

Expert en architectures sécurisées des systèmes d'information

RNCP40165 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326, 326n
Formacode(s)	31009, 31006, 31094
Code(s) ROME	M1802, M1803, M1804, M1805, M1806
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	31/01/2025
Date d'échéance	31/01/2028

Certificateur(s)

ASSOCIATION SUP DE VINCI (CFA LEONARD DE VINCI) · SIRET : 40955435900037

Partenaires habilités

6 organismes habilités, d'après la liste publiée par France compétences : 6 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
ASSOCIATION SUP DE VINCI (CFA LEONARD DE VINCI)	40955435900037	Former et organiser l'évaluation
ASSOCIATION SUP DE VINCI (CFA LEONARD DE VINCI)	40955435900078	Former et organiser l'évaluation
FACULTE DES METIERS DE L ESSONNE	45235951600021	Former et organiser l'évaluation
SDV-ISI-BORDEAUX	90289074800020	Former et organiser l'évaluation
SDV-ISI-BORDEAUX	90289074800038	Former et organiser l'évaluation
SDV-ISI-BORDEAUX	90289074800046	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

Avec de plus en plus de données à défendre (donc plus de risques), des attaques qui se perfectionnent (donc plus de risques aussi), le développement de la sécurité informatique à tous les niveaux des cycles de vie, l'IA pour optimiser les réponses, les process face aux cyberattaques qui se développent et industrialisent, le DevSecOps qui apparaît en réponse face à un renforcement de la sécurité informatique, ... notre certification a pour objectif de permettre une employabilité durable sur le marché du travail avec des compétences attestées relatives aux besoins actuels et à venir en termes d'architectures sécurisées des systèmes d'information.

ACTIVITÉS VISÉES

Pilotage de la veille et de l'innovation

Analyse de la demande du client interne / externe, et des architectures logicielles et systèmes

Définition d'une stratégie dans le cadre d'un projet de sécurité informatique des SI

Participation au déploiement commercial des services numériques et fidélisation de la relation client

Cadrage technique et méthodologique d'un projet de sécurisation de l'information

Evaluation de la performance d'un projet de sécurisation de l'information
Management d'équipe dans le cadre d'un projet de sécurisation de l'information
Implémentation de la gouvernance des SI
Gestion des risques dans le cadre d'un projet de sécurisation de l'information
Garantie de la conformité dans le cadre d'un projet de sécurisation de l'information
Pilotage de l'investigation numérique
Direction d'un plan de réponse à incidents en cas de cyberattaque
Pilotage du retour d'expériences dans le cadre d'une cybermenace
Supervision de l'intégration de la sécurité dans le cycle de développement
Pilotage du renforcement de la résilience et de la sécurité des systèmes
Optimisation des processus de sécurité opérationnelle

COMPÉTENCES ATTESTÉES

Développer un dispositif de veille basé sur un process structuré afin d'être force de proposition et guider les choix du client dans l'utilisation et l'évolution des solutions, standards et réglementations de sécurité des SI.

Manager l'innovation, dans ses dimensions technologique, organisationnelle et économique, via des outils de conception et prototypage, afin de piloter la construction et l'implémentation de solutions SI innovantes sur le long terme.

Identifier les attentes et besoins utilisateurs et contraintes du client final et de la DSI, dans leur temporalité actuelle et prévisionnelle, dans le but de concevoir une solution informatique conforme aux exigences métier.

Analyser les architectures logicielles, via une topologie logicielle, afin d'identifier les points faibles et les vulnérabilités potentielles.

Évaluer les architectures systèmes et réseaux, via une topologie systèmes et réseaux, en vue d'identifier les vulnérabilités structurelles.

Diagnostiquer la problématique du client, via une étude contextualisée de l'environnement internet et externe du client, afin d'orienter la solution.

Définir une stratégie de sécurité de l'information et un plan d'action adaptés aux enjeux du client ainsi qu'à sa politique de sécurité des systèmes d'information, sur la base des spécifications fonctionnelles, en collaboration avec l'équipe technique informatique du client, en tenant compte des attentes éthiques, réglementaires et sociétales, dans l'optique d'améliorer le niveau de service à l'entreprise.

Déployer une approche Green IT et Low-tech, en identifiant les technologies durables et promouvant des pratiques respectueuses de l'environnement, en encourageant des comportements écoresponsables au sein de l'organisation, en vue de contribuer au développement d'une activité économique durable.

