Fabrique Numérique Paloise

Administrateur d'infrastructures sécurisées

Programme de formation

RNCP niveau 6 (Bac+3/4)

Le métier **d’administrateur d'infrastructures sécurisées**

L’administrateur d’infrastructures sécurisées réalise des tâches qui ont pour objectifs de maintenir en condition opérationnelles et en condition de sécurité les infrastructures d’un système d’information.

Il met en œuvre, administre et sécurise des infrastructures locales et/ou dans le cloud. Il conçoit et met en production des solutions répondant à des besoins d'évolution. Il implémente et optimise les dispositifs de supervision.

Il est également sollicité pour la conception et la mise en œuvre d’ évolution des infrastructures.

Ce spécialiste de l’infrastructure joue un rôle clé dans la sécurisation du système d'information. Ainsi, il met en œuvre les aspects opérationnels de la politique de sécurité du système d'information, participe à l’analyse du niveau de sécurité, à la détection et au traitement des incidents de sécurité.

OBJECTIFS de la formation

A l'issue de la formation, vous serez capable de :

- **Appliquer** les bonnes pratiques dans l'administration des infrastructures
- **Administrer** et **sécuriser** les infrastructures réseaux
- **Administrer** et **sécuriser** les infrastructures systèmes
- **Administrer** et **sécuriser** les infrastructures virtualisées
- **Concevoir** une solution technique répondant à des besoins d'évolution de l'infrastructure
- **Mettre en production** des évolutions de l'infrastructure
- **Mettre en œuvre** et **optimiser** la supervision des infrastructures
- **Participer** à la mesure et à l'analyse du niveau de sécurité de l'infrastructure
- **Participer** à l'élaboration et à la mise en œuvre de la politique de sécurité
- **Participer** à la détection et au traitement des incidents de sécurité

MODALITÉS

Démarrage : **Mars 2024**
Durée : **16 mois en alternance**

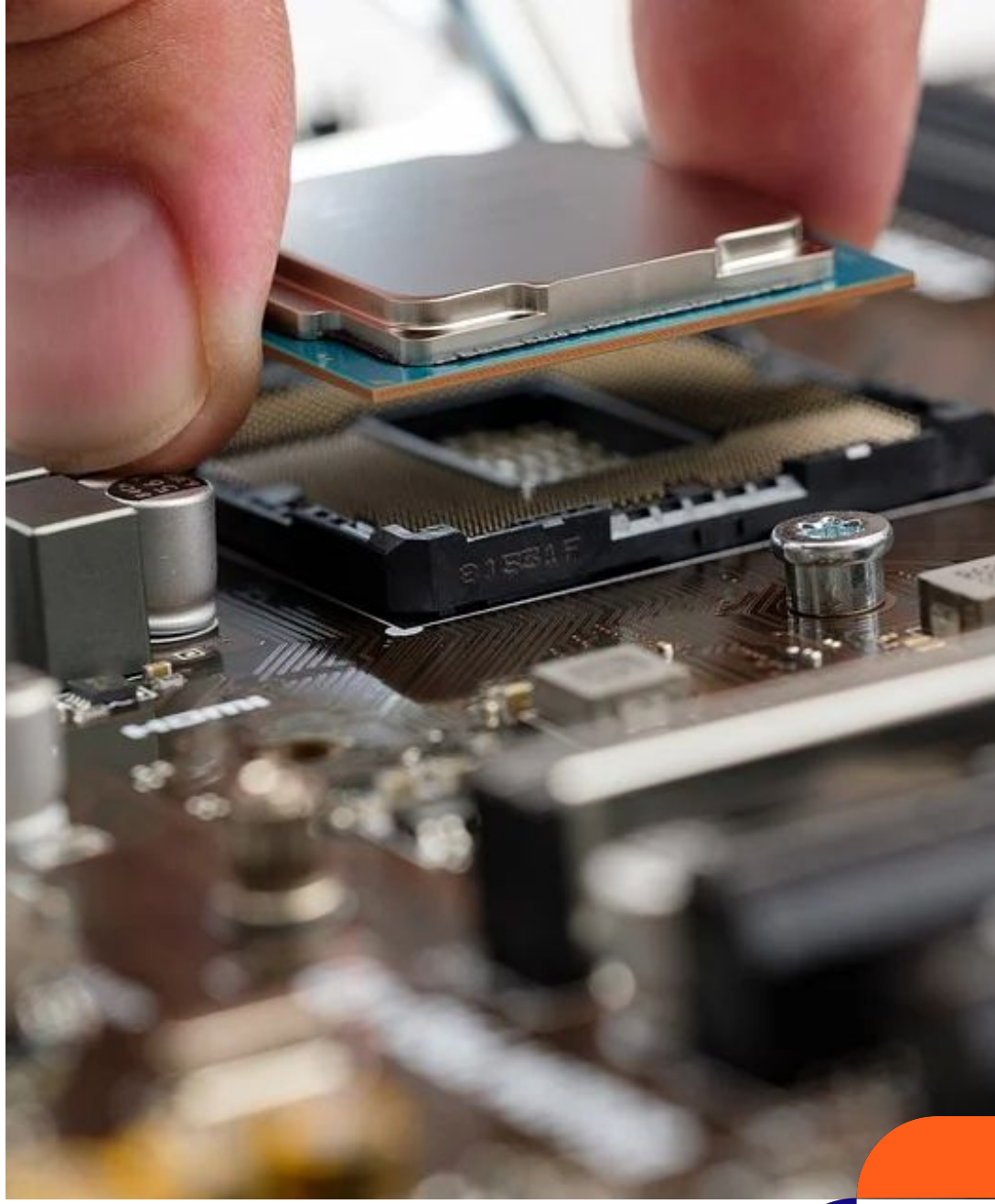
Alternance : **497** heures de formation, à raison d'une semaine de cours par mois, 3 semaines en entreprise.

