Expert En Sécurité Digitale

Titre RNCP de niveau 7 – Code RNCP : 36399

INFORMATIONS GÉNÉRALES

Type de formation : Cursus diplômant

Domaine : Ecole supérieure d'informatique

Filière : Alternance

Rubrique : Niveau 7 - Mastère II

Éligible au CPF : Non

Action collective : Non

PRÉSENTATION

Objectifs & compétences

Les compétences développées lors de la formation :

1. **BLOC 1** - Prévenir et anticiper les menaces cyber pesant sur les systèmes d'information
2. **BLOC 2** - Auditer la sécurité des systèmes d'information et conduire le déploiement des mesures de défenses
3. **BLOC 3** - Analyser et sécuriser les systèmes d'information après une cyber-attaque
4. **BLOC 4** - Piloter la sécurité organisationnelle

Télécharger la documentation

Public visé

Demandeurs d'emploi / Étudiants / Salariés

Pré-requis

En formation initiale, une certification de niveau 6 (Bac+4) est demandée à l'entrée, dans le domaine de l'informatique de l'administration des systèmes et réseau.

En formation continue, une certification de niveau 6 (bac +4) est demandée où un niveau équivalent acquis par l'expérience professionnelle et justifiant des compétences en informatique et en administration des systèmes et réseau.

Les candidats à la certification doivent également justifier de leur motivation, de leur projet professionnel ainsi que de leurs compétences en informatique et en administration des systèmes et réseau au travers d'une lettre de motivation, d'un test de connaissances et d'un entretien professionnel.

PROGRAMME

Bloc 1 - Prévenir et anticiper les menaces cyber pesant sur les systèmes d'information

- Veille stratégique sur les cybermenaces
- Analyse des vulnérabilités et failles de sécurité
- Méthodologie des tests d'intrusion (Pentest)
- Audit technique des infrastructures
- Évaluation des risques liés aux systèmes d'information
- Outils de détection et d'analyse des menaces
- Identification des scénarios d'attaque
- Rédaction de rapports de sécurité et recommandations
- Mise en œuvre des actions préventives

Bloc 2 - Auditer la sécurité des systèmes d'information et conduire le

Code de formation : ESD

#CYBERSÉCURITÉ#CYBERDÉFENSE

€ Tarifs

Tarif & financement :

- Contrat d'apprentissage/ de professionnalisation : Prise en charge de la formation par l'OPCO et l'entreprise d'accueil
- CPF / CPF de transition / VAE / POE ... : nous contacter.

Campus Arcueil : admission@aston-ecole.com
Campus Lille : admission-lille@aston-ecole.com

Plus d'informations

Lieux & Horaires

Durée : 560 heures

Rythme : 14 moisEn alternance - 3 semaines en entreprise/1 semaine en centre de formation

Délai d'accès :
Rentrée entre septembre et novembre. Candidature possible jusqu'à 8 jours avant le début de la formation. Réponse d'admission sous 48h après dossier complet et entretien.
L'intégration à la session visée est conditionnée par la signature du contrat.

informations :
Accessibilité : Formation accessible aux personnes en situation de handicap. Des aménagements (pédagogiques, techniques ou organisationnels) peuvent être mis en place. Pour toute question, contactez notre Référent Handicap à l'adresse s.duhayon@aston-ecole.com ou consultez notre politique d'accessibilité.

Prochaines sessions

Consultez-nous pour les prochaines sessions.

Informations non contractuelles - PDF généré le 2/11/2026

déploiement des mesures de défense

- Audit organisationnel et technique de sécurité
- Analyse de conformité réglementaire
- Construction de plans de remédiation
- Déploiement des mesures de protection
- Supervision de la sécurité opérationnelle
- Mise en œuvre et pilotage d'un SOC
- Administration des outils SIEM
- Gestion des incidents de sécurité
- Suivi des indicateurs de performance cyber
- Coordination des acteurs de la cybersécurité