Présenter la solution informatique proposée, en utilisant des techniques de communication et de négociation, afin de convaincre le client que le dispositif choisi lui permettra d'atteindre ses objectifs.

Participer au développement de la relation client, par le biais de techniques commerciales et développement de process organisationnels, en identifiant les possibles opportunités gagnant gagnant pour les clients et sa propre organisation dans le but de viser la satisfaction et la fidélisation du client.

Rédiger les spécifications techniques à partir des besoins identifiés et en correspondance avec les exigences fonctionnelles ainsi que les contraintes du projet, afin de définir le périmètre de réalisation du projet.

Assurer la conception méthodologique d'un projet informatique complexe de sécurisation des SI, à partir d'un besoin identifié, éventuellement au travers de la participation à l'élaboration / la réponse à un appel d'offres, via une méthodologie de projet informatique, dans l'optique d'optimiser sa réussite en fonction des ressources allouées ainsi que dans une démarche numérique responsable et conforme à la réglementation en vigueur.

Planifier le projet, en déterminant les ressources à allouer, afin de garantir l'atteinte des objectifs fixés.

Décrire la solution informatique et ses fonctionnalités, la structure des bases de données et le schéma général de la sécurité de façon organisé et adapté aux différentes étapes du projet afin de produire une documentation adaptée au suivi du projet et à la maintenance de l'outil produit.

Contrôler et mesurer l'avancement du projet, en termes de coûts, délais, qualité et RSE, au travers d'indicateurs de mesure de la performance, dans l'optique d'obtenir une vision complète de l'avancement du projet / de l'utilisation des ressources en conformité avec le cahier des charges.

Estimer et suivre les coûts tout au long du cycle de vie du projet informatique, en employant des techniques de gestion budgétaire, en analysant le retour sur investissement, afin de garantir sa faisabilité ainsi que sa viabilité économique.

Conduire et superviser des collaborations professionnelles, en adoptant des méthodes et techniques de management

s'inscrivant dans une visée collaborative et inclusive, afin de développer les compétences individuelles et collectives, et inscrire le fonctionnement du groupe supervisé dans une démarche d'amélioration continue.

Mobiliser l'ensemble des parties prenantes, en valorisant le sens des actions menées dans les projets de transformation, au travers de la capitalisation des bonnes pratiques et de situations de travail favorisant l'intelligence collective, dans une logique de génération de valeur à différentes strates, aux niveaux micro, méso et macro.

Développer un réseau responsable de partenaires, en intégrant les dimensions de viabilité, équitabilité et durabilité dans la collaboration, afin de pérenniser l'activité.

Élaborer ou réviser une charte informatique déclinant la politique de sécurité des systèmes d'information, en définissant des règles et bonnes pratiques que doivent suivre les collaborateurs, en conformité avec le cadre légal et réglementaire en vigueur, dans le but de contribuer à la protection globale des actifs numériques de l'entreprise.

Rédiger un Plan de Reprise d'Activité au travers d'une démarche d'élaboration, afin de garantir la résilience des services critiques.

Identifier les vulnérabilités du SI via un audit de sécurité informatique, afin de gérer les risques potentiels des SI.

Prioriser les risques, sur la base d'une cartographie des risques ainsi qu'une matrice des risques, en tenant compte des exigences réglementaires en vigueur, afin de mettre en évidence les failles informatiques du SI.

Contrôler l'application des normes, méthodes et référentiels de sécurité informatique en vigueur, en s'appuyant sur les directives de la gouvernance des SI, dans le but de vérifier la conformité des SI en termes d'obligations sécuritaires.

Concevoir et déployer des actions de sensibilisation ciblée sur l'hygiène informatique visant à instaurer une culture de sécurité proactive et à renforcer l'adhésion des utilisateurs finaux aux standards de sécurité, dans le but d'améliorer le niveau global de sécurité au sein de l'organisation.

Pour piloter la résilience des infrastructures face aux cyberattaques :

Collecter des preuves, en garantissant son état de conservation, via la collecte de la mémoire vive et du disque dur, et avec l'aide de l'IA, pour mener à bien l'investigation numérique.

Mener l'investigation numérique, via des méthodes, techniques et outils de forensique, dans le but d'élaborer un diagnostic précis du profil de l'attaquant.

Définir une stratégie de réponse adaptée, en identifiant le niveau de criticité, en identifiant les macro-actifs critiques et en anticipant les impacts de la cyberattaque, en associant les moyens et ressources en charge de la cellule de crise, pour limiter les impacts stratégiques et opérationnels de l'entreprise.

