Pour les personnels situés en première ligne de la détection des incidents

2022

Formation dédiée aux responsables informatiques (délivrée en ligne)

kaspersky

Essai gratuit : cito-training.com

Cybersecurity for IT Online (CITO)

Formation interactive qui permet d'établir une cybersécurité renforcée et d'acquérir des compétences de gestion de première ligne des incidents destinée aux spécialistes de l'informatique généraliste

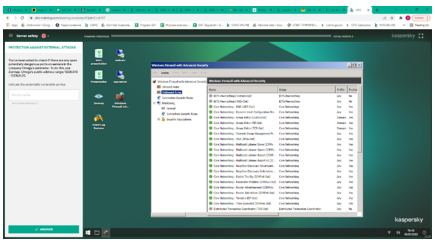
La création d'un solide dispositif de cybersécurité en entreprise est impossible sans la formation systématique des salariés concernés. La plupart des entreprises proposent une formation à la cybersécurité sur deux niveaux : une formation d'experts destinée aux équipes de sécurité informatique et une formation de sensibilisation à la sécurité destinée aux salariés ne travaillant pas dans les services informatiques. Kaspersky propose un ensemble complet de produits pour les deux. Cependant, quelles catégories d'employés nous échappent ? Pour les équipes informatiques, les bureaux de service et les autres personnels techniquement avancés, les programmes de sensibilisation standard ne suffisent pas. Cependant, ces personnes ne doivent pas nécessairement devenir des experts en cybersécurité : cela coûterait trop cher et prendrait trop de temps.

Format du programme de formation

La formation se déroule entièrement en ligne. Les utilisateurs ont uniquement besoin d'un accès à Internet et du navigateur Chrome sur leur ordinateur. Chacun des 6 modules comporte une brève présentation théorique, des conseils pratiques et entre 4 et 10 exercices portant sur des compétences particulières, permettant aux apprenants d'utiliser les outils et les logiciels de sécurité informatique dans leur travail au quotidien.

La formation est prévue pour être étalée sur une année. Le taux de progression recommandé est d'un exercice par semaine. Chaque exercice dure entre 5 et 45 minutes.

L'édition actuelle de la formation est axée sur l'environnement d'entreprise Windows.



Méthode de livraison de la formation :

Format Cloud ou SCORM

Gestion de première ligne des incidents

Kaspersky lance la première formation aux compétences en ligne sur le marché pour les professionnels généralistes de l'informatique d'entreprise. Elle est composée de 6 modules :

- Logiciels malveillants
- Programmes et fichiers potentiellement indésirables
- Notions de base sur les enquêtes
- Gestion des incidents de phishing
- Sécurité du serveur
- Sécurité d'Active Directory

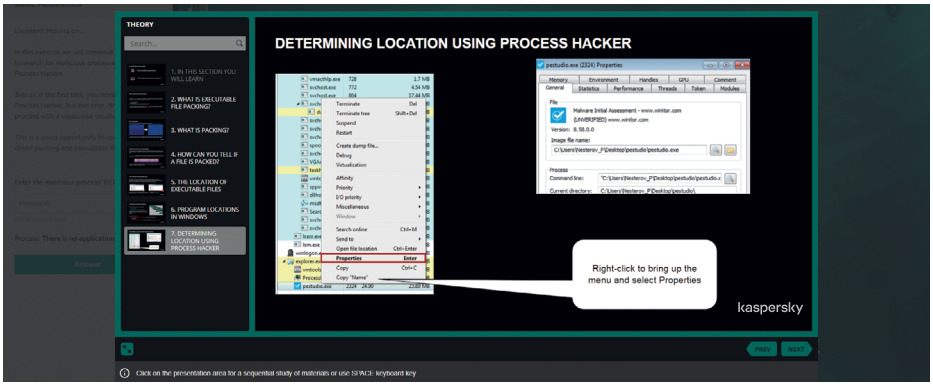
Le programme fournit aux professionnels de l'informatique des compétences pratiques sur la façon de reconnaître une attaque possible au cours d'un incident qui semble inoffensif. Il leur apprend également à recueillir des données sur les incidents pour les transmettre à la sécurité informatique. Ce programme rend la traque des signes d'activité malveillante passionnante et renforce ainsi le rôle de tous les membres de l'équipe informatique en tant que première ligne de défense du point de vue de la sécurité.

Pourquoi la formation CITO est-elle efficace ?

