+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 CASP+©

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

5 jours (35 heures)

Présentation

Notre formation Comptia CASP+© (Advanced Security Practitioner) prouvera votre grande maîtrise des principes de sécuité informatique, en particulier en détection des menaces et en réponse aux incidents.

Chez Ambient IT, vous bénéficierez d'un programme complet pour vous préparer à l'examen. Nous entamerons cette formation par vous enseigner les concepts essentiels garantissant la protection de votre infrastructure tels la résilience, l'allocation distribuée ou encore la virtualisation.

Dans le même principe, nous vous présenterons les outils indispensables de la sécurité informatique comme le SIEM ou l'IDS/IPS. Nous vous rappellerons les technologies à l'œuvre pour protéger vos systèmes que ce soit la cryptographie ou l'authentification.

Nous ne manquerons pas de vous enseigner les différentes normes qui régulent ce domaine et l'application de ces lois sans votre organisation et vis à vis de vos fournisseurs. Enfin, notre formation CASP+© évoquera des domaines comme l'analyse d'impact et la forensic.

Objectifs

- Structurer, concevoir, intégrer et mettre en œuvre des solutions sécurisées dans des environnements complexes pour assurer le bon fonctionnement d'une entreprise résiliente
- Utiliser la surveillance, la détection, la réponse aux incidents et l'automatisation pour gérer de manière proactive les opérations de sécurité en cours dans un environnement professionnel
- Appliquer les pratiques de sécurité dans le cloud, sur site, au point de terminaison et aux appareils mobiles, tout en tenant compte des technologies cryptographiques
- Tenir compte des enjeux de la gestion des risques, de la gouvernance et de la conformité en entreprise

Public visé

- Administrateur système
- Ingénieur sécurité
- Analyste Cybersécurité
- Administrateur réseau

Pré-requis

- Une expérience minimum de 10 ans en informatique et 5 ans dans le domaine de la cybersécurité
- 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 CASP+

ARCHITECTURE DE SÉCURITÉ

- Analyse des exigences de sécurité
- Objectifs pour une architecture de réseau sécurisée
- Intégration sécurisée des applications
- Conception de l'infrastructure sécurisée
- Évaluation des modèles de déploiement cloud

RÉSILIENCE ET SCALABILITÉ

- Haute disponibilité
- Orchestration des actions
- Allocation distribuée et redondance
- Clustering
- Réplication
- Auto-scaling et automatisation

PERFORMANCE ET VIRTUALISATION

- Conteneurisation et virtualisation
- Réseau de diffusion de contenu
- Mise en cache
- Modèles de stockage sécurisés
- Standards de codage sécurisé

GESTION DES MENACES

- Types de renseignements
  - Tactiques
  - Stratégiques,
  - Opérationnels
- Types d'acteurs
  - APT
  - Menace interne
  - Hacktivistes
- Méthodes de collecte de renseignements
- Cadres de gestion des menaces (MITRE ATT&CK, Cyber Kill Chain)

ANALYSE DES INDICATEURS DE COMPROMISSION

- Capture de paquets (PCAP)
- Logs de réseau
- Notifications et alertes
  - SIEM
  - DLP
  - IDS/IPS
- Activités inhabituelles
- Règles de firewall

VULNÉRABILITÉS

- Scans de vulnérabilité (credentialed vs non-credentialed)
- Évaluer et analyser les vulnérabilités
- Techniques d'atténuation proactive
- Réponse aux incidents

CONTRÔLES DE SÉCURITÉ

- Contrôles d'application et de mot de passe
- Configuration de MFA et accès basé sur les jetons
- Repositories de correctifs et de firmware
- Gestion des certificats et chiffrement complet des appareils
- Techniques de durcissement (NX bit, ASLR)

TECHNOLOGIES ET SECTEURS OPÉRATIONNELS

- IoT et systèmes embarqués
- SCADA et systèmes industriels
- Protocoles spécifiques (CAN bus, Modbus)
- Méthodes d'automatisation et d'orchestration

PKI ET CRYPTOGRAPHIE

- Hiérarchie PKI et types de certificats
- Usages courants de PKI (services web, email, signature de code)
- Protocoles cryptographiques
  - SSL/TLS
  - IPSec
  - SSH
- Algorithmes symétriques et asymétriques
- Problèmes de configuration

GESTION DES RISQUES

- Évaluation des risques (facteur de probabilité, impact)
- Techniques de gestion des risques (transfert, acceptation, évitement)
- Cycle de vie de la gestion des risques
- Suivi des risques et indicateurs de performance clés

GESTION DES FOURNISSEURS

- Modèle de responsabilité partagée
- Viabilité des fournisseurs (risque financier, fusion/acquisition)
- Exigences clients (légales, gestion du changement)
- Considérations géographiques et visibilité de la chaîne d'approvisionnement
- Dépendances tierces (code, matériel, modules)

CADRES DE CONFORMITÉ

- Intégration des diverses industries
- Cadres réglementaires autour des données
  - Souveraineté
  - Classification
  - Rétention
- Attestations de conformité tierces
- Régulations et normes
  - PCI
  - DSS
  - RGPD
  - ISO

ANALYSE D'IMPACT

- Objectif du point de reprise (RPO)
- Objectif de temps de reprise (RTO)
- Analyse de la mission essentielle
- Évaluation d'impact sur la vie privée
- Plan de reprise après sinistre (DRP)
- Plan de continuité des opérations (BCP)

- Les types de sites de reprise
  - Cold
  - Warm
  - Hot
- Plans d'intervention en cas d'incident

FORENSIC

- L'importance de la forensique
- Processus de réponse
  - Préparation
  - Détection
  - Analyse
- Collecte et préservation des preuves
- Les outils d'analyse forensique (ExifTool, Nmap, Wireshark)
- Techniques de préservation de l'intégrité

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.