SAS VIAL
1 rue du Grenache
34210 Félines-Minervois
Email : info@vial-formations.fr
Tel : +33468905342

ALT - RNCP37680 - TITRE PROFESSIONNEL - Administrateur d'infrastructures sécurisées (en alternance)

Cette formation vise à former des professionnel·le·s capables de sécuriser et faire évoluer les infrastructures informatiques, tout en assurant la supervision, la réponse aux incidents, et la conformité aux standards de cybersécurité.

Durée : 450.00 heures
Durée estimée indicative hebdomadaire : 10 à 12 heures
CODE RNCP : 37680
Certificateur : : MINISTÈRE DU TRAVAIL DU PLEIN EMPLOI ET DE L'INSERTION
Date d'enregistrement : 01/09/2023 au 01-09-2026

A qui s'adresse cette formation ?

- Destiné aux jeunes de 16 à 29 ans révolus préparant un diplôme ou un titre RNCP.
- Accessible sans limite d'âge pour les personnes en situation de handicap, les sportifs de haut niveau et les porteurs d'un projet de création ou reprise d'entreprise.
- Possible jusqu'à 35 ans révolus (36 ans – 1 jour) pour préparer un diplôme de niveau supérieur ou en cas de rupture indépendante de la volonté de l'apprenti.
- Concerne à la fois les nouveaux recrutés et les salariés déjà en CDI, dont le contrat peut être suspendu pour la durée de l'apprentissage.
- Le dispositif Pro-A est réservé aux salariés en CDI qui ne peuvent pas entrer en apprentissage (hors limite d'âge ou cas dérogatoire), afin de favoriser leur reconversion ou leur évolution professionnelle par la voie de l'alternance.

Prérequis

- Titulaire d'un niveau BAC+2, d'un titre de niveau équivalent ou avoir au moins un (1) an d'expérience professionnelle cumulée en rapport direct avec le titre visé
- Disposer d'un ordinateur portable et d'une connexion internet stable pour suivre la formation en ligne (le matériel peut être mis à disposition ou financé par l'entreprise/OPCO).

Accessibilité et délais d'accès

Entrée tous les mois sous réserve d'un nombre de candidats suffisant.

Un délai de 21 jours minimum avant l'entrée en formation est nécessaire à l'instruction de la demande d'inscription. Dans ce délai, le stagiaire doit entre-autres fournir la copie de ses diplômes ou titres obtenus, un CV à jour, et avoir rempli un questionnaire concernant ses compétences et son projet professionnel. Une fois ces documents renvoyés, le service pédagogique prend contact par téléphone avec le stagiaire pour valider ou invalider son inscription sur le parcours de formation.

Cette formation est accessible aux personnes en situation de handicap. Vous pouvez signaler votre situation à la référente handicap afin d'obtenir des adaptations pour votre action de formation ou les épreuves d'évaluations.
Pour toute question d'accessibilité handicap, prendre contact avec nous : info@vial-formations.fr

Délai d'accès : 3 semaines

SAS VIAL
1 rue du Grenache
34210 Félines-Minervois
Email : info@vial-formations.fr
Tel : +33468905342

Objectifs pédagogiques

- 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 de la formation

BLOC 1 : Administrer et sécuriser les infrastructures

- Appliquer les bonnes pratiques dans l'administration des infrastructures
  - Utiliser un outil de gestion des actifs et des configurations de type GLPI
  - Exploiter les données d'un outil de gestion des incidents de type GLPI
  - Vérifier que la qualité de service mesurée correspond aux accords de niveaux de services (SLA)
  - Exploiter les informations fournies par un système de supervision
  - Mettre en œuvre une démarche structurée de diagnostic
  - Établir une procédure de traitement d'incident ou d'exploitation
  - Planifier et organiser les interventions d'administration et de MCO sur les infrastructures.
  - Utiliser l'anglais à l'écrit et à l'oral dans son activité professionnelle. (Compréhension et expression orale niveau A2, compréhension et expression écrite niveau B1 du CERCL)
  - Connaissance des principes généraux des normes et bonnes pratiques de la gestion des services (type iso20000, ITIL, ITSM)

