TP - Administrateur d'infrastructures sécurisées

Formation Cybersécurité, Formation Systèmes & Réseaux informatiques

29/05/2026

RÉSUMÉ

Le parcours de formation Administrateur d'Infrastructures Sécurisées (AIS) permet d'acquérir l'ensemble des compétences nécessaires pour administrer, sécuriser et faire évoluer des infrastructures informatiques et cloud, tout en intégrant les enjeux majeurs de cybersécurité, de continuité de service et de conformité réglementaire.
À l'issue de la formation, le candidat est préparé à la certification du Titre Professionnel AIS (RNCP – Niveau 6) délivrée par le ministère du Travail.

CODE RNCP

37680

CENTRES DE FORMATION

Le Mans

ACCUEIL PSH

Formation ouverte aux personnes en situation de handicap. Moyens de compensation à étudier avec le référent handicap du centre concerné.

PUBLIC ET PRÉREQUIS

Niveau Bac +2 en informatique (ou expérience professionnelle équivalente)

Connaissances de base en systèmes, réseaux et environnement informatique

Appétence pour la cybersécurité et les infrastructures IT

LES OBJECTIFS PÉDAGOGIQUES ET PROFESSIONNELS

Le Titre Professionnel Administrateur d'Infrastructures Sécurisées (AIS) forme des professionnels capables de :

- Administrer et sécuriser des infrastructures systèmes, réseaux et virtualisées (on-premise et cloud)
- Concevoir et déployer des solutions techniques répondant à des besoins d'évolution
- Participer activement à la gestion de la cybersécurité (prévention, détection, réaction)
- Assurer le maintien en conditions opérationnelles (MCO) et de sécurité (MCS)
- Communiquer efficacement dans un contexte professionnel, en français et en anglais technique

Le diplômé intervient sur l'ensemble du cycle de vie des infrastructures numériques : exploitation, évolution, sécurisation et supervision.

OUTILS PÉDAGOGIQUES

Formation en présentiel, avec alternance d'apports théoriques et de mises en situation pratiques

Possibilité de modules en distanciel selon l'organisation du parcours

- Formation en présentiel :
  Salles de formation équipées pour utilisation de supports pédagogiques classiques et numériques. Plateaux techniques adaptés et
  aménagés d'équipements spécifiques

Les + Fab'Academy

• + de 1400 Jeunes formés en apprentissage chaque année
• + de 5300 salariés accompagnés en formation continue
• + de 1720 entreprises nous font confiance (TPE, PME, groupes industriels)
• Diplômes reconnus par l'Etat

• Pédagogie innovante (par projets, en îlots, parcours individualisés...)
• Equipement en machines modernes qui préparent aux métiers de demain
• 7 implantations en Pays de la Loire avec des campus neufs et modernes
• 24000m² de plateaux techniques et performants (outils numériques, cellules robotisées...)

MODALITÉ D'ÉVALUATION

Modalités d'évaluation et d'examen du Titre Professionnel : Les connaissances et/ou capacités professionnelles de l'apprenant sont évaluées en cours de formation par différents moyens : mises en situations, études de cas, QCM. En fin de formation, les compétences sont évaluées par un jury à l'occasion, d'une mise en situation professionnelle, de l'analyse du dossier professionnel et d'un entretien final. Le Titre professionnel sera obtenu après validation de l'ensemble des compétences

MODALITÉS D'ACCÈS

6 mois

CONTENU DE LA FORMATION

Bloc 1 – Administrer et sécuriser les infrastructures
Bonnes pratiques d'administration des infrastructures
Administration et sécurisation des réseaux (LAN, WAN, VPN, Wi-Fi, pare-feu)
Administration et sécurisation des systèmes (Windows, Linux, services d'infrastructure)
Infrastructures virtualisées et cloud (on-premise, IaaS, PaaS, SaaS)
Sauvegardes, PRA / PCA / PRI / PCI
Supervision, performance et disponibilité

Bloc 2 – Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution
Analyse d'un besoin d'évolution technique
Conception de solutions sécurisées (Security by Design)
Environnements de test et validation
Mise en production des évolutions
Supervision avancée et tableaux de bord
Gestion de projet technique (classique et agile)

Bloc 3 – Participer à la gestion de la cybersécurité
Analyse des risques (EBIOS, ISO 27005)
Mesure et évaluation du niveau de sécurité
Politique de sécurité du SI (PSSI)
Détection et traitement des incidents de sécurité
Outils de cybersécurité : IDS/IPS, EDR, SIEM, XDR
Sensibilisation des utilisateurs et veille cyber

Compétences transversales
Communication professionnelle en français et en anglais technique
Apprentissage continu et veille technologique

EQUIVALENCE

Licences professionnelles :
Administration systèmes et réseaux
Infrastructures, cloud et cybersécurité
Réseaux et télécommunications (parcours systèmes)

SUITE DE PARCOURS ET PASSERELLES POSSIBLES

Licences professionnelles (systèmes, réseaux, cybersécurité)
Bachelors informatiques
Écoles d'ingénieurs (admissions parallèles)

Certifications complémentaires cybersécurité (ISO 27001, cloud, sécurité réseau)

MÉTIERS - DÉBOUCHÉS

Administrateur systèmes et réseaux
Administrateur infrastructures et cloud
Administrateur cybersécurité
Technicien systèmes et réseaux confirmé
Responsable infrastructure junior

VALIDATION ET CERTIFICATION

Titre Professionnel