière d'ingénierie, d'opportunités commerciales et de sécurité face au coût d'une cyberattaque réaliste, les équipes analysent des données et prennent des décisions stratégiques en fonction d'informations incertaines et de ressources limitées. Si cela semble réaliste, c'est parce que tous les scénarios reposent sur des événements de la vie réelle.

* https://www.forbes.com/sites/louiscolumbus/2020/05/29/cybersecuritys-greatest-insider-threat-is-in-the-c-suite/?sh=466624f87626

** https://www.kaspersky.com/blog/speak-fluent-infosec-2023/

KIPS est un jeu de sensibilisation dynamique avec une approche d'apprentissage par la pratique :

- Amusant, attrayant et rapide (2 heures).
- Travail d'équipe favorisant la coopération.
- La compétition favorise l'initiative et l'analyse.
- Jeu développant la compréhension des mesures de cybersécurité.
- L'ensemble des attaques et des scénarios reposent sur des cas réels.

Pourquoi la formation KIPS fonctionne

La formation KIPS vise les experts en systèmes commerciaux, les agents informatiques et les cadres opérationnels afin de les sensibiliser aux risques et aux problèmes de sécurité posés par l'exploitation de systèmes informatisés modernes.

Chaque équipe de 4 à 6 personnes est chargée de gérer une entreprise qui implique des installations de production et des ordinateurs qui les contrôlent. Dans le jeu, les unités de production génèrent des revenus, sensibilisent le public et génèrent des résultats commerciaux. Dans le même temps, les équipes doivent faire face aux cyber-attaques qui risquent de compromettre les performances de l'entreprise.

À la fin du jeu, les joueurs auront acquis des connaissances importantes et exploitables qu'ils pourront appliquer dans leur travail.

- Les cyber-attaques nuisent au chiffre d'affaires et doivent être prises en compte par les cadres dirigeants
- Pour assurer une cybersécurité efficace au sein de chaque entreprise, il est essentiel que les décideurs informatiques et non informatiques coopèrent
- Un budget de sécurité approprié ne fera pas exploser le budget, mais la perte de revenus résultant d'une cyber-attaque réussie pourrait...
- Les gens se familiarisent rapidement avec les contrôles de sécurité et leur importance (formation à l'audit, antivirus, etc.).

La formation KIPS est disponible en deux versions :

La version **KIPS Live**, très populaire, crée une atmosphère d'excitation et d'enthousiasme, et constitue un excellent outil pour engager et construire une culture de la cybersécurité au sein d'une organisation.

Dans la **version KIPS Online**, les utilisateurs peuvent interagir avec un grand nombre de participants à partir de l'endroit qui leur convient le mieux.

Parfait pour les organisations internationales ou les activités publiques, KIPS Online peut être associé à KIPS Live pour ajouter des équipes à distance à l'événement sur site.

- Jusqu'à 300 équipes (soit 1 000 stagiaires) simultanément, depuis n'importe quel endroit.
- Les équipes peuvent choisir une interface de jeu dans différentes langues.
- Les clients peuvent personnaliser les scénarios préinstallés en déterminant le nombre et les types d'attaques prévues dans le jeu à partir de la bibliothèque.
- Les clients disposant d'une licence leur permettant de jouer à KIPS aussi souvent qu'ils le souhaitent pendant la durée de la licence peuvent utiliser les paramètres prédéfinis ou personnaliser le scénario de jeu à chaque fois qu'ils jouent, en choisissant et en combinant différentes attaques disponibles dans la bibliothèque. Cette fonctionnalité permet de modifier le jeu en permanence, ce qui le rend encore plus intéressant.
- Un autre avantage de la version en ligne tient à la possibilité d'obtenir des statistiques sur les décisions prises par les joueurs, des données sur les actions des équipes dans certaines situations et une analyse comparative des actions des joueurs par rapport à leurs performances passées.

KIPS montre :

- Le rôle de la cybersécurité dans la continuité et la rentabilité des entreprises.
- Les nouveaux défis et les nouvelles menaces auxquels sont confrontées les entreprises.
- Les erreurs typiques que commettent les entreprises dans la mise en place de leur cybersécurité.
- Comment la coopération entre les entreprises et les équipes de sécurité permet de maintenir des opérations stables et une protection durable contre les cybermenaces.

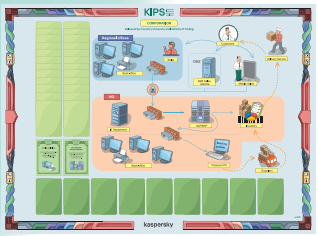
Selon le scénario, les équipes sont responsables de la sécurité informatique de l'entreprise dans le secteur concerné. Leur tâche consiste à assurer le fonctionnement normal et ininterrompu de l'entreprise, à maintenir les relations avec les clients et les fournisseurs, ainsi qu'à détecter et à neutraliser les cybermenaces.

