# Descriptif de la formation TSSR
# Technicien(ne) Supérieur
# Systèmes et Réseaux

*1ère partie de la formation : Exploiter les éléments de l'infrastructure et assurer le support aux utilisateurs*

## 1 Assurer le support utilisateur en centre de services

Utiliser un logiciel de gestion de parc et de gestion d'incidents. Réaliser des opérations de maintenance avec un outil de prise de contrôle à distance. Prendre en compte la sécurité, dans la résolution des incidents et dans la proposition de solutions de contournement. Appliquer un script de questionnement ou une méthode d'analyse en résolution d'incident. Respecter les phases d'une intervention d'assistance (prise en compte, suivi, escalade, transfert…). Utiliser les techniques d'investigation et de récupération d'informations auprès de l'utilisateur. Sensibiliser les utilisateurs à une utilisation éco-responsable des équipements numériques. Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique. Communiquer à l'oral avec un niveau de langage et un vocabulaire adapté à l'utilisateur. Rédiger des comptes rendus d'intervention clairs, concis et correctement orthographiés. Faire valider les résultats de l'intervention par le demandeur. Maîtriser sa communication en situation de crise. Connaissance de l'architecture matérielle et logicielle des équipements numériques et les systèmes d'exploitation. Connaissance des fonctions courantes des outils bureautiques. Connaissance de la configuration et de l'utilisation d'un client de messagerie et d'un navigateur Internet. Connaissance des fonctionnalités d'un téléphone IP. Connaissance de base des directives européennes relatives à la gestion des déchets électriques et électroniques. Connaissance de base des directives européennes relatives au RGPD. Connaissance des règles de sécurité et de protection des données. Connaissance de l'usage des outils de communication en entreprise dont les outils collaboratifs (réseaux sociaux, sites web, ...). Connaissance des processus de gestion des incidents et de gestion des problèmes au sens ITIL. Connaissance des fondamentaux du câblage réseau et des connexions sans fil. Connaissance de base des systèmes d'adressage IP.

## 2 Exploiter des serveurs Windows et un domaine ActiveDirectory

Exploiter un serveur Windows (utiliser les outils d'administration, surveiller les événements). Configurer les partages, les droits d'accès et les permissions conformément aux demandes des administrateurs. Créer, modifier et supprimer des objets dans un annuaire Active Directory. Intégrer un poste client au domaine. Appliquer un script de questionnement ou une méthode d'analyse en résolution d'incident. Adopter une démarche de diagnostic logique et efficace. Communiquer avant toute évolution, dégradation ou interruption d'un service. Etablir et mettre à jour la documentation technique. Assurer la veille technologique sur les systèmes d'exploitation Windows (mises à jour, problèmes recensés, évolution). Communiquer à l'oral avec un niveau de langage et un vocabulaire adapté à l'utilisateur. Savoir lire et comprendre sans erreur une documentation technique en français et en anglais. Exploiter une documentation technique ou une interface de logiciel en français et en anglais. Savoir communiquer sur des forums, éventuellement en anglais. Connaissance des concepts de base des annuaires de type LDAP. Connaissance des principes des partages, des autorisations d'accès et des permissions. Connaissance des principes de base de la sécurité informatique (bonnes pratiques). Connaissance des différents moyens d'authentification. Connaissance des éléments d'une charte de sécurité informatique (politique de mots de passe, règles de sécurité, plan de sauvegardes et de secours).

## 3 Exploiter des serveurs Linux

Exploiter un serveur Linux (utiliser les outils d'administration, surveiller les événements, suivre les mises à jour). Gérer les utilisateurs, les droits et les partages. Assurer la veille technologique sur les systèmes d'exploitation Linux (mises à jour, problèmes recensés, évolution). Connaissance de la culture Unix/Linux et du « monde » open source. Connaissance des familles de distributions. Connaissance des principes des partages, des autorisations d'accès et des permissions. Connaissance des principes de base de la sécurité informatique (bonnes pratiques).

## 4 Exploiter un réseau IP

Exploiter les remontées d'un outil de supervision (utilisation, alarmes). Utiliser des outils de diagnostic et d'analyse réseau. Configurer et sécuriser un réseau sans fil. Assurer la maintenance matérielle et logicielle des équipements actifs du réseau local. Appliquer les recommandations de l'ANSSI en matière de sécurité du réseau. Adopter une démarche de diagnostic logique et efficace. Etablir et mettre à jour la documentation technique du réseau (schémas physique et logique). Assurer la veille technologique sur les réseaux (évolutions techniques et logicielles).
Connaissance du modèle OSI et de l'architecture TCP-IP. Connaissance des protocoles de la suite TCP-IP. Connaissance approfondie de l'adressage IP. Connaissance de la technologie des équipements d'interconnexion.
Connaissance des topologies physique et logique des réseaux. Connaissance des principes de base de la sécurité informatique (bonnes pratiques).

**Stage en entreprise de 4 semaines orienté service de maintenance informatique en entreprise ou SSII**

*2ème partie de la formation : Maintenir l'infrastructure et contribuer à son évolution et à sa sécurisation*

## 5 Maintenir des serveurs dans une infrastructure virtualisée

Utiliser un outil de gestion centralisé d'environnement virtuel pour exploiter les hôtes et les machines virtuelles. Utiliser l'outil de gestion centralisé pour surveiller les ressources et suivre les performances. Utiliser les outils d'administration dédiés. Spécifier et implémenter les nouvelles règles de gestion (GPO) dans un annuaire Active Directory. Créer, modifier et supprimer des objets dans un annuaire Active Directory. Personnaliser le système Linux en fonction du rôle du serveur. Exploiter la solution de messagerie et de bureautique distribuée en Cloud. Exploiter les espaces de stockage en Cloud. Coordonner les interventions (acteurs, périmètre, actions, enchainement).
Etablir et mettre à jour la documentation technique de l'environnement de virtualisation. Consulter et tenir compte des contrats de service. Prendre en compte les principes d'écoresponsabilité. Assurer la veille technologique sur les différentes offres et techniques (logiciels de virtualisation, offres Cloud). Identifier les différents interlocuteurs.
Connaissance des spécificités d'un data center (énergie, refroidissement, réseau, sécurité d'accès). Connaissance des équipements matériels du cluster (serveurs, baies de stockage, switch). Connaissance de la notion de container
Connaissance des différentes architectures de Cloud Computing : IaaS, PaaS, SaaS. Connaissance des offres des principaux opérateurs de Cloud. Connaissance des différents métiers liés au Cloud et au BigData.

## 6 Automatiser des tâches à l'aide de scripts

Rechercher un script d'automatisation de tâche et l'adapter à un besoin donné. Tester et documenter un script d'automatisation de tâche. Planifier sur un serveur le déclenchement d'une tâche automatisée. Adopter une démarche de résolution d'erreurs logique et efficace. Gérer les versions et les évolutions des scripts. Savoir lire et comprendre sans erreur la documentation d'un langage de script en français et en anglais. Connaissance des bases de la programmation nécessaires à l'écriture d'un script (variables, paramètres et structures de contrôle). Connaissance des notions élémentaires des langages de script en environnement Windows et Linux.

