CompTIA Advanced Security Practitioner (CASP+)

Durée: 5 Jours **Réf de cours: GK2951** **Version: CAS-004**

Résumé:

CompTIA Advanced Security Practitioner (CASP+) est une certification de cybersécurité de niveau avancé destinée aux architectes de sécurité et aux ingénieurs de sécurité seniors chargés de diriger et d'améliorer la préparation à la cybersécurité d'une entreprise.
CASP+ est une certification qui couvre les compétences techniques en matière d'architecture de sécurité et d'ingénierie de sécurité senior dans des environnements traditionnels, cloud et hybrides, les compétences en matière de gouvernance, de risque et de conformité, l'évaluation de la préparation à la cybersécurité d'une entreprise et la direction d'équipes techniques pour mettre en œuvre des solutions de cybersécurité à l'échelle de l'entreprise.

Les candidats retenus auront les connaissances nécessaires pour : Architecturer, concevoir, intégrer et mettre en œuvre des solutions sécurisées dans des environnements complexes afin de soutenir une entreprise résiliente.Utiliser la surveillance, la détection, la réponse aux incidents et l'automatisation pour soutenir de manière proactive les opérations de sécurité en cours dans un environnement d'entreprise.Appliquer les pratiques de sécurité à l'infrastructure cloud, sur site, endpoint et mobile, tout en prenant en compte les technologies et techniques cryptographiquePrendre en compte l'impact des exigences en matière de gouvernance, de risque et de conformité dans l'ensemble de l'entreprise.

CASP+ est conforme aux normes ISO 17024 et approuvé par le DoD américain pour répondre aux exigences de la directive 8140/8570.01-M. Les organismes de réglementation et les gouvernements s'appuient sur l'accréditation ANSI, car elle garantit la confiance dans les résultats d'un programme accrédité. Plus de 2,3 millions d'examens CompTIA accrédités ISO/ANSI ont été délivrés depuis le 1er janvier 2011.

Public visé:

Architecte de sécurité Ingénieur sécurité senior Responsable SOC Analyste de sécurité

Objectifs pédagogiques:

- **À l'issue de la formation, les participants seront capables de :**
- **Créer une architecture de sécurité**
- Analyse élargie pour évaluer les exigences de sécurité dans les réseaux hybrides afin d'élaborer une architecture sécurisée zero trust à l'échelle de l'entreprise avec des solutions cloud et de virtaulisation avancées.
- **Gérer la gouvernance, risque et conformité**
- Extension de la couverture pour prendre en charge les techniques avancées permettant de prouver la mesure de la résilience globale de la cybersécurité d'une organisation et la conformité aux réglementations, telles que CMMC, PCI-DSS, SOX, HIPAA, GDPR, FISMA, NIST et CCPA.
- **Gérer les opérations de sécurité**
- Accent mis sur les nouvelles techniques de gestion avancée des menaces, de gestion des vulnérabilités, d'atténuation des risques, de tactique de réponse aux incidents et d'analyse criminalistique numérique.
- **Ingénierie de la sécurité et cryptographie**
- Analyse des configurations de cybersécurité avancées pour les contrôles de sécurité des endpoints, la mobilité d'entreprise, les environnements cloud/hybrides, les solutions PKI et cryptographiques à l'échelle de l'entreprise.

Pré-requis:

La participation à nos formations **Internetworking with TCP/IP** et **Switching in IP Networks** est fortement recommandée

Cours de préparation à la sécurité+ (Security+ Prep Course) est un plus.

Test et certification

Contenu:

- Leçon 1 : Réaliser des activités de gestion des risques
- Leçon 2 : Recapituler les stratégies de gouvernance et de conformité
- Leçon 3 : Mettre en oeuvre la continuité des activités et de la reprise après sinistre
- Leçon 4 : Identifier les services d'infrastructure
- Leçon 5 : Effectuer l'intégration des logiciels
- Leçon 6 : Expliquer la virtualisation, le cloud et les technologies émergentes
- Leçon 7 : Explorer les configurations sécurisées et le durcissement des systèmes
- Leçon 8 : Comprendre les considérations de sécurité de l'informatique en cloud et des plateformes spécialisées
- Leçon 9 : Mettre en œuvre la cryptographie
- Leçon 10 : Mettre en œuvre l'infrastructure à clé publique (PKI)
- Leçon 11 : Concevoir des endpoints sécurisés
- Leçon 12 : Résumer les concepts de l'IIoT et de l'IoT

Méthodes pédagogiques :

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.

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.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement