Le Campus Numérique in the Alps

Formation Administrateur d'infrastructure sécurisée (AIS)

Objectifs de la formation

La formation Administrateur d'infrastructure sécurisée est un parcours de 10 mois formant au métier de technicien sécurité réseau, de responsable infrastructure systèmes et réseaux, de technicien cybersécurité, d'analyste en cybersécurité, ou encore de consultant infrastructures et sécurité.

Ces différents acteurs de la cybersécurité ont pour mission :

- **Analyse des menaces** et mise en place des mesures de sécurité et de réaction en cas d'incident.
- **Mise en œuvre, administration et sécurisation** des éléments actifs des réseaux, les serveurs, les services d'infrastructure et les plateformes de virtualisation (dans les locaux de l'entreprise, les datacenters et les services de cloud public)
- **Conception des solutions techniques** pour répondre aux besoins d'évolution des infrastructures
- **Protection des infrastructures de l'entreprise** contre les menaces informatiques : analyse des risques, identification des vulnérabilités, réalisation des audits de sécurité en interne et sensibilisation des utilisateurs et contribue. Il contribue également à former les équipes d'exploitation en matière de cybersécurité.

Au terme de cette formation, vous serez en mesure d'administrer et de sécuriser des infrastructures, de concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution, et de participer à la gestion de la cybersécurité au sein d'une organisation.

Compétences développées

Le programme aborde les méthodes et technologies de sécurisation des réseaux, systèmes et infrastructures virtualisées ; la conception de solutions techniques et leur mise en production, les méthodologies de détection et de traitement des incidents de sécurité ainsi que l'ensemble des soft skills indispensables en entreprise. Les méthodes d'apprentissage « apprendre à apprendre » permettent aux apprenants de se former en autonomie tout au long de leur carrière pour suivre les évolutions technologiques.

Compétences développées à l'issue de la formation :

1. Administrer et sécuriser les infrastructures :

- 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

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
- Mettre en production des évolutions de l'infrastructure
- Mettre en œuvre et optimiser la supervision des infrastructures

3. Participer à la gestion de la cybersécurité :

- 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

Méthodes pédagogiques

Le Campus adopte une approche par compétences, les modules de formation étant construits sur la base de compétences à acquérir : savoirs, savoir-faire, savoir-être, outils, méthodologies… Cette approche permet d'assurer une formation professionnalisante avec le développement de compétences opérationnelles correspondant aux exigences des métiers visés.

Le modèle de pédagogie par projet mis en place dans les modules de formation permet de rendre les stagiaires acteurs de la formation et de l'apprentissage. L'autonomie développée dans les modules (e-learning et classes inversées), la transversalité marquée des enseignements et une pratique pédagogique hautement professionnalisante sont au cœur du projet pédagogique.

Modalités d'évaluation et diplôme visé

La formation est sanctionnée par l'obtention du Titre professionnel Administrateur d'infrastructures sécurisées par le Ministère du Travail, de l'Emploi et de l'Insertion, RNCP de niveau 6 (équivalent Bac+3) n°37680 enregistré le 13/05/2023.

La formation prépare à l'ensemble des blocs de compétences du titre professionnel.

Modalités d'évaluation :

- **Validation des compétences** (auto-validation et validation par un formateur professionnel de l'ensemble des compétences associées à chacun des modules de formation)
- **Réalisation de rapports relatifs à la mission professionnelle réalisée**
- **Soutenance devant un jury** accrédité par le Ministère du Travail, de l'Emploi et de l'Insertion.

Durée de la formation

La formation se décompose en deux phases :

- **6 mois de formation intensive au Campus (805 heures) permettant d'acquérir le socle de compétences techniques et de travail en équipe ;**
- **Mission professionnelle de 4 mois (stage) afin d'élargir et d'approfondir les compétences techniques et les soft skills développées.**

Modalités d'accès et prérequis

Tous les candidats possédant un diplôme de niveau 5 (équivalent bac+2) en informatique ou une expérience professionnelle supérieure à 2 ans dans le domaine peuvent s'inscrire à la formation.

