EXPERT CYBERSECURITE

Titre professionnel : BAC+3/4 (Niveau 6) / Code RNCP : 37680
Certificateur : Ministère du travail du plein emploi et de l'insertion
Validité du titre jusqu'au : 01/09/2026

L'ÉCOLE TECH,
OÙ QUE VOUS SOYEZ !

www.oclock.io

EXPERT CYBERSECURITE

TITRE PROFESSIONNEL
BAC+3/4 (NIVEAU : 6)
CODE RNCP : 37680

“

NEUF MOIS POUR ENTRER DANS LE MONDE DE L’INFRASTRUCTURE RESEAU ET DE LA CYBERSECURITE

La formation “Expert Cybersécurité” est proposée sur le format téléprésentiel, d’une durée de 9 mois (798 heures théoriques + 350 heures pratiques), prépare au Titre Professionnel “Administrateur d’Infrastructures sécurisées”.

Format 100 % téléprésentiel (FOAD)

La formation se déroule entièrement à distance grâce au format téléprésentiel. Celui-ci prévoit une obligation de présence à distance aux cours animés en direct vidéo par le formateur, ainsi qu’à des travaux dirigés encadrés.

La formation a lieu tous les jours ouvrés de 9 h à 17 h.

Des temps de travaux dirigés sont prévus tout le long de la formation. Ils ont le plus souvent lieu à partir de 15 h, après un cours en salle de classe virtuelle.

Les apprenants doivent alors réaliser au moins deux heures de travail dirigé en suivant les consignes du formateur (challenges, etc.).

Un espace d’échange partagé entre l’équipe pédagogique et les apprenants permet d’encadrer la progression et d’encourager l’entraide entre pairs pour la réalisation des travaux dirigés.

CONDITIONS D'INTÉGRATION

PUBLIC VISÉ

- Tout public en reconversion : demandeur d'emploi ou salarié.
- Public avec une reconnaissance RQTH : un accompagnement spécifique peut être dédié à chaque personne qui le formalise auprès de notre service "Admissions". Notre référent handicap évaluera les adaptations nécessaires au bon suivi de la formation.

PRÉ-REQUIS

- La motivation et la capacité à s'inscrire dans un parcours de formation
- Les compétences informatiques et numériques de base en lien avec le référentiel européen des compétences digitales
- La capacité à résoudre des problèmes de logique simples
- Le niveau de compréhension en anglais (lecture principalement) équivalent à un niveau A2

NOTRE OBJECTIF ?

VOUS OUVRIR LES PORTES DU MONDE DE L'INFRASTRUCTURE ET DE LA CYBERSECURITÉ POUR Y DÉBUTER VOTRE NOUVELLE CARRIÈRE

MODALITÉ D'ACCÈS

- **Tests d'aptitude :** connaissances en informatique et numérique, capacité à manipuler des concepts logiques .
- **Une évaluation de la motivation :** échange avec un conseiller admissions, pour évaluer :
  - Le parcours scolaire et professionnel, en vue du positionnement sur la formation visée
  - Les compétences de base nécessaires pour optimiser l'intégration
  - La pertinence du projet professionnel "post formation"
  - Le matériel requis (poste informatique, connexion)

Objectifs DE LA FORMATION

La formation est validée par le passage du Titre professionnel “Administrateur d’Infrastructures sécurisées”, diplôme de niveau 6 (BAC+4), inscrit au Répertoire National des Certifications Professionnelles (RNCP)

1. ADMINISTRER ET SECURISER 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 OEUVRE UNE SOLUTION EN REPONSE 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

ENCADREMENT PÉDAGOGIQUE

Les formateurs

Chaque formateur qui enseigne chez O'clock a déjà plusieurs années d'expérience dans les métiers visés, mais aussi une expérience dans la formation.

En fonction du public accueilli (reconnaissance RQTH), une équipe formée et dédiée peut être mobilisée afin d'enseigner à des personnes en situation de handicap. Les cours seront enregistrés en vidéo afin de pouvoir être visionnés à tout moment.

LES TUTEURS

Leurs missions :
- Accompagner individuellement les apprenants pour l'acquisition des notions abordées, la préparation au passage de la certification.
- S'assurer de leur capacité à s'approprier les outils techniques nécessaires au suivi de la formation et de se coordonner si besoin avec l'équipe technique afin de s'assurer que les apprenants disposent des outils et matériels requis.
- Établir les relais auprès des différents acteurs de l'équipe pédagogique afin de répondre aux besoins des apprenants, de prévenir les abandons ou ruptures de parcours.
- Impulser, entretenir la dynamique de groupe et d'entraide au sein du collectif "apprenant".