Témoins d'une cyber-attaque affectant la production et les revenus de leur entreprise, les participants apprennent à mettre en œuvre diverses stratégies et solutions opérationnelles et IT afin d'en minimiser l'impact sans pour autant entraîner une réduction du chiffre d'affaires.

L'équipe qui termine le jeu avec le plus de revenus, ayant trouvé et analysé tous les pièges du système de cybersécurité et y ayant répondu de manière appropriée, **GAGNE !**

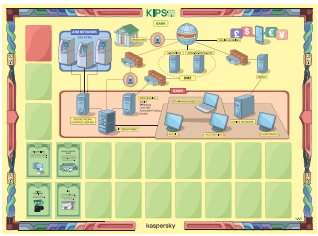
Scénarios KIPS destinés aux entreprises de tous les secteurs verticaux

Société



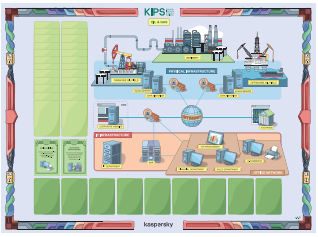
Protégez les entreprises contre **les ransomwares, les menaces persistantes avancées (Advanced Persistent Threats ou « APT »), les failles de sécurité liées à l'automatisation.**

Banque



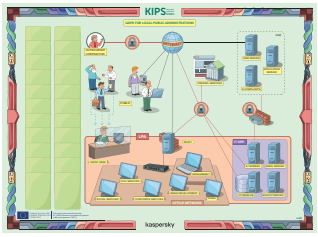
Protégez les établissements financiers contre **les nouvelles APT à haut risque comme Tyukpin et Carbanak.**

Pétrole et gaz



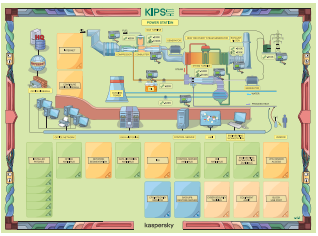
Comprenez l'influence de diverses menaces, qu'il s'agisse **d'une défiguration de site Web, d'un ransomware réel ou d'une APT sophistiquée.**

Administrations publiques locales



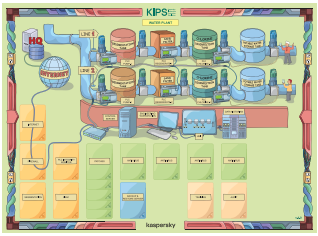
Protégez les serveurs Web publics contre les attaques et les exploits.

Centrale électrique



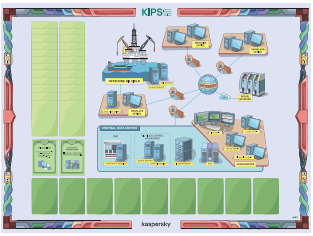
Protégez les infrastructures et les systèmes de contrôle industriels contre des cyberattaques de type Stuxnet.

Usine de traitement de l'eau



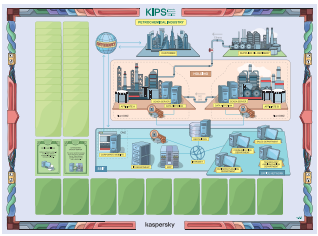
Protégez l'infrastructure informatique d'une usine de purification de l'eau, en assurant la stabilité de deux lignes de production.

Réservoirs de pétrole



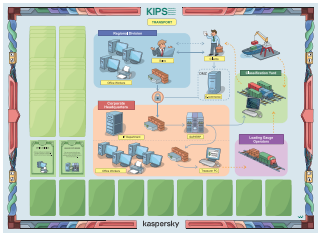
Veillez à la cybersécurité pour protéger les revenus d'une société pétrolière et énergétique internationale disposant de bureaux dans le monde entier.

Industrie pétrochimique



Garantissez le fonctionnement normal de la nouvelle branche d'une importante exploitation pétrochimique, centrée sur la production d'éthylène.

Transports

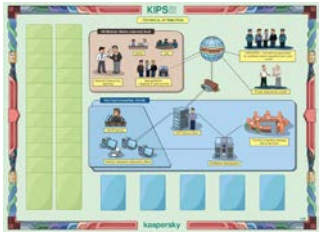


Protégez des entreprises de logistique contre **Heartbleed, les APT, les ransomwares BtoB et Insider.**

Aéroport

Garantissez la sécurité des passagers et la livraison dans les délais de marchandises à l'aéroport, en protégeant ses ressources de nombreuses cyberattaques et menaces.

