CompTIA S+ : les bases de la cybersécurité

Date et durée

Code formation : C-SECU
Durée : 5 jours
Nombre d'heures : 35 heures

Formation avec certification

CompTIA Security+

Description

Avec les attaques informatiques que subissent les organisations, **la sécurité des infrastructures** fait partie des points importants qui préoccupent tous les secteurs. En tant que professionnel de l'informatique, **développer des compétences en cybersécurité** devient indispensable pour démarrer ou poursuivre une carrière. De plus en plus d'entreprises proposent des postes d'administrateur sécurité ou encore d'auditeur informatique pour sécuriser leur système d'information, leur application et leur matériel.
Notre formation CompTIA S+ vous permet d'acquérir des connaissances et des compétences pratiques en cybersécurité. Pendant 5 jours, vous apprendrez **les bases de la sécurité informatique** en entreprise. Vous aborderez les menaces, les attaques et les vulnérabilités, la cryptographie, l'architecture réseau sécurisée et bien plus encore. Enfin, vous vous familiariserez avec les normes de conformité et les bonnes pratiques en matière de **gestion des risques et de sécurité des données**.
Au terme de cette formation intensive, vous serez également **préparé pour le passage de l'examen CompTIA SY0-701** inclus dans notre offre. Cet examen est un prérequis pour obtenir la certification CompTIA Security+ (*en savoir plus dans l'onglet certification*).

Objectifs

À l'issue de la **formation CompTIA Security +**, vous atteindrez les objectifs suivants :

- établir un modèle de menaces pour protéger les points d'accès réseau et les services informatiques d'une entreprise ;
- administrer un système de détection d'intrusion (IDS) afin de détecter les attaques vers un réseau ou une infrastructure informatique ;
- mettre en œuvre une sécurité réseau avec la création et la configuration d'un hôte Bastion ;
- créer et configurer une liste de contrôle d'accès (ACL) ;
- établir des services de pare-feu avec des règles personnalisées en appliquant des filtres dynamiques de paquets et un filtrage de périphériques ;
- identifier les ports réseau et les différents outils de piratage les plus utilisés par les hackers ;
- réaliser un balayage de port et s'en servir judicieusement pour protéger un système d'information ;
- surveiller et identifier des attaques et des vulnérabilités pour les affaiblir avant leurs déploiements dans un système d'information ;
- assimiler la virtualisation sécurisée, le déploiement d'applications sécurisées et les concepts d'automatisation ;
- caractériser, conseiller et appliquer les meilleures solutions de sécurité au sein d'une entreprise ;
- connaître et comprendre les lois et les politiques de sécurité informatique ;

- repérer, examiner et répondre aux événements et incidents de sécurité ;
- passer l’examen SY0-701 CompTIA S+ et décrocher la certification.

Points forts

5 domaines de compétences en sécurité informatique maîtrisés ; une opportunité pour débuter une carrière en cybersécurité et le passage de l'examen de certification CompTIA Security+ compris dans l'offre.

Certification

Notre formation CompTIA Security+ vous permettra de **passer l'examen officiel CompTIA SY0-701** à tout moment et en ligne. Pour planifier votre examen, vous devez vous inscrire sur CompTIA.org. Après avoir réussi cet épreuve, vous obtiendrez la **certification CompTIA Security+ valable 3 ans**.

Détail de l'examen CompTIA SY0-701 :

L'examen attestera que vous posséder les connaissances et les compétences requises pour **évaluer le niveau de sécurité d'un environnement informatique d'entreprise**. Vous devrez en outre être en mesure de recommander et de mettre en œuvre des solutions de sécurité appropriées, de surveiller et de sécuriser les environnements hybrides, d'opérer en tenant compte des réglementations et des politiques applicables, d'identifier et d'analyser les événements et les incidents de sécurité et d'y répondre.

