Architecte en cybersécurité

Intitulé officiel : Titre RNCP Niveau 6 Concepteur en architecture informatique parcours Cybersécurité

Présentation

Publics / conditions d'accès

Cette formation est ouverte aux titulaires d'un diplôme Bac+2 en informatique.

Les titulaires d'un diplôme Bac+2 scientifique ou technique non informatique peuvent aussi suivre cette information après avoir acquis les deux unités d'enseignement NFP135 (Valeur d'Accueil et de Reconversion en Informatique 1) et NP136 (Valeur d'Accueil et de Reconversion en Informatique 2)

L'accès à cette formation est aussi possible par la voie de la validation d'acquis de l'expérience (VAE) ou encore par la voie de la validation des études supérieures (VES). Des dispenses d'unités d'enseignement peuvent être accordées aux titulaires d'un diplôme Bac+3 en informatique.

Objectifs

Ce titre de concepteur en architecture informatique option cybersécurité vise à développer la capacité de concevoir, de développer et maintenir en condition opérationnelle une architecture de sécurité en respectant une démarche qualité, en tenant compte du contexte de l'entreprise, des attentes et besoins des utilisateurs et en veillant aux évolutions technologiques. Il fournit aussi les bases pour l'organisation et l'encadrement d'une équipe technique. A l'issue de sa formation, l'auditeur pourra, à titre d'exemple, exercer ses compétences dans le maintien en sécurité du système d'information de son entreprise. Il peut se voir confier la conduite d'une analyse des risques informatiques ou encore la mise en œuvre de politiques de sécurité ou le rôle d'architecte de sécurité.

Organisation de la formation

Cette formation est composée :

- d'enseignements permettant d'acquérir les compétences de base,
- d'enseignements de spécialisation et d'ouverture,
- d'enseignements en management
- et d'un enseignement d'anglais préparant l'auditeur au test de BULATS niveau II (ou équivalent).

Il est fortement recommandé aux auditeurs (si concernés) :

- de commencer leurs parcours par les unités d'enseignement associés aux compétences de base,
- de suivre l'enseignement d'anglais très tôt dans le parcours.

Remarques :

- *Cette organisation de la formation prend effet dès* ***septembre 2019****. Des mesures transitoires sont prévues pour les auditeurs déjà inscrits au titre RNCP II Concepteur en architecture informatique. Ces mesures transitoires dont vous trouverez le détail* ***ici*** *sont valables jusqu'au* ***30 aout 2021.*** *Passée cette date, l'auditeur souhaitant obtenir une dérogation devra passer par la VES.*
- Les auditeurs ayant validé **avant octobre 2019**, NFE113, auront validé dans le nouveau cursus NFP107
- Les auditeurs ayant validé **avant octobre 2019**, SMB137, auront validé dans le

Non valide depuis le 31-08-2022

Arrêté du 27 décembre 2018. Enregistré au Niveau 6 (ex Niveau II) pour 4 ans. le 27-12-2018

Code : CPN8403A

Titre RNCP Niveau 6

Responsabilité nationale : EPN05 - Informatique / Ilham LAMMARI

Niveau CEC d'entrée requis : Niveau 5 (ex Niveau III)

Niveau CEC de sortie : Niveau 6 (ex Niveau II)

Mention officielle : Arrêté du 27 décembre 2018. Enregistré au Niveau 6 (ex Niveau II) pour 4 ans.

Mode d'accès à la certification :

- Apprentissage
- Contrat de professionnalisation
- Validation des Acquis de l'Expérience
- Formation continue

NSF : Analyse informatique, conception d'architecture de réseaux (326n)

Métiers (ROME) : Administrateur / Administratrice système informatique (M1801) , Développeur / Développeuse de sécurité des systèmes d'information (M1805) , Expert / Experte en tests d'intrusion - sécurité des systèmes d'information (M1802) , Expert / Experte en sécurité des systèmes d'information (M1802) , Expert / Experte en cybersécurité (M1802) , Auditeur / Auditrice en sécurité des systèmes d'information (M1802) , Architecte de sécurité des systèmes d'information (M1802) , Analyste en vulnérabilité de code logiciel (M1802)

Code répertoire : RNCP15253

Code CertifInfo : 52840

Contact national :

