CompTIA Cybersecurity Analyst CYSA+

Durée: 5 jours
Public cible: Professionnel TI

À qui s'adresse cette formation ?

- Analyste de la sécurité informatique
- Analyste du centre des opérations de sécurité
- Analyste de la vulnérabilité
- Spécialiste de la cybersécurité
- Analyste du renseignement sur les menaces
- Ingénieur en sécurité, analyste en cybersécurité
- Architecte de la sécurité

Objectifs de la formation

- Expliquer l'importance des données et des renseignements sur les menaces
- Utiliser les informations sur les menaces pour soutenir la sécurité de l'organisation
- Effectuer des activités de gestion des vulnérabilités
- Analyser la sortie de outils communs d'évaluation de la vulnérabilité
- Expliquer les menaces et vulnérabilités associées avec une technologie spécialisée
- Expliquer les menaces et les vulnérabilités associées à l'exploitation dans le cloud
- Mettre en œuvre des contrôles pour atténuer attaques et vulnérabilités logicielles
- Appliquer des solutions de sécurité pour la gestion des infrastructures
- Expliquer les meilleures pratiques de Software Assurance
- Expliquer les meilleures pratiques en matière d'assurance matérielle
- Analyser les données dans le cadre des activités de surveillance de la sécurité
- Implémenter les modifications de configuration aux contrôles existants pour améliorer la sécurité
- Expliquer l'importance de la chasse proactive aux menaces
- Comparer et contraster les concepts et technologies d'automatisation
- Expliquer l'importance du processus de réponse aux incidents

- Appliquer la procédure de réponse aux incidents appropriée
- Analyser les indicateurs potentiels de compromis
- Utiliser des techniques de criminalistique numérique de base
- Comprendre l'importance de la confidentialité et de la protection des données
- Appliquer les concepts de sécurité dans soutien à l'atténuation des risques organisationnels
- Expliquer l'importance des cadres, politiques, procédures et contrôles

Description sommaire

CySA+ se concentre sur la capacité non seulement à capturer, surveiller et répondre de manière proactive aux résultats du trafic réseau, mais met également l'accent sur la sécurité des logiciels et des applications, l'automatisation, la recherche de menaces et la conformité aux réglementations informatiques, ce qui affecte le travail quotidien des analystes de la sécurité. CySA+ couvre les compétences les plus récentes des analystes de la sécurité et les compétences professionnelles utilisées par les analystes de l'intelligence de la menace, les analystes de la sécurité des applications, les analystes de la conformité, les intervenants et gestionnaires d'incidents et les chasseurs de menaces, apportant de nouvelles techniques pour combattre les menaces à l'intérieur et à l'extérieur du Centre des opérations de sécurité (SOC).

Contenu du plan de cours

- Explaining the Importance of Security Controls and Security Intelligence
- Utilizing Threat Data and Intelligence
- Analyzing Security Monitoring Data
- Collecting and Querying Security Monitoring Data
- Utilizing Digital Forensics and Indicator Analysis Techniques
- Applying Incident Response Procedures
- Applying Risk Mitigation and Security Frameworks
- Performing Vulnerability Management
- Applying Security Solutions for Infrastructure Management
-

Understanding Data Privacy and Protection

- Applying Security Solutions for Software Assurance
- Applying Security Solutions for Cloud and Automation

Approche et méthode pédagogique

Approche analytique et orientée données, mettant l’accent sur l’analyse comportementale, la chasse aux menaces, l’automatisation et la réponse aux incidents à partir de cas concrets de cybersécurité.

Recommandations

- Network+ ou contenu équivalent, Security+ ou contenu équivalent.
- Minimum de 4 ans d'expérience pratique en sécurité de l'information ou expérience connexe.

Certifications

Examen associé : CompTIA CySA+ (CS0 003) (ou version en vigueur) Certification obtenue : CompTIA Cybersecurity Analyst (CySA+)® Lien avec le cours : Prépare à l’examen CySA+, avec un accent sur l’analyse, la détection et la réponse aux menaces.

Notes légales