DIPLÔME

Titre RNCP Niveau 6 Concepteur intégrateur d'infrastructures informatiques (systèmes et réseaux, applicatives, ou de sécurité) parcours Cybersécurité

Code : CRN0803A



Niveau d'entrée : Bac + 2
Niveau de sortie : Bac + 3, Bac + 4
ECTS : 120
Diplôme national
Oui

Déployabilité
Apprentissage : Fomation pouvant se suivre en apprentissage
A la carte : Formation pouvant s'effectuer au rythme de l'élève, en s'inscrivant aux unités du cursus
Package : Formation pouvant se suivre en s'inscrivant à un "package" (groupe d'enseignements indissociables)
Contrat de professionnalisation : Formation pouvant se suivre en contrat de professionnalisation

Objectifs pédagogiques

Ce titre de concepteur en architecture informatique option cybersécurité vise à développer la capacité de concevoir, 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, 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 associées aux compétences de base,
- de suivre l'enseignement d'anglais très tôt dans le parcours.

Remarques :

- Toute personne ayant validé SEC104, SEC106 ou SEC107 avant octobre 2026 conserve ces crédits au titre des UE de cybersécurité avancée.
- Toute personne ayant validé SEC103 avant octobre 2026 conserve ces 6 crédits au titre des 12 crédits à choisir parmi le bloc proposant au choix CCE208, DNT104, GDN100, GDN209, ..., STA101
- SEC101 sera retirée du cursus à partir de septembre 2027.
- L'auditeur souhaitant obtenir une dérogation devra passer par la VES.

Passerelles :
vers le Master Sécurité informatique, cybersécurité et cybermenaces

- Pour l'année académique 2026-2027, le candidat qui souhaite poursuivre son cursus en Master devra avoir choisi et validé les UE suivantes dans chaque bloc :
  - dans les blocs d'UE cybersécurité, choisir RSX112 et CYB105
  - dans le premier bloc « 1 UE d'ouverture », choisir NFE115
  - dans le bloc « 1 UE de gestion de la qualité », choisir RCP103, RCP104 ou NFP101
  - dans le second bloc « 1 UE d'ouverture », choisir RSX103 ou SMB111
  - dans le bloc « 12 crédits », DNT104 est conseillé sans être obligatoire

vers le diplôme Ingénieur informatique, parcours cybersécurité

- Pour l'année académique 2026-2027, le candidat qui souhaite poursuivre son cursus en diplôme ingénieur devra avoir choisi et validé les UE suivantes dans chaque bloc :
  - dans les blocs d'UE cybersécurité, choisir RSX112 et CYB108
  - dans le premier bloc « 1 UE d'ouverture », choisir RCP105, RCP101, SMB101, NFP107, NFE114, NFE108, NSY103 ou GLG105
  - dans le bloc « 12 crédits », DNT104 et GDN100 sont conseillés sans être obligatoires

Compétences et débouchés

- 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

Méthodes pédagogiques

Les enseignements théoriques, couplés à des mises en application en travaux dirigés et travaux pratiques sur matériels et logiciels métiers permettront une professionnalisation rapide. L'espace numérique de formation du Cnam (Moodle) permet à chaque enseignant de rendre accessible des ressources spécifiques à ses enseignements. Des modalités plus détaillées seront communiquées au début de chaque cours.

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 : voir les deux procédures.
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.**

Prérequis et 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, au choix :

- les deux unités d'enseignement NFA031 (Programmation avec Java : notions de base) et NFA032 (Programmation Java : programmation objet)
- ou les deux unités d'enseignement NFP135 (Valeur d'Accueil et de Reconversion en Informatique 1) et NFP136 (Valeur d'Accueil et de Reconversion en Informatique 2), mais qui ne sont plus programmées à partir de septembre 2025.

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.

MENTIONS OFFICIELLES

Code RNCP
38461

Date d'enregistrement au RNCP
21/12/2023

Date de l'échéance de l'enregistrement au RNCP
21/12/2028

Mots-clés

- Réseaux et télécommunications
- Informatique - Réseaux informatiques
- Réseaux informatiques
- Transmission des données
- Réseau de télécommunications
- Politique de sécurité
- Conduite de projet informatique
- sécurisation du poste de travail
- Cryptographie
- Protocoles sécurisés
- Sécurité de l'information
- sécurité des systèmes d'informations
- Gestion des risques des systèmes d'information

Cybersécurité

Architecture client-Serveur

Protocole TCP/IP

Internet

Informations complémentaires

Type de diplôme

Titre RNCP Niveau 6 (ex niveau II)

