

PLAN DE FORMATION POUR LE TPAIS – GRETA

Bloc 1 : Administrer et sécuriser les infrastructures

1. Introduction au métier d'Administrateur d'Infrastructures Sécurisées

- Présentation du métier, rôle, posture professionnelle
- Environnement de travail hybride (on-premise / cloud)
- Règles d'éthique, confidentialité, RGPD
- Acteurs et interlocuteurs du métier

2. Bonnes pratiques d'administration et maintien en condition opérationnelle (MCO)

- ITIL, ISO 20000
- Supervision, diagnostic, résolution d'incidents
- GLPI, gestion de configuration
- Évaluation de la qualité de service

3. Administration et sécurisation des infrastructures réseaux

- VLAN, VPN, pare-feu, IDS/IPS
- Normes ANSSI
- Sécurisation du réseau local et distant (nomadisme)
- Mise en pratique (projet)

4. Administration et sécurisation des infrastructures systèmes

- Windows, Linux, Unix
- AD, DNS, DHCP, services Microsoft 365
- Gestion des accès, MFA, PKI
- Scripts Bash, PowerShell, Python

5. Administration des infrastructures virtualisées (On-premise et Cloud)

- Hyperviseurs, conteneurs, stockage virtualisé
- AWS, Azure : administration, sécurité, outils
- Sauvegardes VEEAM, restauration
- Infrastructure hybride, migration Cloud

Bloc 2 : Concevoir et mettre en œuvre une solution technique

6. Conception d'une solution technique répondant à un besoin d'évolution

- Cahier des charges, contraintes, sécurité by design
- Veille, benchmarking, prototypage
- Présentation argumentée de solutions techniques

7. Mise en production d'évolutions de l'infrastructure

- Planification projet (mode Agile ou classique)
- PRI/PCI, tests de validation
- Transfert de compétences & documentation

8. Mise en œuvre de la supervision des infrastructures

- Indicateurs de performance, seuils d'alerte
- Outils : Zabbix, Grafana, ELK, Syslog, SNMP
- Construction de tableaux de bord
- Respect du RGPD et des normes ANSSI

Bloc 3 : Participer à la gestion de la cybersécurité

9. Analyse du niveau de sécurité des infrastructures

- Audits de sécurité, tests de vulnérabilité
- Méthodes EBIOS, ISO 27005
- Outils Kali Linux, CVE, scripts d'analyse

10. Politique de sécurité et plan d'action

- PSSI : élaboration, déclinaison opérationnelle
- Sécurisation AD, VPN, postes clients
- Sauvegardes, PRA/PCA
- Sensibilisation et formation utilisateurs

11. Détection et traitement des incidents de sécurité

- SIEM, XDR, SOAR, UEBA
 - Journalisation, forensic, RETEX
 - Plan de réaction à incident
-

? Compétences transversales et professionnelles

12. Communication professionnelle en français et en anglais

- Échange oral et écrit, documentation technique
- Présentations orales, comptes rendus
- Anglais technique (niveau B1 CECRL)

13. Apprentissage en continu et veille technologique

- Suivi de l'actualité tech & cybersécurité
- Plateformes de formation continue
- Communautés professionnelles, RSS, CVE, GitHub

14. Préparation à la certification TP AIS

- Simulations d'épreuves
- Préparation aux évaluations : QCM, projets, mises en situation
- Entretien technique

15.Stage en alternance et intégration en entreprise

- Suivi en entreprise, missions type
- Évaluation en situation professionnelle
- Suivi pédagogique hybride et e-portfolio