

Expert(e) en sécurité digitale

RNCP27836 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	31006
Code(s) ROME	M1802, M1801, M1803, M1806
Type d'enregistrement	Enregistrement sur demande
Date d'échéance	03/03/2022

Certificateur(s)

ASTON INSTITUT · SIRET : 49868549400029

Partenaires habilités

8 organismes habilités, d'après la liste publiée par France compétences : 8 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
ADEN FORMATIONS ENTREPRISE	78071407700101	Former et organiser l'évaluation
ADEN FORMATIONS ENTREPRISE (ADEN ENTREPRISE)	78071407700069	Former et organiser l'évaluation
ASSOCIATION POUR L'ENSEIGNEMENT DU NUMERIQUE	80875076400025	Former et organiser l'évaluation
ASTON INSTITUT	49868549400052	Former et organiser l'évaluation
ENI ECOLE	39280706100024	Former et organiser l'évaluation
ENI ECOLE	39280706100040	Former et organiser l'évaluation
EXPERNET	44276468400027	Former et organiser l'évaluation
IT-KAMPUS	82990584300027	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

A compléter (Reprise)

ACTIVITÉS VISÉES

L'expert en sécurité digitale est responsable de la conception et de la sécurisation du système d'information de l'organisme. Interlocuteur privilégié de la DSI ou de la DG, il est chargé de mettre en place un système de management de la sécurité de l'information, dont il s'assure qu'il est d'une part en adéquation avec les objectifs généraux de l'entreprise et d'autre part compris et approprié par les équipes techniques et par les acteurs de la structure. Pour cela, il développe une vision globale du système de management de la sécurité de l'information, prenant en compte les impacts économiques, organisationnels, humains, techniques et juridiques pour le système cible. Polyvalent, l'expert en sécurité digitale est donc à la fois compétent sur les questions techniques, managériales et stratégiques.

Ainsi, l'expert en sécurité digitale accomplit toutes les activités en lien avec la conception, la mise en application et la gestion de la sécurité de l'information pour un système cible. Il est susceptible de réaliser chacune des étapes de la mise en œuvre d'un SMSI : définition des objectifs, organisation générale de la structure, mise en œuvre de la

politique de défense, évaluation du niveau de sécurité, évaluation des impacts, définition des objectifs de sécurité, animation des équipes, conseil auprès des décideurs, suivi des budgets...

1) Conception d'un plan stratégique de sécurité pour un système cible

L'expert en sécurité digitale analyse les besoins d'un système cible donné et formalise un plan stratégique de sécurité. Pour cela il prend en compte l'ensemble des facteurs contraignants internes et externes, et s'intéresse notamment au positionnement business de l'entreprise, afin de formaliser un schéma directeur des Systèmes de Sécurité de l'Information et d'émettre des préconisations à destination des donneurs d'ordres.

2) Structuration d'une solution technique et organisationnelle répondant aux besoins de sécurité du système cible

En accord avec le schéma directeur SSI préalablement défini, ce professionnel structure des solutions adaptées aux besoins et aux contraintes du système cible. Pour cela, il est amené réaliser des études de marché concernant les technologies, les architectures et les prestataires susceptibles de contribuer à la structuration de la solution. Il est également chargé d'implémenter un SMSI (système de management de la sécurité de l'information) et les indicateurs de pilotage stratégiques, fonctionnels et opérationnels qui lui sont inhérents.

3) Conduite d'un audit de sécurité des systèmes d'information

Une fois la solution de sécurité implémentée dans un système cible, l'expert en sécurité digitale réalise des audits de sécurité afin d'en vérifier l'opérationnalité. Il prépare et réalise l'ensemble des phases de l'audit suite à quoi il rédige des préconisations d'améliorations ou de corrections à apporter. Il est également susceptible de réaliser, d'une part, des pentest ou test d'intrusion dans le système cible, c'est-à-dire tenter de trouver les failles du système en simulant une attaque. Et d'autre part, il peut réaliser des forensics ou investigations numériques légales, c'est-à-dire recueillir des preuves numériques d'un acte de cyber-criminalité.