Les critères de sélection sont basés sur :

- **La motivation et le projet professionnel défini ;**
- **La capacité à travailler en équipe et la bienveillance ;**
- **La maîtrise des fondamentaux du développement informatique ;**
- **La curiosité, l'autonomie et la créativité.**

Processus de sélection :

- **Participation à une réunion d'informations collectives**
- **Envoi d'une lettre de motivation, d'un CV et d'une vidéo pitch**
- **Entretiens de motivation et tests techniques.**

Délais d'accès : la formation débute en moyenne deux mois après l'ouverture des candidatures.

Prix de la formation

Sans reste à charge grâce aux partenaires financeurs de la formation et les fonds de financement de la formation.

Lieux de formation

Campus de Grenoble

Le Totem, 3ème étage

16 boulevard Maréchal Lyautey, 38000 Grenoble

07 50 66 51 51 / audrey.graffagnino@le-campus-numerique.fr

Campus de Valence

M3 Rovaltain

1 rue Roland Moreno

26300 ALIXAN

06 21 00 66 54 / contact.valence@le-campus-numerique.fr

Campus d'Annecy

Papeteries Image Factory

3 Esplanade Augustin Aussedat – Cran Gevrier

74960 ANNECY

07 69 37 90 37 / carole.ritrovato@le-campus-numerique.fr

Accessibilité aux personnes en situation de handicap

La formation est accessible aux personnes en situation de handicap, avec une adaptation possible des modalités pédagogiques et d'évaluation. Le Campus Numérique est engagé dans la démarche H+ Formation de la Région Auvergne Rhône-Alpes.

Référentes handicap : Audrey Graffagnino (audrey.graffagnino@le-campus-numerique.fr) / Pauline Lacour (pauline.lacour@le-campus-numerique.fr)

Suites de parcours

A visée professionnalisante, la formation vous permet d'exercer les métiers d'administrateur d'infrastructures sécurisées, de responsable infrastructure systèmes et réseaux, de technicien cybersécurité, d'analyste en cybersécurité, ou encore de consultant infrastructures et sécurité.

Contenus Pédagogiques

Pour cette formation, un accent fort sera mis sur la différenciation pédagogique. A partir des compétences antérieures des stagiaires et des missions en entreprise, les compétences à développer et les volumes horaires associés seront adaptées.

805 heures de formation		
Positionnement	Bilan, diagnostic et définition du parcours individualisé de formation	3.5 heures
Outils numériques pour formation à distance	Mise en place de l'environnement de formation à distance, formation sur les outils numériques utilisés à distance (installation de logiciels, vérification de connexion internet, tests techniques)	3.5 heures
Remise à niveau : Introduction aux infrastructures informatiques et à la cybersécurité	Comprendre les bases des réseaux (TCP/IP, routage, DNS). Introduction aux systèmes d'exploitation (Windows, Linux). Principes fondamentaux de la cybersécurité et des bonnes pratiques.	**32 heures**
Système d'information et architecture SI	Comprendre la structuration d'un SI, ses composants (réseaux, serveurs, postes, services), les typologies d'architectures (client-serveur, cloud, hybride) et leurs enjeux en termes de disponibilité, sécurité et évolutivité.	**35 heures**
Administration et sécurisation des réseaux	Configuration et sécurisation des équipements réseaux (switches, routeurs, pare-feu). Mise en place de VPN et gestion des VLANs. Surveillance et analyse du trafic réseau (outils comme Wireshark).	**105 heures**