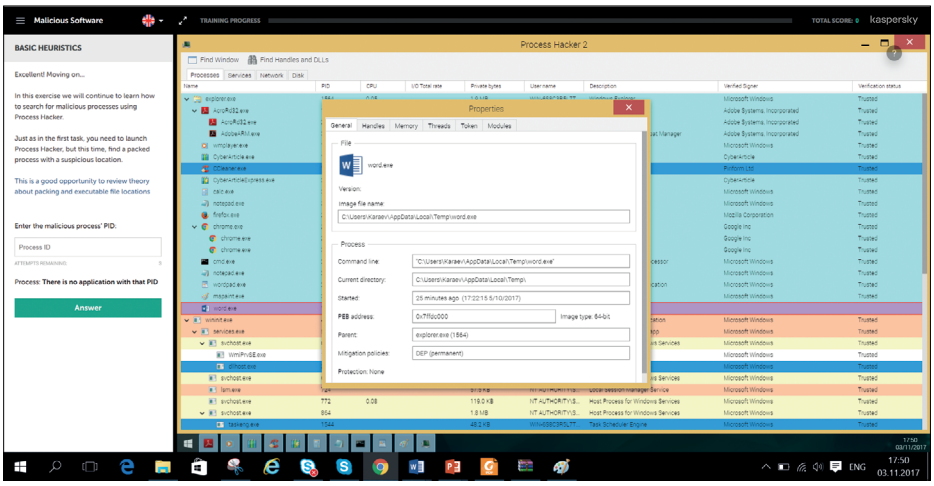
- Interactive : la stimulation de processus réels sans aucun risque pour l'ordinateur
- Développe des compétences et des connaissances : l'apprentissage par la pratique
- Processus d'apprentissage intuitif : navigation et conseils pratiques
- Couvre tous les principaux sujets et problèmes relatifs à la sécurité informatique auxquels le personnel informatique ordinaire est confronté dans le cadre de son travail

Processus d'apprentissage

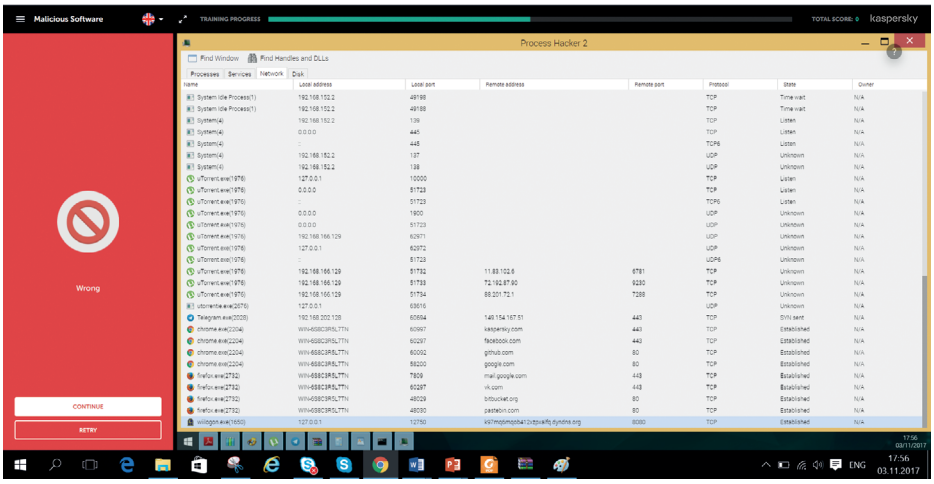
Chaque bloc d'exercices d'apprentissage se compose de deux parties : l'éducation et la pratique, avec des tâches simulant des processus réels liés aux explications précédentes.



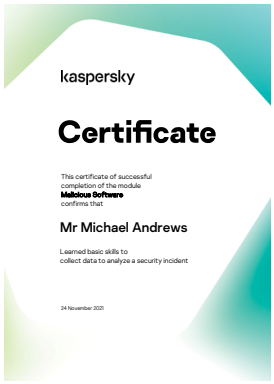
Si vous n'avez pas réussi à accomplir la tâche correctement, il vous sera demandé de réessayer et de réussir la partie éducative.



Si vous réussissez la pratique, vous serez redirigé vers le prochain bloc d'exercices.



Certificats
Des certificats personnels sont disponibles pour les employés après l'achèvement de chaque module


kaspersky

Certificate

This certificate of successful completion of the module **Malicious Software** confirms that

