

Intégration cybersécurité

RS3116 · 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

Elle concerne plus particulièrement les ESN (Entreprises de Service Numérique), intervenant sur l'ensemble des secteurs d'activité.

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'architecture sécurisée ;

aux compétences nécessaires à l'exercice de fonctions d'Intégrateur spécialisé en Cybersécurité. A l'issue de cette formation, il leur sera possible de connaître les systèmes, sous-systèmes et composants de sécurité à la fois physiques et virtuels, appréhender les enjeux et méthodologies des projets d'intégration sécurisée ainsi que de bénéficier d'une dimension juridique et managériale. A ce titre, la formation intervient en complément

- des métiers existant traditionnellement dans le domaine informatique / télécoms / réseaux, en proposant aux intégrateurs informatiques d'acquérir des compétences en sécurité et ainsi accompagner leur reconversion professionnelle ;

- des métiers de l'architecture sécurisée, en proposant aux experts fonctionnels en sécurité une vue technique sur les systèmes de sécurité, ainsi que leur principaux processus et composants.

COMPÉTENCES ATTESTÉES

La formation est construite suivant 2 composantes :

Intégration

1. Mettre en oeuvre des solutions de sécurité (services, fonctionnalité de sécurité, plateforme d'intégration) dans les nouvelles architectures et celles existantes
2. Planifier et coordonner les actions issues des exigences d'intégration exprimées
3. Installer des composants matériels, des composants logiciels ou des sous-systèmes supplémentaires de sécurité dans un système existant ou en cours de développement
4. Respecter les processus et procédures afin de garantir intégrité et interopérabilité des solutions sécurisées
5. Qualifier et intégrer les solutions sécurisées dans l'environnement de production
6. Documenter les processus de mise en oeuvre, de mise à jour et d'exploitation des composants de sécurité
7. Organiser les conditions de mise en oeuvre du maintien en condition de sécurité

Management

1. Appréhender les enjeux du management d'équipe
2. Appréhender la méthodologie et les enjeux de la gestion de projets de sécurité
3. Identifier les outils nécessaires au bon déroulement d'un projet
4. Etre initié aux bases juridiques et de la réglementation

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

intervenants :

Architecture

1. Mettre en oeuvre des solutions de sécurité (services, fonctionnalité de sécurité, plateforme d'intégration) dans les nouvelles architectures et celles existantes :

Cohérence de la démarche, respect de la méthodologie, vérification de connaissances, analyse de l'existant

2. Planifier et coordonner les actions issues des exigences d'intégration exprimées :

Vérification du niveau de priorité accordé aux actions, respect de la démarche projet, validation de l'avancée projet en situation

3. Installer des composants matériels, des composants logiciels ou des sous-systèmes supplémentaires de sécurité dans un système existant ou en cours de développement :

Respect de la méthodologie, vérification de connaissances, analyse de l'existant, anticipation des risques, validation lors de mises en situation

4. Respecter les processus et procédures afin de garantir intégrité et interopérabilité des solutions sécurisées :

Respect de la méthodologie, exhaustivité de la démarche, validation lors de mises en situation

5. Qualifier et intégrer les solutions sécurisées dans l'environnement de production :

Respect de la méthodologie, exhaustivité de la démarche, validation lors de mises en situation

6. Documenter les processus de mise en oeuvre, de mise à jour et d'exploitation des composants de sécurité :

Structure documentaire, exhaustivité, validation fond et forme lors de mises en situation

7. Organiser les conditions de mise en oeuvre du maintien en condition de sécurité :

Respect de la méthodologie, exhaustivité de la démarche, validation lors de mises en situation

Management

1. Gérer un projet de sécurité complexe :

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

2. Appréhender les enjeux humains en temps de crise :

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

3. Appréhender les enjeux juridiques :

Contrôle de connaissances

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 INTEGRATION)

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/3116/>

Demande CPF — formations engagées

Dossiers CPF engagés	1
Montant total engagé	3 000 €
Coût moyen par dossier	3 000 €
Durée moyenne	352 h
Période	05/2021
France compétences	100 %

Formations engagées via le CPF — Caisse des Dépôts (open data), tous organismes confondus.