FORMATION À LA CYBER-SÉCURITÉ

Kaspersky Lab vous fait bénéficier de son expérience et de son savoir-faire en matière de cyber-sécurité grâce à ce programme de formation innovant.

La sensibilisation et la formation à la cyber-sécurité sont devenues des impératifs pour les entreprises confrontées à un volume croissant de menaces en constante évolution. L'amélioration des compétences techniques des salariés en matière de sécurité est un atout essentiel à toute stratégie de lutte contre les menaces.

Spécialement conçu pour les entreprises cherchant à renforcer la protection de leur infrastructure et de leur propriété intellectuelle, le programme de formation à la cyber-sécurité de Kaspersky Lab inclut un large choix de cours et de certifications, couvrant tous les thèmes et techniques dans ce domaine, des plus simples aux plus avancés.

RENFORCEZ VOS COMPÉTENCES EN SÉCURITÉ INFORMATIQUE

UNE OFFRE COMPLÈTE

Tous les cours sont proposés en anglais et dispensés soit dans les locaux de Kaspersky Lab, soit dans ceux de votre entreprise, sur demande. Les cours regroupent des enseignements théoriques et pratiques (ateliers). Le matériel de formation et les ordinateurs portables pour les ateliers sont fournis. À l'issue de la formation, les participants peuvent passer un examen de certification pour valider leurs connaissances.

DÉBUTANT, INTERMÉDIAIRE OU EXPERT ?

Le programme porte sur de nombreux sujets, des principes de sécurité de base à l'analyse avancée des programmes malveillants et investigations numériques pour aider les clients à améliorer leurs connaissances en matière de cyber-sécurité dans trois domaines principaux :

- Connaissances fondamentales du sujet
- Investigations numériques et réaction aux incidents
- Analyse avancée des programmes malveillants et reverse engineering

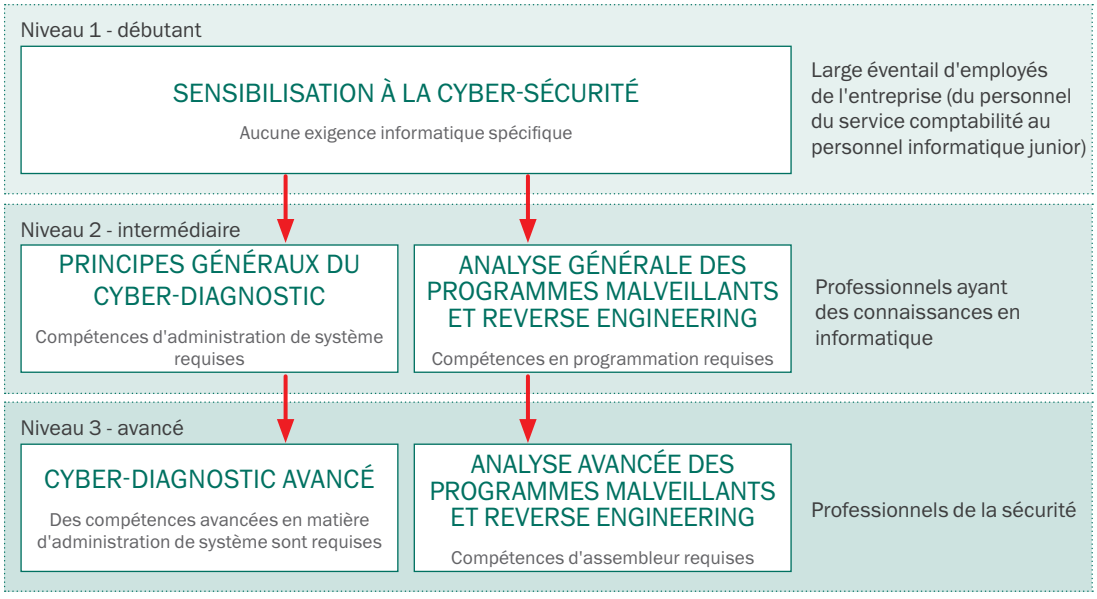
AVANTAGES DU SERVICE

La formation du personnel en matière de cyber-sécurité aide les entreprises à :

- **NIVEAU 1 : Sensibilisation à la cyber-sécurité**
  réduire les dépenses / atténuer les risques liés à la réputation / atténuer les fuites d'informations confidentielles liées aux problèmes génériques de sécurité et à la méconnaissance des principales menaces.
- **NIVEAUX 2-3 : Cyber-diagnostic**
  améliorer l'expertise des services internes de cyber-diagnostic et de réaction aux incidents.
- **NIVEAUX 2-3 : analyse des programmes malveillants et reverse engineering**
  améliorer l'expertise des services internes d'analyse des programmes malveillants et de reverse engineering.

