
Modules de formation Kaspersky



Les modules de formation Kaspersky présentés ci-dessous – quatre au total – peuvent être réservés sous forme de journées de cours individuelles ou sous forme de package complet. Ceci grâce à la structure modulaire de la formation, qui permet une formation flexible et adaptée aux besoins.

Chaque journée de cours forme un tout. Ainsi, les participants peuvent choisir librement les modules qui leur conviennent, en fonction de leurs tâches et de leurs responsabilités au sein de l'entreprise. En outre, les participants peuvent répartir les jours de cours souhaités de manière flexible sur plusieurs mois tout au long de l'année. Le cours préparatoire est parfois recommandé, mais pas obligatoire.



Description:

Ce cours s'adresse aux revendeurs et aux clients finaux qui découvrent Kaspersky ou qui vont prochainement introduire Kaspersky. Cette journée peut être réservée comme cours d'introduction.

Contenu du cours:

La formation de base permet aux participants de se familiariser avec Kaspersky et son portefeuille de produits. Après le cours, les participants sont en mesure de positionner Kaspersky de manière compétente lors d'entretiens de vente. Les participants sont en mesure de répondre à des questions tech-

niques simples, mais aussi à des questions sur les licences et de fournir des renseignements. Ils acquièrent en outre le savoir-faire nécessaire pour expliquer théoriquement le Kaspersky Security Center (sur site ou dans le cloud) et démontrer son utilité ainsi que les différences essentielles.

Objectifs du cours:

Ce module permet aux participants

- de se familiariser avec Kaspersky et son portefeuille de produits
- de comprendre et d'appliquer les bases les plus importantes
- de comprendre et d'expliquer les licences et leur structure
- d'acquérir des connaissances sur tous les portails importants
- d'acquérir une compréhension de base du KSC (Kaspersky Security Center, on-premise ou cloud) et de pouvoir en expliquer le contenu et l'utilité.

Prérequis:

Compréhension de base de la sécurité informatique, des solutions antivirus, des licences et de la technique.

Public cible:

Ingénieurs système, administrateurs informatiques, assistants/techniciens informatiques, spécialistes de la prévention et de la vente.

Autres infos:

Cours sans hands-on labs.

Pour plus
d'informations





Description:

Ce cours s'adresse aux revendeurs et aux clients finaux qui ont déjà une expérience pratique de Kaspersky, ainsi qu'aux personnes qui ont suivi le cours 1 «Kaspersky Silver» et qui souhaitent approfondir les connaissances de Kaspersky. Ce module peut être réservé comme journée de formation complémentaire au cours 1 «Kaspersky Silver».

Contenu du cours:

Le cours explique comment installer et configurer Kaspersky Security Center (sur site ou dans le cloud). Les participants apprennent à installer les licences et à les répartir sur les clients. Le Security Center, y compris le set-up et l'AD, est mis en

place non seulement en théorie, mais aussi dans un laboratoire préparé à cet effet. La distribution et le roll-out sont simulés avec les participants.

Objectifs du cours:

À l'issue de ce module, les participants sont en mesure de prendre des décisions autonomes quant à l'installation et la configuration du KSC qui conviennent à leurs clients. Ils ont une compréhension de base du KSC et peuvent l'installer, le configurer et déployer la sécurité des terminaux. En outre, les participants sont en mesure de comprendre la Default Policy ainsi que d'administrer et de gérer les licences.

Prérequis:

Afin de suivre la formation avec succès et d'effectuer les travaux de laboratoire de manière efficace, les participants doivent disposer des connaissances et compétences suivantes:

- compréhension TCP/IP et du fonctionnement d'Internet et de l'e-mail
- compétences de base dans l'administration de réseaux Microsoft Windows et Active Directory
- expérience dans l'utilisation du système d'exploitation Microsoft Windows
- connaissances de base de SQL Server

Public cible:

Ingénieurs système, administrateurs informatiques, assistants/techniciens informatiques et prévente.

Il n'est pas nécessaire d'avoir suivi le cours 1 «Kaspersky Silver».

Pour plus
d'informations





Description:

Cette journée de formation s'adresse aux revendeurs et clients finaux expérimentés ainsi qu'aux personnes qui ont suivi les journées de formation 1 et 2 et qui souhaitent approfondir leur connaissance du sujet. En outre, le cours s'adresse aux participants qui ont déjà installé et utilisent Kaspersky.

Ce jour de formation peut être réservé séparément des cours 1 et 2.

Contenu du cours:

Les participants apprennent à connaître de manière approfondie les fonctions de sécurité des politiques et apprennent à les adapter aux besoins.