- Administrer et sécuriser les infrastructures réseaux
  - Réaliser un diagnostic et apporter une solution curative à un dysfonctionnement au niveau 2 et plus sur une infrastructure réseau.
  - Administrer et sécuriser des commutateurs de niveau 2 et 3 et des routeurs en mettant en œuvre les technologies de type vlan, redondance et agrégat de liens, sécurité des accès, routage statique et dynamique, monitoring.
  - Administrer et sécuriser les réseaux sans fil.
  - Administrer les dispositifs de sécurisation des accès réseaux de type pare feu, proxy, portail captif, bastion.
  - Administrer et sécuriser des solutions de prévention et détection d'intrusion (IPS, IDS)
  - Administrer les dispositifs réseaux en haute disponibilité utilisant des technologies de type HSRP, STP, agrégat de lien.
  - Administrer et sécuriser les accès distants des utilisateurs nomades et les connexions inter sites de type VPN
  - Administrer et sécuriser les accès au réseau des périphériques mobiles de type BYOD conformément à la politique de sécurité.
  - Adapter le plan d'adressage réseau aux besoins d'administration du MCO.
  - Configurer et contrôler la qualité de service au niveau des flux réseau (QoS).
  - Évaluer les performances du réseau : taux de disponibilité, temps de réponse, évolution des flux.
  - Utiliser un outil de gestion centralisé des équipements réseaux
  - Créer et faire évoluer la documentation technique et les procédures d'exploitation.
  - Appliquer les recommandations de l'ANSSI en matière de sécurité réseau.
  - Appliquer la politique de sécurité du système d'information de l'entreprise.
  - Tester les procédures des plans de reprises et de continuité informatique (PRI, PCI) associés aux infrastructures réseaux.
  - S'assurer du respect des SLA par les fournisseurs.
  - Prendre en compte la réglementation concernant les accès au réseau Internet. (Filtrage sites illégaux, gestion des journaux...)
  - Collaborer avec les différents acteurs de la direction des systèmes d'information.
  - Communiquer de façon adaptée à l'écrit et à l'oral, avec les clients ou les différents acteurs du système d'information.
  - Utiliser l'anglais à l'écrit et à l'orale dans son activité professionnelle. (Compréhension et expression orale niveau A2,

SAS VIAL
1 rue du Grenache
34210 Félines-Minervois
Email : info@vial-formations.fr
Tel : +33468905342

- compréhension et expression écrite niveau B1 du CERCL)
- Connaissance des objectifs et des usages des plans de reprise et de continuité d'activité et informatique (PRA, PCA, PRI, PCI).
- Connaissance des caractéristiques et limites techniques des équipements réseaux.
- Connaissance des principales technologies et des normes utilisées dans les réseaux convergents (voix, données, images)
- Connaissance des risques et principales menaces sur les infrastructures réseau, et des moyens de protection associés
- Connaissance des solutions d'interconnexion proposées par les opérateurs

- Administrer et sécuriser les infrastructures systèmes
  - Réaliser un diagnostic et apporter une solution curative à un dysfonctionnement sur les systèmes au niveau 2 et plus.
  - Administrer et sécuriser un système d'exploitation serveur (Windows, Linux, Unix)
  - Administrer et sécuriser les services réseaux type DNS, DHCP, certificats
  - Administrer et sécuriser les services de type bureau à distance de Microsoft
  - Administrer et sécuriser un annuaire de réseau de type LDAP, Active Directory (AD), Azure AD,
  - Administrer et sécuriser la synchronisation d'annuaires dans un modèle de cloud hybride.
  - Administrer et sécuriser une solution Saas de type MS 365 ou Google Workspace
  - Administrer et sécuriser les outils et les ressources d'accessibilité à destination des personnes en situation de handicap.
  - Administrer et sécuriser les échanges entre systèmes hétérogènes en utilisant des protocoles de type SSH, SFTP, IPsec, TLS, SMB chiffré
  - Administrer des systèmes d'authentification forte de type Multifactor Authentication (MFA), One Time Password (OTP)
  - Administrer et sécuriser une infrastructure à clés publiques (PKI)
  - Automatiser et planifier une tâche d'administration par script basé sur un langage type Python, PowerShell, Bash.
  - Administrer et sécuriser une solution de gestion des mises à jour systèmes
  - Administrer et sécuriser une solution de sauvegarde de type Veritas Backup Exec, VEEAM.
  - Analyser et exploiter les évènements systèmes à partir de la supervision et des journaux
  - Évaluer les performances des systèmes : taux de disponibilité, charges de calcul, temps de réponse, etc.
  - Créer et faire évoluer la documentation technique et les procédures d'exploitation.
  - Appliquer les recommandations de l'ANSSI dans le domaine des systèmes.
  - Appliquer la politique de sécurité du système d'information de l'entreprise.
  - Tester et valider les procédures des plans de reprises et de continuité informatique (PRI, PCI) associés aux infrastructures systèmes et applicatives.
  - Prendre en compte le Règlement général sur la protection des données (RGPD)
  - Prendre en compte la réglementation relative à l'accessibilité du Référentiel général d'amélioration de l'accessibilité (RGAA)
  - Prendre en compte les bonnes pratiques d'éco-conception et de sobriété énergétique
  - S'assurer du respect des SLA par les fournisseurs.
  - Collaborer avec les différents acteurs de la direction des systèmes d'information.
  - Communiquer de façon adaptée à l'écrit et à l'oral, avec les clients ou les différents acteurs du système d'information.
  - Utiliser l'anglais à l'écrit et à l'orale dans son activité professionnelle. (Compréhension et expression orale niveau A2, compréhension et expression écrite niveau B1 du CERCL)
  - Connaissance des objectifs et des usages des PRA, PCA, PRI, PCI.
  - Connaissance des spécificités de chaque environnement système
  - Connaissance des dispositifs relatifs aux accès sécurisés (authentification multi facteur, OTP, web application firewall (WAF), modèle Zero trust, SASE)
  - Connaissance des principes d'une infrastructure à clés publiques (PKI)
  - Connaissance des règles de gestion relatives aux licences systèmes et logicielles

