Formation Formation CompTIA Security+

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Le cours CompTIA Security+ est conçu pour vous aider à préparer l'examen SY0-701. L'examen CompTIA Security+ certifie que le candidat retenu possède les connaissances et les compétences requises pour installer et configurer des systèmes afin de sécuriser les applications, les réseaux et les appareils ; effectuer une analyse des menaces et y répondre par des techniques d'atténuation appropriées ; participer à des activités d'atténuation des risques ; et opérer en étant conscient des politiques, des lois et des réglementations applicables.

Référence	G013
Durée	5 jours (35h)
Tarif	2 995 €HT
Repas	100 €HT(en option)

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 7 au 11 juillet 2025
du 13 au 17 octobre 2025
du 16 au 20 février 2026

VOIR TOUTES LES DATES

Objectifs

| Évaluer la posture de sécurité d'un environnement d'entreprise et recommander et mettre en oeuvre des solutions de sécurité appropriées.
| Surveiller et sécuriser les environnements hybrides, y compris le cloud, le mobile, l'Internet des objets (IoT) et la technologie opérationnelle.
| Opérer en étant conscient des réglementations et des politiques applicables, y compris les principes de gouvernance, de risque et de conformité.
| Identifier, analyser et répondre aux événements et incidents de sécurité.

Public

| professionnels de l'informatique exerçant des fonctions telles que
| Administrateur de sécurité
| Spécialiste de la sécurité
| Administrateur de systèmes
| Analyste du service d'assistance
| Ingénieur sécurité
| Analyste de sécurité

Prérequis

| Compétences en matière de mise en réseau et d'administration de réseaux TCP/IP basés sur Windows et connaissance d'autres systèmes d'exploitation, tels que OS X, Unix ou Linux.

Programme de la formation

Concepts généraux de sécurité 12%
| Comparer et opposer les différents types de contrôles de sécurité.
| Résumer les concepts de sécurité fondamentaux.
| Expliquer l'importance des processus de gestion du changement et leur impact sur la sécurité.
| Expliquer l'importance de l'utilisation de solutions cryptographiques appropriées.

Menaces, vulnérabilités et mesures d'atténuation 22%
| Comparer et opposer les acteurs et les motivations des menaces les plus courantes.
| Expliquer les vecteurs de menace courants et les surfaces d'attaque.
| Expliquer les différents types de vulnérabilités.
| Analyser, à partir d'un scénario, les indicateurs d'une activité malveillante.
| Expliquer l'objectif des techniques d'atténuation utilisées pour sécuriser l'entreprise.

Architecture de sécurité 18%
| Comparer et opposer les implications de différents modèles d'architecture sur la sécurité.
| A partir d'un scénario, appliquer les principes de sécurité pour sécuriser l'infrastructure de l'entreprise.
| Comparer et opposer les concepts et les stratégies de protection des données.
| Expliquer l'importance de la résilience et de la récupération dans l'architecture de sécurité.

Opérations de sécurité 28%
| À partir d'un scénario, appliquer les techniques de sécurité courantes aux ressources informatiques.
| Expliquer les implications en matière de sécurité d'une bonne gestion du matériel, des logiciels et des données.
| Expliquer les différentes activités associées à la gestion des vulnérabilités.
| Expliquer les concepts et les outils d'alerte et de surveillance de la sécurité.
| Dans le cadre d'un scénario, modifier les capacités de l'entreprise pour améliorer la sécurité.
| Dans le cadre d'un scénario, mettre en oeuvre et maintenir la gestion des identités et des accès.
| Expliquer l'importance de l'automatisation et de l'orchestration dans le cadre d'opérations sécurisées.
| Expliquer les activités appropriées de réponse aux incidents.
| Dans le cadre d'un scénario, utiliser les sources de données pour soutenir une enquête.

Gestion et supervision du programme de sécurité 20
| Résumer les éléments d'une gouvernance efficace de la sécurité.
| Expliquer les éléments du processus de gestion des risques.
| Expliquer les processus associés à l'évaluation et à la gestion des risques par des tiers.
| Résumer les éléments d'une conformité efficace en matière de sécurité.
| Expliquer les types et les objectifs des audits et des évaluations.
| Dans le cadre d'un scénario, mettre en oeuvre des pratiques de sensibilisation à la sécurité.

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.