Créer la cellule de crise, en réunissant l'ensemble des ressources nécessaires à la compréhension de l'attaque, afin d'aboutir aux prises de décisions stratégiques et opérationnelles nécessaires par le client.

Orchestrer la communication de crise auprès de l'ensemble des parties prenantes : N-users, instances gouvernementales, partenaires et fournisseurs en vue d'appliquer les obligations légales.

Réaliser un retour d'expériences post-attaque afin d'élever la maturité de la sécurité du système d'information et accompagner le retour au fonctionnement nominal.

Organiser des tests d'intrusion afin de développer la résilience des infrastructures du client.

Pour piloter l'alignement stratégique entre architectures et DevSecOps :

Intégrer les contrôles de sécurité dans les pipelines CI/CD pour une détection précoce des vulnérabilités.

Automatiser les tests de sécurité des applications, en utilisant des outils de SAST, DAST, et IAST, en vue d'optimiser les ressources.

Concevoir des processus pour appliquer des mesures de sécurité robustes, via des pratiques de robustness testing, afin de protéger les environnements cloud et on-premise contre les menaces émergentes.

Développer des stratégies de renforcement de la sécurité basées sur les meilleures pratiques et les normes de l'industrie dans le but de prévenir les attaques et les intrusions.

Développer des processus de standardisation et contrôler les pratiques de gestion des secrets et des identités, via une gestion des identités et des accès (IAM) pour minimiser les risques d'exposition.

Concevoir et déployer un dispositif de gestion des connaissances relatives à la sécurité informatique, dans le but de favoriser l'alignement des processus.

Blocs de compétences

RNCP40165BC01 — Définir la stratégie du projet de sécurisation des architectures des systèmes d'information

LISTE DE COMPÉTENCES

Développer un dispositif de veille basé sur un process structuré afin d'être force de proposition et guider les choix du client dans l'utilisation et l'évolution des solutions, standards et réglementations de sécurité des SI

Manager l'innovation, dans ses dimensions technologique, organisationnelle et économique, via des outils de conception et prototypage, afin de piloter la construction et l'implémentation de solutions SI innovantes sur le long terme

Identifier les attentes et besoins utilisateurs et contraintes du client final et de la DSI, dans leur temporalité actuelle et prévisionnelle, dans le but de concevoir une solution informatique conforme aux exigences métier

Analyser les architectures logicielles, via une topologie logicielle, afin d'identifier les points faibles et les vulnérabilités potentielles

Évaluer les architectures systèmes et réseaux, via une topologie systèmes et réseaux, en vue d'identifier les vulnérabilités structurelles

Diagnostiquer la problématique du client, via une étude contextualisée de l'environnement internet et externe du client, afin d'orienter la solution

Définir une stratégie de sécurité de l'information et un plan d'action adaptés aux enjeux du client ainsi qu'à sa politique de sécurité des systèmes d'information, sur la base des spécifications fonctionnelles, en collaboration avec l'équipe technique informatique du client, en tenant compte des attentes éthiques, réglementaires et sociétales, dans l'optique d'améliorer le niveau de service à l'entreprise

Déployer une approche Green IT et Low-tech, en identifiant les technologies durables et promouvant des pratiques respectueuses de l'environnement, en encourageant des comportements écoresponsables au sein de l'organisation, en vue de contribuer au développement d'une activité économique durable

Présenter la solution informatique proposée, en utilisant des techniques de communication et de négociation, afin de convaincre le client que le dispositif choisi lui permettra d'atteindre ses objectifs

Participer au développement de la relation client, par le biais de techniques commerciales et développement de process organisationnels, en identifiant les possibles opportunités gagnant-gagnant pour les clients et sa propre organisation dans le but de viser la satisfaction et la fidélisation du client

MODALITÉS D'ÉVALUATION

2 mises en situation professionnelle reconstituées ou réelles, relatives à l'ensemble du bloc de compétences :

- Evaluation 1 : Dossier écrit, en individuel portant sur la définition d'un projet de sécurisation des SI
- Evaluation 2 : Présentation orale, en individuel portant sur le référentiel de compétences du bloc de manière générale et la production écrite en particulier

RNCP40165BC02 — Manager un projet de sécurisation des architectures des systèmes d'information

LISTE DE COMPÉTENCES

Rédiger les spécifications techniques, à partir des besoins identifiés et en correspondance avec les exigences fonctionnelles ainsi que les contraintes du projet, afin de définir le périmètre de réalisation du projet

