

# Bac +3 - Administrateur d'infrastructures sécurisées

Financement	
Formation professionnelle continue	
Non conventionnée / sans dispositif	
Organisme responsable et contact	
CFA ASPECT AQUITAINE CFA ASPECT AQUITAINE 05.56.15.83.40 contact@aspect-aquitaine.fr	
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 :	
Dossier Entretien	
Niveau d'entrée requis :	
Niveau 5 : DEUG, BTS, DUT, DEUST (Niveau 5 européen)	
Conditions d'accès :	
Sous statut contrat d'apprentissage, nécessité d'obtenir un contrat d'apprentissage auprès d'une entreprise, accompagnement à la recherche possible par notre établissement. Renseignements sur le statut d'apprenti sur le site : <a href="http://www.aspect-aquitaine.fr">www.aspect-aquitaine.fr</a>	
Prérequis pédagogiques :	
Etre titulaire d'un BTS SIO, BTS CIEL, DUT Info, Licence 2 Info, DEUST Info.	
Contrat de professionnalisation possible ?	
Non	

## Objectif de la formation

L'administrateur d'infrastructures sécurisées (AIS) met en œuvre, administre et sécurise les infrastructures informatiques locales et 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. Objectif Il participe à la gestion de la cybersécurité en analysant les menaces et en mettant en place des mesures de sécurité et de réaction en cas d'incident. L'administrateur d'infrastructures sécurisées met en œuvre, administre et sécurise les éléments actifs des réseaux, les serveurs, les services d'infrastructure et les plateformes de virtualisation situées dans les locaux de son entreprise ou dans des datacenters ainsi que les ressources et services de cloud public. Il effectue le suivi des tâches de maintenance et fournit un support de niveau 2 et 3 pour résoudre les incidents et les problèmes. Il conçoit des solutions techniques pour répondre aux besoins d'évolution des infrastructures. Il définit les critères d'évaluation et met en place un environnement de test pour valider une solution, puis présente le dispositif choisi aux décideurs. Il planifie et implémente l'intégration de la solution dans l'environnement de production, en vérifiant que les plans de reprise et de continuité informatique (PRI, PCI) associés sont testés et validés. Il met en œuvre les outils de supervision, choisit les indicateurs et événements associés et définit les tableaux de suivi des niveaux de performance et de disponibilité des infrastructures. L'administrateur d'infrastructures sécurisées protège les infrastructures de l'entreprise contre les menaces informatiques. Il analyse les risques, identifie les vulnérabilités et effectue des audits de sécurité en interne. Il participe au choix et à la mise en place de solutions de sécurisation. Il sensibilise les utilisateurs et contribue à la formation des équipes d'exploitation en matière de cybersécurité. Il met en place et utilise des dispositifs de détection d'événements de sécurité et applique les mesures de réaction appropriées en cas d'incident. Il reste vigilant sur les nouvelles menaces et vulnérabilités et adapte les règles de détection et de gestion des incidents en conséquence.

...

## Contenu et modalités d'organisation

CCP 1 : Administrer et sécuriser les infrastructures - Gestion de parc et bonnes pratiques - Virtualisation / Conteneurisation - Stockage, sauvegardes - Administration système (Windows / Linux) - Automatisation - Haute-disponibilité - Administration des actifs réseau - Sécurité : Firewall, VPN, IDS/IPS CCP 2 : Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution - Veille technologique - Analyse des besoins / contraintes - Gestion de projets - Réalisation de tests / POC - Rédaction de documentations - Supervision des infrastructures et des services CCP 3 : Participer à la gestion de la cybersécurité - Rédaction / analyse d'un audit de sécurité - Analyse des risques - Durcissement d'OS - Cryptographie - Mise en œuvre et exploitation de SIEM - Sensibilisation / Formation à la cybersécurité - Veille technologique sur les CVE

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

Entrée dans la vie active principalement.

## Calendrier des sessions

Numéro Carif	Dates de formation	Ville	Organisme de formation	Type d'entrée	CPF	Modalités
00488978	du 02/09/2024 au 30/06/2025	Limoges (87)	INSTITUTION BEAUPYRAT	Non éligible		
00654965	du 01/06/2025 au 30/06/2026	Brive-la-Gaillarde (19)	LYCÉE PROFESSIONNEL PRIVÉ BAHUET	Non éligible		
00654949	du 01/09/2025 au 30/06/2026	Limoges (87)	INSTITUTION BEAUPYRAT	Non éligible		

**00537253**du 01/09/2025 au  
30/06/2026

Limoges (87)

**INSTITUTION  
BEAUPEYRAT**Non  
éligible**00654950**du 01/09/2026 au  
30/06/2027

Limoges (87)

**INSTITUTION  
BEAUPEYRAT**Non  
éligible**00654966**du 18/09/2026 au  
30/06/2027Brive-la-  
Gaillarde (19)**LYCÉE  
PROFESSIONNEL  
PRIVÉ BAHUET**Non  
éligible