Les participants travaillent avec l'environnement KSC Lab préparé. Ils sont initiés à la structure étendue du KSC et à

l'architecture des politiques, apprennent à regrouper, à définir des ensembles de règles, à gérer et à exploiter la console, à mettre en œuvre des mécanismes de protection ciblés et à effectuer le déploiement des terminaux. Le thème du testing occupe également une place importante.

Objectifs du cours:

Les participants sont en mesure d'exploiter le Kaspersky Security Center (KSC) de manière autonome. En outre, à la fin du cours, ils connaissent toutes les fonctions et tous les paramètres pertinents et peuvent définir et administrer l'ensemble de l'architecture des politiques de manière autonome. En outre, ils connaissent les principaux mécanismes de protection et sont en mesure d'effectuer eux-mêmes le déploiement des terminaux.

Public cible:

Ingénieurs système, administrateurs informatiques, assistants/techniciens informatiques

Prérequis:

Afin de suivre la formation avec succès et d'effectuer les travaux de laboratoire de manière efficace, les participants doivent posséder les connaissances et compétences suivantes:

- compréhension de TCP/IP et du fonctionnement d'Internet et de l'e-mail, compétences de base dans l'administration de réseaux Microsoft Windows et d'Active Directory
 - expérience dans l'utilisation du système d'exploitation Microsoft Windows
 - connaissances étendues de la sécurité informatique
 - connaissance du portefeuille Kaspersky et de son système de licences
 - connaissance de la manière pratique d'installer et d'exploiter le KSC
- Pour participer au cours 3 «Kaspersky Advanced», les participants doivent disposer de solides connaissances de base.*

Pour plus
d'informations





Description:

Ce cours s'adresse aux participants des journées 2 et 3 ainsi qu'aux revendeurs et aux clients finaux qui ont déjà une connaissance approfondie des produits de Kaspersky. Sont également invitées les personnes qui se penchent sur le thème de l'EDR. Le cours sera divisé en deux thèmes et comprendra d'une part l'EDR et d'autre part le troubleshooting dans le KSC.

Contenu du cours:

Deux thèmes seront abordés lors de cette journée de formation:

- Thèmes principaux du matin: EDR (Endpoint Detection and Response) et MDR (Managed Detection and Response).
- Thème principal de l'après-midi: troubleshooting dans le KSC

Les participants apprennent à connaître les principales fonctions de la solution EDR/MDR et à les différencier. Ils savent en outre comment l'EDR peut être mis en place et déployé de manière optimale et quelle valeur ajoutée on peut en tirer. Ils verront également comment le flux d'informations peut être analysé et évalué à l'aide de rapports ciblés. En outre, les participants apprennent quelles tâches doivent être exécutées le

plus rapidement possible en cas d'attaque et comment réagir et agir. En outre, le cours répond aux questions suivantes: pourquoi la sandbox joue-t-elle un rôle prépondérant dans l'interaction avec l'EDR et quels sont les avantages qu'elle apporte.

Le cours montre également comment un troubleshooting ciblé dans le Kaspersky Security Center (KSC) permet d'analyser plus rapidement les erreurs et de résoudre plus efficacement les problèmes de performance. Les participants peuvent également profiter de l'expérience pratique du formateur lors des migrations du KSC (que ce soit d'une installation sur site vers le cloud ou simplement d'un serveur à un autre).

Objectifs du cours:

- Connaître Kaspersky EDR/MDR, comprendre les différences essentielles au sein des solutions, définir sur la base de ces connaissances la solution optimale pour sa propre entreprise.
- Les participants sont en mesure de configurer et d'exploiter l'EDR avec la sandbox, de sélectionner les principaux paramètres, de détecter les attaques et de prendre les mesures appropriées sur la base des rapports définis.
- En outre, ils sont en mesure d'assurer le support du KSC de manière autonome et de tirer les bonnes conclusions en cas de dysfonctionnement.

Prérequis:

Afin de suivre la formation avec succès et d'effectuer les travaux de laboratoire de manière efficace, les participants doivent disposer des connaissances et compétences suivantes:

- très bonne connaissance de la sécurité informatique et des concepts de protection de la sécurité informatique
- connaissances approfondies des produits Kaspersky utilisés et de leurs licences
- très bonnes connaissances et compétences de l'exploitation d'un KSC

La participation aux cours 2 et 3 est obligatoire pour tous les participants qui ne connaissent pas Kaspersky.

Public cible:

Le prix s'entend en CHF hors TVA et comprend le PC de formation, les documents de formation et le repas.



Modules de formation Kaspersky



kaspersky