LES CONSEILLERS PARCOURS APPRENANTS & CARRIÈRE

Une équipe de conseillers parcours apprenants est à disposition des stagiaires afin de leur proposer un accompagnement individuel relatif à des problématiques péri-pédagogiques. Cet accompagnement se fait à la demande du stagiaire et/ou de l'équipe pédagogique et se concrétise par la conduite d'entretiens individuels, confidentiels.
Les conseillers parcours apprenants peuvent être amenés à orienter les stagiaires vers des structures et dispositifs répondant à leur problématique de réinsertion post formation.

MANAGER & RÉFÉRENT HANDICAP

Le rôle de notre référent handicap est de favoriser l'inclusion, et de permettre à tout apprenant, quel que soit son handicap (visible ou invisible), de réaliser sa formation avec les moyens (matériels et humains) dont notre organisme dispose.
Les besoins en matériels spécifiques (selon le handicap) peuvent être financés (en totalité ou en partie) par l'AGEFIPH. Ces demandes doivent être formulées en amont du parcours visé.
Chaque apprenant avec une reconnaissance RQTH pourra demander l'appui, l'aide et l'accompagnement de notre référent handicap, en plus des moyens pédagogiques mis à disposition.

EXPERT CYBERSECURITÉ

LE PROGRAMME

SAVOIRS DE BASE (63H) — MODULE A1

Histoire de l'informatique, bits/octets, adresse IP, composants et assemblage d'un PC, installation de système d'exploitation

CENTRES DE SERVICES (70H) — MODULE A2

Démarche ITIL, gestion de parc et ticketing avec GLPI, assistance des utilisateurs, résolution d'incidents

RESEAUX (70H) — MODULE A3

Administration de réseaux d'entreprise, Modèle OSI, protocoles DHCP, DNS, Adressage IPv4 et IPv6, NAT, routage statique.

WINDOWS SERVER (105H) — MODULE A4

Administration système Windows (client et serveur), Active Directory et protocole LDAP, GPO, déploiement de logiciels.

GNU/LINUX (70H) — MODULE A5

Administration système GNU/Linux (client et serveur), stack LAMP, licences logicielles et logiciel libre.

VIRTUALISATION (35H) — MODULE B1

Hyperviseurs de type 1 et 2, cluster et basculement automatique, haute disponibilité.

STOCKAGE & SAUVEGARDE (35H) — MODULE B2

Mise en oeuvre d'une stratégie de sauvegarde, solutions de stockage NAS/SAN, élaboration d'un plan de reprise ou de continuité informatique.

SUPERVISION (35H) — MODULE B3

Supervision d'infrastructure avec Zabbix, Prometheus/Grafana, et d'autres solutions fréquemment rencontrées.

EXPERT CYBERSECURITÉ

LE PROGRAMME

SCRIPTING (70H) — MODULE B4

Langage Python, scripts shell Bash et Powershell, gestion de versions avec Git, automatisation.

GESTION DE PROJET ET ANALYSE DE RISQUE (35H) — MODULE C1

Élaboration d'une politique de sécurité, méthodes de gestion des risques et gestion de projet Agile.

CLOUD (35H) — MODULE C2

Administration Microsoft 365, IaaS/PaaS/SaaS, découverte des plateformes AWS/GCP/Azure.

SÉCURITÉ SYSTÈME & RÉSEAU (70H) — MODULE C3

Routage dynamique, pare-feu, VPN, agrégation/redondance, durcissement de système d'exploitation.

CONTENEURS ET ORCHESTRATION (35H) — MODULE C4

Conteneurs Docker, orchestration avec Kubernetes et Docker Swarm.

PENTESTING (35H) — MODULE C5

Tests d'intrusion, audit de sécurité, SOC.

PROJET TUTORÉ / RÉVISION (21H)

Mise en situation professionnelle

ACCOMPAGNEMENT PREPARATION A L'EMPLOI & PREPARATION AU TITRE PROFESSIONNEL (14H)

Rédaction des dossiers à présenter (Dossier professionnel et Dossier de projet), Modalités de la journée de certification, Préparation aux entretiens, Atelier CV et LinkedIn, Techniques de recherche d'emploi

STAGE OBLIGATOIRE (350H)

SÉQUENCEMENT DU PARCOURS

Tout au long du parcours théorique, différents projets professionnels seront réalisés afin de développer et acquérir les compétences du titre, comme en situation réelle (emploi).

Conformément au référentiel de certification, accompagnement et préparation au passage du Titre Professionnel d'Administrateur d'Infrastructures Sécurisées de niveau 6.

