POE Consultant Cybersécurité

57 j (399 heures) Ref : POE-CYB

Public

BAC +3+5 issus de filières Ingénieurs ou filières Universitaires scientifiques
BAC+3 autodidacte, curieux et naturellement attirés par les métiers du Développement
Salarié en reconversion

Pré-requis

Maîtrise du rédactionnel et capacité à analyser et à restituer de l'information
Réussite de nos tests de recrutement

Moyens pédagogiques

Formation réalisée en présentiel ou à distance selon la formule retenue et résolument opérationnelle
Présentation des concepts, discussion technique, démonstrations, exercices et TP
Un poste de travail par stagiaire, vidéoprojecteur, support de cours

Modalités de suivi et d'évaluation

Feuille de présence émargée par demi-journée par les stagiaires et le formateur
Exercices de mise en pratique ou quiz de connaissances tout au long de la formation permettant de mesurer la progression des stagiaires
Questionnaire d'évaluation de la satisfaction en fin de stage
Auto-évaluation des acquis de la formation par les stagiaires
Attestation de fin de formation

Cette formation vise l'acquisition d'une compétence pointue dans le domaine de la sécurité de l'information, et répondant aux bonnes pratiques et recommandations de l'Agence Nationale de la Sécurité des Systèmes d'information (ANSSI). Ce parcours de formation ambitionne de former des experts maîtrisant les standards et référentiels liés à la norme ISO 27001, ainsi que l'outillage et les méthodes nécessaires (EBIOS, conduite d'audits, etc.) nécessaires à une intégration rapide dans une équipe de sécurité ou une direction SI. Cette formation intègre aussi toute une partie SMSI (Système de management de la sécurité de l'information) pour permettre aux futurs consultants de mieux communiquer avec les métiers de la production et les fonctions supports de l'entreprise.

Objectifs

Développer le savoir, le savoir-faire et le savoir-être nécessairement requis pour assumer des fonctions de consultant en Cybersécurité

Gérer des projets en environnement complexe

Analyser les menaces et les risques SI ainsi que les impacts

Tracer des plans de traitement adaptés

Rédiger des spécifications de fonctions de sécurité

Analyser, exprimer, synthétiser de manière rigoureuse

Mener des réunions
Gérer les intéractions avec les responsables Qualité
Mettre en oeuvre le SMSI
Maitriser le travail en équipe en mode Agile
Maitriser la méthode EBIOS

Programme détaillé

TEAM BOOSTER (1 JOUR)

Créer une cohésion de groupe
Travailler son savoir-être en équipe
Se connaître : ses points forts et ses axes de progrès
Savoir se présenter
Connaître les autres et s'enrichir de la diversité : profils de personnalité, cursus de formation, expérience
Assimiler la puissance de la notion d'intelligence collective

PRESENTATION DE LA SECURITE DES SI (2 JOURS)

Etat de l'art
Tendances de la sécurité
Cyber Criminalité
Intelligence économique

CADRES REGLEMENTAIRES, LEGAUX DE LA SECURITE DES SI (3 JOURS)

Rappel des cadres légaux règlementaires (LPM, Lois françaises (sécurité, numérique, données personnelles, obligations des FAI)
Le problème de l'extra-territorialité
Règlementations (Bâle II, III, PCI DSS, Sox, cobit, Itil)
Test de Contrôle

MISE EN œUVRE DU SMSI (SYSTEME DE MANAGEMENT DE LA SECURITE DE L'INFORMATION) (8 JOURS)

Les normes de la sécurité (ISO/CEI 2700x)
Les différents domaines adressés
Formation (SMSI) : ISO/CEI27002/27001
Présentation (Analyse de risques) : ISO/CEI 27005 + ISO 31000 + ISO 21827
Méthodes d'analyse de risques : NIST, EFQM
Tests de contrôle (étude de cas)
Rédaction de PSSI

ANALYSE DE RISQUE (2 JOURS)

ISO 27005

ISO 3100

Analyse de risques numériques EBIOS RM 2018

MISE EN PRATIQUE EBIOS RM (7 JOURS)