Attribution technique



Menez une enquête et procédez à l'attribution technique d'une attaque APT complexe sur les serveurs de l'ONU.

Petites et moyennes entreprises

Aidez les PME à protéger leur entreprise contre les menaces de cybersécurité liées aux DDoS, aux ransomwares, au piratage d'applications mobiles et au vol d'identité.

Télécommunications

Protégez les ressources d'une grande holding de télécommunications composée d'un fournisseur de télécommunications, d'un fournisseur de services cloud, d'un développeur de jeux et du siège social.

Vous voulez profiter encore plus de la formation KIPS ?

Pourquoi ne pas compléter votre expérience KIPS par une **formation pour dirigeants**, qui fait partie du portfolio de sensibilisation à la sécurité de Kaspersky ? Cette formation pour les dirigeants peut être suivie avant ou après avoir joué à KIPS, en fonction de votre approche de la sensibilisation à la sécurité. Améliorez votre expérience KIPS en découvrant ce que le paysage actuel des menaces implique pour votre entreprise, les mesures à prendre en cas de cyberattaque ainsi qu'une foule d'autres informations intéressantes, pertinentes et utiles (la formation pour dirigeants se présente sous deux formes : un atelier interactif hors ligne ou une formation en ligne).

Ce que les utilisateurs et les clients de KIPS disent du jeu

La formation Kaspersky Industrial Protection Simulation a été particulièrement instructive et devrait être obligatoire pour tous les professionnels de la sécurité.

Warwick Ashford,
Computer Weekly

Le CERN possède des quantités de systèmes IT et d'ingénierie qui mobilisent des milliers de personnes. C'est pourquoi il est tout aussi essentiel de mettre en place des contrôles techniques que de sensibiliser nos employés à la cybersécurité et de les inciter à s'en soucier. La formation de Kaspersky s'est révélée stimulante, brillante et efficace.

Stefan Luders,
responsable de la sécurité des systèmes d'information au CERN

Cette formation a été extrêmement enrichissante et bon nombre de participants ont demandé à pouvoir l'utiliser dans leur entreprise.

Joe Weiss, PE,
CISM, CRISC, membre de l'ISA

Rien de tel que cette formation KIPS pour entamer la construction d'un réseau axé sur l'affiliation et la collaboration.

Daniel P. Bagge,
Národní centrum kybernetické bezpeč nosti, République tchèque

Comment se préparer à une session KIPS

Calendrier : programmez la formation KIPS à part ou bien dans le cadre d'un événement/d'une conférence/d'un séminaire (dans ce cas, organisez-la le soir du premier jour).

Groupe : entre 20 et 100 personnes réparties en équipes de 3 ou 4. Dans l'idéal, chaque équipe doit se composer de dirigeants, d'ingénieurs et de responsables de la sécurité des systèmes d'information ou de la sécurité IT :

- il est préférable que chaque équipe comporte au moins un membre de chacun de ces postes ;
- il n'est pas obligatoire que les membres d'une équipe appartiennent à la même entreprise / au même service ;
- le fait que les participants se connaissent ou non n'a pas d'importance.

Configuration : le jeu dure entre 1 h 30 et 2 heures, mais la salle doit être mise à disposition de l'équipe de formation de Kaspersky 2 heures avant le début du jeu afin qu'elle puisse tout préparer et installer.

Pièce : prévoyez ~3m2/personne, pas de colonnes, équipement audiovisuel standard : Projecteur (de 6 à 8 lumens), écran, système de sonorisation (haut-parleurs, télécommande, microphones).

Réseau Wi-Fi avec accès Internet (pour l'accès au serveur du jeu KIPS), au minimum un iPad à 4 Mo/s par équipe (4 personnes) avec prise en charge du réseau Wi-Fi ou autres tablettes.

Meubles : tables de participants pour 4 personnes (rectangulaires ne mesurant pas moins de 75 × 180 cm, ou rondes d'un diamètre de 1,5 m au maximum). Les participants doivent pouvoir s'asseoir en groupes de 4 à chaque table. Tables pour le co-animateur, chaises pour tous les participants.

Références et témoignages clients

Le jeu KIPS a conquis des professionnels de la sécurité industrielle de plus de 50 pays.

