Organisme de formation professionnelle continue
Numero agrément 91 30 03332 30
France : +33 (0)188 24 70 33 / 34
Site : www.oo2.fr
Mail : contact@oo2.fr

CompTIA CASP+ : praticien avancé en cybersécurité

Date et durée

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

Formation avec certification

CompTIA CASP+

Description

Étant donné que le secteur des TIC a besoin de personnes dotées de **compétences solides en cybersécurité**, le programme de cette **formation CompTIA** vous permet d'acquérir des techniques avancées. CompTIA CASP+ est l'unique certification orientée sur les performances qui s'adresse aux techniciens et non aux cadres en cybersécurité. Si les responsables de la cybersécurité contribuent à définir les politiques et **les modèles de cybersécurité** envisageables, les praticiens certifiés CASP+ apprennent à appliquer des stratégies et techniques adaptées à ces politiques et modèles.
Durant cette formation, vous intègrerez des principes avancés destinés à assurer la sécurité informatique de votre entreprise. Par conséquent, vous aborderez **la gestion des risques, les opérations et l'architecture de sécurité** d'entreprise, la recherche et la collaboration ainsi que l'intégration de la sécurité d'entreprise.
Au terme de ce programme de 5 jours, vous serez également **préparé pour le passage de l'examen CompTIA CAS-004** inclus dans notre offre. Cet examen est un prérequis pour obtenir la certification CompTIA Advanced Security Practitioner (*en savoir plus dans l'onglet certification*).

Objectifs

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

- identifier les risques et les systèmes de sécurité mise en place relatifs aux exigences sectorielles propres à chaque organisation ;
- appliquer des solutions adaptées pour limiter les menaces émergentes d'une organisation spécifique ;
- mettre en œuvre des systèmes de protection générale et des éléments de sécurité réseau afin de procéder à des analyses de sécurité au niveau de l'hôte, des périphériques mobiles et des périphériques de type "small form factor" ;
- introduire un processus de réponse aux incidents et de reprise après incident puis mener des analyses de sécurité via des logiciels adaptés ;
- intégrer des serveurs hôtes, des espaces de stockage, des équipements réseau et des logiciels de sécurité informatique au sein de systèmes sur site, dans le Cloud ou dans des systèmes de virtualisation ;
- utiliser des techniques de recherche visant à établir les perspectives du secteur industriel et leurs conséquences sur les organisations ;
- passer l'examen CAS-004 CompTIA CASP+ et décrocher la certification.

La certification CompTIA CASP+ est renouvelable en cumulant 75 unités de formation continue (CEU) sur 3 ans.
En savoir + sur le programme de formation continue CompTIA

Points forts

12 cours pour acquérir des compétences en tant que praticien de la cybersécurité ; une formation qui traite de la gestion des risques actuels e passage de l'examen de certification CompTIA CASP+ compris dans l'offre.

Certification

Notre formation CompTIA CASP+ vous permettra de **passer l'examen officiel CompTIA CAS-004** 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 CASP+ valable 3 ans**.

Détail de l'examen CompTIA CAS-004 :

L'examen aborde les connaissances et les compétences techniques indispensables à **la conception, l'ingénierie, l'intégration** et la bonne application d'un processus sécurisé au sein de structures informatiques spécifiques d'entreprises. Il permet ainsi de prouver votre expertise dans ce domaine, notamment en matière de gouvernance, de gestion des risques et de la compliance.

- Type d’examen : 90 questions à choix multiples et basés sur la performance
- Durée : 2 h 45
- Livre ouvert : non
- Langues : anglais, japonais ou Thai
- Attribution : réussite ou échec, pas de barème

Modalités d'évaluation

Quiz / QCM
Travaux Pratiques

Pré-requis

Suivre la **formation CompTIA CASP+** nécessite les prérequis suivants :

- posséder un minimum de compétences dans le domaine de la sécurité de l'information ;
- avoir une expérience pratique de 10 ans minimum dans le domaine de l’informatique en général et plus particulièrement 5 ans dans le domaine de la cybersécurité ;
- savoir lire et comprendre l'anglais, le japonais ou le Thai pour le passage de l’examen CompTIA CAS-004.