Mettre en place à travers un cahier des charges l’ensemble des méthodes et technologies vues lors de l’ensemble de la formation

Analyse d’impact sur la vie privée (PIA)

Comparaison et corrélation PIA-EBIOS RM

ITIL (2 JOURS)

Terminologie et les concepts d'ITIL®

Connaître la chaîne de valeur de la gestion des services IT

Comprendre la valeur ajoutée d'ITIL®

VULNERABILITES ET MENACES (5 JOURS)

Impacts et type de menace

Mesure de sécurité, PTR

Veille technologique, CERT-FR

CVSS / CPE"

Cyberwolf / MITRE &TTACK

Hunting / MISP

OUTILS DE SURVEILLANCE DU SI (4 JOURS)

PREUDE/ Logpoint/ Prelude/ Splunk/ Elasticsurch (Rapports)

Détection de vulnérabilités d’application : App Scan, AVDS, Qualys

SOC (Security Opération Center)

Sondes IDS / IPS

Test de Contrôle"

LOG et Collecteur de log

RSYSLOG

Format de log (normes utilisées par les éditeurs et les OS : CEF / SYSLOG / JSON)

REFERENTIEL GENERAL DE SECURITE (3 JOURS)

Présentation de la démarche RGS ANSSI, des règles, des outils, référentiel PASSI / PRIS / PDIS / PACS

Les étapes : découverte, classification des données, anonymisation.

Protection des données structurées : Guardium (Contrôle de conformité, firewalking, traçabilité)"

LPM / homologation / SIIV / I901 IG1300

AUDITS ET CONTROLES (5 JOURS)

Les étapes : conduite d'entretiens, analyses, rédaction, sensibilisation, implantation, contrôles (Tableaux de Bord)

Plan de sensibilisation, entretiens

EXPLOITATION SYSTEME (5 JOURS)

Introduction Linux / Windows

Base du Shell

Commandes système

Gestion des logs et des services Linux-Windows / Observateur Evènement windows

Contrôle d'intégrité

IPTable

Registre / Powershell /Active Directory

Outils de contrôle d'intégrité.

Développement script / python (base)

FONCTIONS RELATIVES A LA VIE PRIVEE (1 JOUR)

De nouvelles fonctions (Règlement européen (GPDR & DPO), Le responsable des traitements)

Procédures de dépôt de plainte en France

Les organismes officiels (CNIL, ANSSI, ENISA, OSINT, NATO, Gendarmerie)

Test de Contrôle

GESTION DE REPONSES AUX INCIDENTS (1 JOUR)

SIRP / SOAR / CTI /

CONTINUITE ET REPRISE D'ACTIVITE (1JOUR)

Norme ISO/CEI 22301

PCA/PSI/PRA : Définition, implantation, mise en œuvre, contrôles

Gestion des incidents, CSIRT, préservation des preuves (FORENSICS)

Tests de contrôle

SECURITE SI EMBARQUE & INDUSTRIEL (2 JOURS)

Contexte cyber industriel, enjeux de sureté de fonctionnement (AMDEC, HAZOP)

Maintenance et achat Système d'information Industriel

Approche globale et structuré

Best Practices

Veille cyber sur internet

HARDENING (2 JOURS)

Méthode de Hardening : Hardening logique, Physique, Cots, Configuration firewall, Matrice flux

Recommandation CIS NIST : Retranscription, Lecture

CODAGE (1 JOUR)

Règles de codage de sécurité (SEI CERT Coding Standards - Confluence -SONARCUBE)

CHIFFREMENT (1 JOUR)

Crypto - SSH - Telnet - SFTP - FTPS - Notion de hachage

Certificats

Chiffrement synchrone et asynchrone.

PKI

SECURITE OPERATIONNELLE (1 JOUR)

Pentests avec démonstration : ensemble des processus opérationnels pour évaluer au quotidien la sécurité afin réduire la surface d'exposition du système d'information aux risques. SECOPS

Simulation de crise cyber : Scénario de crise opérationnelle ANSSI