+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 19/06/2024

S'inscrire

Formation Comptia CySA+©

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

5 jours (35 heures)

Présentation

Notre formation CySA+© vous préparera à la célèbre certification de Comptia© destinée aux analystes en cybersécurité. Ce titre mondialement reconnu renforcera grandement votre employabilité.

Notre préparation à la certification se veut complète en regroupant l'essentiel du contenu de l'examen. Vous débuterez par un rappel dans le domaine de la gestion des menaces, celui-ci vous permettra de détecter efficacement les intrusions et sécuriser les points d'accès.

En parlant de menace, vous apprendrez les bonnes pratiques de configuration pour les scans de vulnérabilités, vous saurez de même, analyser ses rapports. Notre formation contient une partie sur les réponses aux incidents : comment catégoriser des menaces, l'utilisation d'outils de forensique ou encore les méthodes de communication.

Vous en saurez plus sur les politiques de conformité, les pratiques de codage ou encore les outils de sécurité informatique. Enfin, nous vous préparerons au passage de la certification grâce à des études de cas.

Objectifs

- Savoir utiliser les techniques de renseignement et de détection des menaces
- Analyser et interpréter des données
- Identifier et corriger des vulnérabilités
- Savoir proposer des mesures préventives
- Introduire un processus efficace de réponse aux incidents et de reprise après incident

Public visé

- Analyste cybersécurité
- Analyste du renseignement sur les menaces
- Ingénieur cybersécurité
- Analyste de la sécurité des applications
- Analyste responsable de la conformité
- Threat hunters

Pré-requis

- Une expérience de 3 à 4 ans en cybersécurité est recommandée
- Maîtrise de l'anglais technique

Note : Ambient IT n’est pas propriétaire de Comptia Certifications©, cette certification appartient à Comptia, Inc.

PROGRAMME DE NOTRE FORMATION CYSA©

GESTION DES MENACES

- Techniques de reconnaissance
- Outils de détection des menaces (NMAP, NETSTAT)
- Analyse des résultats de reconnaissance réseau
- Réponse et contre-mesures aux menaces réseau
- Sécurité des points d'accès et des politiques de groupe

GESTION DES VULNÉRABILITÉS

- Identification des exigences réglementaires et politiques
- Établissement de la fréquence de scan
- Configuration des outils pour les scans de vulnérabilités
- Exécution et analyse des rapports de scan
- Techniques de remédiation et suivi continu

RÉPONSE AUX INCIDENTS

- Classification des menaces (Zero day, APT)
- Préparation et utilisation des kits de forensic
- Importance de la communication pendant une réponse aux incidents
- Techniques de confinement et d'éradication
- Validation des correctifs et actions correctives

ARCHITECTURE DE SÉCURITÉ ET ENSEMBLES D'OUTILS

- Cadres de conformité et politiques de sécurité (NIST, ISO)
- Analyse des données de sécurité (tendances, historique)
- Meilleures pratiques pendant le cycle de vie du développement logiciel (SDLC)
- Pratiques de codage sécurisé (OWASP, SANS)
- Comparaison des outils de cybersécurité (IPS, SIEM, IDS)

CAS PRATIQUES ET EXAMENS

- Mise en œuvre des techniques de reconnaissance en situation réelle
- Simulation de scan de vulnérabilités et analyse de résultats
- Scénarios de réponse aux incidents et gestion en temps réel
- Revue des architectures de sécurité et recommandations de contrôles compensatoires
- Examen blanc et révisions finales pour la certification

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.