- Administrer et sécuriser les infrastructures virtualisées
  - Réaliser un diagnostic et apporter une solution curative à un dysfonctionnement sur une infrastructure virtuelle.
  - Administrer la haute disponibilité et la répartition de charge au niveau des hyperviseurs.
  - Administrer et sécuriser les dispositifs de stockage type SAN, VSAN, NAS, DAS.
  - Administrer et sécuriser les réseaux virtuels dans des infrastructures virtualisées
  - Ajouter, configurer, administrer et sécuriser des ressources (VM, Conteneurs, accès réseaux ...) dans un cloud public (Azure, AWS …) à partir des différentes interfaces proposées.
  - Configurer, administrer et sécuriser les sauvegardes et la restauration des environnements Cloud et locaux avec un outil de type (VEEAM Backup, Veritas NetBackup …)
  - Déplacer des services (VM, conteneur) locaux vers le cloud et inversement.

SAS VIAL
1 rue du Grenache
34210 Félines-Minervois
Email : info@vial-formations.fr
Tel : +33468905342

- Administrer et sécuriser les environnements virtualisés locaux et distribués en ligne de commandes et par scripts du type PowerShell, Bash, Python.
- Implémenter, administrer et sécuriser des conteneurs.
- Publier une image sur un dépôt de conteneurs (Docker Hub Registery, Azure Container Registry ..)
- Créer et faire évoluer la documentation technique et les procédures d'exploitation
- Suivre les « consommations à l'usage »
- Appliquer les recommandations de l'ANSSI en matière de sécurité des infrastructures virtualisée
- Appliquer la politique de la sécurité du système d'information de l'entreprise
- Tester les procédures des plans de reprises et de continuité informatique (PRI, PCI) associés aux infrastructures virtualisées.
- Prendre en compte le Règlement général sur la protection des données (RGPD)
- Prendre en compte les bonnes pratiques d'éco-conception et de sobriété énergétique
- S'assurer du respect des SLA par les fournisseurs.
- Collaborer avec les différents acteurs de la direction des systèmes d'information
- Utiliser l'anglais à l'écrit et à l'orale dans son activité professionnelle. (Compréhension et expression orale niveau A2, compréhension et expression écrite niveau B1 du CERCL)
- Connaissance des objectifs et des usages des PRA, PCA, PRI, PCI.
- Comprendre les différents types de cloud public, privé, hybride et multicloud
- Comprendre les modèles de service Cloud IaaS, PaaS et SaaS
- Connaissances des principes, des enjeux et des risques du cloud-computing
- Connaissance des principales solutions de gestion d'environnements virtualisés
- Connaissance des fonctions avancées de la gestion des environnements virtualisés (clustering, stockage, migration)
- Connaissance des solutions convergentes ou hyper-convergentes
- Connaissance de l'impact de la virtualisation sur la consommation d'énergie et l'optimisation des équipements
- Connaissance des spécificités d'un datacenter (énergie, refroidissement, réseau, sécurité d'accès)
- Connaissance des équipements matériels du cluster (serveurs, baies de stockage, switch)
- Connaissance des risques inhérents à l'infogérance et à l'externalisation des systèmes d'information
- Connaissances des techniques de virtualisation basées sur les conteneurs
- Connaissance des principes des environnements de déploiement des infrastructures de cloud computing de type OpenStack, AzureStack, OpenNebula.
- Connaissance des pratiques d'intégration continue de la démarche DEVOPS.
- Connaissance des usages des solutions d'orchestration des conteneurs de type Kubernetes.