Code NSF

326 - Informatique, traitement de l'information, réseaux de transmission
326n - Analyse informatique, conception d'architecture de réseaux
326u - Exploitation informatique

Codes ROME

Responsable sécurité informatique[M1802]
Opérateur / Opératrice en cybersécurité[M1810]
Analyste en cybersécurité[M1805]
Ingénieur / Ingénieure sécurité web[M1802]
Ingénieur / Ingénieure sécurité informatique[M1802]
Expert / Experte sécurité, méthode et qualité informatique[M1802]
Expert / Experte sécurité informatique[M1802]
Expert / Experte en sécurité des systèmes d'exploitation[M1802]
Administrateur / Administratrice sécurité 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]
Auditeur / Auditrice en sécurité des systèmes d'information[M1802]
Architecte de sécurité des systèmes d'information[M1802]
Analyste en vulnérabilité de code logiciel[M1802]
Expert / Experte en cybersécurité[M1802]
Administrateur / Administratrice système informatique[M1801]

Formacode

Protocole télécommunication [24237]
Informatique - Systèmes d’information et numérique [31054]
Réseau informatique [24231]
Cybersécurité [31045]
Sécurité télécommunication [24293]
Logiciel cybersécurité [73054]
Sécurité informatique [31006]
ITIL [31048]

Code du parcours

CRN0803

Modules d'enseignement

- Analyse des données : méthodes descriptives
- Anglais général pour débutants
- Anglais professionnel
- Applications réparties
- Architecture d'Entreprise et Urbanisation des Systèmes d'Information
- Architectures des systèmes informatiques
- Audit des systèmes d'information
- Coaching et dynamiques collaboratives des équipes d'innovation
- Conception et facilitation d'ateliers collaboratifs
- Conception et urbanisation de services réseau
- Conduite d'un projet informatique
- Contrôle d'accès et Gestion des identités numériques
- Cybersécurité : référentiel, objectifs et déploiement
- Démarches et outils de l'organisateur
- Droit du numérique
- Droit du travail : relations individuelles
- Durcissement et mise en œuvre de mesures de sécurité avancées pour les données, les réseaux et les systèmes (Hardening)
- Évaluation de performances
- Expérience professionnelle et rapport d'activité
- Génie Logiciel et Architecture Cloud Native
- Ingénierie des processus et systèmes d'information
- Introduction à la cyberstructure de l'internet : réseaux et sécurité
- Introduction à la gestion de données à large échelle
- ITIL et la gestion des services des systèmes d'information
- Linux : principes et programmation
- Management d'équipe et communication en entreprise
- Management de projet
- Management et organisation des entreprises
- Management social et humain
- Menaces informatiques et codes malveillants : analyse et lutte
- Mercatique I : Les Etudes de marché et les nouveaux enjeux de la Data à l'heure de l'IA
- Méthodologies des systèmes d'information
- Modélisation, optimisation, complexité et algorithmes
- Mondialisation et Union européenne
- Optimisation en informatique
- Organisation du travail et des activités
- Outils mathématiques pour Informatique
- Paradigmes de programmation
- Principes fondamentaux des Systèmes d'exploitation
- Programmation avancée
- Programmation Fonctionnelle : des concepts aux applications web
- Programmation orientée objet en Python, Java et autres
- Recherche opérationnelle et aide à la décision
- Réseaux et protocoles pour l'Internet
- Réseaux mobiles et sans fil
- Sécurité des réseaux
- Systèmes d'exploitation : principes, programmation et virtualisation
- Systèmes d'Information et Bases de Données
- Systèmes d'information web
- Systèmes de gestion de bases de données
- Systèmes et applications répartis pour le cloud
- Technologies pour les applications en réseau : contribution au profil NetDevOps
- Test anglais
- Test et Validation du Logiciel
- Théories & formes des organisations
- Union européenne : enjeux et grands débats

Blocs de compétences

Un bloc de compétences est constitué d'un ensemble d'Unités qui répond aux besoins en formation de l'intitulé du bloc.

Les unités ci-dessus sont réparties dans les Blocs de compétences ci-dessous.
Chaque bloc de compétences peut être validé séparément.

Concevoir un composant informatique utilisable dans l'infrastructure applicative, système, technique ou de la sécurité d'un Système d'Information d'une entreprise
CRN08B10

Développer, tester et intégrer un composant informatique dans l'infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise
CRN08B20

Analyser et qualifier l'infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise
CRN08B30

Maintenir les conditions de sécurité d'un système d'information et de son infrastructure de sécurité
CRN08B63

Analyser, organiser et piloter des projets informatiques de développement d'une infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise.
CRN08B70