Formation à la cyber sécurité de Kaspersky Lab

www.kaspersky.fr
#truecybersecurity

Formation à la cyber sécurité de Kaspersky Lab

La formation à la cybersécurité est un impératif pour les entreprises confrontées au volume croissant et à l'évolution des menaces. Le personnel chargé de la sécurité IT doit bien maîtriser les techniques avancées : un élément clé d'une stratégie efficace de gestion et d'atténuation des menaces.

Cette formation couvre un large éventail de thèmes et de techniques de cybersécurité et proposent des certifications allant du niveau débutant au niveau expert. Tous les cours sont dispensés soit dans les bureaux de Kaspersky Lab, soit dans ceux de l'entreprise du client, en fonction des possibilités.

Les cours regroupent des enseignements théoriques et des ateliers pratiques. À l'issue de chaque cours, les participants sont invités à passer un examen de validation des connaissances.

Avantages

Cyberdiagnostic – Standard et avancé

Améliorer l'expertise de votre équipe interne en matière de cyberdiagnostic et de réponse aux incidents. Les formations sont destinées à combler des lacunes en termes d'expérience : développez et renforcez vos compétences pratiques de veille et d'analyse des différents types de données pour identifier la chronologie et les sources des attaques. Une fois la formation terminée, les participants seront en mesure d'enquêter efficacement sur les incidents d'ordre IT et d'améliorer le niveau de sécurité de l'entreprise.

Analyse des programmes malveillants et reverse engineering – Standard et avancée

La formation de reverse engineering vise à aider les équipes de réponse aux incidents à enquêter sur les attaques malveillantes. Elle s'adresse aux salariés du service IT et aux administrateurs système. Les participants découvriront comment analyser des logiciels malveillants, recueillir des indicateurs de compromission, créer des signatures pour identifier les machines contaminées et restaurer des fichiers et des documents infectés/chiffrés.

Réponse aux incidents

La formation guidera votre équipe interne à travers toutes les étapes du processus de réponse aux incidents et lui apportera les connaissances nécessaires pour une résolution efficace.

Yara

Les participants apprendront comment rédiger les règles YARA les plus efficaces et comment les tester et les améliorer au point d'identifier des menaces jusque-là indétectables.

Administration de la plate-forme Kaspersky Anti-Targeted Attack

La formation sur l'administration de la plate-forme Kaspersky Anti-Targeted Attack fournit tout le savoir-faire nécessaire pour planifier, installer et configurer cette dernière afin d'optimiser la détection des menaces.

Analyste en sécurité Kaspersky Anti-Targeted Attack

Cette formation comprend divers exercices pratiques basés sur des scénarios de détection de menaces réelles et apporte les connaissances nécessaires pour surveiller, interpréter et gérer les alertes de Kaspersky Anti-Targeted Attack en toute confiance.

Expérience concrète

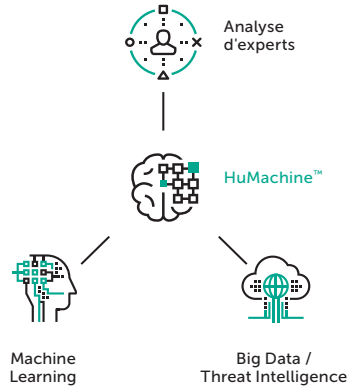
Avec l'aide d'un des principaux fournisseurs de sécurité informatique, travaillez et apprenez aux côtés de nos experts mondiaux qui inspirent les participants en partageant leur propre expérience de la détection et de la prévention de la cybercriminalité à son plus haut niveau.

