Cefim
L'école de la Tech

www.cefim.school

Administrateur Infrastructures Sécurisées

RNCP 37680 – Titre Professionnel de niveau 6 (bac+3/4)

PLAN DE FORMATION

Cycle 2025/2026

Pitch du référent : Thomas Cherrier

L'Administrateur Infrastructures Sécurisées (AIS) est avant tout un spécialiste des systèmes et réseaux, qu'il s'agisse d'infrastructures on-premise ou dans le cloud.

Son rôle ne se limite pas à la gestion technique : il joue un rôle clé dans les projets de transformation des infrastructures, répondant aux nouveaux besoins stratégiques des organisations.

Une expertise technique diversifiée
L'AIS s'inscrit dans une démarche d'innovation et d'amélioration continue, intégrant les outils et pratiques modernes pour garantir la performance, la résilience et la sécurité des systèmes. Bien qu'il collabore souvent avec les équipes de cybersécurité, son expertise couvre un éventail plus large, allant de la gestion des environnements cloud et hybrides à l'optimisation des infrastructures réseau.

Il peut également contribuer à des missions spécifiques comme l'audit ou le renforcement de la sécurité des systèmes, sans pour autant se limiter à un rôle exclusivement orienté vers la cybersécurité.

Des débouchés variés et stratégiques
L'AIS évolue dans des contextes professionnels diversifiés :

- ESN (Entreprises de Services Numériques), où il intervient sur des projets clients variés, souvent complexes ;
- Administrations, jouant un rôle central dans la modernisation et la sécurisation des systèmes publics ;
- Entreprises privées, en soutien à la Direction des Systèmes d'Information (DSI) pour garantir la continuité et l'efficacité des opérations.

Une carrière en constante évolution
En fonction de ses aspirations, l'AIS peut se spécialiser davantage, par exemple dans des domaines comme les environnements SOC/SIEM, mais également étendre ses compétences vers d'autres fonctions stratégiques. Ce professionnel polyvalent est un acteur incontournable pour relever les défis technologiques d'aujourd'hui et de demain.

Objectifs de la formation

(reprenant ceux de la certification)

- Administrer et sécuriser les infrastructures
- Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution.
- Participer à la gestion de la cybersécurité.

Accueil / onboarding

(14h en alternance / 14h en initiale)

Nous faisons connaissance et nous commençons à installer les premiers outils de la formation, c'est aussi le moment de l'administratif pour que la formation se déroule pour le mieux.

ITIL CDS

(28h en alternance / 28h en initiale)

ITIL est un ensemble de bonnes pratiques pour le centre de support des DSI. Il fournit un cadre standardisé pour encadrer les opérations de support tout en assurant une traçabilité et une démarche qualité. En tant que futur professionnel de l'infra, il est indispensable d'appréhender et de maitriser ces outils très répandus dans les entreprises aujourd'hui.

Quelques mots clés de cette séquence : GLPI, SCCM, Benchmark, SLA, ITIL.CDS Maitriser la réponse à appel d'offre et créer une maquette de Centre de Services conforme à ITIL pour la gestion d'un helpdesk du niv1 à 3 (hors compétences SOC)

Netadmin

(42h en alternance / 70h en initiale)

L'objectif de cette séquence permet de passer en revue les compétences déjà acquises et de s'immerger dans la formation avec un premier sujet incontournable.

Durant ces premiers jours vous apprendrez donc à administrer une appliance Firewall pour sécuriser l'accès public de l'entreprise. Au menu, entre autres, durant cette phase d'introduction : metrologie, Ntop, Wifi radius, proxy, dnsbl, sonde, fail over, load balancing, VPN Site 2 Site et bien entendu VLANs.

Sysadmin

(42h en alternance / 56h en initiale)

L'active directory reste incontournable au coeur de l'infrastructure d'une entreprise, il est donc essentiel de maitriser l'installation, le paramétrage d'une infra LAN complète sous Windows Server autour d'une PKI.

Quelques mots clés de cette séquence : DNS, DHCP, AD, NFS, SMB, PKI, HTTPS, WSUS,ESXI.

Hypervision

(35h en alternance / 70h en initiale)

Durant cette séquence, vous aborderez une compétence clé de l'admin infra qui consiste à être capable de manager un ensemble de machines virtuelles dansun environnement d'ESXIs lié par un Cluster VCenter afin de réaliser des déplacements à chaud (VMotion) pour gérer l'infra-on premise et ceux sur un stockage hybride locale type NAS NFS et VSAN pour tendre vers les principes de l'hyperconvergence.

Ensuite nous lierons cette maquette via des VPN site-à-site à un cloud Azure et/ou AWS

Gestion de projet

(105h en alternance / 105h en initiale)

Durant cette dernière séquence, l'objectif est d'acquérir les outils et la méthodologie vous permettant de mettre en oeuvre des projets innovants sur des technologies émergentes au sein de votre entreprise. Cette séquence se déroule en deux temps, après une présentation et une prise en main des outils et des formalismes, il vous sera proposé de réaliser un vrai cas d'étude, chiffré, de la mise en place d'un nouveau projet.

Mots clés de la séquence : Gestion de projet, maquette, chiffrage, prestataires divers (fournisseurs, opérateurs..)

Supervision

(35h en alternance / 70h en initiale)

En tant qu'admin infra, vous devez être capable, en temps réel, de programmer des sondes pour remonter des indicateurs de supervision réseaux et systèmes et vous devez être en capacité de créer des dashboards qui permettent de synthétiser et donc de partager en équipe les remontées d'anomalies sur l'infra.

Ce sera donc l'objet de cette séquence qui vous permettra de croiser quelques nouveaux mots clés : Supervision, SNMP, Syslog, WMI, dashboard, Netflow.

Cybersécurité

(175h en alternance / 217h en initiale)

Durant cette longue séquence, vous serez initié à la sécurité offensive et au pentest. L'objectif est d'appréhender les points clés de la sécurité et d'être en capacité de réaliser un audit afin d'envisager des actions de sécurisation.

Cette séquence est en partie organisé sous forme de projet réel, qui consistera à réaliser un audit pour le compte d'une collectivité. Sur ce module, il vous sera proposé de passer la certification CompTIA Security Plus. Vous pourrez également suivre le parcours SecNum Academy de l'ANSSI qui vous d'obtenir une nouvelle attestation de compétence sur ce sujet de la sécurité.

Quelques jargons de cette séquence : Sécurité, Audits, Pentest, Secnum Academy, RGPD, PSSI, Anssi, TryHackMe (abonnement payé),HackTheBox,RootMe Vous serez également formé sur la sécurité défensive pour créer et exploirerr un SOC avec un SIEM complet (au choix GRAYLOK,SPLUNK ou ELK) afin de d'être en capacité d'occuper un poste d'analyste SOC

Accompagnement certification

(49h en alternance / 49h en initiale)

Jury blanc, dossier professionnel, accompagnement à l'emploi, entrainement et passage des certifications… Pour assurer la réussite de votre formation et l'obtention du titre pro, nous vous proposerons tout au long un accompagnement adapté pour maximiser vos chances de réussites.

Entrainement & Passage de certification : Microsoft Azure AZ-90

ACTIVITÉS TRANSVERSALES

Communiquer en français et en anglais

Cette compétence englobe l'analyse des besoins et des fonctionnalités d'une application web ou web mobile, l'adaptation du langage utilisé lors des interactions avec le client, ainsi que la participation active aux réunions techniques en exprimant ses idées de manière structurée, le tout, aussi bien en français qu'en anglais.

Elle inclut également la capacité à adapter sa communication lors d'échanges avec des personnes en situation de handicap, à rédiger des documents techniques clairs et concis, et à rechercher des informations dans des documents techniques tout en étant capable de communiquer efficacement sur leur contenu.

Mettre en œuvre une démarche de résolution de problème

Cette compétence implique la capacité à déterminer une approche structurée de diagnostic pour résoudre les dysfonctionnements d'un applicatif, en identifiant leur origine et en les résolvant.

Elle englobe l'identification des tests logiciels appropriés dérivés de la démarche de résolution, la planification de ces tests pour couvrir tous les cas nécessaires, l'exécution des tests de manière logique, l'analyse des résultats obtenus, la restauration de la situation initiale et la vérification du bon fonctionnement de l'application.

Apprendre en continu

Cette compétence consiste à maintenir ses compétences et sa capacité opérationnelle en mettant en place un système de veille technologique pour rester à jour sur les évolutions technologiques et les problématiques de sécurité des applications web ou web mobiles.

Elle implique également la capacité à s'auto-former en recherchant des informations sur Internet, en consultant des documentations techniques (y compris en anglais) et en sollicitant l'aide de personnes compétentes pour résoudre les problèmes rencontrés.

Accompagnement emploi

En fonction de vos besoins, le service emploi du CEFIM peut vous accompagner dans ces démarches et proposer des actions personnalisées :

- Identifier le secteur d'activité
- Bilan professionnel et personnel
- Confronter son projet à la réalité du marché
- Réaliser son CV
- Identifier les annonces
- Construire son parcours
- Identifier ses points forts et ses axes d'améliorations
- Remettre en forme son CV
- Préparer des entretiens professionnels
- Travailler sur sa candidature
- Technique de communication utile pour les entretiens
- Etre identifié sur les Réseaux Sociaux