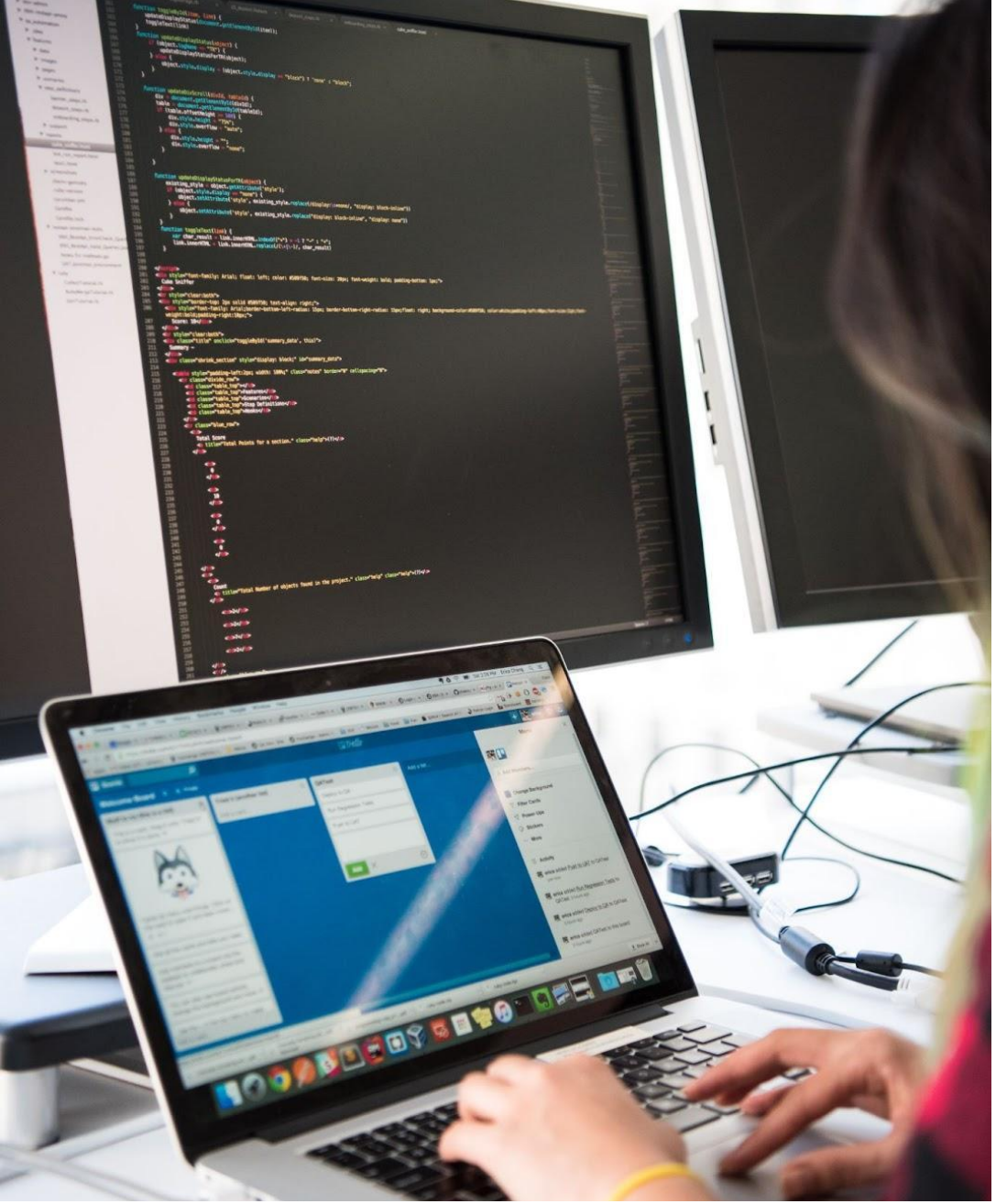
PRÉ**REQUIS**

- Pas de prérequis concernant les diplômes, mais un niveau Technicien Supérieur Systèmes et Réseaux et/ou une expérience significative est demandé.
- Une très forte motivation !

Vos **ATOUTS** pour réussir

De la curiosité, de la créativité, une bonne expression à l'oral et à l'écrit, une représentation claire du métier… et bien sûr, l'envie de s'engager dans une formation intense !





En route vers la **certification**

La certification d'**administrateur d'infrastructures sécurisées** est destinée aux futurs techniciens spécialistes de l'infrastructure et de la sécurité des systèmes d'information.

Elle atteste de leur capacité à :

- **Administrer** et **sécuriser** des infrastructures
- **Concevoir** et **mettre en œuvre** des solutions en réponse à des besoins d'évolution
- **Participer** à la gestion de la cybersécurité

L'examen final à lieu en fin d'année et débouche sur l'obtention d'un **Titre Professionnel** de niveau 6 (Bac+3/4) inscrit au **RNCP**.

Plusieurs options en termes de suite de parcours…

- Rechercher d'emploi à l'issue de la formation.
- Poursuite d'étude et spécialisation dans le domaine des réseaux, de l'infrastructure ou de la cybersécurité.

CONTENUS *de formation*

Module 0 - Prairie

Accueil, présentation des objectifs de formation, de l'équipe pédagogique, du référentiel et des outils de formation

Module 1 - Administrer et sécuriser les infrastructures

