Formation CompTIA Security+

Durée: 5 Jours Réf de cours: G013

Résumé:

CompTIA Security+ est la certification en sécurité qui démontre sa connaissance des concepts, des outils et des procédures de sécurité informatiques. Elle confirme la capacité du professionnel à réagir aux incidents de sécurité, et valide ses compétences pour anticiper les risques de sécurité et protéger les organisations.
Cette formation permet aux participants d'acquérir les compétences et connaissances nécessaires pour mettre en œuvre de manière proactive des protocoles de sécurité sonore pour atténuer les risques de sécurité, réagir rapidement aux problèmes de sécurité, identifier de manière rétroactive où des violations de sécurité peuvent avoir eu lieu, concevoir un réseau, sur site ou dans le cloud, en toute sécurité.
Mise à jour : 05.12.2022

Public visé:

Cette formation s'adresse aux Ingénieurs réseaux qui cherchent à acquérir une connaissance fondamentale de la sécurité du réseau à travers l'obtention de la certification Security +

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Appréhender les menaces et contrôles de sécurité
- Découvrir la cryptographie et le contrôle d'accès
- Paramétrer la sécurité Internet
- Paramétrer la sécurité des hôtes, des données et des appareils
- Mettre en oeuvre la sécurité au sein d'un réseau

Pré-requis:

Connaître les fondamentaux systèmes et réseaux, ou avoir suivi les formations suivantes :

- G004 - Préparation à la Certification A+
- G005 - Préparation à la Certification Network+
- GKRES1 - Les bases du réseau
- G005 - Préparation à la certification Network+ - Compétences support

Test et certification

CompTIA Security+ fournit une référence mondiale pour les meilleures pratiques en matière de sécurité informatique. La certification valide les connaissances sur la sécurité des réseaux, la conformité et la sécurité des opérations, les menaces et vulnérabilités, etc.

Ce titre de certification s'obtient par la réussite de l'examen SY0-601 (en anglais), à passer ultérieurement.

Après cette formation, nous vous conseillons le(s) module(s) suivant(s):

- GK5867 - CompTIA CySA+ Cybersecurity Analyst
- G015 - CompTIA Pentest +
- GK2951 - CompTIA Advanced Security Practitioner (CASP) Prep Course

Contenu:

Menaces et contrôles de sécurité

- Contrôles de sécurité
- Menaces et attaques
- Attaques réseau
- Outils et techniques d'évaluation

Cryptographie et contrôle d'accès

- Chiffrements, Hashes, et Steganography
- Infrastructure à clé publique (PKI)
- Authentification avec mot de passe
- Autorisations et gestion de comptes

Sécurité Réseau

- Conception d'un réseau sécurisé
- Appliances de sécurité et Applications
- Sécurité réseau du Wifi
- VPN et sécurité de l'accès distant
- Sécurité des applications réseau

Hôtes, Données, et Sécurité des applications

- Sécurité des hôtes
- Sécurité des données
- Sécurité des services web
- Sécurité des applications web
- Virtualisation et Sécurité du Cloud

Sécurité opérationnelle

- Sécurité d'un Site
- Sécurité des périphériques mobiles et intégrés
- Gestion des risques
- Reprise après sinistre
- Réponse aux incidents et forensics
- Règles de sécurité

Travaux pratiques

Les activités comprennent des sessions de questions et de réponses dirigées par l'instructeur, des discussions de groupe interactives, ainsi que des activités pratiques

- Using Hyper-V
- Trojans and Malware Protection
- Network Vulnerabilities
- Baseline Security Analyzer
- Steganography
- Configuring Certificate Services
- Password Sniffing
- Configuring a VPN
- Telnet and FTP
- Attacks Against DHCP and DNS
- Network Access Protection
- Data Leakage Prevention
- HTTP and HTTPS
- Web Application Vulnerabilities
- Computer Forensics Tools

Méthodes pédagogiques :

Support de cours officiel remis aux participants

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• Modalités d'évaluation : le participant est invité à s'auto-évaluer par rapport aux objectifs énoncés.
• Chaque participant, à l'issue de la formation, répond à un questionnaire de satisfaction qui est ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

•Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
•Votre place sera confirmée à la réception d'un devis ou ""booking form"" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
•Attention, si vous utilisez votre Compte Personnel de Formation pour financer votre inscription, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés.