Kaspersky® Security Awareness

Formation en ligne à la cybersécurité, pour les services informatiques

Formation interactive pour développer les compétences des responsables informatiques généralistes, en matière de cybersécurité et de réponse aux incidents de premier niveau

La création d'un solide dispositif de cybersécurité en entreprise est impossible sans la formation systématique des salariés. La plupart des entreprises proposent une formation à la cybersécurité sur deux niveaux : une formation d'experts pour les équipes de sécurité informatique et une formation de sensibilisation à la sécurité pour les salariés ne travaillant pas dans les services informatiques (Kaspersky Lab offre un ensemble complet de produits pour les deux). Cependant, quelles catégories de salariés nous échappent ? Bien sûr : les équipes informatiques, les équipes de support technique et les autres salariés ayant un niveau avancé d'un point de vue technologique. Les programmes de sensibilisation standard ne leur suffisent pas, mais les entreprises n'ont pas besoin d'en faire des experts de la cybersécurité : ce serait trop coûteux, trop long et trop risqué.

Format du programme de formation

Il s'agit d'une formation exclusivement en ligne : les salariés suivant la formation ont seulement besoin d'un accès Internet et du navigateur Chrome sur leur PC. Chacun des 5 modules comporte une brève présentation théorique, des conseils pratiques et de 4 à 10 exercices. Ces exercices permettent de mettre en pratique certaines compétences et d'enseigner la manière d'utiliser les logiciels et les outils de sécurité informatique dans son travail au quotidien.

Le rythme de formation recommandé est d'un module par semaine, chaque module durant 45 minutes au maximum. La formation doit ainsi être terminée en un mois et demi, pour une durée totale de 4 à 5 heures par salarié.

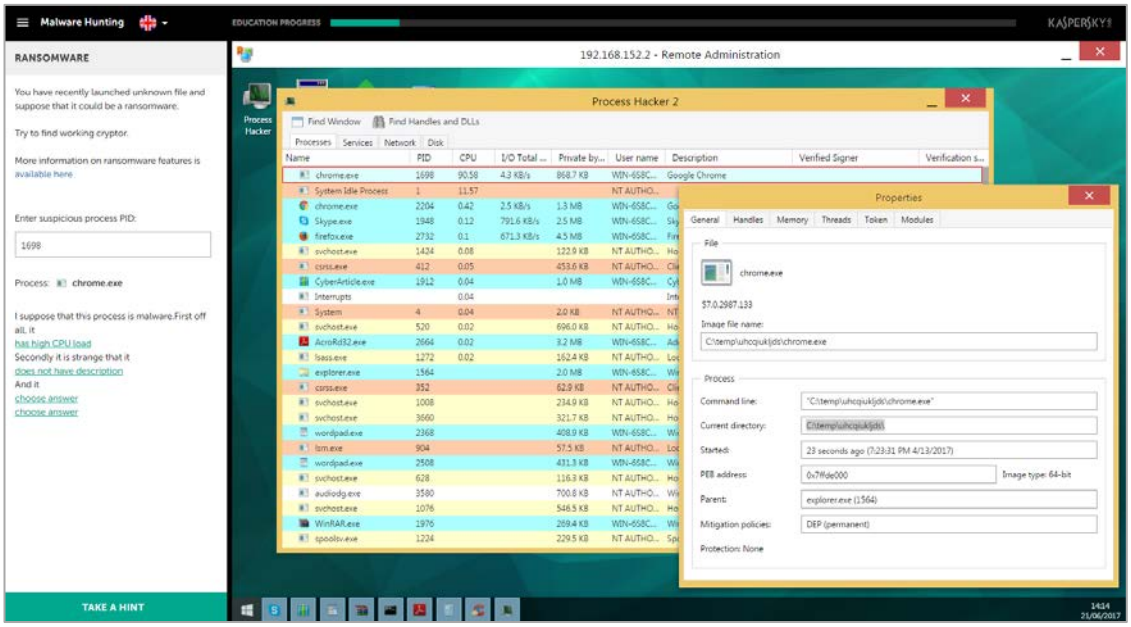
La version actuelle de la formation est destinée à un environnement professionnel Windows.

