COMPTIA - CSA+

Durée: 5 jours
Public cible: Professionnel TI

À qui s'adresse cette formation ?

Cette formation est conçue pour les analystes en sécurité informatique, les analystes de vulnérabilités ou les analystes de renseignement sur les menaces. L'examen certifiera que le candidat ayant réussi possède les connaissances et compétences requises pour configurer et utiliser des outils de détection des menaces, effectuer une analyse de données et interpréter les résultats afin d'identifier les vulnérabilités, les menaces et les risques pour une organisation, dans le but ultime de sécuriser et de protéger les applications et systèmes au sein d'une organisation.

Objectifs de la formation

- Configurer et utiliser des outils de détection des menaces
- Analyser des données et interpréter les résultats pour identifier des vulnérabilités, des menaces et des risques
- Gérer les incidents cybernétiques et appliquer des processus de réponse appropriés
- Évaluer des architectures de sécurité et recommander des mesures compensatoires adaptées

Description sommaire

CompTIA Cybersecurity Analyst (CSA+) est une certification informatique professionnelle internationale et indépendante des fournisseurs qui applique l'analyse comportementale pour améliorer l'état général de la sécurité informatique. Elle valide les connaissances et compétences requises pour configurer et utiliser des outils de détection des menaces, effectuer une analyse de données et interpréter les résultats afin d'identifier les vulnérabilités, les menaces et les risques pour une organisation, dans le but ultime de sécuriser et de protéger les applications et systèmes au sein d'une organisation. Les attaquants ayant appris à contourner les solutions traditionnelles basées sur les signatures, comme les pare-feu, une approche basée sur l'analyse au sein de l'industrie de la sécurité informatique est devenue extrêmement importante et essentielle pour la plupart des organisations. Les compétences en analyse comportementale couvertes par la certification CompTIA

CSA+ permettent d'identifier et de combattre les logiciels malveillants et les menaces persistantes avancées (APT), offrant une meilleure visibilité des menaces sur une vaste surface d'attaque en se concentrant sur le comportement du réseau, y compris le réseau interne d'une organisation.

Contenu du plan de cours

Module 1 - Gestion des menace

- Étant donné un scénario, appliquer des techniques de reconnaissance environnementale à l'aide des outils et processus appropriés
- Étant donné un scénario, analyser les résultats d'une reconnaissance réseau
- Étant donné une menace basée sur le réseau, mettre en œuvre ou recommander la réponse et la contre-mesure appropriées
- Expliquer l'objectif des pratiques utilisées pour sécuriser un environnement d'entreprise

Module 2 - Gestion des vulnérabilités

Étant donné un scénario, mettre en œuvre un processus de gestion des vulnérabilités en matière de sécurité de l'information

Étant donné un scénario, analyser les résultats d'une analyse de vulnérabilités

Comparer et opposer les vulnérabilités courantes trouvées dans les cibles suivantes au sein d'une organisation

Module 3 - Réponse aux incidents cybernétiques

Étant donné un scénario, distinguer les données ou comportements de menace afin de déterminer l'impact d'un incident

Étant donné un scénario, préparer une trousse à outils et utiliser les outils d'investigation numérique appropriés lors d'une enquête

Expliquer l'importance de la communication pendant le processus de réponse aux incidents

Étant donné un scénario, analyser les symptômes courants afin de sélectionner la meilleure ligne de conduite pour appuyer la réponse aux incidents

Résumer le processus de récupération suite à un incident et de réponse post-incident

Module 4 - Architecture de sécurité et ensembles d'outils

Expliquer la relation entre les cadres de référence, les politiques courantes, les contrôles et les procédures

Étant donné un scénario, utiliser les données pour recommander des mesures correctives liées à la gestion des identités et des accès

Étant donné un scénario, examiner l'architecture de sécurité et formuler des recommandations pour mettre en œuvre des contrôles compensatoires

Étant donné un scénario, appliquer les meilleures pratiques de sécurité des applications dans le cadre du cycle de vie du développement logiciel (SDLC)

Comparer et opposer l'objectif général et les raisons d'utiliser divers outils et technologies de cybersécurité

Approche et méthode pédagogique

Approche pratique et structurée combinant théorie ciblée et ateliers guidés.

Recommandations

- Avoir la certification CompTIA Network+ ou contenu équivalent
- Avoir la certification CompTIA Security+ ou contenu équivalent
- 3 à 4 années d'expérience pratique en sécurité informatique ou dans un domaine connexe

Certifications

CompTIA Cybersecurity Analyst (CSA+) — Examen CS0-001

Notes légales

Cette formation est offerte en français ; le matériel didactique est en anglais.