Séquencement du parcours :
- 798 heures théoriques
- 7 heures/jour
- FOAD : Formation synchrone
- 350 heures de stage pratique en entreprise

L'ÉCOLE TECH,

OÙ QUE VOUS SOYEZ !

www.oclock.io

MODALITÉS TECHNIQUES

L'accès au contenu et aux ressources de la formation s'effectue par connexion à la plateforme BigBlueButton.
:

- Connexion internet : haut débit
- Équipements visioconférence : webcam, micro-casque

- PC ou Mac (à processeur Intel) avec les caractéristiques suivantes :
- 16Go de mémoire vive / RAM (strict minimum), 32Go recommandés
- Disque dur SSD obligatoire, avec idéalement au moins 100Go d'espace disque libre
- Processeur :
  - de type Intel Core i3, i5, i7 ou i9, ou AMD Ryzen
  - Celeron, Pentium et anciens processeurs AMD à bannir
  - Attention : Mac M1, M2, M3 ou M4 : non conforme pour suivre la formation dans de bonnes conditions.
- Deux écrans minimum (si PC portable, un seul écran externe supplémentaire suffit)
- Idéalement, prévoir un disque dur externe avec environ 500Go d'espace disponible. Ce n'est pas indispensable, mais très utile pour la formation.

NATURE DES TRAVAUX

Durant le cours, les apprenants réalisent les activités dont le formateur fait la démonstration, posent des questions et interagissent entre eux

Durant les travaux dirigés, les apprenants réalisent des travaux demandés par le formateur:

- Challenges individuels
- Challenges de groupe
- Lecture de documentation technique
- Veille technique et professionnelle

MOYENS D'ACCOMPAGNEMENT

Un formateur dédié et à temps plein est mis à disposition de groupes de 25 apprenants (en moyenne).
Chaque apprenant dispose :

- D'un accès individuel et sécurisé par VPN à la plateforme pédagogique
- D'un nom de domaine et un serveur d'hébergement
- D'une permanence pédagogique pendant les travaux dirigés

L'ÉCOLE TECH,

OÙ QUE VOUS SOYEZ !

www.oclock.io

MODALITÉS DE SUIVI ET D'ÉVALUATION

La participation à la formation est vérifiée par un ou plusieurs des moyens suivants :

- Les journaux de connexion (logs) à la plateforme pédagogique
- L'utilisation de la messagerie instantanée intégrée au cours
- Les réponses aux sondages envoyés par le formateur
- La vérification des travaux demandés par les formateurs, à des intervalles réguliers
- L'activité sur la messagerie instantanée pendant les activités de formation

L'évaluation des compétences est assurée par :

- Travaux dirigés
- Contrôle Continu
- Évaluations en cours de formation (ECF) réalisées dans le cadre du Titre Professionnel "Administrateur d'infrastructures Sécurisées"
- Entretiens individuels, sur demande du stagiaire ou de l'équipe pédagogique
- Conseils de classe internes entre chaque saison

Contrôle final :

- Session de validation du Titre Professionnel "Administrateur d'Infrastructures Sécurisées"

EXIGENCES DE LA CERTIFICATION VS PROGRAMME

Administrer et sécuriser les infrastructures

Appliquer les bonnes pratiques dans l'administration des infrastructures	- Identifier, classer, enregistrer et résoudre ou escalader des incidents - Planifier et réaliser des tâches de maintenance préventive - Démarche et pratiques ITIL - Rédaction de charte informatique et de procédures - RGPD & CNIL - Déontologie	Module A1 - Savoirs de base Module A2 - Centre de services Module C3 - Sécurité système & réseau
Administrer et sécuriser les infrastructures réseaux	- Maintien en conditions opérationnelles des réseaux - Topologies et types de réseaux - Modèles OSI & suite de protocoles TCP/IP - Adressage IPv4, IPv6, segmentation en sous-réseaux - Routage et interconnexion de réseaux - Optimisation et sécurisation de réseaux	Module A3 - Réseau Module B3 - Supervision Module C2 - Cloud Module C3 - Sécurité système & réseau
Administrer et sécuriser les infrastructures systèmes	- Maintien en conditions opérationnelles des systèmes - Déploiement et maintenance de systèmes - Savoir configurer et administrer Windows, client et serveur - Sécuriser l'accès aux ressources partagées - Exploiter un domaine Active Directory - Maintenir et exploiter un serveur GNU/Linux - Automatisation de tâches à l'aide de scripts	Module A4 - Windows Serveur Module A5 - GNU/Linux Module B1 - Virtualisation Module B4 - Scripting Module C3 - Sécurité système & réseau
Administrer et sécuriser les infrastructures virtualisées	- Virtualisation et conteneurisation - Clusters et hyperconvergence - Réseaux de stockage - Cloud computing : IaaS, PaaS et SaaS vs. on-premises - Gestion des identités et accès	Module B1 - Virtualisation Module B2 - Stockage & sauvegarde Module B3 - Supervision Module C2 - Cloud Module C3 - Sécurité système & réseau Module C4 - Conteneurs et orchestration

