

Expert en cybersécurité

RNCP40897 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326, 326n
Formacode(s)	31045, 31038, 31008, 42881
Code(s) ROME	M1802
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	25/06/2025
Date d'échéance	25/06/2028

Certificateur(s)

YNOV · SIRET : 53056211500101

Partenaires habilités

31 organismes habilités, d'après la liste publiée par France compétences : 31 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
AIRBUS OPERATIONS	42091691800 048	Former et organiser l'évaluation
AIROBJECT	53970902200 039	Former et organiser l'évaluation
AIX YNOV CAMPUS	52831294500 033	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE	39350481600 348	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE	39350481600 355	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600 090	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600 215	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600 223	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600 249	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600 272	Former et organiser l'évaluation

Liste complète des 31 partenaires habilités : <https://data.aktaconseil.fr/certifications/rncp40897-expert-en-cybersecurite/partenaires>

Résumé de la certification

OBJECTIFS ET CONTEXTE

Dans un contexte marqué par la recrudescence et la sophistication des cyberattaques, la cybersécurité est devenue un enjeu stratégique majeur pour les organisations. La certification "Expert en Cybersécurité" répond à cet impératif en combinant maîtrise technique et vision stratégique, garantissant aux professionnels les compétences essentielles pour protéger et accompagner les organisations face aux défis actuels et futurs.

Garant de la résilience numérique, l'expert en cybersécurité anticipe les risques, identifie les vulnérabilités et déploie des stratégies de défense adaptées aux menaces émergentes. Son expertise couvre la mise en conformité réglementaire, la surveillance des infrastructures, l'analyse des incidents et la gestion des crises cyber, contribuant ainsi à la sécurisation des systèmes d'information dans un environnement en constante évolution.

ACTIVITÉS VISÉES

Etude de l'écosystème de l'organisation

- Audit de l'organisation
- Identification des besoins métier, des actifs et des dépendances fonctionnelles.
- Elaboration de la cartographie du SI de l'organisation
- Réalisation d'une veille technologique, technique (ex : menace), normative et réglementaire
- Identification des obligations et opportunités d'amélioration
- Analyse des risques de sécurité pesant sur le SI de l'organisation
- Evaluation de la maturité du SI en termes de sécurité

Conception de la stratégie de sécurité du système d'information de l'organisation

- Définition de la Politique de sécurité du système d'information (PSSI) de l'organisation
- Intégration des référentiels normatifs et réglementation applicables
- Analyse des écarts entre la PSSI et le SI
- Priorisation des actions de sécurité à déployer
- Elaboration d'un plan d'actions de sécurité
- Estimation des ressources nécessaires (moyens et coût)
- Présentation du plan d'actions pour validation par les décideurs de l'organisation

Préparation du déploiement de la stratégie de sécurité au sein de l'organisation

- Elaboration du corpus documentaire de sécurité du SI de l'organisation
- Conception des plans de résilience du SI de l'organisation (plans de sauvegarde, de secours informatique, de reprise d'activité et de continuité d'activité)
- Elaboration du plan de sensibilisation et de formation des utilisateurs à la sécurité du SI
- Identification des besoins spécifiques des utilisateurs du SI
- Conception des contenus et support de formation et sensibilisation

Pilotage des projets d'intégration de solutions de sécurité du SI

- Rédaction des spécifications techniques et fonctionnelles des solutions de sécurité
- Planification du projet d'intégration des solutions de sécurité
- Allocation des ressources nécessaires
- Définition des échéances liées à l'intégration de la solution
- Suivi du projet d'intégration de la solution de sécurité
- Coordination des parties prenantes
- Supervision de l'exécution des tâches

Conception et intégration de solutions de sécurité du SI de l'organisation

- Conception d'une architecture sécurisée du SI
- Gestion des identités, des mécanismes d'authentification et contrôle des accès
- Déploiement de solutions cryptographiques pour protéger les données

Evaluation de l'efficacité des solutions de sécurité du SI mises en place

- Réalisation d'audits techniques de sécurité
- Rédaction d'un rapport d'audit technique
- Suivi des actions correctives

Gestion de l'obsolescence et des mises à jour du SI

- Définition d'une politique de gestion de l'obsolescence et des mises à jour du système d'information
- Réalisation des mises à jour ou des décommissionnements des actifs du SI

- Suivi des mises à jour et de l'obsolescence par la mise en place d'un tableau de bord et d'indicateurs

Contrôle et surveillance continue de la sécurité du SI de l'organisation

- Elaboration d'une politique de contrôle et de surveillance continue
- Mise en place d'un SOC au sein de l'organisation
- Déploiement des outils de détection des menaces et d'analyse avancée
- Définition des indicateurs clés
- Vérification du fonctionnement du SOC (test d'intrusion, simulation d'incidents...)