Gestion des incidents de premier niveau

Kaspersky Lab lance la première formation en ligne pour les responsables informatiques généralistes. Elle est composée de 5 modules :

- Logiciels malveillants
- Programmes et fichiers potentiellement indésirables
- Notions de base sur les enquêtes
- Gestion des incidents de phishing
- [dispensée depuis la fin de l'année 2017] Sécurité des entreprises

Le programme de formation fournit aux professionnels de l'informatique des compétences pratiques sur la façon de reconnaître une attaque possible au cours d'un incident PC qui semble inoffensif. Il leur apprend également à recueillir des données sur les incidents pour les transmettre au service sécurité informatique. Ce programme rend la traque des symptômes de présence d'un logiciel malveillant passionnante et renforce ainsi le rôle de tous les membres de l'équipe informatique qui sont la première ligne de défense de l'entreprise.

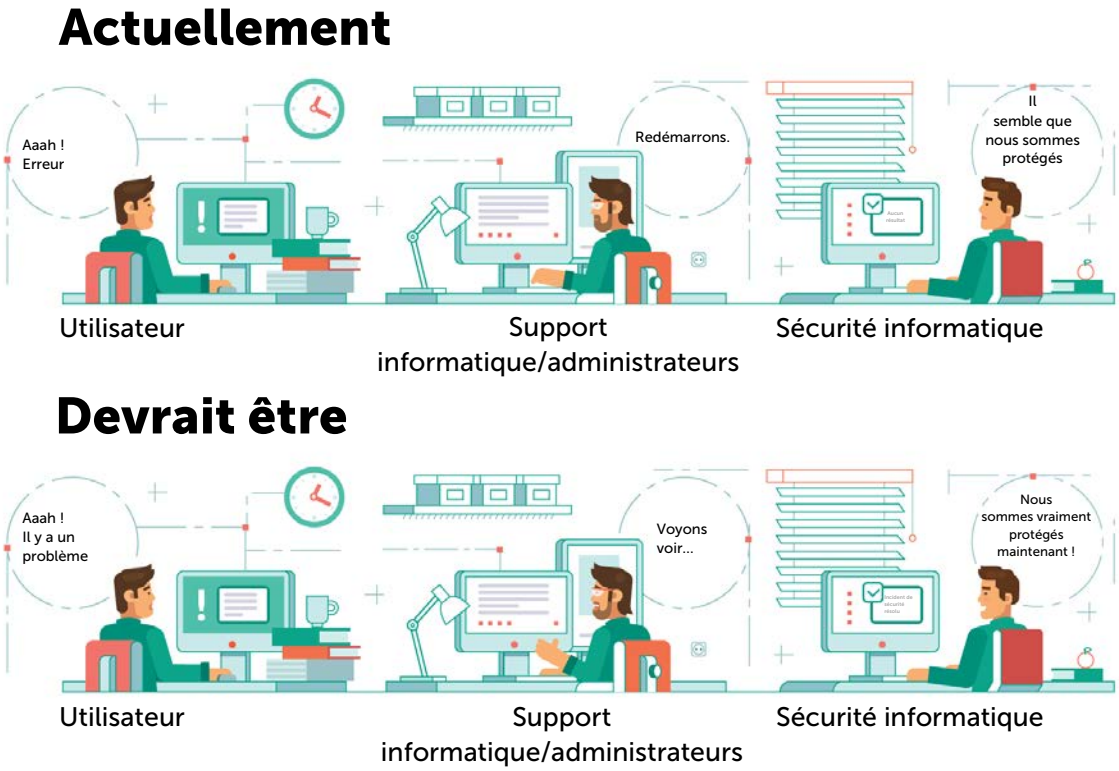


Première formation le 30 septembre 2017.

La version actuelle de la formation est destinée à un environnement professionnel Windows.

Qui former ?

La formation est recommandée pour tous les membres du service informatique de l'entreprise, à commencer par les équipes de support technique et les administrateurs système.



