

Mastère Expert en Architectures, Systèmes, Réseaux et Sécurité Informatique

Titre professionnel de Niveau 7 (équivalent Bac +5) inscrit au RNCP

Le Mastère Expert en architectures, systèmes, réseaux et sécurité informatique (EASI) forme des spécialistes capables de concevoir, déployer et sécuriser des infrastructures complexes, en intégrant les technologies de pointe et les bonnes pratiques de cybersécurité pour garantir la performance, la résilience et la protection des systèmes d'information des entreprises.

Durée de la formation & Rythme

- 987 h sur 24 mois
- Rythme : 2 jours/semaine à l'école

Modalités et moyens pédagogiques

- Présentiel / Salle de formation équipée de télé-connectée
- Méthode active, exercices pratiques, mise en situation, évaluations

Public

- Etudiants, demandeurs d'emploi, personnes en reconversion...

Pré-requis

- Niveau Bac+3/4 en informatique ou expérience équivalente
- Expérience dans le développement et/ou l'administration d'infrastructures informatiques
- Aptitudes relationnelles, rédactionnelles et techniques
- Maîtrise de l'anglais technique

Voies d'accès

- Alternance / Formation continue ou initiale

Modalités d'évaluation

- Contrôle continu
- Projets pratiques
- Évaluations en cours de formation (ECF)
- Examen final devant un jury professionnel

Objectifs de la formation

- Planifier et organiser des projets d'architecture systèmes et réseaux
- Développer des solutions d'infrastructure systèmes et réseaux
- Piloter la sécurité de l'infrastructure informatique

Programme Année 1

TRONC COMMUN

- Agile et Dev Ops
 - Introduction à la cybersécurité et e-reputation
 - Méthode Agile
 - Docker et Conteneurisation – Orchestration
 - DevOps CI/CD
 - Modélisation : BPMN
 - Architecture Web
 - Projet Start Up Agile et DevOps
- Architecture et sécurité du SI
 - Modèle OSI
 - ISO27001

PARTIE RESEAUX / CYBERSECURITE

- Réseaux
 - Architecture des réseaux
 - Architecture des réseaux Cloud Azure
 - Gestion des incidents
 - Qualité de Service Informatique et KPI
- Cybersécurité
 - Sécurité Réseaux
 - Cryptographie
 - Ethical Hacking
 - Sécurité des Systèmes d'Informations
 - Analyse des Vulnérabilités
 - Introduction Blue Team /Red Team
 - Sécurité des Applications Web
 - Principes Blue Team / Red Team
 - Projet Réseaux et Cyber

Programme Année 2

TRONC COMMUN

- *Introduction au Big Data*
- *Veille réglementaire*
 - *Veille technologique*
 - *RGPD / DPD*
- *Gestion de projets et d'équipe*
 - *Gestion de projet*
 - *Management d'équipe*
 - *Rédiger et répondre à un appel d'offre*
- *Architecture et direction des SI*
 - *Urbanisation des SI*
 - *Industrialisation des SI*
 - *Haute Disponibilité*
 - *Evaluation des risques et PCA/PRA*
 - *Green IT*
- *Innovation*
 - *Comprendre les enjeux du Web 3*
 - *Réalité Augmentée /VR*
 - *Block Chain et Cryptomonnaie*

PROJET TRANSVERSE ET PREPARATION A LA SOUTENANCE

PARTIE RESEAUX/ CYBERSECURITE

- Sécurité IoT
- Sécurité Cloud
- Sécurité Mobile
- Pentesting Avancé
- Sécurité des Infrastructures Critiques
- Forensic Informatique
- Python et Scripting

Certificateur

INGETIS

RNCP 38823

Date d'enregistrement : 27/03/2024

Date de validité : 27/03/2028

Débouchés métiers

- Ingénieur système et réseaux
- Ingénieur cybersécurité
- Ingénieur sûreté et réseaux, Ingénieur sûreté, réseaux et télécoms IT Manager en cybersécurité,
- Ingénieur des systèmes d'information (ERP/Infrastructure), Ingénieur de maintenance informatique, Ingénieur informatique,
- Ingénieur DevOps, Consultant ingénieur DevOps, DevOps

Compétences développées

Savoir-faire

- Analyser les besoins et exigences des clients
- Concevoir des architectures réseaux innovantes
- Piloter la maîtrise d'ouvrage de projets informatiques
- Gérer des projets internationaux
- Concevoir et déployer des architectures systèmes et réseaux sécurisées
- Optimiser les performances des réseaux et systèmes
- Élaborer des stratégies de gestion des solutions informatiques
- Superviser le déploiement et l'amélioration des infrastructures
- Élaborer la stratégie de sécurisation de l'infrastructure
- Concevoir et mettre en service des infrastructures de cybersécurité
- Gérer la gouvernance de la sécurité des réseaux et systèmes d'information
- Anticiper, gérer et remédier aux incidents et crises de cybersécurité

Savoir-être

- Capacité à travailler en équipe
- Adaptabilité face aux évolutions technologiques
- Rigueur et organisation
- Autonomie et capacité d'auto-apprentissage
- Gestion du stress
- Maîtrise de l'anglais professionnel

UNLEARN s'engage à respecter pleinement les dispositions légales et réglementaires en matière d'accueil et de formation des personnes en situation de handicap. Conformément à la loi du 11 février 2005 pour l'égalité des droits et des chances, nous mettons en œuvre une politique d'inclusion visant à garantir l'accessibilité de nos formations à tous. Cela comprend l'aménagement des locaux, l'adaptation des supports pédagogiques, et la mise en place de dispositifs d'accompagnement personnalisés. Notre référent handicap est chargé de coordonner les actions nécessaires, d'assurer le suivi des apprenants concernés et de sensibiliser l'ensemble du personnel aux enjeux de l'inclusion. Nous collaborons étroitement avec les acteurs institutionnels et les entreprises partenaires pour faciliter l'insertion professionnelle des apprentis en situation de handicap