- KIPS a été traduit en anglais, en russe, en allemand, en français, en japonais, en espagnol européen et d'Amérique latine, en portugais, en turc, en italien, en chinois, en néerlandais et en arabe
- KIPS est utilisé par de nombreuses agences gouvernementales, dont CyberSecurity Malaysia, la NSA de la République tchèque et le Cyber Security Centrum des Pays-Bas. Il permet à des centaines d'experts de mieux connaître les infrastructures critiques au sein des organisations nationales
- KIPS est homologué par des organismes de formation de premier plan tels que le SANS Institute, où il est utilisé pour former les étudiants du SANS dans le monde entier
- KIPS est utilisé sous licence par des fournisseurs de services de sécurité et des distributeurs, notamment Mitsubishi-Hitachi Power Systems, qui l'utilise pour former ses clients sur les infrastructures critiques
- KIPS fait partie du projet Geiger de la Commission européenne visant à former et à protéger les petites et microentreprises contre les cybermenaces et à améliorer leur gestion de la vie privée

Possibilité d'une « formation pour les formateurs »

Si un client souhaite utiliser la formation KIPS pour former un public plus large, de responsables et d'experts à travers divers services ou sites, il peut acheter la licence correspondante, former des formateurs internes et organiser des sessions de formation KIPS à son propre rythme et selon ses propres besoins.

Ce type de licence comprend :

- les droits d'utiliser en interne le programme de formation KIPS ;
- un ensemble de supports de formation et les droits de les utiliser/reproduire ;
- l'identifiant et le mot de passe permettant d'accéder au serveur du logiciel KIPS pendant la durée de la licence ;
- un guide et une formation destinés aux formateurs pour que les responsables du programme sachent comment dispenser la formation KIPS ;
- un service de maintenance et d'assistance (mises à jour et assistance pour le logiciel KIPS et le contenu de formation) ;
- des options de personnalisation des scénarios KIPS (moyennant un supplément).

KIPS pour les partenaires et les centres de formation

KIPS est une excellente possibilité pour les partenaires de bénéficier de solutions de sensibilisation de diverses manières. Non seulement ils peuvent les vendre en tant que produit, mais ils peuvent également les vendre aux clients de leurs centres de formation, ou même organiser leurs propres sessions (les spécialistes en formation de Kaspersky peuvent développer les compétences des partenaires chargés de la formation s'ils choisissent cette option).

Kaspersky Security Awareness

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.

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

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.

Cycle d'apprentissage continu

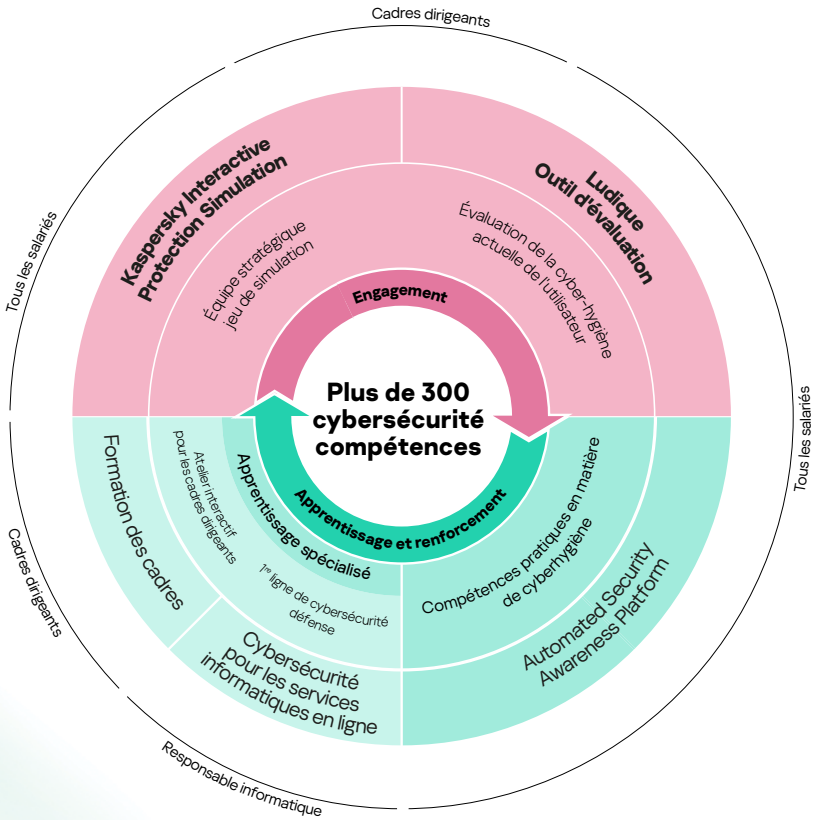
Engagement/ Motivation
- Pourquoi ai-je besoin de cela ?
- Connaissance