RÉSULTATS DE LA FORMATION ET THÈMES ABORDÉS

Nom du module	Public cible	Connaissances acquises	Attitude personnelle	Compétences acquises	Connaissances acquises dans le module
Logiciels malveillants	Les utilisateurs possédant des droits d'administrateur sur les serveurs et/ou les postes de travail	Techniques et classification des programmes malveillants Actions et signes de logiciels malveillants et suspects Notions de base de l'analyse heuristique	Les programmes malveillants peuvent exister à n'importe quel emplacement sur l'ordinateur Les programmes malveillants sont capables de voler des données de multiples façons non anodines Il est obligatoire de signaler tout incident potentiel et suspect à l'équipe de sécurité	Vérification de l'existence ou de l'absence d'incidents liés aux programmes malveillants	Utilisation des outils ProcessHacker, Autoruns, Fiddler et Gmer pour détecter les programmes malveillants
Programmes et fichiers potentiellement indésirables (PUP)	Les utilisateurs détenant les droits nécessaires pour installer des logiciels supplémentaires et les utilisateurs qui évaluent et ouvrent les fichiers reçus de l'extérieur	Notions de base sur l'analyse statistique et dynamique d'échantillons de logiciels et de documents suspects	Les documents (pdf, docx) peuvent contenir des exploits Les fichiers non signés peuvent contenir des programmes malveillants ou des riskwares Tous les fichiers exécutables non signés doivent être examinés pour rechercher une possible infection La signature numérique ne garantit pas que le fichier ne contient pas de fonctionnalités malveillantes	Travailler avec des contrôleurs d'événements de systèmes et de sandbox Utiliser des moteurs statistiques Désinstaller des PUP	Analyse statique (signature) et statistique (VirusTotal) des échantillons de logiciels Recherche d'exploits et de comportements malveillants de logiciels à l'aide de Procmon Analyse de fichiers avec la sandbox Cuckoo Création de scripts de désinstallation de programmes malveillants à l'aide d'AVZ
Notions de base sur les enquêtes	Les salariés des services informatiques impliqués dans les activités de cyberdiagnostic ou de gestion des incidents menées par l'équipe de sécurité	Processus de gestion des incidents, méthodes d'analyse des journaux, caractéristiques du stockage d'informations numériques	Si vous soupçonnez un incident de cybersécurité, signalez-le immédiatement à l'équipe de sécurité et recueillez des preuves numériques L'analyse doit être menée sous la supervision de l'équipe de sécurité et en coopération avec eux	Collecte de preuves numériques Analyse du trafic Netflow Analyse chronologique Analyse du journal des événements	Collecte de données volatiles et non volatiles (FTK-imager) Analyse du journal pour trouver la source et les liens de l'attaque (eventlogexplorer) Enquête de mouvement latéral par analyse Netflow (ntop) Analyse de disque à l'aide d'Autopsy

Nom du module	Public cible	Connaissances acquises	Attitude personnelle	Compétences acquises	Connaissances acquises dans le module
Phishing et renseignement de sources ouvertes (OSINT)	Les salariés des services informatiques impliqués dans les activités de diagnostic ou de gestion des incidents	Méthodes de phishing modernes Méthodes d'analyse des en-têtes d'e-mails	Le phishing peut être très difficile à identifier. Le phishing peut toujours être détecté par une enquête manuelle Les e-mails de phishing doivent être supprimés des messageries des utilisateurs	Analyse d'e-mails de phishing et suppression des e-mails de phishing dissimulés dans les messageries des utilisateurs Renseignement de sources ouvertes pour comprendre ce que les pirates savent au sujet de votre entreprise	Recherche dans les messageries Exchange et suppression des e-mails de phishing Utilisation de Recon-ng pour la reconnaissance Web
Sécurité des entreprises [1]	Les spécialistes informatiques impliqués dans l'installation, la configuration et l'administration de systèmes et serveurs internes ou externes	Méthodes d'évaluation de la la sécurité des systèmes individuels Sécurité multi-niveaux Logiciels de sécurité divers	En l'absence d'instructions concernant la configuration de la sécurité, suivez l'approche de sécurité multi-niveaux. Les antivirus sont obligatoires en toute circonstance Faites en sorte que la réussite de l'attaque soit plus coûteuse que les bénéfices tirés de celle-ci	Vérification des paramètres de sécurité du serveur lors de l'imbrication du système/ serveur des collègues ou des fournisseurs Test de la complexité des mots de passe Configuration du serveur sécurisé Recherche de vulnérabilités et correctifs	Évaluation de sécurité et configuration du serveur Windows