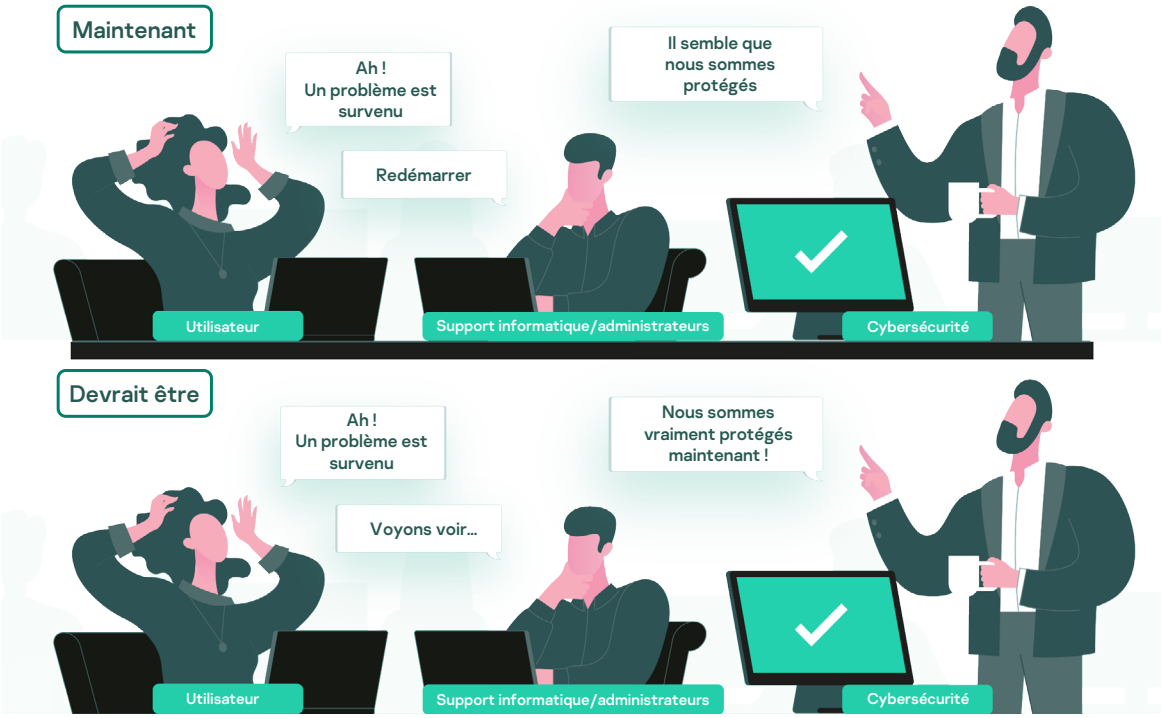
Mr Michael Andrews

Learned basic skills to collect data to analyze a security incident

24 November 2021

À qui s'adresse cette formation ?

Cette formation est recommandée pour tous les spécialistes en informatique au sein de votre entreprise, et surtout aux équipes de support technique et aux administrateurs système. Cependant, la plupart des membres non experts de l'équipe de sécurité informatique bénéficieront également de cette formation.



Thèmes de formation et résultats

Nom du module	Public cible	Connaissances acquises	Attitude personnelle	Compétences acquises	Pratique apprise 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 n'importe où sur l'ordinateur Les programmes malveillants peuvent 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'un incident lié à un programme malveillant	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 activement 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 failles d'exploitation Les fichiers non signés peuvent contenir des programmes malveillants ou des riskwares Tous les exécutables non signés doivent être vérifiés pour détecter une éventuelle infection Une signature numérique ne garantit pas que le fichier ne contient pas de fonctionnalités malveillantes	Utilisation de moniteurs d'événements du système et de sandbox Utiliser des moteurs statistiques Désinstallation de PUP	Analyse statique (signature) et statistique (VirusTotal) des échantillons de logiciels Recherche de failles d'exploitation 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 employés des services informatiques impliqués dans les activités de cyberdiagnostic ou de gestion des incidents menées par l'équipe de sécurité	Le processus de réponse à incidents Méthodes d'analyse du journal Particularités 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 effectuée sous la supervision de l'équipe de sécurité et en coopération avec elle	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
Phishing et renseignement de sources ouvertes (OSINT)	Les employés 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'email	Le phishing peut être très complexe, ce qui le rend difficile à découvrir, mais il peut toujours être détecté par une enquête manuelle Les emails de phishing doivent être supprimés des messageries des utilisateurs	Analyse du phishing par email et suppression des emails de phishing dissimulés des messageries des utilisateurs Renseignement de sources ouvertes pour comprendre ce que les pirates savent au sujet de votre entreprise	Recherche et suppression des emails de phishing dans la boîte aux lettres Exchange Utilisation de Recon-ng pour la reconnaissance Web
Sécurité du serveur	Administrateurs de serveurs	Analyse de l'environnement réseau Renforcement des serveurs Analyse des journaux PowerShell pour détecter les attaques	La compromission du périmètre du réseau est l'un des principaux vecteurs d'attaque. Il est impossible de combler toutes les vulnérabilités. Il faut réduire la surface d'attaque pour rendre la réussite d'une attaque aussi difficile que possible. Même si cette mesure n'arrête pas un intrus, elle vous permettra de gagner du temps pour le détecter.	Recherche de services réseau vulnérables et non standard Configuration des systèmes selon le principe « interdiction par défaut » Recherche de signes d'une attaque dans les journaux PowerShell	Utilisation de Nmap pour trouver les services réseau vulnérables Configuration des stratégies de restriction logicielle pour contrôler les programmes et du pare-feu Windows pour contrôler le réseau Analyse des événements à l'aide d'Event Log Explorer