Description du programme

Sujets	Durée	Compétences acquises
Cyberdiagnostic		
• Introduction au cyberdiagnostic • Réaction en temps réel et obtention de preuves • Contenu du registre Windows • Analyse des artefacts Windows • Analyse des navigateurs • Analyse des e-mails	5 jours	• Mettre en place un laboratoire de cyberdiagnostic • Recueillir les preuves numériques et les traiter correctement • Reconstruire un incident et utiliser les données d'horodatage • Détecter des traces d'intrusion grâce aux artefacts 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 de cyberdiagnostic
Analyse avancée des programmes malveillants et reverse engineering		
• Objectifs et techniques de l'analyse des programmes malveillants et du 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, extraction automatique, etc.) • Techniques de base d'analyse dynamique (débogage, outils de surveillance, interception du trafic, etc.) • Analyse des 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 une sandbox et tous les outils nécessaires • Comprendre les principes d'exécution des programmes Windows • Effectuer l'extraction 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
Cyberdiagnostic avancé		
• Investigations approfondies dans Windows • Récupération des données • Investigations sur le réseau et dans 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
Analyse avancée des programmes malveillants et reverse engineering avancé		
• Objectifs et techniques de l'analyse des programmes malveillants et du reverse engineering • Techniques avancées d'analyse statique (analyse statique de shellcodes, analyse d'en-tête PE, TEB, PEB, chargement de fonctions par différents algorithmes de hachage) • Techniques avancées d'analyse dynamique (structure PE, extraction manuelle et avancée, extraction d'outils de compression malveillants qui stockent le fichier exécutable sous forme chiffrée) • Reverse engineering des menaces APT (couvre un scénario d'attaque APT, des e-mails de phishing aux cas les plus complexes) • Analyse des protocoles (analyse des protocoles de communication chiffrés C2, décryptage du trafic) • Analyse des rootkits et des bootkits (débogage de secteur de démarrage en utilisant Ida et VMware, débogage de noyau en utilisant deux machines virtuelles, analyse des échantillons de rootkit)	5 jours	• Être en mesure de suivre les bonnes pratiques de reverse engineering tout en reconnaissant les techniques d'anti-reverse engineering (obfuscation, anti-débogage) • Être en mesure d'appliquer une analyse avancée des programmes malveillants pour décortiquer les rootkits/ bootkits • Être en mesure d'analyser les shellcodes intégrés dans les différents types de fichiers et les programmes malveillants ciblant des systèmes autres que Windows
Réponse aux incidents		
• Introduction à la réponse aux incidents • Détection et analyse préliminaire • Cyberdiagnostic • Élaboration de règles de détection (Yara, Snort, Bro)	5 jours	• Distinguer les menaces persistantes avancées (APT) des autres types de menaces • Comprendre les techniques des différents cybercriminels et la structure des attaques ciblées • Appliquer des méthodes de surveillance et de détection spécifiques • Suivre le processus de réponse aux incidents • Reconstruire l'historique et la logique des incidents • Élaborer des règles de détection et des rapports

Description du programme

Sujets	Durée	Compétences acquises
Yara		
• Brève introduction sur la syntaxe des règles Yara • Conseils et astuces pour élaborer des règles courtes mais efficaces • Rédacteurs des règles Yara • Recherche de faux positifs au moyen de tests des règles Yara • Recherche de nouveaux échantillons non encore détectés sur VT • Utilisation de modules dans Yara pour une recherche efficace • Recherche d'anomalies • Multiples exemples concrets • Exercices pour améliorer vos compétences Yara	2 jours	• Élaborer des règles Yara efficaces • Tester les règles Yara • Faire en sorte que votre équipe soit la seule à pouvoir identifier des menaces indétectables
Administration de la plate-forme Kaspersky Anti-Targeted Attack		
• Scénarios courants de déploiement de la solution et emplacements de serveur • Dimensions • Modèle de licence • Serveur sandbox • Nœud central • Capteur • Intégration à l'infrastructure • Installation de la sonde de terminaux • Ajout d'une licence et mise à jour des bases de données • Algorithme de fonctionnement de la solution	1 journée	• Concevoir un plan de mise en œuvre adapté à l'environnement du client • Installer et configurer l'ensemble des composants de la plate-forme Kaspersky Anti-Targeted Attack • Maintenir et contrôler la solution
Analyste en sécurité Kaspersky Anti-Targeted Attack		
• Interprétation des alertes de Kaspersky Anti-Targeted Attack • Explication des technologies de détection et d'analyse • Explication du système de notation et des moteurs de risque	1 journée	• Comprendre comment fonctionne le système de notation et comment il est utilisé par les moteurs de risque • Être à même de surveiller, d'interpréter et de gérer les alertes de Kaspersky Anti-Targeted Attack en toute confiance



Solutions de cybersécurité de
Kaspersky Lab pour les entreprises : **https://www.kaspersky.fr/enterprise-security**
Actualités des cybermenaces : **www.viruslist.fr**
Actualités de la sécurité informatique : business.kaspersky.com

#truecybersecurity
#HuMachine

www.kaspersky.fr

© 2017 AO Kaspersky Lab. Tous droits réservés. Les marques déposées et marques de service sont la propriété de leurs détenteurs respectifs.