Public

Cette formation s'adresse aux publics suivants :

- les professionnels informatiques expérimentés qui souhaitent acquérir des compétences et des connaissances en gouvernance, gestion des risques et compliance ;

- les praticiens en cybersécurité qui veulent apprendre à mettre en place des solutions au sein des politiques et des cadres de cybersécurité ;
- les professionnels en cybersécurité qui souhaitent obtenir la certification CompTIA CASP+.

Cette formation s'adresse aux profils suivants

Architecte informatique / SI
Ingénieur système
Analyste cybersécurité

Programme

Cours 1: gestion des risques et gouvernance IT

- Les enjeux de la gestion des risques et de la gouvernance informatique.
- L'évaluation des risques cyber.
- L'atténuation des risques cyber.
- L'inclusion des documents dans le processus de gestion des risques.

Cours 2 : collaboration et communication

- La mise en place d'une collaboration renforcée entre les différents services commerciaux.
- Les outils de communication et de collaboration sécurisés.

Cours 3 : recherche et analyse avancées

- L'identification des stratégies propres à chaque secteur et leur incidence sur les services de l'entreprise.
- L'analyse de cas visant à garantir la sécurité des opérations des entreprises.

Cours 4 : authentification et autorisation complexes

- L'Implémentation et la mise en service de solutions d'authentification et d'autorisation.
- L'application d'un mode de gestion avancée en matière d'identité et de droits d'accès.

Cours 5 : application de la cryptographie symétrique et asymétrique.

- Le choix des bonnes techniques de cryptographie.
- L'implémentation de la cryptographie.

Cours 6 : application des contrôles de sécurité au niveau des hôtes

- Le choix du matériel et du système de l'hôte principal.
- Le renforcement des hôtes secondaires.
- La virtualisation des serveurs et des environnements de bureau.
- La protection des chargeurs d'amorçages.

Cours 7 : application des contrôles de sécurité pour les appareils mobiles

- La mise en place d'une gestion avancée relatives aux appareils mobiles.
- Les questions de sécurité et de confidentialité relative aux appareils mobiles.

Cours 8 : application de la sécurité des réseaux

- La planification du déploiement des systèmes de sécurité du réseau.
- La planification du déploiement des périphériques réseau.

- La mise en place d'une conception avancée du réseau.
- La mise en place de contrôles de sécurité du réseau.

Cours 9 : application de la sécurité dans le processus de développement des systèmes et des applications.

- La sécurité dans le cycle de vie des technologies de l'information.
- La détection des menaces sur les applications.
- La détection des menaces sur les apps Web.
- La mise en place de contrôles de sécurité pour les applications.

Cours 10 : déploiement des processus dans une architecture sécurisée

- L'intégration des normes et des bonnes pratiques dans la sécurité organisationnelle des entreprises.
- Le choix des modèles de déploiement sur le plan technique.
- L'intégration des fonctions de sécurité avancées dans le Cloud Computing.
- La création d'une infrastructure d'entreprise sécurisée.
- L'intégration de la sécurité des données dans les systèmes informatiques des entreprises.
- Le déploiement des logiciels d'entreprise dans une architecture sécurisée.

Cours 11: évaluation de la sécurité

- Le choix des bonnes méthodes d'évaluation de la sécurité.
- La réalisation d'évaluations de sécurité via des logiciels adaptés.

Cours 12 : réponse aux incidents et reprise après incident.

- La préparation pour la réponse aux incidents et les investigations forensiques.
- La conduite de la réponse aux incidents et de l'analyse informatique légale.

Guide des certifications
CompTIA
Télécharger la brochure