- ECF 1 : Administrer et sécuriser les infrastructures L'administrateur d'infrastructures sécurisées administrer et sécuriser l'infrastructure du système d'information sur site et dans le cloud, en respectant les bonnes pratiques et en veillant à la maintenir en condition opérationnelle selon les niveaux de service (disponibilité, performances, sécurité) contractualisés. Cette activité inclut la gestion des réseaux, des systèmes et des environnements de virtualisation.
    - Critères d'évaluation :
        - 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

BLOC 2 : Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution

- <u>Concevoir une solution technique répondant à des besoins d'évolution de l'infrastructure</u>
    - Repérer, tester et évaluer préalablement une solution technique en réalisant des maquettes ou des bancs d'essai comparatifs.
    - Définir les critères à retenir pour évaluer une solution.
    - Mettre en oeuvre un environnement de test ou de simulation
    - Évaluer l'impact d'une solution technique sur le système d'information.
    - Définir, planifier et ordonnancer les tâches du projet.
    - Prendre en compte les aspects de la sécurité dès la phase de conception (Security by design).
    - Intégrer les recommandations de l'ANSSI dans les solutions techniques étudiées.
    - Appliquer la politique de sécurité du système d'information de l'entreprise.
    - Prendre en compte les plans de reprise et de continuité informatique (PRI, PCI) dans l'élaboration de la solution.
    - Prendre en compte le Règlement général sur la protection des données (RGPD)

SAS VIAL
1 rue du Grenache
34210 Félines-Minervois
Email : info@vial-formations.fr
Tel : +33468905342

- Prendre en compte la Réglementation relative à l'accessibilité du Référentiel général d'amélioration de l'accessibilité (RGAA)
- Prendre en compte les bonnes pratiques d'éco-conception et de sobriété énergétique
- Rédiger une proposition de solution argumentée et la présenter.
- Réaliser une veille et se tenir informé de l'évolution des techniques et des offres des prestataires, fournisseurs et opérateurs.
- S'assurer de la fiabilité des informations utilisées pour la recherche de solutions
- Connaissance des objectifs et des usages des PRA, PCA, PRI, PCI.
- Connaissance des solutions techniques de sécurisation d'une infrastructure informatique.
- Connaissance des pratiques ou processus du développement, de la construction, de la transition et de l'assurance qualité des services type iso 20000 et ITIL
- Connaissance de méthodes de gestion de projet de type classique ou agile.
- Connaissance des éléments constitutifs du TCO (Total Cost of Ownership)

- <u>Mettre en production des évolutions de l'infrastructure</u>
  - Appliquer les bonnes pratiques et normes de type ITIL et iso 20000 dans la mise en production et déploiement des services.
  - Élaborer les procédures de test et de validation des plans de reprises et de continuité informatique (PRI, PCI).
  - Évaluer et valider une solution dans un environnement qui prend en compte l'environnement de production.
  - Minimiser l'impact sur la disponibilité du SI lors de la planification et de de la mise en production.
  - Participer à la définition et la planification des tâches d'un projet.
  - Suivre et contrôler l'avancement des tâches de mise en production et en rendre compte.
  - Utiliser un outil de gestion de projets
  - Créer ou mettre à jour les informations et procédures d'exploitation.
  - Assurer le transfert de compétences aux personnes en charge de l'exploitation.
  - Prendre en compte l'accompagnement des utilisateurs dans le changement.
  - Piloter les intervenants internes et externes lors des différentes étapes de mise en production.
  - Appliquer la politique de sécurité du système d'information de l'entreprise.
  - Connaissance des objectifs et des usages des PRA, PCA, PRI, PCI.
  - Connaissance des pratiques ou processus de gestion du déploiement, des mises en production, de la disponibilité, de la continuité et de la capacité de type ITIL et iso 20000.
  - Connaissance de méthodes de gestion de projet de type classique ou agile