Administration des systèmes d'exploitation et des environnements virtualisés	Administration des systèmes Windows Server et Linux. Gestion des droits et permissions utilisateurs. Déploiement et sécurisation des environnements virtualisés (VMware, Hyper-V). Automatisation des tâches avec des scripts (Bash, PowerShell).	**140 heures**
Intégration et gestion d'une infrastructure distribuée	Intégration des services distribués (messagerie, partage de fichiers, impression). Administration des environnements cloud (Azure, AWS). Gestion des environnements de travail des utilisateurs (outils collaboratifs, bureaux virtuels).	**140 heures**
Sécurisation avancée des infrastructures	Analyse des vulnérabilités et application des correctifs. Mise en œuvre des politiques de sécurité (GPO, normes ISO 27001). Gestion des incidents de sécurité et réponse aux cyberattaques.	**70 heures**
Sécurité des données	Mettre en œuvre les principes de confidentialité, intégrité et disponibilité. Sécuriser le stockage, les échanges et les sauvegardes. Maîtriser le chiffrement, la traçabilité, la gestion des droits et la prévention des fuites de données.	**35 heures**
Supervision et optimisation des performances	Mise en place de solutions de supervision (Nagios, Zabbix). Analyse des performances et amélioration de la disponibilité des services. Présentation des rapports de supervision et optimisation des systèmes.	**42 heures**
Informatique industrielle	Identifier les composants des systèmes industriels (OT), comprendre les architectures SCADA, les protocoles (Modbus, OPC-UA), les contraintes temps réel, et appliquer les principes de cybersécurité adaptés aux environnements industriels.	**35 heures**
Intelligence artificielle	Découvrir les bases de l'IA et du machine learning, comprendre leurs applications en cybersécurité (détection d'anomalies, analyse comportementale), et évaluer les enjeux techniques, éthiques et sécuritaires liés à leur déploiement.	**35 heures**
RGPD	Compréhension du RGPD, les différents principes et leur application dans le développement : gestion du consentement, minimisation des données, droit à l'oubli, pseudonymisation, sécurisation des traitements et documentation de conformité.	**14 heures**
Droit et conformité	Identifier les obligations légales liées à la sécurité des systèmes d'information, comprendre les responsabilités en cas d'incident, maîtriser les normes (ISO 27001, LPM, NIS2) et intégrer la conformité dans les pratiques IT.	**21 heures**

Numérique responsable et IA frugale	Impacts environnementaux et sociétaux du numérique. Leviers de réduction de l'empreinte carbone des projets (stockage, traitement, cloud…) Les principes de l'IA frugale : optimisation, consommation énergétique, réutilisation des algorithmes.	**14 heures**
Relations client / usager	Étude de cas - Maîtriser les étapes et les techniques de la communication client/usager. Identifier les besoins, construire un cahier des charges à partir des demandes client/usager et traduire des résultats d'analyse en recommandations compréhensibles et utiles.	**14 heures**
Laïcité, citoyenneté et valeurs de la République	Comprendre les principes de la laïcité, de la citoyenneté et des valeurs de la République pour adopter une posture professionnelle respectueuse, favoriser le vivre-ensemble et réagir de manière adaptée aux situations rencontrées.	**4 heures**
Techniques de recherche d'emploi	Maîtriser les techniques de recherche d'emploi, les techniques de création d'un profil professionnel numérique ainsi que les stratégies nécessaires pour s'engager dans un processus actif de recherche d'emploi.	**21 heures**
Préparation à la certification	Préparation à l'examen de certification RNCP N°37680 - AIS : format de l'examen, des types de questions, et des attentes spécifiques. Méthodologies de construction de la présentation orale et du rapport professionnel. Soutenances blanches.	**35 heures**
Bilans	Bilan intermédiaire : point d'étape sur les apprentissages et l'évolution des apprenants, identification des difficultés éventuelles et ajustement des méthodes pédagogiques. Bilan final : évaluation de l'ensemble du parcours des apprenants et mesure de l'atteinte des objectifs pédagogiques de la formation. Bilan des taux d'insertion dans l'emploi des stagiaires (départs en stage et perspectives d'emploi au terme de la formation). Recueil des impressions des participants sur le contenu, les méthodes et l'animation de la formation, dans une dynamique d'amélioration continue.	**6 heures**

En partenariat avec

La Région Auvergne-Rhône-Alpes

Cofinancé par l'Union européenne

LA FRENCH TECH ALPES

France Travail