Assurer la conception méthodologique d'un projet informatique complexe de sécurisation des SI, à partir d'un besoin identifié, éventuellement au travers de la participation à l'élaboration / la réponse à un appel d'offres, via une méthodologie de projet informatique, dans l'optique d'optimiser sa réussite en fonction des ressources allouées ainsi que dans une démarche numérique responsable et conforme à la réglementation en vigueur

Planifier le projet, en déterminant les ressources (humaines, matérielles, techniques et financières) à allouer, afin de garantir l'atteinte des objectifs fixés

Décrire la solution informatique et ses fonctionnalités (User stories), la structure des bases de données et le schéma général de la sécurité de façon organisé et adapté aux différentes étapes du projet afin de produire une documentation adaptée au suivi du projet et à la maintenance de l'outil produit

Contrôler et mesurer l'avancement du projet, en termes de coûts, délais, qualité et RSE, au travers d'indicateurs de mesure de la performance, dans l'optique d'obtenir une vision complète de l'avancement du projet / de l'utilisation des ressources en conformité avec le cahier des charges

Estimer et suivre les coûts tout au long du cycle de vie du projet informatique, en employant des techniques de gestion budgétaire, en analysant le retour sur investissement, afin de garantir sa faisabilité ainsi que sa viabilité économique

Conduire et superviser des collaborations professionnelles, en adoptant des méthodes et techniques de management

s'inscrivant dans une visée collaborative et inclusive, afin de développer les compétences individuelles et collectives, et inscrire le fonctionnement du groupe supervisé dans une démarche d'amélioration continue

Mobiliser l'ensemble des parties prenantes, en valorisant le sens des actions menées dans les projets de transformation, au travers de la capitalisation des bonnes pratiques et de situations de travail favorisant l'intelligence collective, dans une logique de génération de valeur à différentes strates, aux niveaux micro, méso et macro

Développer un réseau responsable de partenaires, en intégrant les dimensions de viabilité, équitabilité et durabilité dans la collaboration, afin de pérenniser l'activité

MODALITÉS D'ÉVALUATION

2 mises en situation professionnelle reconstituées ou réelles, relatives à l'ensemble du bloc de compétences :

- Evaluation 1 : Dossier écrit, en individuel portant sur le management de projet de sécurisation de l'information
- Evaluation 2 : Présentation orale, en individuel portant sur le référentiel de compétences du bloc de manière générale et la production écrite en particulier

RNCP40165BC03 — Assurer la gouvernance, gestion des risques et de la conformité des architectures des systèmes d'information

LISTE DE COMPÉTENCES

Élaborer ou réviser une charte informatique déclinant la politique de sécurité des systèmes d'information (PSSI), en définissant des règles et bonnes pratiques que doivent suivre les collaborateurs, en conformité avec le cadre légal et réglementaire en vigueur, dans le but de contribuer à la protection globale des actifs numériques de l'entreprise

Rédiger un Plan de Reprise d'Activité (PRA), au travers d'une démarche d'élaboration, afin de garantir la résilience des services critiques

Identifier les vulnérabilités du SI, via un audit de sécurité informatique, afin de gérer les risques potentiels des SI

Prioriser les risques, sur la base d'une cartographie des risques ainsi qu'une matrice des risques, en tenant compte des exigences réglementaires en vigueur, afin de mettre en évidence les failles informatiques du SI

Contrôler l'application des normes, méthodes et référentiels de sécurité informatique en vigueur, en s'appuyant sur les directives de la gouvernance des SI, dans le but de vérifier la conformité des SI en termes d'obligations sécuritaires

Concevoir et déployer des actions de sensibilisation ciblée sur l'hygiène informatique visant à instaurer une culture de sécurité proactive et à renforcer l'adhésion des utilisateurs finaux aux standards de sécurité, dans le but d'améliorer le niveau global de sécurité au sein de l'organisation

MODALITÉS D'ÉVALUATION

3 mises en situation professionnelle réelles, relatives à l'ensemble du bloc de compétences :

- Evaluation 1 : Dossier écrit, en individuel portant sur l'analyse de l'implémentation de la gouvernance des SI dans le cadre d'un projet de sécurisation de l'information
- Evaluation 2 : Présentation orale, en individuel portant sur la gestion des risques et de la conformité dans le cadre d'un projet de sécurisation de l'architecture systèmes
- Evaluation 3 : Présentation orale, en individuel portant sur la gestion des risques et de la conformité dans le cadre d'un projet de sécurisation de l'architecture logicielle

