CompTIA CySA+

Objectifs

- Exploiter des données proactives issues des menaces et les exploiter afin de renforcer la sécurité des entreprises et de procéder à des opérations de gestion des vulnérabilités ;
- Mettre en œuvre des stratégies de sécurité pour gérer efficacement des infrastructures ;
- Décrire les bonnes pratiques relatives à l'assurance des produits logiciels et du matériel ;
- Utiliser des modèles de sécurité visant à réduire les risques organisationnels d'une entreprise ;
- Saisir l'importance d'une mise en place de Framework, de politiques de sécurité, de protocoles et de mesures de contrôle ;
- Analyser des données à des fins de surveillance continue et procéder à une nouvelle configuration sur des contrôles déjà en place pour accroître la sécurité ;
- Mettre en œuvre des procédures adaptées de réponse aux incidents ;
- Identifier des indicateurs de vulnérabilité possibles et recourir à des techniques de base d'investigation numérique ;
- Passer l'examen CS0-003 CompTIA CySA + et décrocher la certification.

Prérequis

- Avoir une expérience pratique de 4 ans minimum dans le domaine de la cybersécurité ou toute autre expérience annexe ;
- Savoir lire et comprendre l'anglais, le japonais, le portugais ou l'espagnol pour le passage de l'examen *CompTIA* CS0-003.

Programme

Introduction

- Vue d'ensemble du métier d'analyste en cybersécurité moderne.

Cours 1

- L'utilisation du renseignement sur les menaces.

Cours 2

- L'identification et la collecte de données de renseignement.

Cours 3

- La conception d'un programme de gestion des vulnérabilités.

Cours 4

- L'analyse des risques et des vulnérabilités.

Cours 5

- La cybersécurité dans le Cloud Computing.

Cours 6

- La sécurité des contrôles d'infrastructures et des services.

Cours 7

- La sécurité de la gestion des identités et des accès.

Cours 8

- L'assurance du développement logiciel et du matériel informatique.

Cours 9

- Les activités de sécurité et de monitoring.

Cours 10

- La mise en œuvre d'un plan de réponse aux incidents.

Cours 11

- L'analyse des indicateurs de corruption.

Cours 12

- Les analyses et techniques d'investigation numériques légales.

Cours 13

- L'isolement, l'éradication et la récupération des menaces.

Cours 14

- La gestion des risques et la réponse aux incidents.

Cours 15

- La politique de sécurité et la conformité.