- <u>Mettre en œuvre et optimiser la supervision des infrastructures</u>
  - Définir les éléments de l'infrastructure qui doivent être suivis.
  - Définir les seuils d'alerte et les indicateurs principaux et les configurer.
  - Définir et mettre en œuvre les sondes, capteurs et les moniteurs à utiliser pour suivre les indicateurs de performance, de disponibilité et de consommation des services.
  - Mettre en œuvre et exploiter une solution de supervision dans une infrastructure distribuée
  - Mettre en œuvre une solution de centralisation et d'analyse des journaux d'événements.
  - Élaborer des tableaux de bord de suivi de production informatique
  - Appliquer les recommandations en matière de sécurisation des données de supervision et de journalisation
  - Appliquer les recommandations de l'ANSSI en matière de sécurité des dispositifs de supervision.
  - Prendre en compte le Règlement général sur la protection des données (RGPD)
  - Rédiger et mettre à jour la documentation et les procédures d'exploitation
  - Présenter par écrit ou lors d'un exposé les résultats de la production informatique. Utiliser l'anglais à l'écrit et à l'oral dans son activité professionnelle. (Compréhension et expression orale niveau A2, compréhension et expression écrite niveau B1 du CERCL)
  - Connaissance des solutions de centralisation et d'analyse des journaux d'événements d'une infrastructure distribuée
  - Connaissance de la gestion des niveaux de services
  - Connaissance des bases de données de série temporelles
  - Connaissance du protocole SNMP
  - Connaissance du standard WBEM et sa déclinaison WMI Connaissance du protocole Syslog
  - Connaissance des protocoles d'analyse de flux réseaux de type Netflow

- ECF 2 : Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution L'administrateur d'infrastructures sécurisées conçoit et met en production des solutions techniques répondant à des besoins d'évolution de l'infrastructure. Il implémente et optimise les dispositifs de supervision.
  - Critères d'évaluation :

SAS VIAL
1 rue du Grenache
34210 Félines-Minervois
Email : info@vial-formations.fr
Tel : +33468905342

- 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

BLOC 3 : Participer à la gestion de la cybersécurité

- Participer à la mesure et à l'analyse du niveau de sécurité de l'infrastructure
  - Caractériser les types de risques informatiques encourus (intrusion, piratage, malveillance, fraude).)
  - Participer à une analyse des risques avec une méthode ou un guide de type EBIOS, ISO 27005
  - Identifier les différents types de menaces redoutées.
  - Analyser le scénario d'une menace.
  - Evaluer la criticité d'une vulnérabilité
  - Réaliser un audit de sécurité interne.
  - Utiliser des outils de détection de vulnérabilité.
  - Utiliser et adapter des scripts dans le cadre d'audit et d'évaluation du niveau de sécurité.
  - Réaliser des tests d'intrusion sur un système informatique de type WhiteBox.
  - Utiliser des outils de test et d'analyse de la sécurité inclus dans des distributions de type Kali linux
  - Réaliser une veille sur les menaces, les failles et les vulnérabilités.
  - Utiliser les common vuneralbility and exposure (CVE) et common weakness enumeration (CWE)
  - Communiquer avec l'ensemble des acteurs de la cybersécurité.
  - Utiliser l'anglais à l'écrit et à l'oral dans son activité professionnelle. (Compréhension et expression orale niveau A2, compréhension et expression écrite niveau B1 du CERCL)
  - Connaissance des risques informatiques encourus et leurs causes
  - Connaissance de base sur les organismes et la réglementation relatifs à la protection des données en France et en Europe (CNIL, RGPD)
  - Connaissance des organismes de lutte et d'information contre les risques Cyber ANSSI, CESIN, CLUSIF, MITRE, NIST, CIS...
  - Connaissance des principes d'une méthode de gestion des risques comme ISO 27005, EBIOS, MEHARI.
  - Connaissance des principaux intervenants dans le domaine de la cybersécurité.
  - Connaissance des principes d'un SOC (Security Operations Center).
  - Connaissance des principes des différents outils de mesures et d'analyse dédiés à la sécurité IDS/IPS, SIEM (Security Information and Event Management), UEBA (User and Entity Behavior Analytics), XDR (eXtended Detection and Response),
  - Connaissance des scripts Python, PowerShell, Bash
  - Connaissance des offres des prestataires spécialisés en cybersécurité

