NIVEAU 7 - BAC+5

Expert(e) en sécurité digitale

Préparation au titre professionnel :
« Expert(e) en sécurité digitale"
Reconnu par l'Etat NIVEAU 7 (NIVEAU BAC +5)
Inscrit au RNCP (arrêté du 23/02/2017, J.O du 03/03/2017)
Code RNCP: RNCP36399
Code diplôme : 16X32633

En partenariat avec ESD Expert(e) en Sécurité Digitale et ASTON L'école informatique

Objectifs de formation

Concevoir un plan stratégique de sécurité pour un système cible,

Structurer une solution technique et organisationnelle répondant aux besoins de sécurité du système cible,

Conduire un audit de sécurité des systèmes d'information,

Maintenir en condition opérationnelle de la sécurité de l'information,

Accompagner la mise en œuvre de la politique de sécurité d'un système cible.

Public et prérequis

- Titulaire du titre : « Administrateur Système et Réseau » (ENI)
- Bac +2/+3 en informatique avec expérience
- Bac +4/+5 en informatique

Durée de la formation

En alternance :

- Formation en centre : 525 heures
- Sur un contrat de 18 à 24 mois

Modalités et délais d'accès

Alternance (contrat de professionnalisation ou d'apprentissage) : Rentrées tout au long de l'année.

Il vous faudra assister à
une réunion d'informations qui sera suivie d'un entretien avec le service relations Ecole / Entreprises ainsi que des tests de logique et de positionnement.

Tarifs

Les tarifs dépendent de la modalité d'accès.
N'hésitez pas à nous consulter

Contact

ecole@eni-ecole.fr

Moyens pédagogiques - techniques - d'encadrement

Equipements pédagogiques :

- Un poste de travail par stagiaire
- Un poste téléphonique à la disposition des stagiaires
- Un vidéoprojecteur fixe ou un tableau blanc interactif installé dans chaque salle de formation
- Une photocopieuse/imprimante en libre accès
- Un accès internet sur chaque poste de travail
- Un serveur et un commutateur Ethernet Gigabit dans chaque salle
- Dix routeurs Cisco

Moyens pédagogiques :

- Travaux dirigés après chaque phase de cours : explications et démonstrations par le formateur et exécutés ensuite par les stagiaires.
- Travaux pratiques pour que le stagiaire apprenne à appliquer seul ce qu'il a appris et cherche par lui-même.
- Mises en situation professionnelle avec des cas spécifiques « entreprise ».
- Création de plateaux techniques qui recréent les conditions d'activités réelles des entreprises.
- Etudes de cas où le stagiaire doit résoudre une problématique technique ou managériale.
- Exposés oraux où le stagiaire doit préparer une présentation sur un thème technique donné.

Supports pédagogiques :

- Supports ENI Editions/internes pour chaque cours
- Un accès la Bibliothèque Numérique des Editions
- Un accès aux agréments techniques des éditeurs (Microsoft IT Academy et Microsoft Imagine Premium- Cisco Academy)
- Un accès aux revues informatiques
- Un accès au Programme Microsoft Imagine Premium et VMware Academic Program (licences logiciels Microsoft et VMware)
- Un accès à la plateforme 7Speaking (plateforme d'autoformation et programme individualisé en anglais)
- Systèmes d'exploitation Microsoft, GNU/Linux et Cisco IOS
- Logiciels bureautiques (Word – Excel - Access, Visio, Project, Open Office, Office 365…)
- Outils de développement (Visual Studio, Oracle, Eclipse, Struts, Hibernate, Tomcat, Java…)
- Systèmes de gestion de bases de données relationnelles (Oracle, SQL* Server…)

Suivi et évaluation :

Les blocs de compétences constituant le titre « Expert(e) sécurité digitale » sont les suivants**:**

- Concevoir un plan stratégique de sécurité pour un système cible
- Structurer une solution technique et organisationnelle répondant aux besoins de sécurité du système cible
- Conduire un audit de sécurité des systèmes d'information
- Maintenir en condition opérationnelle la sécurité de l'information
- Accompagner la mise en œuvre de la politique de sécurité d'un système cible

Les évaluations en cours de formation mesurent compétence par compétence le degré de maîtrise de la situation professionnelle concernée: devoirs écrits, mises en situation professionnelle, QCM, études de cas, exposés oraux

Rédaction d'un mémoire portant sur l'analyse des risques

L'obtention de la mention Acquis sur l'ensemble des blocs de compétences conditionnera l'obtention du titre,

Débouchés et métiers

L'Expert(e) en sécurité digitale participe directement aux projets de l'entreprise liés au domaine de la sécurité.

L'expert(e) en sécurité digitale possède les compétences et qualités nécessaires pour occuper des postes autonomes et à responsabilité dans la préparation et la mise en œuvre de projets informatiques.

Métiers :

- Expert·e en sécurité digitale
- Consultant·e en sécurité des systèmes d'information
- Auditeur·rice en sécurité des systèmes d'information
- Assistant·e RSSI
- Risk Manager (Junior)
- Administrateur·rice système réseau et sécurité

Equivalences et passerelles

La formation Expert(e) en sécurité digitale prépare au titre RNCP du même nom:
https://www.francecompetences.fr/recherche/rncp/36399/

Vous pouvez également poursuivre votre cursus de formation vers un doctorat au sein de l'université de votre choix.