- Appliquer les bonnes pratiques dans l'administration des infrastructures (GLPI, SLA, Supervision, MCO)
- Administrer et sécuriser les infrastructures réseaux (pare feu, proxy, portail captif, bastion, IPS, IDS, VPN, etc.)
- Administrer et sécuriser les infrastructures systèmes (Windows, Linux, Unix, LDAP, Active Directory (AD), Azure AD, SSH, SFTP, IPsec, TLS, SMB chiffré, etc.)
- Administrer et sécuriser les infrastructures virtualisées (SAN, VSAN, NAS, DAS, PowerShell, Bash, Python, Backup, VM, Conteneurs (Docker), accès réseaux)

Module 2 - Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution

- Concevoir une solution technique répondant à des besoins d'évolution de l'infrastructure (Security by design, RGPD)
- Mettre en production des évolutions de l'infrastructure (ITIL, PRI, PCI)
- Mettre en œuvre et optimiser la supervision des infrastructures

Module 3 - Participer à la gestion de la cybersécurité :

- Participer à la mesure et à l'analyse du niveau de sécurité de l'infrastructure (Failles de sécurité, vulnérabilités, Kali linux, CVE)
- Participer à l'élaboration et à la mise en œuvre de la politique de sécurité (sécurisation, stratégies de sauvegardes, PRI, PCI, etc.)
- Participer à la détection et au traitement des incidents de sécurité (CERT, RETEX, IPS/IDS, EDR, MDR, XDR, SIEM, SOAR, UEBA)

Pour de plus amples informations

fabriquenumerique.fr

STEP
Technopole Hélioparc
2 avenue Pierre Angot - 64053 PAU Cedex 9

05 59 14 78 79
candidater@fabriquenumerique.fr