EASRSI
EXPERT EN ARCHITECTURES SYSTEMES-RESEAUX ET EN SECURITE INFORMATIQUE

Formation menant à la certification Expert en Architectures systèmes-réseaux et en Sécurité Informatique, Titre de niveau 7 - RNCP36296 enregistré au Répertoire National des Certifications Professionnelles par décision du directeur général de France Compétences en date du 25/03/2022 délivré sous l'autorité ANAPIJ

OBJECTIFS

Le développement de solutions informatiques implique de nombreux risques pour les systèmes d'informations. Ainsi, l'optimisation des environnements nécessaires à la conception et au déploiement de solutions informatiques implique également d'entrevoir les risques et les failles potentielles liées à la sécurité et la protection des systèmes et des réseaux.

Dans ce contexte, les besoins en recrutement dans la filière informatique ont évolué, et parmi les compétences recherchées peuvent être mentionnées la définition de la stratégie et la supervision de la sécurité des systèmes d'informations, ou encore la connaissance et l'intégration des normes de sécurité et de conformité, mais également, le besoin d'expert sachant rationnaliser les coûts et optimiser les ressources à allouer aux infrastructures informatiques.

COMPÉTENCES DÉVELOPPÉES

- Analyser et concevoir les infrastructures répondant à des besoins identifiés
- Manager les projets du système d'information
- Superviser le déploiement et l'amélioration des infrastructures
- Identifier les risques et définir la politique de sécurité du système d'information

DÉBOUCHÉS PROFESSIONNELS

- Architecte des systèmes d'information / Ingénieur·e Systèmes et réseaux
- Architecte systèmes et réseaux / Ingénieur·e réseaux et sécurité
- Consultant·e en sécurité informatique / Architecte Cloud
- Architecte sécurité / Consultant·e cybersécurité
- Consultant·e en sécurité des systèmes d'information
- Directeur·rice des services informatiques
- Consultant·e sécurité informatique

TAUX D'INSERTION

87.5% de la promotion 2022-2024 étaient en emploi dans l'année suivant l'obtention de leur

certification dont 86% dans l’emploi visé.

PUBLICS ET PRÉREQUIS

Niveau requis : Cette formation est ouverte à tous les titulaires d'une certification de niveau 6 ou ayant validé une 3e année dans l'enseignement supérieur (180 ECTS) dans le domaine de l'informatique et/ou du numérique (BAC +3 en Sécurité Informatique / Cybersécurité)

Qualités attendues : Esprit logique et rigoureux, grande faculté d'adaptation, aptitude à tenir à jour ses connaissances et à suivre les évolutions technologiques, aptitude à la relation humaine et à la communication interpersonnelle.

ACCESSIBILITÉ

Pour l'accès à la formation, une rencontre avec le référent handicap permettra d'évaluer les possibilités d'adaptation : prise de contact alternance@groupe-saintjean.fr. Les locaux sont accessibles aux personnes à mobilité réduite.

MODALITÉS D'ACCÈS ET PROCÉDURE D'ADMISSION

L'admission ne peut être valide qu'à la signature du contrat d'apprentissage ou de professionnalisation avec l'entreprise d'accueil. Elle se déroule en 2 temps :

- 1- Candidater en ligne sur notre site Le dossier de candidature (téléchargeable sur notre site est à compléter et à nous retourner ;
- 2- Après une session de tests écrits, un entretien de motivation avec un membre de l'équipe pédagogique vous sera proposé.

Les candidatures sont ouvertes de début décembre à mi-juillet dans la limite des places disponibles.

VALIDATION

La validation de l'ensemble des blocs de compétences permet la délivrance de la certification.

En cas de validation partielle, l'obtention de chaque bloc de compétences fait l'objet de la délivrance d'une attestation de compétences.

La mise en pratique en entreprise est une condition sine qua non pour garantir l'aptitude à mettre en œuvre les compétences acquises en formation : un minimum de 130 jours est attendu.

La formation octroie un niveau 7 (Bac+5).

RÉSULTATS ET TAUX DE SATISFACTION

Résultats : Lors de la session 2025, le taux d'obtention de ce titre au CFA de La Salle a été de 100%.

Taux de satisfaction : Nous nous engageons à évaluer le taux de satisfaction de nos alternants à la fin de chaque cycle.

100 % des alternants de la promotions 2023/2025 sont satisfaits ou très satisfaits de la formation.

DURÉE ET RYTHME

Cette formation est dispensée sous contrat d'apprentissage ou de professionnalisation.

Durée : Le contrat est de 2 ans. Chaque année scolaire, les cours sont répartis sur 10 mois, de septembre à juin. 1 120 heures de cours sont dispensées sur les deux années.

Rythme : Le rythme de l'alternance est de 1 semaine en centre de formation, 2 à 3 semaines en entreprise.

COÛT

Le coût de la formation est pris en charge par l'OPCO et l'entreprise, l'alternant n'avance aucun frais.

MODALITÉS

- 90 % des cours sont assurés par des professionnels de la cybersécurité
- Les cours sont dispensés en petits groupes
- Un accompagnement individualisé et personnalisé est assuré
- La formation se tient en présentiel

Moyens pédagogiques

- Cours
- Mini-projets
- Projet annuel
- E-learning

Moyens techniques

- Accès wifi dans tout l'établissement
- Laboratoires réseaux (équipement Cisco)
- CyberRange Airbus - Simulateur Cyberdéfense
- Centre de ressources documentaires...

PROGRAMME

Analyser et concevoir les infrastructures répondant à des besoins identifiés

- CCNA Security
- Gouvernance SI
- Linux, administration système et réseau avancée
- Programmation système et réseaux sous Linux
- Sécurité avancée des systèmes - PKI
- Sécurité avancée des réseaux
- Sécurité des Accès Windows
- Sécurité offensive
- Linux sécurité avancée

Manager les projets du système d'information

- Gouvernance SI
- Linux, administration système et réseau avancée
- Management de projets SI
- Marketing de l'IT
- Droit, éthique et cybercriminalité
- Management d'équipe
- Anglais

Superviser le déploiement et l'amélioration des infrastructures

- Forensic
- Analyse avancée des vulnérabilités
- Linux, administration système et réseau avancée
- Programmation système et réseaux sous Linux

Identifier les risques et définir la politique de sécurité du système informatique

- Forensic
- Analyse avancée des vulnérabilités
- CCNA Security
- Cryptographie avancée
- IDS/IPS
- Pentest Android
- Rétro-ingénierie
- Sécurité Python
- Sécurité des IOT
- Audit et test d'intrusion
- Exploitation de binaires
- RedTeam/NFC
- Sécurité des Accès Windows
- Network Forensic
- Sécurité offensive
- Sécurité RFID et Radio
- Operationnal Technology (OT)
- Linux sécurité avancée LPIC 303
- OSCP
- Hackathon Challenge CTF

ÉVALUATIONS

Des évaluations dans chaque module permettent de se situer dans ses apprentissages. Elles peuvent revêtir la forme de QCM ou TP noté ou Oraux.

La validation du titre prévoit le passage d'épreuves certifiantes, selon les modalités d'évaluation inscrites au référentiel : mises en situations professionnelles, étude de cas…

PARTENARIATS ET CERTIFICATIONS