

# Certificat de Spécialisation : cybersécurité

Mis à jour le 2 juin 2025

## Conditions d'entrée et prérequis

Être titulaire d'un baccalauréat.

## Niveau d'entrée

Niveau 4 - BAC

## Niveau de sortie

Niveau 4 - BAC

## Public visé

Etre âgé de 16 à 29 ans, avec un projet de contrat d'apprentissage. Dérogations sous conditions. Pas de condition d'âge pour les personnes reconnues en situation de handicap (RQTH).

## Rythme

Alternance

## Durée en centre

400 heures

## Validation

Obtention de la Certification de Spécialisation « cybersécurité ». En cas d'échec au diplôme, des blocs de compétences pourront être délivrés en fonction des résultats obtenus dans des différentes disciplines.

## Modalités d'évaluation

Contrôle continu, Contrôles en Cours de Formation et/ou épreuves terminales. Conformés au référentiel de certification du diplôme. Unités certificatives (blocs de compétences) constitutives du diplôme :

- Épreuve/Unité (EU)–01. Mise en œuvre de réseaux

## Objectifs professionnels

Le certificat de spécialisation « Cybersécurité » vise à certifier des techniciennes et techniciens capables d'intervenir sur l'installation, l'exploitation et la maintenance des réseaux informatiques notamment dans un environnement industriel. Le technicien participe à la sécurisation des données, des applications, des infrastructures numériques, des produits et des équipements. Il contribue à la gestion des incidents, à l'audit des installations et systèmes, ainsi qu'à la diffusion d'une culture d'hygiène informatique.

Véritable enjeu de souveraineté, ce diplôme s'inscrit dans un contexte de développement de la connectivité des produits avec des risques très élevés de cyberattaques.

## Contenu

**Activités professionnelles** : installation et qualification, exploitation et maintien en condition opérationnelle, gestion de projet et d'équipe, accompagnement du client, maintenance des réseaux informatiques, élaboration et appropriation d'un cahier des charges, audit de l'installation ou du système, gestion d'incidents.

### Connaissances générales et techniques associées :

**Mise en œuvre de réseaux informatiques** : Valider le fonctionnement d'un réseau, coder, installer une infrastructure réseau, exploiter une installation réseau, maintenir un réseau.

**Cybersécurité** : Communiquer en situation professionnelle (français/anglais), analyser une installation réseau, organiser une intervention, gérer un projet.

## Modalités pédagogiques

Intégration dans une classe d'élève ou d'étudiants du lycée.

Alternance de périodes de formation en lycée et de formation en entreprise selon calendrier établi.

## Profil des intervenants

Enseignants de l'Education Nationale

## Possibilité d'aménagement du parcours

Oui

## Méthodes pédagogiques

En Lycée : apports théoriques, mises en situation, travaux pratiques, exposés, débats, études cas. Utilisation des plateaux techniques et équipements, CDI, cours à distance...

En entreprise : apprentissage basé sur l'expérience et la réalisation d'activités et de tâches en lien avec le diplôme préparé. L'apprenti est guidé et accompagné par un maître d'apprentissage.

# Certificat de Spécialisation : cybersécurité

informatiques

- Épreuve/Unité (EU)–02.  
Cybersécurité

## Possibilité de validation par blocs de compétences

Oui

## Nombre de participants

Variable selon le nombre de places  
disponibles dans les classes

## Entrée et sortie permanente

Oui

## Codes réglementaires

- Code RNCP : [RNCP37488](#)
- Code diplôme : 46125509

## Moyens pédagogiques

Plateaux techniques adaptés aux compétences professionnelles du diplôme préparé – Salles de cours équipées – ordinateurs – centre de ressources – Espace Numérique de Travail

## Durée

Durée moyenne de la formation en centre pour un contrat de 1 ans : 400 heures La durée de la formation en lycée sera ajustée en fonction de la durée du contrat et des acquis de l'apprenti dans le respect des minima réglementaires

## Délais et modalités d'accès

Entrée sept/nov principalement  
Autres périodes d'intégration sous conditions

## Financements possibles

Entreprises relevant du secteur privé : application des niveaux de prise en charge définis par France Compétences. Coûts de la formation pris en charge par les OPCO. Frais annexes (hébergement, restauration, 1er équipement, mobilité internationale, handicap) pris en charge par les OPCO sous conditions.

Organisations relevant du secteur public : application des niveaux de prise en charge définis par chaque fonction publique.

## Poursuite de parcours

### Insertion professionnelle

Le certificat de spécialisation « cybersécurité » permet d'entrer dans la vie professionnelle. Les métiers concernés par la gestion de la cybersécurité peuvent se retrouver dans les domaines de la cybersécurité industrielle ou dans le domaine des objets connectés.

Les emplois pouvant être exercés sont : intégrateur ou intégratrice de solutions de sécurité, opérateur ou opératrice en cybersécurité, technicien ou technicienne de maintenance en informatique, installateur ou installatrice de réseaux informatiques ...

**Poursuite d'études** : Possibilité de poursuivre en BTS Cybersécurité, Informatique et Réseaux, Electronique.

**Passerelles et Equivalences** : En fonction du parcours de formation des équivalences et passerelles sont envisageables, se renseigner auprès du lycée ou du CIO.

## Référent handicap

Locaux accessibles aux personnes à mobilité réduite. Accompagnement

# Certificat de Spécialisation : cybersécurité

spécifique au projet et durant la formation en lien avec notre référent handicap.

## Réseau

- GIP FCIP – CFA de l'académie de Reims
- 17, boulevard de la Paix CF 50033  
51722 REIMS CEDEX
- cfa@ac-reims.fr
- Marne : 07 76 15 77 62  
Ardennes : 06 13 02 47 51  
Haute-Marne et Aube Est : 06 17 83 54 69  
Aube : 06 27 48 88 64
- cfa.gipfcip-reims.fr
- SIRET : 185 109 063 00031
- Numéro d'activité : 21 51 P003 751
- Date d'obtention : 11/03/2003