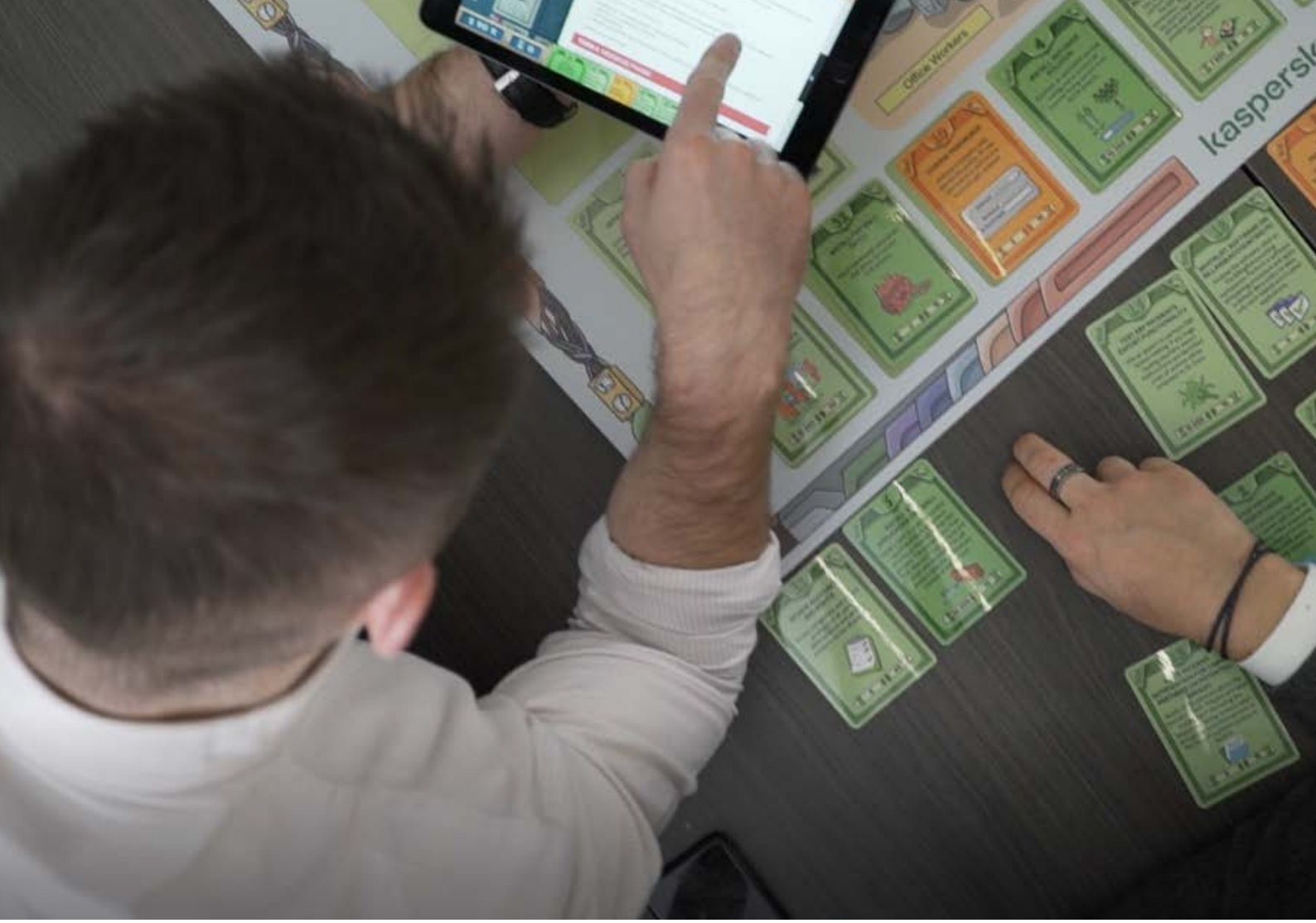
Point de départ
- En suis-je conscient ?
- Que sais-je et où sont les lacunes ?

Apprentissage
- Micro-apprentissage
- Formation continue
- Adaptativité

Renforcement
- Ai-je bien compris ?
- Est-ce que je m'en souviens ?
- Est-ce que j'agis en conséquence ?

Différents formats de formation pour différents niveaux organisationnels





Solutions de cybersécurité pour les entreprises : www.kaspersky.fr/enterprise-security
Kaspersky Security Awareness : www.kaspersky.fr/enterprise-security/security-awareness

www.kaspersky.fr

kaspersky