









24 avenue Léon Gourdault
94600 Choisy le Roi
06 12 57 07 19
www.arimayi.fr

Administrateur d'infrastructures sécurisées RNCP 37680 – niveau 6 – 01352m02

-  Date de session : 02/02/2026
-  Code session : AIS-RNCP6-006
-  Modalité : Hybride (60% classe virtuelle / 40% présentiel)
-  Durée : 525h sur 4 mois en **intensif** ou 1050h sur 8 mois en **progressif**
-  Public : Tout public – 10 participants maximum
-  Tarif : 5 499 € HT / 6 600 € TTC (4 mois) ou 9 999 € HT / 11 999 € TTC par participant

Description

La formation AIS permet d'acquérir les compétences essentielles pour administrer, sécuriser et faire évoluer des infrastructures informatiques locales, virtualisées et cloud. Elle prépare aux enjeux actuels des systèmes d'information : cybersécurité, supervision, continuité de service et évolutions technologiques.

Le participant apprend à déployer, maintenir, sécuriser et superviser une infrastructure complète, puis à contribuer activement à la politique de cybersécurité de l'organisation.

Profil des participants

Cette formation s'adresse aux techniciens, administrateurs débutants, alternants, reconversions IT, ou professionnels souhaitant évoluer vers l'administration d'infrastructures sécurisées et la cybersécurité.

Pré-requis

- Connaissances de base en systèmes (Windows/Linux) et réseaux
- Aisance avec l'environnement informatique professionnel
- Une première expérience technique (support, helpdesk, technicien) est un plus

Objectifs

Former des spécialistes capables d'administrer et sécuriser des infrastructures hybrides (réseaux, systèmes, virtualisation, cloud) tout en appliquant les bonnes pratiques de cybersécurité.

Préparer les apprenants à concevoir, déployer, superviser et faire évoluer une infrastructure dans un contexte professionnel exigeant.



24 avenue Léon Gourdault
94600 Choisy le Roi
06 12 57 07 19
www.arimayi.fr

Aptitudes et compétences visées/attestées

- Administrer et sécuriser des infrastructures réseaux, systèmes et virtualisées
- Déployer et mettre en production des solutions techniques d'évolution
- Mettre en œuvre et optimiser une supervision complète (KPIs, alertes, logs)
- Participer à la gestion opérationnelle de la cybersécurité (analyse, détection, réaction)
- Formaliser, documenter et présenter une solution technique
- Appliquer les bonnes pratiques opérationnelles (résolution incidents, maintenance, sécurité)

Contenu pédagogique

Bloc 1 : Administrer et sécuriser les infrastructures

Objectif pédagogique : Maîtriser l'administration quotidienne des infrastructures réseaux, systèmes et virtualisées, tout en appliquant les bonnes pratiques de sécurité.

Activités pédagogiques :

- Configuration et sécurisation des réseaux : VLAN, routage, firewall
- Administration Windows Server & Linux (AD, DNS, DHCP, partage, permissions)
- Gestion des plateformes virtualisées (VMware/Hyper-V, snapshots, HA)
- Sécurisation des services : durcissement, mises à jour, règles de sécurité
- Gestion des incidents et support N2/N3
- Mise en pratique via ateliers d'administration complets

Bloc 2 : Concevoir et mettre en œuvre une solution

Objectif pédagogique : Être capable de concevoir, documenter et déployer une solution technique en réponse à un besoin métier ou infrastructurel.

Activités pédagogiques :

- Analyse du besoin, rédaction des spécifications techniques
- Choix et justification des solutions (coûts, contraintes, sécurité)
- Mise en place d'environnements de test
- Intégration d'évolutions dans l'infrastructure
- Validation fonctionnelle et sécurité
- Mise en production sécurisée et documentée
- Soutenance et présentation de la solution proposée

Bloc 3 : Superviser, mesurer, analyser la sécurité

Objectif pédagogique : Installer et optimiser un dispositif de supervision, mesurer la performance et évaluer le niveau de sécurité de l'infrastructure.

Activités pédagogiques :

- Mise en œuvre d'outils de supervision (Zabbix, Centreon, Grafana...)
- Collecte et analyse d'événements, logs, métriques
- Suivi des performances, disponibilité, montée en charge
- Définition des seuils, alertes, tableaux de bord
- Réalisation d'audits internes : vulnérabilités, configurations, conformité
- Mise en place d'indicateurs de sécurité (SIEM / journaux)

Bloc 4 : Participer à la gestion de la cybersécurité

Objectif pédagogique : Contribuer activement à la détection, prévention et réponse aux incidents de sécurité.

Activités pédagogiques :

- Identification des menaces et vulnérabilités
- Utilisation d'outils de détection (IDS, antivirus, EDR, journaux événements)
- Traitement d'incidents : méthodologie, analyse, actions correctives
- Participation à la politique de sécurité : procédures, sensibilisation, PRA/PCI
- Application des bonnes pratiques ANSSI (Durcissement, hygiène informatique)
- Études de cas : simulations d'incidents & analyse post-mortem

Pédagogie et organisation

- Apprentissage par la pratique : ateliers, labs, mises en situation réelles
- Encadrement expert : formateurs issus du terrain (systèmes, réseau, cloud, cybersécurité)
- Suivi individualisé : coaching, corrections techniques, accompagnement
- Supports complets : documentation, fiches pratiques, outils professionnels
- Évaluations continues + projet final (conforme aux exigences du titre pro)

Positionnement et modalités d'évaluation des acquis

Compétence visée	Modalités d'évaluation	Critères d'évaluation
Administrer et sécuriser des infrastructures réseaux, systèmes et virtualisées	Mises en situation + TP d'administration	Configuration correcte, sécurisation conforme, diagnostics pertinents, respect des bonnes pratiques d'exploitation
Concevoir et mettre en œuvre une solution d'évolution de l'infrastructure	Étude de cas + mini-projet documentaire	Cohérence technique, justification du choix des solutions, prise en compte des contraintes métier, qualité de la documentation
Superviser l'infrastructure et analyser le niveau de sécurité	TP supervision + analyse de logs	Pertinence des indicateurs, qualité des tableaux de bord, capacité à interpréter des événements et détecter anomalies ou risques
Participer à la gestion de la cybersécurité et au traitement des incidents	Mise en situation d'incident + restitution	Identification correcte de l'incident, actions adaptées, respect des procédures sécurité, qualité de l'analyse post-incident

Mode de validation

Titre professionnel de niveau 6 (Bac +3/4) délivré par le Ministère du Travail, obtenu par blocs de compétences.

Modalités et délai d'accès

- Entrée possible tout au long de l'année
- Dossier de candidature + entretien de motivation
- Réponse sous 7 jours après étude du dossier

Référent handicap

Samir Bedouhene – samir.bedouhene@arimayi.fr – 06 12 59 07 17