mail: courriel@ya-consulting.com
contact: (225) 01 52 22 63 12

CompTIA CySA+ : prévention, détection et suppression des menaces de cybersécurité

Date et durée

Code formation : C-CYSA
Durée : 3 mois

Formation avec préparation à la certification

CompTIA CySA+

Description

Dans le monde de l'informatique, les attaquants sont capables de contourner les systèmes basés sur les signatures, comme les logiciels antivirus et les pare-feux. Par conséquent, une **analyse de la sécurité informatique** est de plus en plus importante pour les entreprises. CompTIA CySA + apporte une solution d'analyse comportementale des réseaux permettant ainsi de renforcer la capacité de sécurité générale grâce à l'identification et à la lutte contre les logiciels malveillants et les menaces persistantes avancées (APT), ce qui accroit **la vulnérabilité des menaces** sur une surface d'attaque étendue.
Les 15 cours de notre formation officielle sont élaborés pour répondre à la certification **CompTIA Cybersecurity Analyst (CySA)+**. Ils permettent aux participants d'acquérir les bases indispensables pour prévenir, détecter et supprimer des menaces de cybersécurité. Ils aident à comprendre les différentes méthodes efficaces pour diagnostiquer le réseau, les systèmes d'exploitation, les équipements et la sécurité d'une infrastructure. CySA + traite des plus **récentes techniques fondamentales de l'analyste en sécurité** et des futures pratiques professionnelles des analystes du renseignement sur les menaces, des analystes de la sécurité des applications, des analystes de la conformité, des responsables de la gestion des incidents et des chasseurs de menaces.
Grâce aux 5 domaines de compétences informatiques que vous avez abordés, vous serez préparé pour le **passage de l'examen CompTIA CS0-002.** Cet examen est un prérequis pour obtenir la certification CompTIA CySA +, qui prouve que vous disposez de réelles techniques de lutte contre les menaces à l'intérieur et à l'extérieur des centres d'opérations de sécurité (SOC).

Objectifs

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

- 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 frameworks, 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 ;
- être bien préparé pour le passage de l'examen CS0-002 CompTIA CySA +.

Points forts

15 cours pour acquérir ou valider des compétences en analyse de risques cybersécurité ; une formation qui traite des dernières technologies ; une préparation à la certification intermédiaire CompTIA CySA +.

Certification

La formation CompTIA CySA + vous prépare au passage de l'examen CS0-002 qui est nécessaire pour obtenir la **certification** CompTIA Cybersecurity Analyst. Vous pouvez passer cet examen dans notre centre Pearson VUE Oo2 Formations ou en ligne sur CompTIA.org.
L'examen CS0-002 permet de tester vos aptitudes en tant que professionnel de la cybersécurité en vue de garantir une défense proactive et une amélioration continue de la sécurité d'une entreprise. Il atteste que vous avez les bonnes connaissances et les bonnes compétences requises pour **mener à bien les tâches suivantes** :

- tirer parti des meilleures techniques de renseignement et de détection des menaces ;
- analyser et exploiter des données ;
- identifier et éliminer les menaces et les vulnérabilités ;
- recommander des solutions préventives contre les menaces existantes ;
- répondre aux incidents et en assurer le traitement.

Informations complémentaires :

- type d'examen : 85 questions à choix multiples ;
- durée : 2 h 45 ;
- livre ouvert : non ;
- langue : anglais et japonais ;
- attribution : 750 points basés sur une échelle de 900 points.

Modalités d'évaluation

Travaux Pratiques

Pré-requis

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

- avoir suivi notre formation CompTIA N + , notre formation CompTIA S + ou obtenir des connaissances similaires ;
- avoir une expérience pratique de 4 ans minimum dans le domaine de la cybersécurité ou toute autre expérience annexe (c*onseiller pour le passage de l'examen CompTIA CySA* + CS0-002).

Les formations ci-dessous sont recommandées.

CompTIA N+ : configuration, gestion et dépannage des réseaux
CompTIA S+ : les bases de la cybersécurité

Public

Cette formation s'adresse aux publics suivants :

- les analystes en sécurité informatique, les analystes en vulnérabilité ou les analystes du renseignement sur les menaces désireux de maîtriser la configuration et la bonne utilisation des outils de détection des menaces ;
- les professionnels de la cybersécurité qui souhaitent obtenir la certification CompTIA CySA +.

Cette formation s'adresse aux profils suivants

Ingénieur système

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.