4) Maintien en condition opérationnelle de la sécurité de l'information

Les préconisations suite aux audits de sécurité permettent le maintien en condition opérationnelle de la sécurité de l'information. Des modifications sont apportées à la gestion du système de sécurité notamment concernant la révision des indicateurs de suivi (de nouveaux indicateurs peuvent être créés, ou le niveau d'alerte concernant ces indicateurs peut être revu). Des modifications sont également apportées aux dispositifs techniques ou organisationnels en place. L'expert en sécurité digitale est garant, d'une part, du maintien des objectifs budgétaires liés à ce maintien en condition opérationnel, et d'autre part, du respect de la stratégie de l'entreprise.

5) Accompagnement de la mise en œuvre de la politique de sécurité SI d'un système cible

Enfin, les modifications apportées à la gestion de la sécurité doivent être mises en œuvre de manière homogène à tous les niveaux de l'entreprise. Pour cela, l'expert en sécurité digitale accompagne la direction dans la mise en place des outils de déploiement de la politique, notamment en termes de recrutements, de sensibilisation ou de formation des collaborateurs. Il s'assure également de la mise en œuvre d'une charte informatique conforme à la stratégie de sécurisation digitale de l'entreprise.

COMPÉTENCES ATTESTÉES

Les capacités attestées renvoient à cinq grands domaines de compétences couvrant l'ensemble de la conception et de la mise en œuvre de la sécurité d'un système cible :

BLOC 1 : Concevoir un plan stratégique de sécurité pour un système cible

C1. Identifier l'ensemble des enjeux (techniques, humains, organisationnels, financiers et juridiques) liés aux besoins de sécurité d'un système cible afin de rédiger un schéma directeur SSI

C2. Mener une analyse de risques, auquel est exposé un système d'information afin de formaliser des objectifs de sécurité de l'organisation

C3. Conceptualiser et formaliser des préconisations adaptées au système cible en tenant compte du principe de sécurité en profondeur, du R.O.I (Return On Investment) et du B.I.A. (Business Impact Analysis), afin de convaincre des donneurs d'ordre.

BLOC 2 : Structurer une solution technique et organisationnelle répondant aux besoins de sécurité du système cible

C4. Concevoir un cahier des charges fonctionnel et technique dans le but de diffuser un appel d'offres

C5. Formaliser une proposition technique et organisationnelle complète, en réalisant un benchmark des produits ou dispositifs de sécurité dans le but de convaincre des décideurs

C6. Extrapoler une politique de sécurité des systèmes d'information basée sur une analyse de risques.

C7. Concevoir des indicateurs de différents niveaux (stratégiques, fonctionnels et opérationnels) liés à la sécurité de l'information

BLOC 3 : Conduire un audit de sécurité des systèmes d'information

C8. Piloter l'audit d'un système d'information en préparant les différentes phases afin d'estimer ou de faire estimer le niveau de sécurité d'un SI

C9. Réaliser une ou plusieurs phases de l'audit en effectuant des tests de vulnérabilité et d'intrusion afin d'identifier les failles de sécurité du système

C10. Réaliser une investigation numérique légale (Forensic) en appliquant des protocoles d'investigation numérique respectant les procédures légales afin d'apporter des preuves d'un acte malveillant

C11. Formaliser les résultats de l'audit de sécurité afin d'émettre des préconisations techniques et organisationnelles

BLOC 4 : Maintenir en condition opérationnelle de la sécurité de l'information

C.12 Gérer les incidents de sécurité en apportant des réponses adaptées à chaque incident grâce à la lecture des indicateurs afin de maintenir le niveau de sécurité en accord avec la stratégie de l'entreprise.

C13. Analyser le dépassement des indicateurs de pilotage et de contrôle en relevant des incidents et en vérifiant la pertinence des alertes afin de garantir l'opérationnalité de la protection

C14. Garantir le suivi des risques de façon constant en réalisant une veille sur les nouvelles menaces, sur les solutions de sécurité, afin de prévenir les failles du système

C15. Assurer le suivi des budgets liés à la sécurité de l'information d'une organisation. afin de maintenir les objectifs fixés

BLOC 5 : Accompagner la mise en œuvre de la politique de sécurité d'un système cible

C16. Conseiller les décideurs en identifiant les profils d'agent impactés par la sécurité du SI pour l'ensemble des services de la structure, et en identifiant les résistances, afin de fluidifier la mise en œuvre sur le terrain

C17. Sensibiliser et former les équipes en rédigeant, en diffusant et en mettant en application des documents liés à la SSI afin de susciter l'adhésion des acteurs quant aux règles de sécurité