## 7 Maintenir et sécuriser les accès à Internet et les interconnexions des réseaux

Configurer des réseaux locaux virtuels (VLAN). Configurer, tester et dépanner un service de filtrage IP (pare-feu). Configurer, tester et dépanner les systèmes de protection d'accès à Internet (serveur proxy, antivirus, antispam, anti-malware). Configurer, tester et dépanner des listes d'accès sur les équipements d'interconnexion (routeurs, commutateurs). Participer à la mise en œuvre d'une DMZ. Participer à la configuration d'un protocole de routage statique et dynamique. Participer à la configuration et surveiller le fonctionnement des connexions inter sites (VPN site à site). Intervenir sur une infrastructure de clés publiques (PKI). Participer à la configuration, installer et configurer les clients locaux et surveiller le fonctionnement des accès distants sécurisés des utilisateurs nomades (VPN). Gérer les outils de journalisation (logs) et assurer les sauvegardes. Appliquer les recommandations de l'ANSSI en matière de sécurité du réseau. Adopter une démarche de diagnostic logique et efficace. Communiquer avant toute évolution, dégradation ou interruption d'un service. Etablir et mettre à jour la documentation technique. Assurer la veille technologique sur les différentes offres des fournisseurs d'accès. Sensibiliser les utilisateurs à une utilisation éco-responsable des équipements numériques. Connaissance des risques liés à la sécurité. Connaissance des principes de la QoS (Quality of Service). Connaissance des principes fondamentaux d'une authentification sécurisée. Connaissance des notions de chiffrement, clé secrète, clé publique, certificat, …Connaissance des offres d'interconnexion des opérateurs. Connaissance des principales obligations légales liées à la protection des données. Connaissance des organismes compétents en sécurité (agence ANSSI, PSSI, RSSI). Connaissance des dispositifs de détection et de prévention d'intrusion. Connaissance d'un outil de gestion de l'infrastructure en Cloud (de type Meraki, Ubiquiti, Aruba HP).

## 8 Mettre en place, assurer et tester les sauvegardes et les restaurations des éléments de l'infrastructure

Utiliser les solutions de sauvegardes adaptées aux fichiers, aux bases de données (CRM, ERP, Messagerie, …), aux systèmes, aux configurations et aux machines virtuelles. Mettre en œuvre et tester les restaurations. Maintenir le fonctionnement et assurer la disponibilité des outils de sauvegarde et de restauration. Prendre en compte et respecter la stratégie de sauvegarde, le PCA et le PRA. Définir les procédures et planifier les sauvegardes. Définir les procédures et planifier les tests de restauration. Assurer la traçabilité de la politique de sauvegarde : documenter les procédures, les outils, les actions, etc. Assurer la veille technologique sur les différentes solutions de sauvegardes (logiciels, matériel, virtuelles, cloud, …). Communiquer avant toute évolution, dégradation ou interruption d'un service. Prendre en compte les principes d'écoresponsabilité. Communiquer à l'écrit et à l'oral avec un niveau de langage et un vocabulaire adapté à l'utilisateur. Savoir lire et comprendre sans erreur une documentation technique en français et en anglais. Exploiter une documentation technique ou une interface de logiciel en français et en anglais. Savoir communiquer sur des forums, éventuellement en anglais. Communiquer avec les fournisseurs. Connaître les objectifs et les contraintes des sauvegardes. Connaitre les types de sauvegardes totales, incrémentielles, différentielles. Connaitre les différents types de supports. Connaitre les différentes solutions de sauvegardes du marché et leurs contraintes. Connaitre la classification des sauvegardes : on-line, near-line, off-line.

## 9 Exploiter et maintenir les services de déploiement des postes de travail.

Administration et exploitation d'un serveur de déploiement (création et mises à jour des images, définition des clients, planification, etc.). Mise à jour de la documentation et mise à jour de la base de données de configuration. Rédaction d'une procédure de déploiement. Préparation, test et suivi du déploiement des mises à jour logicielles (de type WSUS/dépôt local Linux). Configuration d'un serveur et d'une architecture de client léger. Déploiement des bureaux et des applications virtuelles. Adopter une démarche de test et de résolution d'erreurs logique et efficace. Communiquer avant toute évolution, dégradation ou interruption d'un service. Établir et mettre à jour la documentation technique. Assurer la veille technologique sur les différentes offres (outils de déploiement et VDI). Connaissance des bases de l'administration des systèmes d'exploitation. Connaissance du fonctionnement des services réseau nécessaires au déploiement (annuaire, DNS, DHCP, boot Pxe). Connaissance de base des règles juridiques relatives aux licences logicielles. Connaissance des différents outils de déploiement en fonction des systèmes d'exploitation. Connaissance des différents outils de mise à jour centralisée en fonction des systèmes d'exploitation. Connaissance des principes d'une infrastructure VDI et des clients légers. Connaissance de la notion de BYOD.

**Stage en entreprise de 7 semaines orienté service de maintenance informatique en entreprise ou SSII**