- Participer à l'élaboration et à la mise en œuvre de la politique de sécurité
  - Participer à l'élaboration des mesures à prendre et des dispositifs à mettre en œuvre dans le cadre du plan de reprise informatique et de continuité informatique (PRI, PCI).
  - Appliquer les recommandations des organismes de lutte et d'information contre les risques Cyber de type ANSSI.
  - Prendre en compte le Règlement général sur la protection des données (RGPD).
  - Prendre en compte les environnements et les conditions de travail des utilisateurs afin de choisir des solutions de sécurité adaptées et compatibles.
  - Sécuriser et gérer les accès avec des méthodes et outils de type Pare-feu, Bastion, authentification multi facteur, méthode Zéro trust
  - Sécuriser les systèmes d'exploitation. Durcissement des systèmes Microsoft, Linux, Android …
  - Sécuriser les échanges avec des solutions de chiffrement, de VPN et de signatures.
  - Mettre en œuvre une stratégie de sauvegarde, en réaliser les procédures et tester les restaurations.
  - Mettre en œuvre la haute disponibilité pour des infrastructures réseaux, systèmes et pour les applications.
  - Identifier et proposer des systèmes de détection de menace type EDR, IPS/IDS, XDR, SIEM adaptés à l'entreprise.
  - Rédiger des procédures dans le respect des bonnes pratiques.
  - Réaliser une veille sur les menaces et les dispositifs de protection.
  - Réaliser une veille et analyser les offres des prestataires de services de sécurité managés.
  - Préparer une action de formation courte conforme aux objectifs et adaptée à destination des équipes techniques.
  - Communiquer avec l'ensemble des acteurs de la cybersécurité
  - Animer une action de sensibilisation ou de formation courte.
  - Utiliser l'anglais à l'écrit et à l'oral dans son activité professionnelle. (Compréhension et expression orale niveau A2,

SAS VIAL
1 rue du Grenache
34210 Félines-Minervois
Email : info@vial-formations.fr
Tel : +33468905342

compréhension et expression écrite niveau B1 du CERCL)
- Connaissance des menaces et vulnérabilité.
- Connaissance des normes et recommandations ISO27000 attachées à son domaine d'activité.
- Connaissance des principes d'une méthode de gestion des risques de type EBIOS, ISO27005
- Connaissance des solutions de sécurisation type IPS/IDS, EDR, XDR, SIEM, SOAR
- Connaissance des offres des prestataires spécialisés en cybersécurité
- Connaissance de la structure de la PSSI et de sa méthodologie d'élaboration.
- Connaissance des concepts, objectifs et usages des PRA, PCA, PRI, PCI
- Connaissance des principes de haute disponibilité et des systèmes redondants

- <u>Participer à la détection et au traitement des incidents de sécurité</u>
  - Appliquer les recommandations des organismes de lutte et d'information contre les risques Cyber de type ANSSI, NIS.
  - Configurer et exploiter un système de détection ou réponse à incident de sécurité (SIEM, SOAR, XDR)
  - Adapter les règles de détection des vulnérabilités aux différents environnements.
  - Qualifier un incident de sécurité.
  - Appliquer les mesures de réaction en réponse à un incident de sécurité
  - Assurer la préservation et la disponibilité des journaux d'évènements et de traces.
  - Transmettre les informations nécessaires aux analystes ou aux équipes de réponse sur incidents (CERT)
  - Réaliser la veille sur les menaces et les dispositifs de protection.
  - Réaliser un compte rendu d'incident.
  - Réaliser une veille et analyser les offres des prestataires de services de sécurité managés.
  - Utiliser l'anglais à l'écrit et à l'orale dans son activité professionnelle. (Compréhension et expression orale niveau A2, compréhension et expression écrite niveau B1 du CERCL)
  - Connaissance des menaces et vulnérabilité.
  - Connaissance des règles d'organisation d'un RETEX
  - Connaissance des solutions de sécurisation type IPS/IDS, EDR, MDR, XDR, SIEM, SOAR, UEBA
  - Connaissance de l'organisation et des rôles au sein d'un SOC.
  - Connaissance de tous les acteurs de la cybersécurité
  - Connaissance des offres des prestataires spécialisés en cybersécurité

- ECF 3 : Participer à la gestion de la cybersécurité L'administrateur d'infrastructures sécurisées analyse le niveau de sécurité des infrastructures et met en place des mesures pour renforcer leur sécurité. Il analyse en temps réel les menaces et applique les mesures de réaction en réponse à un incident.
  - Critères d'évaluation :
    - 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

Pour aller plus loin : L'organisme de formation VIAL vous accompagne dans l'amélioration de vos compétences comportementales. Au-delà de votre formation technique métier, nous vous offrons 6 modules axés sur le développement personnel :
- *Trouver son chemin professionnel avec l'IKIGAI*
- *Mettre ses valeurs au service de l'entreprise*
- *Les comportements défensifs*
- *Les biais cognitifs*
- *Améliorer sa communication*
- *Travailler en équipe et déployer son sens du collectif*

Les différents thèmes abordés seront un moyen de vous démarquer sur le marché de l'emploi, alors n'attendez plus, formez-vous chez VIALFormations !

