



Classe Préparatoire

Votre tremplin vers AIS et ISRC !



Pour permettre aux étudiants titulaires d'un diplôme BAC+2 en informatique ou d'un titre professionnel de niveau 5 de poursuivre leurs études, l'Association des Neticiens ouvre dès la rentrée 2026 sa Classe Préparatoire.

Cette formation intensive de 240h est délivrée à distance en visioconférences synchrones par nos enseignants et enseignants-chercheurs. La formation peut être suivie de n'importe où en France ou à l'étranger. Elle a pour but d'offrir une mise à niveau permettant aux étudiants de pouvoir intégrer, dès la rentrée suivante, notre formation en alternance AIS (Administrateur Infrastructures Réseaux - titre professionnel de niveau 6- équivalent Bac+4), puis la formation en alternance ISRC (Ingénieur Sécurité Réseau et Cybersécurité - titre professionnel de niveau 7 - équivalent Bac+5) ou encore d'accéder à une Ecole d'Ingénieurs.

Programme

Bloc 1 – Administration avancée des réseaux d'entreprise (40 h)

Compétences visées :

- Concevoir et segmenter un réseau (VLAN, routage inter-VLAN, OSPF).
- Mettre en œuvre une supervision et diagnostiquer des incidents.

Module	Contenus principaux	Compétences Opérationnelles	Durée
1.1 Réseaux LAN avancés	VLAN, trunking, routage inter-VLAN, OSPF, RIP, redistribution statique/dynamique	Configurer des VLAN et du routage dynamique ; sécuriser le LAN ; documenter la topologie.	20h
1.2 Supervision et diagnostic	SNMP, Syslog, NetFlow, Wireshark, SolarWinds	Mettre en place SNMP, Syslog, NetFlow ; analyser des flux et incidents ; interpréter des logs	20h

Bloc 2 – Virtualisation et infrastructures serveurs (40 h)

Compétences visées :

- Installer, paramétrer et administrer un environnement virtualisé.
- Mettre en œuvre des solutions de stockage et d'hébergement Cloud privé.

Module	Contenus principaux	Compétences Opérationnelles	Durée
2.1 Virtualisation des serveurs	VMware ESXi / Proxmox / Hyper-V, snapshots, migration, HA	Déployer des hyperviseurs ; créer des VM ; configurer la haute disponibilité.	20h
2.2 Stockage et Cloud privé	NAS/SAN, RAID, vSAN, OpenStack, principes du Cloud privé	Concevoir des architectures NAS/SAN ; gérer RAID, sauvegardes ; déployer OpenStack/vSphere.	20h

Bloc 3 – Sécurité des infrastructures (50 h)

Compétences visées :

- Sécuriser les réseaux et les systèmes.
- Mettre en conformité le SI (RGPD, ISO 27001).
- Réaliser une analyse de vulnérabilités.

Module	Contenus principaux	Compétences Opérationnelles	Durée
3.1 Sécurisation des réseaux	Firewall (pfSense, Fortigate), VLAN sécurisés, ACL, IDS/IPS	Configurer pare-feux, VPN, ACL ; segmenter et isoler des réseaux sensibles.	20h
3.2 Gouvernance et conformité	ISO 27001, RGPD, politique de sauvegarde, PRA/PCA	Évaluer les risques ; définir les politiques de sauvegarde, PRA/PCA ; appliquer RGPD.	15h
3.3 Pentesting et vulnérabilités	Kali Linux, Nmap, Nessus, Metasploit (initiation)	Utiliser Kali Linux, Nmap, Nessus ; identifier et documenter les failles.	15h

Bloc 4 – Automatisation et scripting d'administration (30 h)

Compétences visées :

- Automatiser les tâches récurrentes d'administration.
- Industrialiser les déploiements d'infrastructure.

Module	Contenus principaux	Compétences Opérationnelles	Durée
4.1 PowerShell et Bash	Scripts PowerShell, Bash, tâches planifiées, logs	Écrire des scripts pour la gestion des comptes, des services et des logs.	15h
4.2 Introduction à Ansible et Python	Playbooks, gestion d'inventaire, scripts Python de supervision	Créer des playbooks ; exploiter les API Cisco ; superviser automatiquement des hôtes.	15h

Bloc 5 – Services réseaux et annuaires (40 h)

Compétences visées :

- Gérer les services de base (DNS, DHCP, AD).
- Sécuriser les applications et services Web.

Module	Contenus principaux	Compétences Opérationnelles	Durée
5.1 Active Directory et DNS/DHCP	VMware ESXi / Proxmox / Hyper-V, snapshots, migration, HA	Installer et administrer un domaine ; gérer GPO ; configurer authentification centralisée.	20h
5.2 Services applicatifs et certificats	IIS, Apache, Nginx, SSL/TLS, PKI, certificats, SSO	Déployer IIS/Apache/Nginx ; configurer SSL/TLS ; mettre en œuvre PKI et SSO	20h

Bloc 6 – Gestion de projet et documentation technique (40 h)

Compétences visées :

- Piloter un projet d'infrastructure selon ITIL/Agile.
- Formaliser la documentation technique et les rapports d'incidents.

Module	Contenus principaux	Compétences Opérationnelles	Durée
6.1 Méthodologie ITIL / Agile	ITIL v4, ticketing, gestion du changement, Scrum/Kanban	Gérer incidents et changements ; planifier les livrables ; suivre les tickets.	20h
6.2 Documentation et reporting	Schémas d'archi, fiches d'incident, rapports techniques	Rédiger dossiers d'exploitation, schémas d'architecture ; assurer le reporting.	20h

Valorisation des compétences acquises

Trois leviers complémentaires permettent de valoriser concrètement les compétences acquises

1. Valorisation académique / certificats / badges

Objectif : faire en sorte que les acquis soit pris en compte dans le parcours de l'étudiant.

- Badges Cisco NetAcad : chaque cours (Networking Essentials, Cybersecurity Essentials, Python Essentials 1...) délivre un badge officiel avec lien vérifiable (Credly).
- Micro-certifications ADN internes : attestation signée pour chaque bloc validé (« Virtualisation », « Cybersécurité »...)
- Portfolio de compétences : tableau de correspondance "Compétence/Activité /Preuve" (TP, badge, livrable)
- Reconnaissance RNCP / VAE partielle

2. Valorisation professionnelle

Objectif : rendre les acquis visibles par les entreprises.

- Profil LinkedIn / Europass Skills Passport : intégration automatique des badges NetAcad avec description des compétences.
- Mini-projets documentés : chaque TP final (ex : "Déploiement d'un réseau sécurisé sous pfSense") publié sur GitHub ou Google Drive professionnel.
- Simulation d'entretien technique : l'étudiant présente son projet final (type PRA, infra virtualisée, script Python) comme étude de cas.
- Recommandation ADN : lettre de validation signée du formateur mentionnant les technologies maîtrisées (Cisco, VMware, Windows Server, Python).

3. Valorisation pédagogique interne

Objectif : suivre et prouver la montée en compétence dans la passerelle.

- Grille d'évaluation par compétence (1 – 4) :
1 = découverte ; 2 = application guidée ; 3 = autonomie ; 4 = maîtrise démontrée (TP validé).
- Portfolio numérique : chaque livrable (TP, rapport, capture Packet Tracer, script, vidéo de démo) est ajouté dans un dossier Drive individuel.

- Badge ADN final "Passerelle AIS – Ready for AIS Bac+4" : décerné si 80 % des livrables validés + 4 badges NetAcad obtenus.

Copyright Association des Neticiens 2030