RNCP40165BC04 — Option : Piloter la résilience des infrastructures face aux cyberattaques

LISTE DE COMPÉTENCES

Collecter des preuves, en garantissant son état de conservation, via la collecte de la mémoire vive et du disque dur, et avec l'aide de l'IA, pour mener à bien l'investigation numérique

Mener l'investigation numérique, via des méthodes, techniques et outils de forensique, dans le but d'élaborer un diagnostic précis du profil de l'attaquant

Définir une stratégie de réponse adaptée (ou suivre le plan si déjà existant), en identifiant le niveau de criticité, en identifiant les macro-actifs critiques et en anticipant les impacts de la cyberattaque, en associant les moyens et ressources en charge de la cellule de crise, pour limiter les impacts stratégiques et opérationnels de l'entreprise

Créer la cellule de crise, en réunissant l'ensemble des ressources nécessaires à la compréhension de l'attaque, afin d'aboutir aux prises de décisions stratégiques et opérationnelles nécessaires par le client

Orchestrer la communication de crise auprès de l'ensemble des parties prenantes : N-users, instances gouvernementales, partenaires et fournisseurs en vue d'appliquer les obligations légales

Réaliser un retour d'expériences post-attaque afin d'élever la maturité de la sécurité du système d'information et accompagner le retour au fonctionnement nominal

Organiser des tests d'intrusion afin de développer la résilience des infrastructures du client

MODALITÉS D'ÉVALUATION

2 mises en situation professionnelle reconstituées ou réelles, relatives à l'ensemble du bloc de compétences :

- Evaluation 1 : Dossier écrit, en individuel portant sur le pilotage de la résilience des infrastructures face à une cyberattaque
- Evaluation 2 : Présentation orale, en individuel portant sur le référentiel de compétences du bloc de manière générale et la production écrite en particulier

RNCP40165BC05 — Option : Piloter l'alignement stratégique entre architectures et DevSecOps

LISTE DE COMPÉTENCES

Intégrer les contrôles de sécurité dans les pipelines CI/CD pour une détection précoce des vulnérabilités

Automatiser les tests de sécurité des applications, en utilisant des outils de SAST , DAST , et IAST , en vue d'optimiser les ressources

Concevoir des processus pour appliquer des mesures de sécurité robustes, via des pratiques de robustness testing, afin de protéger les environnements cloud et on-premise contre les menaces émergentes

Développer des stratégies de renforcement de la sécurité basées sur les meilleures pratiques et les normes de l'industrie dans le but de prévenir les attaques et les intrusions

Développer des process de standardisation et contrôler les pratiques de gestion des secrets et des identités, via une gestion des identités et des accès (IAM).

pour minimiser les risques d'exposition

Concevoir et déployer un dispositif de gestion des connaissances relatives à la sécurité informatique, dans le but de favoriser l'alignement des processus

MODALITÉS D'ÉVALUATION

2 mises en situation professionnelle reconstituées ou réelles, relatives à l'ensemble du bloc de compétences :

- Evaluation 1 : Dossier écrit, en individuel portant sur le pilotage de l'alignement entre les architectures et la démarche DevSecOps
- Evaluation 2 : Présentation orale, en individuel portant sur le référentiel de compétences du bloc de manière générale et la production écrite en particulier

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

L'expert en architecture sécurisée des SI travaille majoritairement dans une société de services et plus précisément dans les activités informatiques.

Les offres d'emploi sont émises à 57% par des sociétés de conseils et services en informatique, s'ensuivent ensuite les domaines de l'architecture et de l'ingénierie informatique, le traitement-hébergement de données, les activités des sociétés holding, et enfin l'assurance.

TYPE D'EMPLOIS ACCESSIBLES

Principales fonctions visées : Analyste, Architecte, Chef de projet (dans un premier temps), Consultant, Ingénieur, Manager, Responsable

Domaines de spécialisation visés : Cloud, Cybersécurité, DevSecOps / DevOps, Etudes et développement informatique, Infrastructures, Réseaux, Sécurité informatique, Systèmes

RÈGLEMENTATIONS D'ACTIVITÉ

L'emploi-type cible n'est pas réglementé en lui-même mais il convient de tenir compte du cadre légal et réglementaire dans lequel les activités s'inscrivent, notamment par rapport aux normes, lois et directives suivantes : Règlement Général sur la Protection des Données (RGPD), Directive européenne Network and Information System Security (NIS), Norme ISO 27001, Normes sur l'écoconception des services numériques (notamment présentées dans un guide AFNOR SPEC 2201du même nom), Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques, Loi du 6 janvier 1978, dite « Informatique et Libertés », PCI-DSS, norme de sécurité de l'industrie des cartes de paiement est un standard de sécurité des données qui s'applique aux différents acteurs de la chaîne monétique.