SAS VIAL
1 rue du Grenache
34210 Félines-Minervois
Email : info@vial-formations.fr
Tel : +33468905342

Organisation de la formation

Équipe pédagogique

ORGANISATION VIAL :

Mme Virginie Billiet, référente handicap info@vial-formations.fr
Mme Virginie Billiet, responsable pédagogique : responsable.pedagogie34@gmail.com
Formateur référent, en cours d'affectation

Contacts :

Référente handicap: info@vial-formations.fr 04 68 90 53 42
Assistante de direction: info@vial-formations.fr
Responsable pédagogique : responsable.pedagogie34@gmail.com
Formateur Référent :
Secrétariat général: 04 68 90 53 42
Support technique : vialspprt@gmail.com

Assistance/Aléas et réclamations disponibles par mail à info@vial-formations.fr 04 68 90 53 42 du lundi au vendredi de 09h à 17h (délai de réponse maximale : 24h)

ORGANISATION YYYOURS FORMATIONS :

Equipe pédagogique :
Mme Guibergia Cécilia, référente handicap (contact.yyyours@gmail.com)
Mme Lesbarreres Perrine, responsable pédagogique
Mme Sigrid Richard, responsable pédagogique
Mme Diane Gauthier, coordinatrice pédagogique
M. Penicaud Laurent, Formateur référent
Coach professionnel, en cours d'affectation
Mme Allard Laetitia, psychologue du travail

Contacts :
Référente handicap : contact.yyyours@gmail.com
Assistante de direction : assistante.direction.nec47@gmail.com (04 85 88 03 45)
Coordinatrice pédagogique : coordinateur.pedagogie@gmail.com
Psychologue du travail : psy.travail.nec47@gmail.com
Formateur référent : formateur.sup.accgo@yyyours-formations.com
Secrétariat général : 04 22 84 04 94
Assistance/Aléas et réclamations disponibles par mail à ad.yyyours@gmail.com 04 82 81 01 63 du lundi au vendredi de 09h à 17h (délai de réponse maximale : 24h)

Ressources pédagogiques et techniques

- Accès illimité à la plateforme de cours 24/7;
- Cours théoriques au format vidéo;
- Formations accessibles via un ordinateur ou une tablette;
- Assistance technique par téléphone, et email (vialspprt@gmail.com)
- Mise à disposition en ligne de documents supports à télécharger librement
- Mise en place des ECF (Évaluation en Cours de Formation) avec l'aide du formateur référent

SAS VIAL | 1 rue du Grenache Félines-Minervois 34210 | Numéro SIRET : *94372692700016* |
Numéro de déclaration d'activité : *76 34 14046 34 (auprès du préfet de région de : Béziers)*
Cet enregistrement ne vaut pas l'agrément de l'État.

SAS VIAL
1 rue du Grenache
34210 Félines-Minervois
Email : info@vial-formations.fr
Tel : +33468905342

Modalités d'évaluation
ECF (Évaluation en Cours de Formation)
Suivi des connexions à la plateforme
Travaux dirigés à rendre
Travaux pratiques à exécuter
Stage professionnel au sein d'une entreprise (optionnel)
Rédaction d'un dossier professionnel (obligatoire)
Validation de l'ensemble des blocs de compétences,
Validation partielle possible des blocs individuellement. Obtention par validation des examens continus.

Dispositif de suivi de l'exécution de l'évaluation des résultats de la formation

- Suivi d'assiduité réalisé par notre responsable pédagogique qui est dédiée et disponible par téléphone et courriel : responsable.pedagogie34@gmail.com (réponse en moins de 48h du lundi au vendredi de 09h à 17h);
- Relevés de connexion à la plateforme e learning;
- Un suivi de la formation et de l'accompagnement seront réalisés tout au long de la formation.
- Entretien téléphonique et visio-conférence avec le formateur référent pour la validation des compétences acquises
- Livret ECF complété à la fin de l'action de formation par le formateur référent.
- La formation pourra être adaptée pour pallier des difficultés majeures par l'apprenant.
- Dossier professionnel obligatoire à remplir par le bénéficiaire.
- Livret de suivi de formation complété par le stagiaire et le formateur référent.
- Certificat de réalisation signé par le stagiaire et le formateur.
- Convention de formation professionnelle.

