

# Formation

## Expert en développement de solutions de cybersécurité-



Niveau BAC+5 (Niveau 7) · Titre inscrit au RNCP (fiche 38463)

### OBJECTIFS DE LA FORMATION

Cette formation te prépare à analyser les besoins en cybersécurité d'une entreprise et à proposer des solutions adaptées.

Tu apprends à concevoir, développer, tester et intégrer des outils de sécurité fiables. Tu es formé à repérer les failles, sécuriser les systèmes et améliorer les solutions existantes. Le parcours développe aussi des compétences en gestion de projet, veille technologique et pilotage d'équipe.

L'objectif : devenir capable de créer et déployer des solutions concrètes face aux cybermenaces.

**Aptitudes à l'emploi** · Rigoureux – Curieux – Méthodique – Réactif – Analytique – Fiable

**Compétences** · Mettre en place une stratégie de cybersécurité dans une démarche de développement de solutions

- Analyser les besoins, les risques et les contraintes; Définir une stratégie de cybersécurité adaptée.
- Piloter le projet et assurer une veille sur les innovations du secteur.

**Compétences** · Construire des solutions de cybersécurité en utilisant les technologies émergentes

- Auditer l'existant et repérer les failles et développer des solutions conformes aux bonnes pratiques.
- Utiliser des technologies comme l'IA, le machine learning ou les systèmes embarqués.

**Compétences** · Intégrer des solutions de cybersécurité dans le système d'information

- Prototyper, tester et valider une solution de sécurité ainsi que préparer son déploiement
- Accompagner les équipes et prévoir les évolutions nécessaires.

**Compétences** · Assurer la mise en exploitation et la maintenance de solutions de cybersécurité développées

- Mettre la solution en service auprès des utilisateurs.
- Identifier et corriger les dysfonctionnements ou vulnérabilités et suivre les incidents et améliorer la solution dans le temps.

**Compétences** · Animer et encadrer une équipe au quotidien et en mode projet

- Encadrer une équipe projet, animer des réunions, partager les informations clés et organiser le travail
- Vulgariser les sujets techniques auprès des équipes et des décideurs.



### FORMATION

#### Dates de démarrage et de fin de formation

Octobre 2026 - Septembre 2028

#### Durée

2 ans en alternance sous contrat d'apprentissage

**Le CFA IFIR t'accompagne dans ta recherche d'entreprise.**

#### Rythme d'alternance

1 semaine en centre de formation, 3 semaines en entreprise

#### Lieux de formation possibles

- FORMATIK- La Fouillouse (42)

#### Conditions tarifaires

Formation financée par les OPCO\* et gratuite pour les apprentis avec une participation obligatoire de 750€ pour les employeurs (Décret n° 2025-585 du 27 juin 2025 relatif à la prise en charge des actions de formation par apprentissage).

\*OPCO : Opérateurs de compétences

### PRÉ-REQUIS

Conditions de diplôme et d'expérience

Être titulaire d'un titre ou diplôme de niveau 6 (Bac+3/4) dans le domaine de l'informatique ou des sciences de l'ingénieur.

OU justifier d'une expérience professionnelle d'au moins trois ans ans le champ de la certification visée.

Des admissions exceptionnelles peuvent être accordées par dérogation pour :

\* Les profils ayant exercé plusieurs années des fonctions informatiques de haut niveau (notamment dans le cadre d'une évolution de poste proposée par l'employeur).

\* Les personnes en reconversion professionnelle.

\* Les candidats engagés dans une démarche de Validation des Acquis de l'Expérience (VAE).

Cette formation est accessible aux personnes en situation de handicap et/ou titulaires d'une Reconnaissance de la Qualité de Travailleur Handicapé (RQTH).

\*Pas de limite d'âge pour les personnes bénéficiant d'une Reconnaissance de la Qualité de Travailleur Handicapé.

### MODALITÉS DE RECRUTEMENT & DÉLAIS D'ACCÈS

Étude du dossier, entretien individuel & test de positionnement écrit (si besoin) avant la date d'entrée en formation.

Le recrutement s'organise par le dépôt d'un dossier de candidature en ligne sur le site : [www.ifir.fr/candidature-en-ligne](http://www.ifir.fr/candidature-en-ligne)

### ACCESSIBILITÉ AUX PUBLICS EN SITUATION DE HANDICAP

Pour tout besoin spécifique et toute adaptation, consultez notre référente H+ :

Diane BERLUCCHI · [referenthandicap@ifir.fr](mailto:referenthandicap@ifir.fr)

### CONTACTS

Contacte ton interlocutrice privilégiée pour un accompagnement plus précis !

Aurélien Le Beller · 06 40 67 23 19 · [alebeller@ifir.fr](mailto:alebeller@ifir.fr)



### ET APRÈS LA FORMATION ?

#### Que fait le titulaire de cette formation ?

Le titulaire du titre Expert en développement de solutions de cybersécurité conçoit et déploie des solutions pour protéger les systèmes d'information des entreprises. Son rôle ? Analyser les risques, imaginer des outils de sécurité adaptés, piloter leur développement, les tester, puis accompagner leur mise en place. Il peut aussi encadrer une équipe projet, assurer la maintenance des solutions développées et proposer des améliorations face à l'évolution des cybermenaces.

#### Emplois accessibles

• **Postes** : lead-concepteur cybersécurité, expert développeur en produits de sécurité, consultant expert DevOps, intégrateur expert de solutions de sécurité, Security Product Developer Manager, consultant expert en cybersécurité.

• **Divers secteurs** : association, caisse d'allocations familiales, caisse d'assurance maladie, crèche parentale, service d'éducation et de soin à domicile, collectivité territoriale, etc.

#### Poursuite d'études

Cette formation prépare principalement à l'insertion professionnelle sur des postes d'expertise, car elle correspond à un niveau 7, soit un niveau Bac +5.

#### Équivalences

Nous contacter pour étudier les éventuelles possibilités d'équivalences.

#### Passerelles

Nous contacter pour étudier les éventuelles passerelles possibles (en fonction du parcours et du site de formation).

### MODALITÉS D'ÉVALUATION

Bloc de compétence	Mode
BC01 - Mettre en place une stratégie de cybersécurité dans une démarche de développement de solutions	L'ensemble des évaluations se font sous la forme de mise en situation au travers d'étude cas d'entreprise (réels et/ou fictifs).
BC02 - Construire des solutions de cybersécurité en utilisant les technologies émergentes	L'ensemble des évaluations se font sous la forme de mise en situation professionnelle, d'étude cas d'entreprise (réels et/ou fictifs) et sous la forme d'une questionnaire à visée professionnelle.
BC03 - Intégrer des solutions de cybersécurité dans le système d'information	L'ensemble des évaluations se font sous la forme de mise en situation professionnelle et d'étude cas d'entreprise (réels et/ou fictifs).
BC04 - Assurer la mise en exploitation et la maintenance de solutions de cybersécurité développées	L'ensemble des évaluations se font sous la forme de mise en situation professionnelle (réelle et/ou fictive)
BC05 - Animer et encadrer une équipe au quotidien et en mode projet	L'ensemble des évaluations se font sous la forme de mise en situation au travers d'étude cas d'entreprise (réels et/ou fictifs).