Marché du travail

Indicateurs au niveau des familles professionnelles (FAP) des métiers visés, agrégés au niveau national — France Travail / DARES (open data).

Tension de recrutement (DARES 2024)	Très élevée (5/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 4 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 892 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (41 % des actifs en emploi)
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique · tension 4/5 (Élevée) M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée) M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom · tension 5/5 (Très élevée) M2X91 — Chefs de projet et directeurs de service informatique · tension 4/5 (Élevée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	42 073
Jugés difficiles à recruter	50 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom M2X91 — Chefs de projet et directeurs de service informatique M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

MODALITÉS D'ACCÈS

Formation initiale, Formation continue, Apprentissage, Contrat de professionnalisation, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Être titulaire d'un diplôme, titre professionnel ou certification professionnelle de niveau 6.
Ou être titulaire d'un diplôme, titre professionnel ou certification professionnelle de niveau 5, avec au moins 2 années d'expérience professionnelle dans le champ visé par la certification.
Une dérogation peut être accordée par le jury de sélection qui aura à statuer sur le non-respect d'un des critères prérequis.

PRÉREQUIS À LA VALIDATION

Par la voie de la formation : avoir suivi au moins 85% du parcours de formation

COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE, APPRENTISSAGE, CONTRAT DE PROFESSIONNALISATION

Le jury est composé de 3 membres minimum dont 2 professionnels externes

COMPOSITION DU JURY — VAE

Conformément au décret n° 2024-332 du 10 avril 2024 relatif au jury et au congé de validation des acquis de l'expérience, le jury de certification pour l'obtention par voie de la VAE réunit au moins deux personnes, dont au moins une personne qualifiée au titre de la certification visée

Financement en alternance (NPEC)

Niveau de prise en charge d'un contrat d'apprentissage par les OPCO, fixé par France compétences par branche professionnelle (CPNE).

Prise en charge usuelle	9 774 €
Selon la branche	7 500 € – 10 952 €
Prise en charge	Branches concernées
9 774 €	Valeur par défaut · 189 branches
10 952 €	CPNE Casinos, CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique, CPNE des Télécoms, CPNEF de l'audiovisuel, CPNEF des Espaces de Loisirs, d'Attractions et Culturels (ELAC)
9 992 €	CPNEF branche retraite complémentaire et prévoyance, CPNEFP Mutualité
9 556 €	CPNEFP Grands Magasins/ Magasins Populaires, CPNEFP du Négoce de l'ameublement
8 500 €	CPNEFP de la Mutualité Sociale Agricole, CPNEFP de la métallurgie
10 514 €	CPNE Travail Temporaire
10 268 €	CPNE de la branche de l'hospitalisation privée à statut commercial et du thermalisme
10 000 €	CPNEFP de l'enseignement privé indépendant
9 055 €	CPNEFP Habillement succursaliste
8 775 €	CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
8 750 €	CPNEFP Commerce à distance
8 400 €	CPNEFP de la branche des prestataires de services du secteur tertiaire
8 195 €	CPNE FP Branche des magasins du Bricolage
7 901 €	CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
7 700 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager
7 500 €	CPNE des industries de santé (CPNEIS)

Base légale

Date de décision	31/01/2025
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	31/01/2028
Date de dernière délivrance possible	31/01/2032

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2023	99	0	91 %	—
2022	65	0	98 %	—
2021	22	0	100 %	92 %
2020	39	0	98 %	92 %

Liens avec d'autres certifications

CORRESPONDANCES (PAR BLOCS)

RNCP35544, RNCP36296, RNCP36297, RNCP36469, RNCP38823, RS5145

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.supdevinci.fr/formations/mastere-specialisation-cybersecurite/>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/40165/>

Se former en apprentissage

Formations en apprentissage	5
Organismes gestionnaires (CFA)	2
Organismes formateurs	4
Régions couvertes	4
Départements couverts	4
Organismes certifiés Qualiopi	4
Sessions	de 09/2025 à 10/2028

Catalogue des formations en apprentissage — réseau des Carif-Oref. Sans frais pour l'alternant : formation financée par l'OPCO de la branche (NPEC).