Ref. formation 202402218220

Administrateur d'infrastructures sécurisées

Financement

Formation professionnelle continue
Non conventionnée / sans dispositif

Organisme responsable et contact

STEP - FABRIQUE NUMERIQUE PALOISE
Jean-Michel Chauveau
05.59.14.78.79
jmchauveau@step.eco

Accès à la formation

Publics visés :

Demandeur d'emploi
Jeune de moins de 26 ans
Personne handicapée
Salarié(e)
Actif(ve) non salarié(e)

Sélection :

Tests
Entretien

Niveau d'entrée requis :

Niveau 5 : DEUG, BTS, DUT, DEUST (Niveau 5 européen)

Conditions d'accès :

Non renseigné

Prérequis pédagogiques :

Pas de prérequis concernant les diplômes, mais un niveau Technicien Supérieur Systèmes et Réseaux et/ou une expérience significative sont demandés.

Contrat de professionnalisation possible ?

Oui

Objectif de la formation

L'administrateur d'infrastructures sécurisées réalise des tâches d'administration qui ont pour objectifs de maintenir en condition opérationnelles et en condition de sécurité les infrastructures d'un système d'information qu'i soit sur des infrastructures locales et/ou dans le cloud. Il conçoit et met en production des solutions répondant à des besoins d'évolution, implémente et optimise les dispositifs de supervision et participe à la conception et la mise en œuvre d'évolution des infrastructures. L'administrateur d'infrastructure sécurisée joue un rôle clé dans la sécurisation des infrastructures 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. Le responsable d'infrastructures sécurisées occupe généralement un poste étroitement lié à celui d'administrateur système. Il garantie le bon fonctionnement technique des équipements réseau, veillant à ce qu'ils répondent en permanence aux besoins de l'entreprise ou du client. Son rôle s'étend également à la protection des systèmes d'information (SI) contre les pannes, les défaillances et les cybermenaces en forte augmentation eut aux conséquences de plus en plus graves. 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

Contenu et modalités d'organisation

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)

Parcours de formation personnalisable ? **Oui** **Type de parcours** **Modularisé**

Validation(s) Visée(s)

Titre professionnel administrateur d'infrastructures sécurisées - *Niveau 6 : Licence, licence professionnelle, BUT (Niveau 6 européen)*

Et après ?

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.

Calendrier des sessions

Numéro Carif	Dates de formation	Ville	Organisme de formation	Type d'entrée	CPF	Modalités
00438593	du 23/09/2024 au 13/03/2026	Pau (64)	STEP - FABRIQUE NUMERIQUE PALOISE		Non éligible	Contrat pro
00438594	du 23/09/2024 au 13/03/2026	Pau (64)	STEP - FABRIQUE NUMERIQUE PALOISE		Non éligible	Contrat app