CompTIA CASP+

Durée: 5 jours
Public cible: Professionnel TI

À qui s'adresse cette formation ?

Les techniciens et les praticiens en cybersécurité qui appliquent des stratégies et des techniques adaptées aux politiques et aux modèles de cybersécurité d'une organisation. Les personnes qui souhaitent obtenir une certification avancée qui démontre l'expertise et les connaissances des concepts de sécurité, outils, procédures, conception et ingénierie de solutions sécurisées à travers des environnements d'entreprises de grandes envergures.

Objectifs de la formation

- Acquérir les compétences avancées pour concevoir et créer des solutions sécurisées dans des environnements professionnels complexes
- Maîtriser la sécurité de l'entreprise, y compris les opérations et les concepts d'architecture, les techniques et les exigences
- Développer des compétences en analyse des risques et en anticipation de la cyberdéfense
- Gérer la sécurité des appareils mobiles et des appareils à petit facteur de forme
- Analyser la vulnérabilité des logiciels
- Intégrer les technologies de cloud et de virtualisation dans une architecture d'entreprise sécurisée
- Maîtriser les techniques cryptographiques, telles que la blockchain, les crypto-monnaies et le cryptage des appareils mobiles

Description sommaire

Développez des compétences avancées pour concevoir et créer des solutions sécurisées dans des environnements professionnels complexes. Votre instructeur expert vous fournira les connaissances techniques et les compétences nécessaires pour conceptualiser, concevoir, intégrer et mettre en œuvre des solutions sécurisées dans des environnements complexes pour soutenir une entreprise résiliente.

Contenu du plan de cours

Gestion des risques (19% de l'examen)

- Résumer les influences de l'entreprise et de l'industrie et les risques de sécurité associés
- Comparer et opposer les politiques et procédures de sécurité et de protection de la vie privée en fonction des exigences de l'organisation.
- A partir d'un scénario, mettre en œuvre des stratégies d'atténuation des risques et des contrôles
- Analyser les scénarios de mesure des risques pour sécuriser l'entreprise

Architecture de sécurité de l'entreprise (25 % de l'examen)

- Analyser un scénario et intégrer les composants, concepts et architectures de réseau et de sécurité pour répondre aux exigences de sécurité.
- Analyser un scénario pour intégrer les contrôles de sécurité pour les dispositifs hôtes afin de répondre aux exigences de sécurité
- Analyser un scénario pour intégrer les contrôles de sécurité pour les appareils mobiles et les appareils à petit facteur de forme afin de répondre aux exigences de sécurité
- Compte tenu des scénarios de vulnérabilité des logiciels, sélectionner les contrôles de sécurité appropriés.

Opérations de sécurité d'entreprise (20 % de l'examen)

- A partir d'un scénario, effectuer une évaluation de la sécurité en utilisant les méthodes appropriées
- Analyser un scénario ou un résultat et sélectionner l'outil approprié pour une évaluation de la sécurité
- Dans le cadre d'un scénario, mettre en œuvre des procédures de réponse aux incidents et de récupération.

Intégration technique de la sécurité de l'entreprise (23% de l'examen)

- Dans le cadre d'un scénario, intégrer les hôtes, le stockage, les réseaux et les applications dans une architecture d'entreprise sécurisée
-

Dans le cadre d'un scénario, intégrer les technologies du nuage et de la virtualisation dans une architecture d'entreprise sécurisée.

- Dans le cadre d'un scénario, intégrer les technologies avancées d'authentification et d'autorisation et les dépanner afin de soutenir les objectifs de sécurité de l'entreprise.
- Dans le cadre d'un scénario, mettre en œuvre des techniques cryptographiques
- Dans le cadre d'un scénario, sélectionner le contrôle approprié pour sécuriser les communications et les solutions de collaboration.

Recherche, développement et collaboration (13% de l'examen)

- Dans le cadre d'un scénario, appliquer des méthodes de recherche pour déterminer les tendances de l'industrie et leur impact sur l'entreprise.
- Dans le cadre d'un scénario, mettre en œuvre des activités de sécurité tout au long du cycle de vie de la technologie.
- Expliquer l'importance de l'interaction entre les différentes unités de l'entreprise pour atteindre les objectifs de sécurité.

Approche et méthode pédagogique

Approche avancée, stratégique et analytique, basée sur l’étude de scénarios complexes, la conception d’architectures sécurisées et la prise de décision en contexte d’entreprise à grande échelle.

Recommandations

- Les candidats doivent avoir dix ans d'expérience dans l'administration informatique, dont au moins cinq ans d'expérience pratique en matière de sécurité technique
- Bien qu'il ne s'agisse pas d'un prérequis, la formation CASP+ suit généralement la formation CompTIA Security+ ou contenu équivalent.

Certifications

Examen associé :

- CompTIA CASP+ (CAS 004) (ou version en vigueur)

- Certification obtenue : CompTIA Advanced Security Practitioner (CASP+)®

Lien avec le cours : Préparation avancée à l’examen CASP+, axée sur la conception et l’architecture de sécurité.

Notes légales