

## Formation CompTIA Security+

Durée: 5 Jours    Réf de cours: G013    Version: SY0-701

### Résumé:

Le cours CompTIA Security+ est conçu pour vous aider à préparer l'examen SY0-701.

CompTIA Security+ est la première certification mondiale qui établit les compétences essentielles requises pour les fonctions de sécurité de base et une carrière dans la sécurité informatique. Elle met en avant les capacités des professionnels à sécuriser les réseaux, les applications et les appareils, tout en garantissant l'intégrité, la confidentialité et la disponibilité des données.

La formation CompTIA Security+ a pour objectif de prouver qu'un candidat possède les connaissances et les compétences requises pour :

- Évaluer l'état de sécurité d'un environnement d'entreprise et recommander et mettre en œuvre des solutions de sécurité appropriées
- Surveiller et sécuriser les environnements hybrides, y compris le cloud, le mobile et l'IoT
- Agir en tenant compte des lois et politiques applicables, y compris les principes de gouvernance, de risque et de conformité
- Identifier, analyser et répondre aux événements et incidents de sécurité

Mis à jour : 18/11/2025

### Public visé:

CompTIA Security+ s'adresse aux professionnels de l'informatique exerçant des fonctions telles que : Administrateur de

### Objectifs pédagogiques:

- À l'issue de la formation, les participants seront capables de :
- Identifier différents types de menaces, d'attaques et de vulnérabilités, notamment les logiciels malveillants, l'ingénierie sociale et les attaques d'applications.
- Utiliser des technologies et des outils de sécurité, tels que des pare-feu, des systèmes de détection d'intrusion et des solutions de sécurité des terminaux, pour protéger les systèmes.
- Concevoir des architectures réseau sécurisées, mettre en œuvre des systèmes sécurisés et appliquer des protocoles sécurisés pour l'architecture et la conception.
- Gérer les concepts d'identité et d'accès, notamment l'authentification, l'autorisation et la comptabilité, afin de garantir un contrôle d'accès sécurisé
- Évaluer et gérer les risques grâce à l'analyse des risques, aux stratégies d'atténuation et à la planification de la continuité des activités.
- Appliquer les concepts de cryptographie, notamment les algorithmes de chiffrement, l'infrastructure à clé publique (PKI) et les signatures numériques, pour sécuriser les données.
- Mettre en œuvre des mesures de conformité et de sécurité opérationnelle, notamment des politiques, des procédures et des bonnes pratiques en matière de sécurité.

### Pré-requis:

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.

La formation G005 et/ou la certification CompTIA Network+ est recommandée mais pas impérative.

- G005 - Préparation à la certification CompTIA Network+

### Test et certification

CompTIA Security+ est la première certification de cybersécurité de début de carrière qu'un candidat devrait obtenir. Elle permet aux professionnels de la cybersécurité d'acquérir les compétences de base nécessaires pour protéger les réseaux, détecter les menaces et sécuriser les données grâce à des questions basées sur les performances.

Elle les aide à ouvrir la voie à une carrière dans la cybersécurité et à devenir un défenseur de confiance des environnements numériques.

- Examen requis : SY0-701
- Nombre de questions : Maximum de 90

- **Types de questions** : Questions à choix multiples et questions basées sur la performance
- **Durée du test** : 90 minutes
- **Expérience recommandée** : Un minimum de 2 ans d'expérience dans l'administration informatique avec un accent sur la sécurité, une expérience pratique de la sécurité technique de l'information et une large connaissance des concepts de sécurité.

---

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

- GK5867 - CompTIA CySA+ Cybersecurity Analyst
  - G015 - CompTIA PenTest+ Certification Prep Course
  - GK2951 - CompTIA SecurityX Certification Prep Course
- 

### Contenu:

#### 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 œuvre 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 œuvre des pratiques de sensibilisation à la sécurité.

## Méthodes pédagogiques :

Accrédité par l'ANSI pour démontrer la conformité à la norme ISO 17024.

Les participants réalisent un test d'évaluation des connaissances en amont et en aval de la formation pour valider les connaissances acquises pendant la formation.

Un support de cours officiel sera remis aux stagiaires.

La certification CompTIA Security+ a une validité de trois ans à compter de la date à laquelle le candidat l'a obtenue.

La dernière version de la certification CompTIA Security+ est CompTIA Security+ SY0-701.

Les mises à jour de CompTIA Security+ reflètent les compétences pertinentes pour les postes de sécurité informatique et préparent les candidats à être plus proactifs dans la prévention de la prochaine attaque. Pour lutter contre ces menaces émergentes, les professionnels des TI doivent être en mesure de :

- Aider à identifier les attaques et les vulnérabilités et à les atténuer avant qu'elles ne pénètrent le SI
- Comprendre la virtualisation sécurisée, le déploiement sécurisé d'applications et les concepts d'automatisation
- Identifier et mettre en œuvre les meilleurs protocoles et cryptage
- Comprendre l'importance de la conformité

---

## 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.
- En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera 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 cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via [moncompteformation.gouv.fr](http://moncompteformation.gouv.fr).

Accueil des bénéficiaires :

- En cas de handicap : plus d'info sur [globalknowledge.fr/handicap](http://globalknowledge.fr/handicap)
- Le Règlement intérieur est disponible sur [globalknowledge.fr/reglement](http://globalknowledge.fr/reglement)