NIVEAU 7 - BAC+5

Expert·e en Sécurité Digitale

Préparation au Titre Professionnel : « Expert en Sécurité Digitale »

Reconnu par l'État de niveau 7 (ou niveau BAC+5)
Inscrit au RNCP (enregistrement du 25/04/2022)

Code RNCP : RNCP36399 – Code NSF : 326 – Formacode : 31006

Code Diplôme : 16X32633 – Délivré par ESD Expert(e) en Sécurité Digitale / 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

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.

Durée de la formation

En alternance :

- Formation en centre : 525 heures parcours standard (1 an)
- Formation en centre : + 385 heures si parcours en 2 ans.
- Sur un contrat de 12 à 24 mois (selon profil et prérequis)

Tarifs

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

Contact

ecole@eni-ecole.fr

N.B. : Dans un souci de lisibilité, le masculin utilisé dans ces différents textes pourra également désigner le féminin, et ce, sans recours systématique à l'écriture inclusive.

Moyens pédagogiques - techniques - d'encadrement

Équipements pédagogiques :

- Un poste de travail par apprenant équipé (en quasi-totalité) :
  - d'un processeur i5
  - d'un disque NVMe (32 Go de RAM)
- 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.
- Études 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 Azure (licences logiciels Microsoft)
- Un accès à la plateforme goFluent (plateforme d'autoformation et programme individualisé en anglais)
- Systèmes d'exploitation Microsoft, GNU/Linux et Cisco IOS
- Logiciels bureautiques (Microsoft Office 365 : Word, Excel, Powerpoint, ...)
- Outils de développement (Visual Studio, Oracle, Eclipse, Struts, Hibernate, Tomcat, Java...)
- Systèmes de gestion de bases de données relationnelles (Oracle Database, MySQL, SQL Server, ...)

Suivi et évaluation :

Les blocs de compétences constituant le titre « Expert 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

Évaluations en cours de formation mesurant compétence par compétence le degré de maîtrise de la situation professionnelle concernée : devoirs écrits, mises en situation professionnelle, QCM, études de cas, exposés oraux...

Épreuve finale : rédaction d'un rapport d'activité – soutenance orale devant un jury de professionnels extérieurs à l'École.

Possibilité d'accès au titre par capitalisation de blocs de compétences.

Débouchés et métiers

L'**Expert en Sécurité Digitale** participe directement aux projets de l'entreprise liés au domaine de la sécurité.

Il 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 en sécurité digitale
- Consultant en sécurité des systèmes d'information
- Auditeur en sécurité des systèmes d'information
- Assistant RSSI
- Risk Manager (Junior)
- Administrateur système réseau et sécurité
- …

Équivalences 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 / 2 ans

Gestion des identités et outils collaboratifs

- Gestion des domaines, forêts, et sites Active Directory
- Synchronisation Azure (Azure AD Connect)
- Gestion des identités (SSO, MFA)
- Mise en œuvre des comptes à privilèges
- Protocoles et flux de messagerie
- Gestion et interconnexion Microsoft 365

Cisco CCNA 2 – Notions de base sur la commutation, le routage et le Wi-Fi

- Les concepts de commutation Ethernet
- La configuration des routeurs et commutateurs
- Les VLAN
- Les concepts et protocoles Spanning-Tree
- Les agrégations EtherChannel
- Le protocole HSRP
- Les protocoles DHCPv4/v6, SLAAC
- La sécurité des réseaux locaux et des commutateurs
- Les réseaux Wi-Fi
- Le routage IP statique inter VLAN
- Le dépannage du routage statique

Scripting Linux

- Créer des scripts
- Les variables dans les scripts
- Les caractères spéciaux du shell
- Les commandes internes au shell
- Introduction à l'algorithmique
- Les conditions (if, case)
- Les boucles (while, until, for)
- Les fonctions
- L'arithmétique entière
- Gestion avancée des variables

Services d'infrastructure réseaux

- Configuration réseau des systèmes d'exploitation
- Le service DHCP
- Le service DNS
- Les services réseau dans un contexte Active Directoy
- Le service RDS (Remote Desktop Services)

Cisco CCNA 3 – Réseaux d'entreprise, sécurité et automatisation

- Le routage dynamique OSPFv2
- Les listes de contrôle d'accès IPv4
- Le protocole NAT IPv4
- Les concepts WAN
- Les concepts QoS
- Les concepts de tunnels VPN et IPsec
- La gestion, conception et dépannage du réseau
- La virtualisation et l'automatisation du réseau

Sécurisation et mise en conformité des accès au système d'information

- Présentation du Système d'Information
- Introduction à la sécurité : défense en profondeur
- Hébergement d'infrastructure : hébergement physique et contraintes, hébergement dans le Cloud public/privé/hybride
- Interconnexion de réseaux : modèles de pare-feu, matrice de flux, proxy, reverse proxy, NAT, reverse NAT
- Services d'infrastructure : RADIUS, Infrastructure PKI
- Application avec les solutions Stormshield :
- Présentation de Stormshield, de ses produits et fonctionnalités
- Prise en main du pare-feu Stormshield Network Security (SNS)
- Configuration des traces et supervision
- Objets réseau
- Configuration du réseau (types d'interfaces, routage)
- Translation d'adresses statique et dynamique
- Politique et règles de filtrage
- Protection et analyse applicative
- Gestion d'annuaires et utilisateurs
- Politiques, méthodes et règles d'authentification
- Portail captif
- VPN IPsec et VPN SSL

- **Passage de la certification Administrateur Stormshield CSNA**

Mise en Situation Professionnelle : Projet n°3 – Infrastructure sécurisée

- Réponse à un appel d'offre pour la conception d'un Système d'Information complexe
  - Maquettage des solutions techniques proposées
  - Rédaction d'un dossier technique et de procédures

Puis, poursuite sur le programme ESD en 1 an ci-après…

Programme détaillé / 1 an

Lead Pentester (2 semaines)

- 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 œuvre 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

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 : Étude 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.
- Étude 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 œuvre 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
- Étude et mise en place de la suite Elastic (ELK/Kibana/ElasticSearch)
- Étude 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'exploitation 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, …)
- 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

- Définition d'un système de management
- Présentation de la norme ISO27001/ISO27002
- Contexte d'utilisation et d'implémentation
- Compréhension des relations entre le SMSI, le management des risques, les contrôles, et les différentes parties prenantes.
- Savoir conseiller efficacement une organisation sur les meilleures pratiques.
- Analyse détaillée des exigences de la norme
- Plan de réponse à incident
- Savoir créer une méthodologie alignée sur l'ISO 27001 pour le déploiement d'un SMSI
- Méthodologie rédaction PSI & PSSI

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, ...)
- Pentest applicatif (Méthode OWASP)

Préparation jury

- Préparation Examen (soutenance)

Évaluations Finale
▪ Livraison Questions CTF ▪ Livraison Mémoire / Correction ▪ Livraison Finale Mémoire