- Type d’examen : 90 questions à choix multiples et basés sur la performance
- Durée : 1 heure
- Livre ouvert : non
- Langue : anglais, japonais, portugais et espagnol
- Attribution : 750 points basés sur une échelle de 100 à 900 points

La certification CompTIA Security+ est renouvelable en cumulant 50 unités de formation continue (CEU) sur 3 ans.
En savoir + sur le programme de formation continue CompTIA

Modalités d'évaluation

Quiz / QCM
Travaux Pratiques

Pré-requis

Suivre la **formation CompTIA S +**, nécessite les prérequis suivants :

- savoir lire et comprendre l’anglais, le japonais, le portugais ou l'espagnol pour le passage de l'examen SY0-701 ;
- avoir obtenu la certification CompTIA Network+ et 2 ans d'expérience en tant qu'administrateur système ou sécurité (*recommandé).*

Public

Cette formation s'adresse aux publics suivants :

- toute personne qui souhaite acquérir des compétences de base en cybersécurité ;
- tout professionnel de l'informatique qui souhaite obtenir la certification CompTIA Security+.

Cette formation s'adresse aux profils suivants

Administrateur système
Ingénieur système
Directeur des Systèmes d'Information (DSI)
Chef de projet / Responsable de projet
Technicien Support / HelpDesk
Développeur
Auditeur interne / externe

Programme

1. A propos de la cybersécurité

- Les notions de base de la sécurité informatique.
- La gestion des risques d'un projet informatique.
- L'évaluation de la vulnérabilité et du risque.

2. Comprendre les cyberattaques

- Le hacking et les hackers.
- La pratique de l'ingénierie sociale.
- Les programmes malveillants.
- Les attaques réseau.
- Les attaques de malwares.

Lab informatique :

- détecter des logiciels malveillants ;
- effectuer une analyse de vulnérabilité d'un site web ;
- simuler une attaque DDoS ;
- casser un mot de passe ;
- réaliser un test d'intrusion ;
- effectuer une analyse de vulnérabilité d'application ;
- observer des attaques par injection de commandes SQL ;
- observer des attaques côté client.

3. Comprendre la cryptographie

- Les différentes techniques de cryptographie.
- Les infrastructures à clés publiques (ICP).

Lab informatique :

- mettre en œuvre une cryptographie symétrique et asymétrique ;
- utiliser des fonctions de hachage pour des fichiers ;
- mettre en place une autorité de certification.

4. Connaitre les fondamentaux des réseaux

- Les composants de base d’un réseau.
- Le système d’adressage IP.
- Les ports réseaux et les ports logiciels.

Lab informatique :

- Utiliser des outils de dépannage TCP/IP en ligne de commande.

5 : Sécuriser un réseau d’entreprise

- Les composants de la protection réseau.
- Le chiffrement de la couche transport.
- L’amélioration des performances du réseau.
- L’analyse et la détection des anomalies.

Lab informatique :

- configurer une stratégie de pare-feu avec des règles personnalisées ;
- vérifier et tester des certificats SSL ;
- sécuriser un WAP (Wireless Application Protocol) ;
- analyser un journal d'événement système ;
- mettre en œuvre des procédures de numérisation réseau.

6. Sécuriser des hôtes et assurer la confidentialité

- La sécurité des ordinateurs hôtes.
- La sécurité des données.
- La sécurité des appareils mobiles.

Lab informatique :

- chiffrer et sécuriser avec BitLocker.

7. Sécuriser les services réseaux

- La sécurité d’une application.
- La sécurité des machines virtuelles.
- La sécurité des services dans le cloud.

Lab informatique :

- identifier des codes vulnérables.

8. Comprendre les processus d’authentification

- Les différents types de facteurs d’authentification.
- Les différents types de protocoles d’authentification.

Lab informatique :

- installer et configurer un serveur RADIUS ;
- effectuer une analyse avec Active Directory.

9. Comprendre le contrôle d'accès des SI

- Les différentes techniques de contrôle d'accès.
- La gestion des comptes utilisateurs.

Lab informatique :

- effectuer un audit et rédiger un rapport sur les autorisations NTFS ;
- utiliser des outils de ligne de commande pour gérer les objets Active Directory ;
- appliquer des objets de stratégie de groupe ;
- créer un modèle de sécurité informatique.

10. Gérer les risques

- Les lois, les normes et les politiques de sécurité informatique.
- La formation des utilisateurs.
- La sécurité physique et la sûreté des systèmes d’information.

11. Planifier la récupération après sinistre

- La reprise après sinistre.
- La haute disponibilité.
- La tolérance de pannes et la récupération.
- La réponse aux incidents.

Lab informatique :

- paramétrer et utiliser des sauvegardes sur Windows Server.

Guide des certifications
CompTIA
Télécharger la brochure