EPN05 -IRSM

nouveau cursus SMB101

- Les auditeurs ayant validé **avant octobre 2019**, NSY116, auront validé dans le nouveau cursus MUX101
- Les auditeurs ayant validé **avant octobre 2019**, SMB104, auront validé dans le nouveau cursus RSX101

2 rue Conté
75003 Paris

KONTOULI Konstantina
konstantina.kontouli@lecnam.net

Modalités de validation

Ce titre de « Concepteur en Architecte Informatique, option Cybersécurité » est délivré, par le jury diplômant du Cnam Paris, à tout auditeur remplissant les conditions suivantes :

- Validation de l'ensemble des unités d'enseignements de ce titre
- Obtention du niveau d'anglais B1 du CECRL
- Justification d'une expérience professionnelle :
  - de 2 ans à temps plein dans le domaine du diplôme
  - ou de 3 ans à temps plein dans un autre domaine complété par un stage d'au moins 3 mois en relation avec cette certification.
- Rédaction d'un rapport d'activité professionnelle décrivant cette expérience professionnelle.

La demande de délivrance du diplôme ainsi que celle de l'analyse de l'expérience professionnelle se font en ligne. Les deux procédures sont décrites **ici**

Remarques :

- *Une unité d'enseignement ne peut être validée qu'une seule fois.*
- *La validation de l'expérience professionnelle se fait* ***en fin de parcours.***

Compétences

- Capturer des exigences métiers, les traduire en un ensemble cohérent d'exigences fonctionnelles et non-fonctionnelles, les formaliser
- Participer à la rédaction d'un cahier des charges
- Analyser un cahier des charges et proposer des solutions techniques
- Élaborer un document de spécification technique servant d'appui à la mise en œuvre d'un composant du Système d'Information
- Mettre en œuvre une solution technique, associée à un composant du Système d'Information en respectant une spécification
- Élaborer des tests et les exécuter
- Rédiger un cahier de tests
- Intégrer un composant développé dans son environnement d'exploitation
- Piloter les phases de développement, de tests et d'intégration
- Conduire une analyse des risques informatiques
- Définir et rédiger les protocoles de validation informatique pour la qualification d'un composant du Système d'Information
- Coordonner les essais décrits dans les protocoles de validation et de qualification
- Investiguer sur les déviations
- Proposer et exécuter les mesures correctives
- Rédiger les rapports de qualification
- Piloter des projets informatiques
- Communiquer sur le projet en français ou en anglais
- Participer aux choix de progiciels, d'outils et/ou de technologies
- Assurer le rôle de support et d'assistance auprès des équipes informatiques dans le cadre de son périmètre d'expertise
- Rédiger des politiques de sécurité
- Mettre en œuvre des politiques de sécurité en installant ou en mettant à jour des équipements et logicielles de sécurité
- Administrer des dispositifs de Sécurité Opérationnelle en Services Managés
- Mettre en place un processus de supervisions avant incidents et post-mortem

- Résoudre des incidents de sécurité

Enseignements

Outils mathématiques pour Informatique	UTC501
Principes fondamentaux des Systèmes d'exploitation	UTC502
Paradigmes de programmation	UTC503
Systèmes d'Information et Bases de Données	UTC504
Introduction à la cyberstructure de l'internet : réseaux et sécurité	UTC505

1 UE au choix d'anglais à choisir parmi

Anglais général pour débutants	ANG100
Anglais professionnel	ANG330

1 UE de cybersécurité à choisir parmi :

Architectures et bonnes pratiques de la sécurité des réseaux, des systèmes, des données et des applications	SEC105
Cybersécurité : référentiel, objectifs et déploiement	SEC101
Menaces informatiques et codes malveillants : analyse et lutte	SEC102

1 UE de réseaux informatiques à choisir parmi :

Réseaux et protocoles pour l'Internet	RSX101
Technologies pour les applications en réseau	RSX102

1 UE d'ouverture à choisir parmi :

Modélisation, optimisation, complexité et algorithmes	RCP105
Recherche opérationnelle et aide à la décision	RCP101
Systèmes d'exploitation : principes, programmation et virtualisation	SMB101
Systèmes de gestion de bases de données	NFP107
Systèmes d'information web	NFE114
Introduction à la gestion de données à large échelle	NFE115
Méthodologies des systèmes d'information	NFE108
Linux : principes et programmation	NSY103
Architectures des systèmes informatiques	NSY104
Applications réparties	NSY014
Génie logiciel	GLG105
Spécification logique et validation des programmes séquentiels	NFP120
Programmation Fonctionnelle : des concepts aux applications web	NFP119
Programmation avancée	NFP121