Programme détaillé

Lead Pentester

(semaine 1)

- Principes de la sécurité de l'information
- Définition et encadrement et aspect réglementaire d'un test d'intrusion
- Frameworks et méthodes pour un test d'intrusion
- Socle technique : Foot & Fingerprinting, OSINT, Analyse de vulnérabilités, Recherche d'exploit.
- Création de charge, mise en oeuvre de persistances, mouvements latéraux, C&C
- Introduction sécurité Wifi, Web (Top10 Owasp), Applicative (Buffer Overflow)
- Création et analyse d'un rapport de test d'intrusion

(Semaine 2)

Techniques de hacking avancées

- Identification et compréhension des attaques pesant sur les entreprises
- Identification et exploitation de vulnérabilités
- Attaques avancées : Old school vs New school
- Dans la peau d'un hacker : Etude des mouvements et actions « post-offensive »
- Compromission par rebond
- Persistance et dissimulation de présence
- Red Team #TIPS
- Réduction et défenses des surfaces d'attaques

Test Intrusion avec Python

- Bases / Exécutables
- Scan de ports / ARP poisoning (MITM)
- Reverse Shell
- Exfiltration de données
- Création d'un RAT / Keylogger
- Notions sur les programmes auto-répliquants
- Cryptographie : Ransomware
- Requêtes HTTP(s) / Création d'un crawler
- API Web / Frame Injections

Wargame

- Travail en groupe
- Préparation d'infrastructures vulnérables avec un "write-up" détaillé
- Mode "wargame" : Attaques entre groupes des différentes infrastructures
- Création d'un rapport complet

Cyberdéfense

- Introduction aux menaces de ses dernières années pesant sur les organisations françaises.
- Etude de framework lié à la sécurité de l'information
- Présentation des cadres réglementaire nécessitant des produits certifiés par l'ANSSI
- Analyse et compréhension des "VISA ANSSI"
- Bonnes pratiques de la SSI (Hygiène ANSSI)
- Mise en oeuvre de moyens de défense des infrastructures
- Durcissement des mécanismes de défenses
- Auditer la sécurité SI d'une organisation

SOC security manager

- Présentation et compréhension des principales composantes d'un SOC
- Les phases de déploiement d'un projet SOC
- Présentation technologie SIEM
- Mise en place d'un lab complet sur environnement Active Directory
- Etude et mise en place de la suite Elastic (ELK/Kibana/ElasticSearch)
- Etude de scénarios d'attaques

Investigation numérique - réseau et Windows

- Découverte du monde de l'investigation
- Présentation d'une méthodologie de relevé de preuves
- Collecte de données, timeline, analyse, rapport
- Étude et protection après incident sur les systèmes d'exploitations WIndows
- Création d'un plan de réponse à incident

Fondamentaux de l'analyse de malware

- Création de shellcodes (polymorphisme, encoders XOR)
- Base des PE, ELF, Framework .net (Windows, Linux)
- Analyse statique d'une charge
- Analyse dynamique d'une charge
- Packing et depacking
- Particularité des Malwares (.net, Powershell, Python, .vbs, etc)
- Plateforme MISP et partage des connaissances

Gestion de projets et juridique

- Base de la gestion de projet en cascade et Agile
- Création d'un cahier des charges fonctionnel
- Réponse à un appel d'offre
- Étude de l'écosystème juridique cyber en France et en Europe
- CNIL / RGPD
- VISA ANSSI & Homologation

Gestion des risques SI avec ISO 27005 & EBIOS 2010/RM

- Analyse et compréhension d'une stratégie d'entreprise
- Compréhension de la gouvernance SSI et de l'importance de l'alignement stratégique
- Obtenir les compétences nécessaires pour piloter une analyse de risque.
- Mise en œuvre d'une analyse de risques basée sur l'ISO 27005 au travers de la méthode (EBIOS)
- EBIOS Risk manager

Intégration SMSI avec ISO 27001

Plan de continuité (PCA) avec ISO 22301

- PCA / PRA / PSI / PCI Explications
- Compréhension des besoins en sécurité de l'information de l'entreprise
- Savoir mener une analyse d'impact sur le business (Business Impact Analysis)
- Méthodologie d'implémentation et prérequis d'un PCA
- Les erreurs courantes liées aux PCA
- Maintien en condition opérationnel (MCO) du PCA
- Etude des exigences de la norme ISO 22301
- Appréhender la notion de système intégré (ex : ISO 27001)

DevOps Security Manager

- Compréhension des attaques WEB les plus utilisés (top 10 OWASP) et protection.
- Mise en place d'un cycle de développement sécurisé (SDL), ISO 27034, protection des DaCP
- Mise en place d'un modèle de maturité pour la sécurité des applications
- Réduction des attaques de surface, secure by default, séparation des privilèges
- Hardening - conception sécurisé (intégration d'outils, durcissement server/client, architecture sécurisé, HTTPOnly, CSP, etc
- Pentest applicatif (Méthode OWASP)

Préparation jury

Evaluations Finales

Présentation projet final