

METIERS DU NUMERIQUE

RECRUTER - PROFESSIONNALISER - EVOLUER



Qualification T.S.S.R Cybersécurité

Technicien/ne Sup. Systèmes & Réseaux spécialisés en cybersécurité

PROFILS & PRÉREQUIS

- La formation TSSR Cybersécurité vise à qualifier dans le domaine de l'infrastructure systèmes & réseaux en spécialisant in fine les apprentissages dans le domaine de la cybersécurité
- Ouverte à tous publics, sans prérequis spécifique mais au profit d'une forte motivation et d'une capacité à travailler de façon autonome au sein d'une dynamique de groupe, dans des conditions d'entreprise.
- Autonomie, capacité d'organisation.
- Savoir être professionnel : ponctualité, assiduité, autonomie et motivation
- Anglais : Niv. B1 compréhension et A2 expression orale

DEROULEMENT

Durée : 1200 heures

Lieux de formation possibles : Toulouse, Montpellier

Effectif : De 12 à 15

Formation : Temps plein continu individualisé

OBJECTIFS DE LA FORMATION

A l'issue de la formation Technicien Supérieur Systèmes et Réseaux, le stagiaire sera autonome et en maîtrise de l'ensemble des méthodes, compétences techniques et technologiques exigées par le référentiel de l'examen final : TP TSSR Niveau 5

- Assister les utilisateurs en centre de services
- Maintenir, exploiter et sécuriser une infrastructure centralisée
- Maintenir et exploiter une infrastructure distribuée et contribuer à sa sécurisation.

Il sera également capable de sécuriser une Infrastructure Réseaux et en connaissances des enjeux liés à la cybersécurité

VALIDATION & CERTIFICATIONS

Titre Pro. TSSR «Technicien.ne Sup. Systèmes & Réseaux»
de niveau 5 (Bac + 2) (code RNCP : 31113)

en option **CCP 1 «Administrer et sécuriser les composants constituant l'infrastructure» du Titre Professionnel AIS (Administrateur.ice d'Infrastructures Sécurisées)** de niveau 6 (Bac + 3 / 4)

Examen : 1 j. à l'ADRAR en présence de jurys professionnels

CONTENU DE LA FORMATION TSSR :

Au delà du référentiel de certification, le contenu de la formation Technicien Supérieur Systèmes et Réseaux s'articule sur plusieurs modules orientés sur les compétences techniques et méthodes de la maintenance et l'administration des systèmes et réseaux.

INSTALLER, CONFIGURER ET MAINTENIR LE PARC INFORMATIQUE D'UNE ENTREPRISE

- Apporter un support technique- Installer, mettre à jour le système d'exploitation d'un poste de travail
- Diagnostiquer et réparer une panne sur un poste de travail

INSTALLER, ADMINISTRER ET MAINTENIR DES SYSTÈMES

- Comprendre le fonctionnement des systèmes Windows et Linux
- Comprendre, mettre en place, maintenir et exploiter un environnement de virtualisation (Hyper-V, Cluster d'hyperviseur)
- Installer, configurer et maintenir les serveurs nécessaires à l'installation d'une infrastructure réseau selon un cahier des charges
- Mettre en place, configurer et exploiter un Contrôleur de Domaine (Windows et Linux)
- Intégrer, de paramétrer et de maintenir des postes clients dans un réseau
- Mettre en place et maintenance d'un serveur Linux de partage de fichiers (SAMBA)
- Mettre en place et exploiter la téléphonie (Ipbx Asterix, 3CX)

INSTALLER, ADMINISTRER ET MAINTENIR DES RÉSEAUX

- Comprendre le fonctionnement des réseaux.
- Choisir les équipements nécessaires à l'installation d'une infrastructure réseau
- Mettre en place et configurer des équipements réseaux (Vlan, Acl...)
- Installer, configurer et maintenir des réseaux sans fil
- Installer, configurer et utiliser un outil de supervision des réseaux
- Installer, administrer et maintenir des Serveurs d'application
- Conception d'une application (UML, Merise)
- Mettre en place et exploiter une Base de Données (SQL)
- Installer, configurer et maintenir un serveur de messagerie (Exchange, PostFix)
- Déployer l'installation d'applications sur les postes clients
- Mettre en place et exploiter des applications sur le Cloud
- Installer, configurer et mettre à jour une base de connaissances

SÉCURISER LES RÉSEAUX

- Installer, configurer, utiliser un réseau privé virtuel
- Maintenir et exploiter un pare-feu et un proxy.
- Mettre en place un système de prévention d'intrusion

AUTOMATISER DES TÂCHES

- Mettre en place des scripts d'automatisation de tâche système Powershell, Shell, Python

Ces modules peuvent être individualisés et font l'objet d'évaluation pré et post-formative.

CONTENU DE LA SPECIALISATION CYBERSECURITE :

PRISE EN MAIN DE L'INFRASTRUCTURE D'APPRENTISSAGE

- Remise et étude du cdc d'une infrastructure
- Identification des oublis du cdc en matière de sécurité
- Remise de l'infrastructure contenant des failles de sécurité
- Sécurisation de l'infrastructure
- Réalisation de tests d'intrusion, Pentesting

SÉCURISER UNE INFRASTRUCTURE

- Sensibilisation des Utilisateurs
- Sécurité Systèmes, Sécurité Réseaux
- Mise en place d'un système de prévention d'intrusion
- Sauvegardes
- Pare-feu Linux
- Proxy Linux
- DMZ
- Sécuriser les Accès Wifi
- VPN
- Sécuriser les équipements Mobiles
- Utilisateurs Nomades
- Supervision

CYBERATTQUES

- Comprendre La Cybersécurité et les Cyberattaques
- Gestion d'une Cyberattaque
- Catégories des moyens d'attaques
- Attaques de masse, attaques Ciblées
- Types de Menace
- Conséquences d'une attaque
- Démonstration d'une attaque

TEST D'INTRUSION

- Exploration des différents types de tests
- Plan de périmètre de tests
- Plan d'exécution de tests
- Exécutions de tests
- Pentesting
- Attaque de son infrastructure

RGPD

- Points essentiels de la RGPD
- Gestion des données personnelles
- Accompagnement de l'Entreprise

IDENTITÉ NUMÉRIQUE

- Définir l'Identité Numérique
- Garder le contrôle de ses données sur Internet
- Gestion des Mots de Passe
- Vie privée sur les Réseaux Sociaux
- Vérifier les informations trouvées sur Internet

Contacts :

ADRAR Pôle Numérique Occitanie

Florence CALMETTES
Coordinatrice Filière Infrastructures & Développement (FAD)
Tél. : 07 76 16 81 83 / Email : florencecalmettes@adrar-formation.com

Anne MORIVAL
Conseillère Entreprise
Tél. : 07 76 61 88 14 / Email : annemorival@adrar-formation.com

