CompTIA CASP+

Objectifs

- 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.

Prérequis

- 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.

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.3