Conduite d'un projet informatique	NSY115

2 UE de cybersécurité avancée à choisir parmi :

Menaces informatiques et codes malveillants : analyse et lutte	SEC102
Conception d'architecture de sécurité à partir d'un audit de sécurité	SEC107
Mise en œuvre de mesures de sécurité avancées (Hardening)	SEC108
Analyses de sécurité : vulnérabilités et attaques	SEC106

Architectures et bonnes pratiques de la sécurité des réseaux, des systèmes, des données et des applications	SEC105
Droit, enjeux de sécurité, conformité	SEC103
Analyse de risques des données, réseaux et systèmes	SEC104

1 UE de gestion de la qualité à choisir parmi :

Évaluation de performances et sûreté de fonctionnement	RCP103
ITIL et la gestion des services des systèmes d'information	NFE155
Audit des systèmes d'information	NFE130
Test et Validation du Logiciel	GLG101
Optimisation en informatique	RCP104

1 UE d'ouverture à choisir parmi :

Urbanisation et Architecture des Systèmes d'Information	NFE107
Ingénierie des processus et systèmes d'information	NFE109
Réseaux mobiles et sans fil	RSX116
Systèmes et applications répartis pour le cloud	SMB111

12 crédits à choisir parmi :

Conception et facilitation d’ateliers collaboratifs	CCE208
Droit du numérique	DNT104
Management de projet	GDN100
Coaching et dynamiques collaboratives des équipes d'innovation	GDN209
Union européenne : enjeux et grands débats	UEU001
Mondialisation et Union européenne	UEU002
Droit du travail : relations individuelles	DRS101
Organisation du travail et des activités	DSY005
Démarches et outils de l'organisateur	DSY006
Théories & formes des organisations	DSY103
Mercatique I : Les Etudes de marché et les nouveaux enjeux de la Data	ESC101
Management et organisation des entreprises	MSE102
Principes généraux et outils du management d'entreprise	MSE146
Management social et humain	TET101
Management d'équipe et communication en entreprise	TET102

Test anglais	UA2B40
Expérience professionnelle et rapport d'activité	UAAL0V

Blocs de compétences

Code, N° et intitulé du bloc	Liste de compétences
CPN84B43 RNCP15253BC04 Concevoir un composant utilisable dans l'infrastructure de sécurité d'un SI d'une entreprise (Concevoir un composant utilisable dans l'infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise)	- Capturer des exigences métiers, les traduire en un ensemble cohérent d'exigences fonctionnelles et non-fonctionnelles, les formaliser - Participer à la rédaction d'un cahier des charges - Analyser un cahier des charges et proposer des solutions techniques - Elaborer un document de spécification technique servant d'appui à la mise en œuvre d'un composant du Système d'Information
CPN84B53 RNCP15253BC05 Développer, tester et intégrer un composant utilisable dans l'infrastructure applicative, de sécurité d'un SI d'une entreprise (Développer, tester et intégrer un composant utilisable dans l'infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise)	- Mettre en œuvre une solution technique, associée à un composant du Système d'Information en respectant une spécification - Elaborer des tests et les exécuter - Rédiger un cahier de tests - Intégrer un composant développé dans son environnement d'exploitation - Piloter les phases de développement, de tests et d'intégration
CPN84B63 RNCP15253BC06 Maintenir une infrastructure de sécurité ((option Cybersécurité) : Maintenir en condition opérationnelle une infrastructure de sécurité)	- Rédiger des politiques de sécurité - Mettre en œuvre des politiques de sécurité en installant ou en mettant à jour des équipements et logicielles de sécurité - Administrer des dispositifs de Sécurité Opérationnelle en Services Managés - Mettre en place un processus de supervision avant incident et post-mortem - Résoudre des incidents de sécurité
CPN84B70 RNCP15253BC07 Qualifier l'infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise	- Conduire une analyse des risques informatiques - Définir et rédiger les protocoles de validation informatique pour la qualification d'un composant du Système d'Information - Coordonner les essais décrits dans les protocoles de validation et de qualification - Investiguer sur les déviations - Proposer et exécuter les mesures correctives - Rédiger les rapports de qualification