C18. Piloter la formation et le recrutement des équipes techniques, en s'assurant de la montée en compétence en interne afin d'atteindre une maturité de l'entreprise sur les questions de sécurité

Blocs de compétences

RNCP27836BC01 — Accompagner la mise en œuvre de la politique de sécurité d'un système cible

LISTE DE COMPÉTENCES

Descriptif :

- Conseiller les décideurs en identifiant les profils d'agent impactés par la sécurité du SI pour l'ensemble des services de la structure, et en identifiant les résistances, afin de fluidifier la mise en œuvre sur le terrain
- Sensibiliser et former les équipes en rédigeant, en diffusant et en mettant en application des documents liés à la SSI afin de susciter l'adhésion des acteurs quant aux règles de sécurité
- Piloter la formation et le recrutement des équipes techniques, en s'assurant de la montée en compétence en interne afin d'atteindre une maturité de l'entreprise sur les questions de sécurité

Modalités d'évaluation :

Modalité II : Mémoire professionnel

Partie consacrée au plan de sensibilisation ou de formation

RNCP27836BC02 — Concevoir un plan stratégique de sécurité pour un système cible

LISTE DE COMPÉTENCES

Descriptif :

- Identifier l'ensemble des enjeux (techniques, humains, organisationnels, financiers et juridiques) liés aux besoins de sécurité d'un système cible afin de rédiger un schéma directeur SSI
- Mener une analyse de risques, auquel est exposé un système d'information afin de formaliser des objectifs de sécurité de l'organisation
- Conceptualiser et formaliser des préconisations adaptées au système cible en tenant compte du principe de sécurité en profondeur, du R.O.I (Return On Investment) et du B.I.A. (Business Impact Analysis), afin de convaincre des donneurs d'ordre.

Modalités d'évaluation :

Modalité I.a : Elaboration et restitution d'une analyse de risques SSI

RNCP27836BC03 — Structurer une solution technique et organisationnelle répondant aux besoins de sécurité du système cible

LISTE DE COMPÉTENCES

Descriptif :

- Concevoir un cahier des charges fonctionnel et technique dans le but de diffuser un appel d'offres
- Formaliser une proposition technique et organisationnelle complète, en en réalisant un benchmark des produits ou dispositifs de sécurité dans le but de convaincre des décideurs
- Extrapoler une politique de sécurité des systèmes d'information basée sur une analyse de risques.
- Concevoir des indicateurs de différents niveaux (stratégiques, fonctionnels et opérationnels) liés à la sécurité de l'information

Modalités d'évaluation :

Modalité I.f : Présentation d'un cahier des charges fonctionnel

Modalité I.d : Etude de cas sur un SMSI

RNCP27836BC04 — Conduire d'un audit de sécurité des systèmes d'information

LISTE DE COMPÉTENCES

Descriptif :

- Piloter l'audit d'un système d'information en préparant les différentes phases afin d'estimer ou de faire estimer le niveau de sécurité d'un SI
- Réaliser une ou plusieurs phases de l'audit en effectuant des tests de vulnérabilité et d'intrusion afin d'identifier les failles de sécurité du système
- Réaliser une investigation numérique légale (Forensic) en appliquant des protocoles d'investigation numérique respectant les procédures légales afin d'apporter des preuves d'un acte malveillant
- Formaliser les résultats de l'audit de sécurité afin d'émettre des préconisations techniques et organisationnelles

Modalités d'évaluation :

Modalité II : Mémoire professionnel

Partie consacrée à l'audit de sécurité d'un SI

Modalité I.b : Réalisation et présentation d'un test d'intrusion

Modalité I.c : Réalisation d'une investigation numérique légale (Forensic)

RNCP27836BC05 — Maintenir en condition opérationnelle de la sécurité de l'information

LISTE DE COMPÉTENCES

Descriptif :

- Gérer les incidents de sécurité en apportant des réponses adaptées à chaque incident grâce à la lecture des indicateurs afin de maintenir le niveau de sécurité en accord avec la stratégie de l'entreprise.
- Analyser le dépassement des indicateurs de pilotage et de contrôle en relevant des incidents et en vérifiant la pertinence des alertes afin de garantir l'opérationnalité de la protection
- Garantir le suivi des risques de façon constant en réalisant une veille sur les nouvelles menaces, sur les solutions de sécurité, afin de prévenir les failles du système
- Assurer le suivi des budgets liés à la sécurité de l'information d'une organisation. afin de maintenir les objectifs fixés

Modalités d'évaluation :

Modalité I.d : Présentation d'une gestion d'incidents au sein d'un SMSI

Modalité I.d : Etude de cas sur un SMSI

Modalité I.e : Veille technologique

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Secteurs d'activité

Les fonctions exercées par l'expert-e en sécurité digitale peuvent concerner toute structure disposant d'un système d'information et susceptible de mettre en œuvre un système de management de la sécurité de l'information. Elles sont donc transversales à tout secteur d'activité.

