

Architecture Cybersécurité

RS3115 · RS · Publiée

L'essentiel

Code(s) NSF	326
Formacode(s)	31006
Type d'enregistrement	Enregistrement sur demande
Date d'échéance	31/12/2021

Certificateur(s)

ISEP FORMATION CONTINUE · SIRET : 38256402900017

Résumé de la certification

OBJECTIFS ET CONTEXTE

Il s'agit de former les professionnels

- exerçant déjà un métier dans le secteur des NTIC et n'ayant aucune expertise dans le domaine de la Sécurité Numérique ;
 - des métiers de l'intégration sécurisée ;
- aux compétences nécessaires à l'exercice de fonctions d'Architecte spécialisé en Cybersécurité. A l'issue de cette formation, il leur sera possible de concevoir des architectures sécurisées et de comprendre de façon transverse les enjeux de la sécurité des structures et organisations. A ce titre, la formation intervient en complément
- des métiers existant traditionnellement dans le domaine informatique / télécoms / réseaux, en proposant aux architectes informatiques d'acquérir des compétences en sécurité et ainsi accompagner leur reconversion professionnelle ;
 - des métiers de l'intégration sécurisée, en proposant aux experts techniques en sécurité une vue globale et transverse sur les architectures et les systèmes de sécurité, ainsi que leur place dans les organisations.

COMPÉTENCES ATTESTÉES

La formation est construite suivant 2 composantes :

Architecture

1. Auditionner et évaluer le niveau de sécurité des architectures à déployer et existantes
2. Structurer les choix technologiques et méthodologiques d'un ensemble répondant à des exigences de sécurité
3. S'assurer de la déclinaison optimale des exigences fonctionnelles et techniques spécifiques à la sécurité
4. Identifier et valider la cartographie en s'assurant que les hypothèses de sécurité de son architecture sont clairement énoncées et prises en compte dans sa conception
5. Concevoir les nouvelles architectures sécurisées des solutions cibles
6. Vérifier que les exigences de sécurisation sont effectivement déclinées
7. Fournir la connaissance de l'état de l'art des architectures sécurisées
8. Rédiger les dossiers de conception et de justification

Management

1. Bénéficier d'un panorama complet de la sécurité
2. Appréhender la gestion projet : gérer une réponse à appel d'offre dans le cadre d'une architecture sécurisée
3. Identifier les outils nécessaires au bon déroulement d'un projet de sécurité
4. Comprendre les bases juridiques et de la réglementation d'un projet de sécurité
5. Appréhender les enjeux d'une communication optimale en cas de gestion de crise de sécurité

L'ensemble des compétences précitées sont évaluées au moyen de contrôles de connaissances proposés par les intervenants :

Architecture

1. Auditionner et évaluer le niveau de sécurité des architectures à déployer et existantes :

Cohérence de la démarche, respect de la méthodologie, exhaustivité de l'analyse, identification des points à risques, validation lors de mises en situation

2. Structurer les choix technologiques et méthodologiques d'un ensemble répondant à des exigences de sécurité :

Définition des priorités, cohérence de la démarche, respect de la méthodologie, pertinence des choix d'équipements, validation lors de mises en situation

3. S'assurer de la déclinaison optimale des exigences fonctionnelles et techniques spécifiques à la sécurité :

Définition des priorités, cohérence de la démarche, respect de la méthodologie, justification de la pertinence des choix effectués, validation lors de mises en situation

4. Identifier et valider la cartographie en s'assurant que les hypothèses de sécurité de son architecture sont clairement énoncées et prises en compte dans sa conception :

Définition des priorités, cohérence de la démarche, respect de la méthodologie, exhaustivité de l'analyse, validation lors de mises en situation

5. Concevoir les nouvelles architectures sécurisées des solutions cibles :

Démonstration de la viabilité technicoéconomique des architectures, du niveau d'adéquation avec le besoin exprimé, justification de la pertinence des choix effectués, validation lors de mises en situation

6. Vérifier que les exigences de sécurisation sont effectivement déclinées :

Définition des priorités, exhaustivité de l'analyse, cohérence de la démarche, respect de la méthodologie

7. Fournir la connaissance de l'état de l'art des architectures sécurisées :

Vérification de connaissances

8. Rédiger les dossiers de conception et de justification :

Validation de la structure documentaire, exhaustivité, validation fond et forme lors de mises en situation

Management

1. Gérer un projet de sécurité complexe :

Validation de la démarche projet lors de mises en situation

2. Anticiper, identifier et gérer les risques :

Contrôle de connaissances, validation de la démarche projet lors de mises en situation

3. Appréhender les enjeux humains, organisationnels et juridiques :

Contrôle de connaissances, validation de la démarche projet lors de mises en situation

4. Les outils du Manager pour communiquer et faire adopter ses idées :

Contrôle de connaissances, validation de la démarche projet lors de mises en situation

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

- Bénéficier de connaissances dans le domaine informatique, des télécommunication ou des réseaux
- Détenir un diplôme de type Master 2 (BAC+5) ou équivalent
- Détenir un diplôme de type Master 1 (BAC+4) ou équivalent et justifier d'une expérience professionnelle de 3 ans minimum
- Détenir un diplôme de type Master 1 (BAC+4) ou équivalent sans justifier d'une expérience professionnelle ou détenir un diplôme de type Licence (BAC+3) et justifier d'une expérience professionnelle de 3 ans minimum, via régime dérogatoire (30% des effectifs maximum)
- Autres cas : via un entretien pour valider les acquis professionnels (10% des effectifs)

Base légale

Date d'échéance de l'enregistrement 31/12/2021

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

Pour en savoir plus : <http://formation-continue.isep.fr/architecture-cyber-securite-et-integration> (focus ARCHITECTURE)

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/3115/>