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	- Gestion de la DSI et gestion de projets - Méthodes d'analyse et de gestion des risques - Accords de niveaux de service - Respect des contraintes budgétaires, environnementales, de sécurité.	Module C1 - Gestion de projet et analyse de risque Module C2 - Cloud Module B1 - Virtualisation Module C4 - Conteneurs et orchestration
Mettre en production des évolutions de l'infrastructure	- Intégrer de nouvelles solutions - Évaluer et valider les étapes et procédures de mise en production pour limiter les risques - Automatisation du déploiement	Module A4 - Windows Serveur Module A5 - GNU/Linux Module B4 - Scripting Module C1 - Gestion de projet et analyse de risque
Mettre en œuvre et optimiser la supervision des infrastructures	- Choix des indicateurs à surveiller - Mettre en oeuvre et optimiser les outils de supervision - Support et pilotage des infrastructures du SI	Module A3 - Réseau Module B1 - Virtualisation Module B3 - Supervision Module C1 - Gestion de projet et analyse de risque Module C2 - Cloud

Participer à la gestion de la cybersécurité

Participer à la mesure et à l'analyse du niveau de sécurité de l'infrastructure	- Réalisation de tests d'intrusion, d'audit de sécurité - Utilisation de Kali Linux ou autre distribution spécialisée - Analyse des risques cyber - Encadrement d'audits réalisés par des tiers	Module C1 - Gestion de projet et analyse de risque Module C3 - Sécurité système & réseau Module C5 - Pentesting
Participer à l'élaboration et à la mise en œuvre de la politique de sécurité	- Participation à la définition et à l'application d'une politique de sécurité - Rédaction d'un plan de reprise ou de continuité informatique/d'activité - Formation des utilisateurs - Proxy, VPN, pare-feu, systèmes de détection d'intrusion - Acteurs de la cybersécurité - Mise en place et test de sauvegardes	Module B2 - Stockage & sauvegarde Module C1 - Gestion de projet et analyse de risque Module C3 - Sécurité système & réseau Module C5 - Pentesting
Participer à la détection et au traitement des incidents de sécurité	- Détection d'intrusion, surveillance du réseau et des systèmes - Vulnérabilités courantes et contre-mesures - Gestion et communication de crise - Participation à la rédaction de RETEX - Veille en cybersécurité	Module A4 - Windows Serveur Module A5 - GNU/Linux Module B2 - Stockage & sauvegarde Module B3 - Supervision Module C3 - Sécurité système & réseau Module C5 - Pentesting

MODALITÉS D'ÉVALUATION DANS LE CADRE DU TITRE PROFESSIONNEL

- Présentation d'un projet réalisé en amont de la session
- Entretien technique
- Questionnaire professionnel
- Entretien final (avec analyse des ECF)

CONCLUSIONS DU JURY HABILITÉ

- Obtention : lorsque le candidat a montré, lors de l'examen, la maîtrise de l'ensemble des compétences (CCP) requises pour le titre.
- Réussite partielle : lorsque le candidat a montré la maîtrise de l'ensemble des compétences requises pour un, ou plusieurs CCP.
- Refus : lorsque le candidat ne maîtrise pas suffisamment de compétences pour valider l'un des CCP du titre.

En cas d'échec ou de réussite partielle, le candidat peut représenter, le ou les CCP non validés, selon les conditions définies par les arrêtés relatifs au TP.

DÉLAI D'ACCÈS À LA FORMATION

2 semaines avant la session visée (selon les places disponibles)

PASSERELLE / POURSUITE D'ÉTUDE

Titre professionnel de niveau 7, dans le domaine de l'informatique et de l'infrastruture, cybersécurité.

PRIX DE LA FORMATION

La formation Expert Cyber Securité est au prix de 8793,96 euros TTC

CONTACT

Rapprochez-vous de votre conseiller formation
ou sur www.oclock.io
ou appelez-nous au 01.89.71.65.30

STATISTIQUES

Année d'obtention de la certification	Nombre de certifiés	Nombre de certifiés à la suite d'un parcours VAE	Taux d'insertion global à 6 mois (en %)	Taux d'insertion dans le métier visé à 6 mois (en %)	Taux d'insertion dans le métier visé à 2 ans (en %)
2021	250	6	67	62	80

Source Fiche RNCP37680 (France compétences)

Document actualisé le 23.04.2025