UNE EXPERIENCE CONCRETE

Le programme exclusif de Kaspersky Lab fournit une expérience pratique (en proposant notamment des ateliers) au sujet des dernières attaques et des derniers programmes malveillants.



DESCRIPTION DU PROGRAMME

SUJETS	Durée	Compétences acquises
NIVEAU 1 : SENSIBILISATION À LA CYBER-SÉCURITÉ		
• Cyber-menaces et aperçu des marchés souterrains • Spam et phishing, sécurité du courrier électronique • Types de cyber-menaces et technologies de protection • Menaces persistantes sophistiquées • Notions d'investigation de base à l'aide d'outils publics basés sur le Web • Sécurisation de votre lieu de travail	2 jours	• Comprendre le paysage des menaces • Être capable d'utiliser votre ordinateur de manière plus sûre • Reconnaître les différents types d'attaques • Classer les cyber-armes et les programmes malveillants et comprendre leurs objectifs et leurs principes de fonctionnement • Analyser les e-mails de phishing • Reconnaître les sites Internet infectés ou faux
NIVEAU 2 : PRINCIPES GÉNÉRAUX DU CYBER-DIAGNOSTIC		
• Introduction au cyber-diagnostic • Réaction en temps réel et acquisition de preuves • Intérieur du Registre Windows • Analyse des artefacts Windows • Analyse des navigateurs • Analyse des e-mails	5 jours	• Construire le lab d'investigation numérique • Recueillir les preuves numériques et les traiter correctement • Reconstruire un incident et utiliser les données d'horodatage. • Détecter des traces d'intrusion dans les artefacts analysés dans le système d'exploitation Windows • Trouver et analyser l'historique du navigateur et des e-mails • Être capable d'appliquer les instruments et les outils d'investigation numérique
NIVEAU 2 : ANALYSE GÉNÉRALE DES PROGRAMMES MALVEILLANTS ET REVERSE ENGINEERING		
• Objectifs et techniques de l'analyse des programmes malveillants et reverse engineering • Système Windows interne, fichiers exécutables, assembleur x86 • Techniques de base d'analyse statique (extraction de données, analyse des importations, aperçu des points d'entrée PE, automatic unpacking, etc.) • Techniques de base d'analyse dynamique (débogage, outils de surveillance, interception du trafic, etc.) • Analyse de fichiers .NET, Visual basic, Win64 • Techniques d'analyse des scripts et non-PE (fichiers batch ; Autoit ; Python ; Jscript ; JavaScript ; VBS)	5 jours	• Construire un environnement sécurisé pour l'analyse des programmes malveillants : déployer sandbox et tous les outils nécessaires • Comprendre les principes d'exécution des programmes Windows • Effectuer l'unpacking des objets malveillants, les déboguer et les analyser, identifier leurs fonctions • Détecter les sites malveillants à travers l'analyse des scripts de programmes malveillants • Réaliser une analyse express des programmes malveillants
NIVEAU 3 : CYBER-DIAGNOSTIC AVANCÉ		
• Investigations approfondies dans Windows • Récupération des données • Investigations sur le réseau et le cloud • Investigations sur la mémoire • Analyse chronologique • Exercices d'investigation des attaques ciblées dans le monde réel	5 jours	• Être capable d'effectuer une analyse approfondie du système de fichiers • Être capable de récupérer les fichiers supprimés • Être capable d'analyser le trafic réseau • Détecter des activités malveillantes à partir de vidages de mémoire • Reconstruire la chronologie de l'incident
NIVEAU 3 : ANALYSE AVANCÉE DES PROGRAMMES MALVEILLANTS ET REVERSE ENGINEERING		
• Objectifs et techniques de l'analyse des programmes malveillants et de reverse engineering • Techniques avancées d'analyse statique et dynamique (manual unpacking) • Techniques de déobfuscation • Analyse Rootkit & Bootkit • Analyse des vulnérabilités (.pdf, .doc, .swf, etc.) • Analyse des programmes malveillants hors Windows (Android, Linux, Mac OS)	5 jours	• Mettre en œuvre les meilleures pratiques de reverse engineering du monde • Reconnaître les techniques anti-reverse engineering (obfuscation, anti-débogage) • Appliquer des techniques d'analyse avancées des programmes malveillants pour les rootkits/ bootkits • Analyser les shellcodes intégrés dans différents types de fichier • Analyser les programmes malveillants hors Windows