Bloc 3 - Analyser et sécuriser les systèmes d'information après une cyberattaque

- Gestion des incidents et des crises cyber
- Investigation numérique (Forensic)
- Collecte et analyse des preuves numériques
- Analyse de malwares et codes malveillants
- Réponse à incident et containment
- Identification des vecteurs d'attaque
- Élaboration des actions correctives
- Retour d'expérience et amélioration continue
- Renforcement des dispositifs de sécurité
- Communication en situation de crise

Bloc 4 - Piloter la sécurité organisationnelle

- Gouvernance de la sécurité des systèmes d'information
- Élaboration d'une stratégie cybersécurité
- Gestion des risques cyber (EBIOS RM, ISO 27005)
- Mise en conformité RGPD
- Mise en œuvre de la norme ISO 27001
- Élaboration et pilotage de la PSSI
- Construction des PCA et PRA
- Pilotage de projets cybersécurité
- Gestion budgétaire et reporting SSI
- Management des équipes et parties prenantes
- Sensibilisation et acculturation à la cybersécurité

MODALITÉS

Modalités

Méthodes pédagogiques
Cours en présentiel et distanciel
Étude de cas et mise en situation
Accès à des plateformes et ressources · Workshops / Ateliers

Dans les cycles supérieurs, d'une manière générale, nous développons et sensibilisons nos équipes et particulièrement celles des niveaux 6 et 7 à la généralisation d'une démarche inductive avec une méthode active : la Pédagogie inversée.

Modalités d'évaluation
Mises en situation professionnelle, jeu de rôles
La certification est acquise par :
- La validation totale des 4 blocs de compétences. Chaque bloc de compétences est acquis par la validation de l'ensemble des compétences du bloc. Evaluations continues
- La réalisation d'une période de stage ou d'alternance d'au moins 2 mois
- La soutenance d'un mémoire professionnel devant le jury de validation

Le programme de la formation est découpé en blocs de compétences. Chaque bloc peut être réalisé et validé de façon autonome et indépendant.

Les plus de la formation

Des enseignements concrets permettant une opérationnalité immédiate en entreprise

Les mission que vous aller pouvoir réaliser lors de votre alternance sont les suivantes :

Mener des audits en sécurité informatique
Définir les politiques en matière de sécurité des systèmes d'information

Informations non contractuelles - PDF généré le 2/11/2026

(PSSI) et en suivre la mise en oeuvre
Informer, conseiller et alerter la direction générale et les fonctions métiers sur les enjeux de la sécurité du SI
Assurer la sensibilisation des employés de l'établissement aux enjeux de la sécurité des systèmes d'information
Proposer et mettre en oeuvre des solutions de consolidation
Assurer la veille technologique.

CERTIFICATIONS

Titre RNCP N° RNCP36399 _ Expert en sécurité digitale
Certificateur : ASTON INSTITUT
Code NSF : 326

Date d'enregistrement : 25-04-2022
Date d'échéance d'enregistrement : 25-04-2027

Possibilité de valider un ou plusieurs blocs de compétences de la certification professionnelle.
La certification est obtenue par la validation de l'intégralité des blocs de compétences.

POUR ALLER PLUS LOIN

Les débouchés

Les métiers possibles

- Expert en sécurité digitale
- Expert en cyberdéfense
- Expert en cybersécurité
- Consultant en cybersécurité
- Consultant sécurité
- Consultant en sécurité des systèmes d'information
- Chef de projet en sécurité des systèmes d'information
- Pentester
- Auditeur en sécurité des systèmes d'information
- IT Risk Manager (Junior)

Information sur les niveaux et les correspondances

Et apres

Certifications ISO

Lead Implementer – certification ISO 27001
https://www.aston-institut.com/nos-formations/lead-implementer-certification-iso-27001-mg208/?highlight=ISO

Risk Manager – certification ISO 27005
https://www.aston-institut.com/nos-formations/risk-manager-certification-iso-27005-mg209/?highlight=ISO

Lead Auditor – certification ISO 27001
https://www.aston-institut.com/nos-formations/lead-auditor-certification-iso-27001-mg215/?highlight=ISO

Informations non contractuelles - PDF généré le 2/11/2026