Prix : 0.00

Qualité et indicateurs de résultats
Pas de données accessibles à ce jour, dès que le nombre minimal de candidats sera suffisant pour obtenir ces taux, ils seront publiés

Examen final

Dans un délai maximum de 6 mois à l'issue de l'action de formation, vous recevrez une convocation pour vous présenter en présentiel sur 2 à 3 journées de certification. Une convocation officielle vous sera adressée par courriel ou courrier simple au moins 30 jours avant la date de début de l'examen par le centre qui vous accueillera.

Sauf en cas de force majeure ou de justificatif médical, les stagiaires en formation dans l'organisme VIAL Formations - Franchise YYYOURS FORMATIONS s'engagent à se présenter sur les plateaux techniques dont le lieu sera précisé sur la convocation 30 jours avant le début de l'examen.

Modalités	Compétences évaluées	Durée	Détail de l'organisation de l'épreuve

SAS VIAL
1 rue du Grenache
34210 Félines-Minervois
Email : info@vial-formations.fr
Tel : +33468905342

résentation d'un projet réalisé en amont de la session	pliquer 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 rticiper à la mesure et à l'analyse du niveau de sécurité de l'infrastructure rticiper 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	00h 40 min	En amont de la session d'examen, le candidat réalise un projet ou plusieurs projets. prépare un dossier de projet et un support de présentation de type diaporama. Le dossier projet rend compte de l'ensemble des projets. ors de l'examen, le jury prend connaissance du dossier de projet imprimé avant la présentation du candidat. Le candidat présente ensuite son projet ou ses projets au jury.
Autres modalités d'évaluation le cas échéant :			

SAS VIAL
1 rue du Grenache
34210 Félines-Minervois
Email : info@vial-formations.fr
Tel : +33468905342

Entretien technique	pliquer 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 rticiper à la mesure et à l'analyse du niveau de sécurité de l'infrastructure rticiper 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	01 h 00 min	e jury questionne le candidat sur la base de son dossier de projet et de sa présentation, afin de s'assurer de la maîtrise des compétences couvertes par le projet ou les projets. n questionnement complémentaire lui permet d'évaluer les compétences qui ne sont pas couvertes par le projet ou les projets. .
Questionnaire Professionnel	pliquer 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 Mettre en œuvre et optimiser la supervision des infrastructures rticiper à la mesure et à l'analyse du niveau de sécurité de l'infrastructure rticiper 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	00 h 30 min	L'ensemble des candidats répondent en même temps au questionnaire professionnel en présence d'un surveillant. candidat étudie une documentation technique rédigée en anglais. Il répond à deux questions fermées à choix unique posées en français ; deux questions ouvertes posées en anglais et amenant des réponses courtes, en rédigeant la réponse en anglais.
Questionnement à partir de production(s)	Sans objet		Sans objet

SAS VIAL
1 rue du Grenache
34210 Félines-Minervois
Email : info@vial-formations.fr
Tel : +33468905342

Entretien final		00 h 20 min	compris le temps d'échange avec le candidat sur le dossier professionnel.
	Durée totale de l'épreuve pour le candidat :	02 h 30 min	

Validation de l'ensemble des blocs de compétences, pas de validation individuelle des blocs.

Le délai d'accès au jury est de la responsabilité du certificateur, il ne peut pas dépasser 6 mois après la fin effective de l'action de formation, sauf en cas de force majeure.

Documents délivrés à l'issue de la formation
Parchemin de certification délivré par le certificateur (les titres professionnels sont délivrés par le Ministère du Travail)
Copie du livret de suivi de formation
Copie du livret ECF
Copie du dossier professionnel
Un certificat de réalisation

Modalité d'obtention de la certification
Par validation de l'ensemble des blocs de compétences qui composent le titre, validation partielle possible des blocs individuellement.

Équivalences, passerelles suites de parcours et débouchés
Niveau équivalent obtenu à l'issue de la certification : Niveau niveau II (licence ou maîtrise universitaire)
Secteurs d'activités :

- Entreprise de services numériques (ESN)
- Toutes les organisations ou entreprises utilisatrices de taille intermédiaire et plus du secteur privé ou public

Type d'emplois accessibles :

- Administrateur systèmes et réseaux (et sécurité)
- Administrateur systèmes (et sécurité)
- Administrateur réseaux (et sécurité)
- Administrateur infrastructures
- Administrateur d'infrastructures et cloud
- Administrateur cybersécurité
- Responsable infrastructure systèmes et réseaux