Organisme de formation professionnelle continue
Numero agrément 91 30 03332 30
France : +33 (0)188 24 70 33 / 34
Site : www.oo2.fr
Mail : contact@oo2.fr

CompTIA CySA+ : détecter, prévenir et répondre aux incidents

Date et durée

Code formation : C-CYSA
Durée : 5 jours
Nombre d'heures : 35 heures

Formation avec certification

CompTIA Cybersecurity Analyst (CySA+)

Description

CompTIA CySA+ est une certification en sécurité informatique axée sur l'analyse et la réponse aux incidents. Reconnue dans le monde entier, elle renforce votre crédibilité et votre valeur sur le marché de l'emploi. En effet, si vous êtes un **professionnel certifié CompTIA CySA+**, vous serez mieux préparé à identifier et à atténuer les menaces de sécurité. Ce qui rend votre rôle essentiel pour les entreprises qui souhaitent protéger efficacement leurs données confidentielles. Par ailleurs, cette certification ouvre la voie à des **opportunités de carrière plus larges et souvent mieux rémunérées**, en raison de la demande croissante d'experts en cybersécurité.
Notre **formation CompTIA CySA+ de 5 jours** vous donnera les compétences et les connaissances nécessaires pour détecter, prévenir et répondre aux incidents de cybersécurité. Vous aborderez en détail toutes les activités liées à la sécurité des opérations, la gestion des vulnérabilités, la réponse et la gestion des incidents, ainsi que les rapports et leur communication. Nos cours CySA + couvrent **les dernières techniques et les meilleures pratiques en matière de sécurité** pour les analystes des renseignements sur les menaces, les analystes de la sécurité de l'information et plus encore.
Grâce aux 4 domaines de compétences que vous aborderez tout au long de ce programme, vous serez **préparer pour l'examen CompTIA CS0-003** inclus dans notre offre. Cet examen est un prérequis pour obtenir la certification CompTIA CySA+ (*en savoir + dans l'onglet certification*).

Objectifs

À l'issue de cette formation, vous atteindrez les objectifs de compétences suivants :

- détecter et analyser des indicateurs de compromission (IOC) ;
- comprendre les principes de la détection et du renseignement sur les menaces ;
- utiliser des outils et des méthodes adaptés pour gérer, hiérarchiser et répondre à des attaques et des vulnérabilités ;
- exécuter une procédure de réponse aux incidents ;
- comprendre la notion de rapport et de communication liée aux activités de gestion des vulnérabilités et de réponse aux incidents.

Points forts

Des cours pour acquérir ou valider des compétences en analyse de risques cybersécurité ; une formation qui traite des dernières technologies et le passage de l'examen de certification CompTIA CySA+ compris dans l'offre.

Certification

Ce programme de formation CompTIA vous permet de vous présenter à l'examen de **certification CompTIA CySA+ (CS0-003)** disponible en ligne. Vous recevrez en fin de formation un bon d'examen (voucher) pour programmer celui-ci sur le site CompTIA.org.

Détail de l'examen CompTIA CS0-003 :

L'examen prouve que vous possédez les connaissances et les compétences requises pour détecter et analyser les indicateurs d'activités malveillantes, comprendre le renseignement sur les menaces et la gestion des menaces, répondre aux attaques et aux vulnérabilités, réagir aux incidents, signaler et communiquer sur les activités liées à ces menaces.

- Type d'examen : 85 questions à choix multiples et basés sur la performanc.
- Durée : 2 h 45.
- Livre ouvert : non.
- Langues : anglais, japonais, portugais ou espagnol.
- Attribution : 750 points basés sur une échelle de 900 points.

A savoir : *la certification CompTIA CySA+ est valable 3 ans à partir de la date de votre examen. Elle peut être renouvelée en suivant des activités et des formations en rapport avec le contenu de votre certification.*

Modalités d'évaluation

Quiz / QCM
Travaux Pratiques

Pré-requis

Suivre la formation CompTIA CySA+ nécessite les prérequis suivants :

- avoir une expérience pratique en cybersécurité comme analyste de réponse aux incidents ou analyste d'un centre d'opérations de sécurité (SOC), ou toute autre expérience similaire ;
- savoir lire et comprendre l'anglais, le japonais, le portugais ou l'espagnol pour le passage de l'examen *CompTIA* CS0-003.

Formations recommandées :

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
Analyste cybersécurité

Programme

1. Les opérations de sécurité

- Comprendre les concepts d'architecture des systèmes et des réseaux dans les opérations de sécurité.
- Analyser des indicateurs d'activités potentiellement malveillantes à partir d'un scénario liées au réseau, à l'hôte, aux applications, aux attaques d'ingénierie sociale et aux Urls cachées.
- Utiliser des outils ou des techniques appropriés pour déterminer des activités malveillantes à partir d'un scénario défini.
- Comparer et opposer les concepts de la threat intelligence et du threat hunting.
- Comprendre l'importance d'améliorer des processus dans les opérations de sécurité.

2. La gestion des vulnérabilités

- Mettre en œuvre des méthodes et des concepts d'analyse de vulnérabilité à partir d'un scénario.
- Analyser des résultats issus d'outils d'évaluation de vulnérabilité à partir d'un scénario.
- Analyser des données pour classer des vulnérabilités par ordre de priorité à partir d'un scénario.
- Recommander des procédures de contrôle pour atténuer des attaques et des vulnérabilités au niveau des logiciels à partir d'un scénario.
- Comprendre les concepts relatifs à la réponse, au suivi et à la gestion des vulnérabilités.

3. La réponse et la gestion des incidents

- Comprendre les concepts liés aux frameworks de cybersécurité :
    - le principe de kill chain ;
    - le modèle diamant d'analyse d'intrusion ;
    - le framework MITRE ATT&CK® ;
    - le cadre OSSTMM (Open Source Security Testing Methodology Manual) ;
    - le guide de test de l'OWASP (Open Web Application Security Project).
- Exécuter des activités de réponse aux incidents à partir d'un scénario :
    - la détection et l'analyse ;
    - le confinement, l'éradication et la récupération.
- Comprendre les phases de préparation et d'activité post-incidents du cycle de vie de la gestion des incidents.

4. Les rapports et la communication

- Comprendre l'importance des rapports et les processus de communication :
    - les rapports sur la gestion des vulnérabilités ;
    - les rapports de conformité ;
    - les plans d'action ;
    - les obstacles à la remédiation ;
    - les métriques et les indicateurs clés de performance (KPI) ;
    - l'identification des parties prenantes et leur mode de communication ;
    - la déclaration et l'escalade des incidents ;
    - le rapport de réponse aux incidents ;
    - les méthodes de communication ;
    - l'analyse des causes profondes ;
    - les enseignements tirés de l'expérience.

CompTIA® est une marque déposée de CompTIA Inc.

Guide des certifications CompTIA
Télécharger la brochure