L'expert-e en sécurité digitale peut exercer dans toute entreprise de grande taille, tout secteur d'activité confondu (industrie, énergie, télécommunications, banques, services...). Il peut aussi exercer ses fonctions dans le SI d'une institution publique de grande taille.

Il peut également intégrer une PME en informatique, spécialisée en sécurité digitale ou délivrant des prestations de service auprès de grands comptes. Des cabinets de conseil spécialisés en informatique sont aussi intéressés par des profils experts en sécurité digitale.

Enfin, il peut intégrer une agence publique pour la sécurité telle que l'ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Information) ou la DCPJ (Direction Centrale de Police Judiciaire).

TYPE D'EMPLOIS ACCESSIBLES

Type emplois accessibles

Expert en sécurité digitale - Expert en cybersécurité - Expert en cybersécurité - Consultant en sécurité des systèmes d'information - Chef de projet en sécurité des systèmes d'information - Pentester - Auditeur en sécurité des systèmes d'information - Architecte en sécurité des systèmes d'information - Assistant RSSI - IT Risk Manager (Junior) - Administrateur système réseau et sécurité

RÉGLEMENTATIONS D'ACTIVITÉ

A compléter (Reprise)

Marché du travail

Indicateurs au niveau des familles professionnelles (FAP) des métiers visés, agrégés au niveau national — France Travail / DARES (open data).

Tension de recrutement (DARES 2024)	Élevée (4/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 942 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (19 % des actifs en emploi)
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée) M2X91 — Chefs de projet et directeurs de service informatique · tension 4/5 (Élevée) M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom · tension 3/5 (Modérée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	16 497
Jugés difficiles à recruter	46 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X91 — Chefs de projet et directeurs de service informatique M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

MODALITÉS D'ACCÈS

Formation initiale, Formation continue, Apprentissage, Contrat de professionnalisation, Candidature individuelle, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

A compléter (Reprise)

COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE, APPRENTISSAGE, CONTRAT DE PROFESSIONNALISATION, CANDIDATURE INDIVIDUELLE, VAE

5 personnes composent le jury :

- 2 membres ASTON

- 3 professionnels externes à ASTON

Financement en alternance (NPEC)

Niveau de prise en charge d'un contrat d'apprentissage par les OPCO, fixé par France compétences par branche professionnelle (CPNE).

Prise en charge usuelle	6 507 €
Selon la branche	5 997 € – 6 905 €
Prise en charge	Branches concernées
6 507 €	Valeur par défaut · 194 branches
6 905 €	CPNEFP des sociétés d'assistance, CPNE de l'ingénierie, des services informatiques et du conseil, CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique, CPNEFP de la branche des industries de produits alimentaires élaborés
6 741 €	CPNE des Télécoms, CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services), CPNEFP de la branche des prestataires de services du secteur tertiaire, CPNEFP de la branche professionnelle des Entreprises du courtage d'assurances et/ou réassurances
6 881 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager, CPNEFP du Négoce de l'ameublement
6 826 €	CPNE Branche Caoutchouc, CPNEFP de la métallurgie
6 375 €	CPNE des industries de santé (CPNEIS), CPNE du Commerce de détail et de gros à prédominance alimentaire
6 890 €	CPNE FP Branche des magasins du Bricolage
6 836 €	CPNEFP Sports Loisirs
6 704 €	CPNEF de la Publicité
6 685 €	CPNE Banque
5 997 €	CPNEF de l'audiovisuel

Base légale

Date d'échéance de l'enregistrement	03/03/2022
--	------------

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)
RNCP36399

Pour plus d'informations

LIEN VERS LE DESCRIPTIF
alternance@aston-ecole.com
<http://www.aston-ecole.com/esd>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/27836/>