Nom du module	Public cible	Connaissances acquises	Attitude personnelle	Compétences acquises	Pratique apprise dans le module
Sécurité d'Active Directory	Administrateurs d'Active Directory	Utilisation d'une API pour vérifier les mots de passe dans une base de données de mots de passe compromis Configuration des stratégies de domaine selon les recommandations Méthodes d'analyse de la sécurité des domaines Active Directory	La configuration par défaut d'Active Directory n'est pas optimale du point de vue de la sécurité. Les pirates informatiques peuvent obtenir des privilèges plus élevés de plusieurs façons. Étude des recommandations en matière de sécurité, utilisation d'outils permettant une meilleure visibilité d'Active Directory	Vérification en toute sécurité des hachages de mots de passe dans une base de données Recherche d'incohérences entre les stratégies de domaine recommandées et les stratégies de domaine réelles Accès à la sécurité des paramètres d'Active Directory	Utilisation de l'API Have I Been Pwned? pour rechercher la présence de mots de passe compromis dans la base de données Utilisation de l'analyseur de stratégies pour comparer les stratégies de domaine actuelles aux pratiques exemplaires Utilisation des rapports Ping Castle

Nous contacter

Pour organiser une démo ou obtenir des informations sur les prix et les délais de livraison, veuillez contacter votre responsable Kaspersky ou envoyer un email à l'adresse awareness@kaspersky.com

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

Principaux facteurs de différenciation des programmes

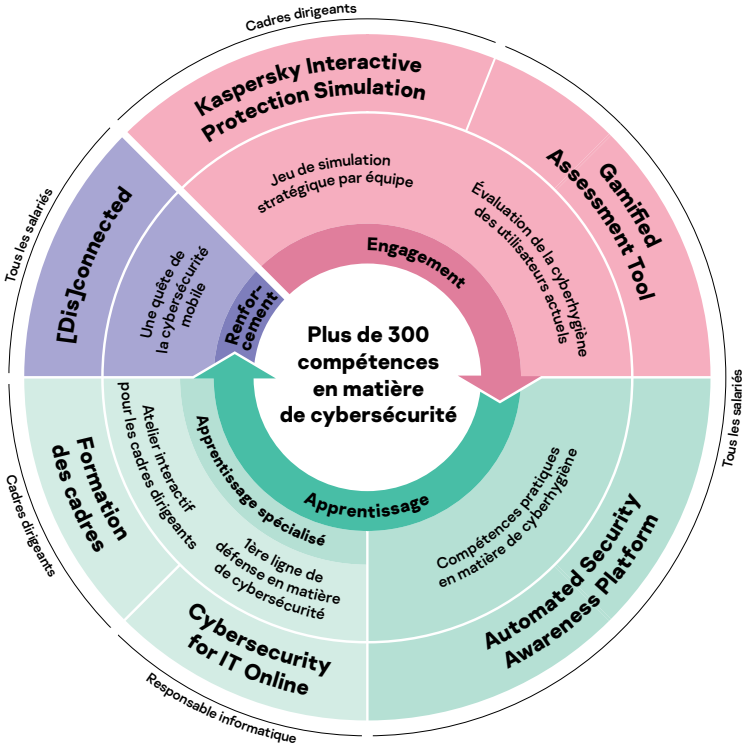
Une expertise considérable en matière de cybersécurité
Plus de 20 ans d'expérience dans le domaine de la cybersécurité transformés en un ensemble de compétences de cybersécurité qui est au cœur de nos produits

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 propose un éventail de solutions qui couvrent l'ensemble des besoins spécifiques des entreprises en matière de cybersécurité et enseigne les compétences que chaque membre du personnel devrait maîtriser en s'appuyant sur les dernières techniques et technologies d'apprentissage.

Une solution de formation flexible accessible à tous

Choisissez une solution unique qui répond à un besoin de sécurité spécifique, ou laissez-nous vous fournir une offre simplifiant le lancement et le ciblage de vos formations sur la base de vos besoins et de vos priorités. Vous trouverez de plus amples informations sur les forfaits à l'adresse suivante : kaspersky.fr/enterprise-security/security-awareness



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 BRING ON THE FUTURE