Nous contacter

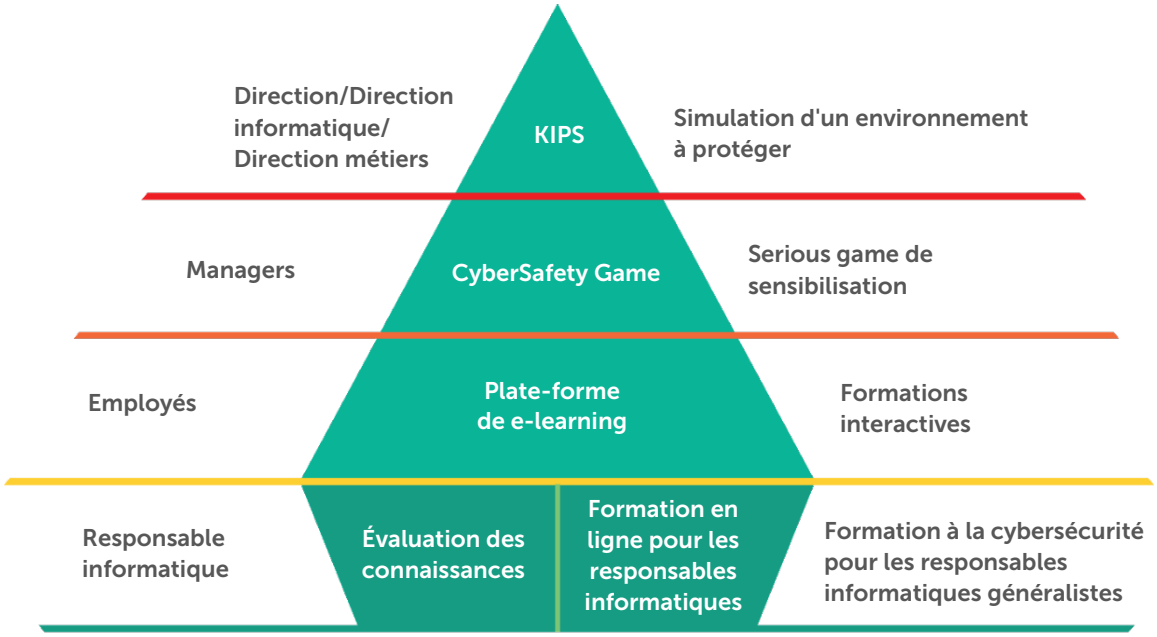
Pour obtenir des informations ou une démonstration, veuillez contacter votre responsable Kaspersky Lab

[1] Dispensée à partir de décembre 2017 (sera ajoutée gratuitement pour les clients ayant acheté une formation avant novembre).

Kaspersky Security Awareness

Kaspersky Lab a lancé une gamme de produits de formation sur ordinateur qui s'appuient sur des techniques d'apprentissage modernes et conviennent à tous les niveaux de la structure de l'entreprise.

Cette approche contribue à créer une culture collaborative de cybersécurité qui assure l'autonomie de la cybersécurité dans toute l'entreprise.



Définition des objectifs et choix du fournisseur

Définition d'objectifs fondée sur les données générales de Kaspersky Lab

Comparaison avec la moyenne mondiale / du secteur

Gestion de l'apprentissage

Automatisation de l'apprentissage

Cursus de formation personnalisé

Calcul du temps passé

Rapports et analyses

Rapports exploitables à tout moment

Analyse instantanée des points à améliorer

Évaluation et efficacité du programme

Apprentissage ludique

Concurrence et défis

Surcharges évitées

jusqu'à

90 %

Baisse du nombre total des incidents

pas moins de

50 %

Baisse des dépenses liées aux incidents

jusqu'à

93 %

Probabilité d'utiliser les connaissances dans le travail quotidien

multiplié par plus de

30

Retour sur investissement en produits de sensibilisation à la sécurité

un taux incroyable de

86 %

Volonté de recommander le programme

www.kaspersky.fr

Kaspersky Lab

Pour les entreprises : **www.kaspersky.fr/enterprise-security**
Sensibilisation à la sécurité : **https://www.kaspersky.fr/enterprise-security/security-awareness**
Démonstration du produit : **www.kaspersky.com/demo-sa**