Détection et correction des vulnérabilités

- Détection et documentation des vulnérabilités
- Traitement des vulnérabilités identifiées

Elaboration d'une stratégie de gestion de crise

- Conception d'une stratégie de communication de crise
- Identification des parties prenantes à contacter en cas de crise
- Organisation d'une cellule stratégique de crise
- Mise en place des critères et des procédures d'activation de la cellule de crise
- Déploiement d'une stratégie d'entraînement de gestion de crise

Analyse des incidents détectés et endiguement

- Qualification et confirmation de l'incident détecté
- Endiguement de l'incident
- Analyse forensique de l'incident

Pilotage opérationnel de la remédiation de l'incident et capitalisation

- Mise en œuvre d'actions d'éviction et d'éradication
- Mise en œuvre des plans de restauration
- Réalisation d'une analyse post mortem
- Capitalisation sur la crise

COMPÉTENCES ATTESTÉES

B1.A1.C1. Auditer l'organisation en identifiant les besoins métiers, les acteurs et les dépendances fonctionnelles, en analysant les processus métiers, en évaluant les interactions entre les systèmes et en recueillant les attentes des parties prenantes afin de garantir une vision exhaustive du fonctionnement opérationnel de l'organisation.

B1.A1.C2. Etablir la cartographie du système d'information (SI) de l'organisation, en réalisant l'inventaire des services et actifs techniques, en identifiant les liaisons et les flux de données, en choisissant le modèle et l'outil de modélisation le plus adapté afin de disposer d'une représentation détaillée du système d'information de l'organisation.

B1.A1.C3.

Assurer une veille technologique, technique, réglementaire et normative à l'aide d'outils adaptés, en surveillant les innovations technologiques, les évolutions des cadres légaux et des standards applicables, en analysant leurs impacts sur l'organisation afin d'identifier les obligations et les opportunités d'amélioration en matière de sécurité du système d'information.

B1.A1.C4. Réaliser une analyse des risques en identifiant le type d'événements pouvant affecter la sécurité du système d'information et leurs sources, en hiérarchisant les risques selon leur gravité et leur impact potentiel afin de mesurer la maturité de l'organisation en matière de sécurité.

B1.A2.C1. Définir la politique de sécurité du système d'information (PSSI) d'une organisation en tenant compte de l'étude de l'écosystème réalisée, en intégrant les référentiels normatifs et réglementation applicables, les modèles de sécurité choisis, en précisant l'homologation visée le cas échéant afin de formaliser un cadre stratégique de sécurité du SI aligné sur l'organisation.

B1.A2.C2. Réaliser une analyse des écarts entre l'état actuel du système d'information et les objectifs de la politique de sécurité du système d'information en classant les écarts selon leur criticité afin de prioriser les actions de sécurité à déployer.

B1.A2.C3. Définir un plan d'actions de sécurité en tenant compte du rapport d'analyse des écarts, de l'impact écologique des actions proposées, en définissant les besoins et moyens techniques et humains nécessaires, en estimant les coûts associés afin de valider le déploiement du plan d'actions de sécurité avec les décisionnaires de l'organisation.

B1.A3.C1. Elaborer le corpus documentaire de sécurité du SI de l'organisation en tenant compte de la politique de sécurité du système d'information (PSSI), en veillant à l'accessibilité des supports pour les personnes en situation de handicap afin d'encadrer l'utilisation du système d'information (SI).

B1.A3.C2. Concevoir les plans de sauvegarde, de secours informatique, de reprise d'activité et de continuité d'activité en s'assurant de la capacité de l'organisation à les mettre en œuvre via des tests et simulations d'incidents, en indiquant leur impact écologique afin d'assurer la résilience globale du système d'information face aux incidents et crises.

B1.A3.C3. Élaborer un plan de sensibilisation et de formation à la sécurité pour les utilisateurs du SI en identifiant les besoins spécifiques selon les profils d'utilisateurs, en fournissant des contenus adaptés en utilisant des supports pédagogiques variés et adaptés aux personnes en situation de handicap afin de renforcer la culture de la sécurité et réduire les risques liés aux erreurs humaines.

B2.A1.C1. Rédiger les spécifications techniques et fonctionnelles des solutions de sécurité en analysant les besoins métiers, les contraintes réglementaires et les enjeux opérationnels afin de répondre aux exigences de sécurité de la politique de sécurité du SI (PSSI).

B2.A1.C2. Organiser le projet d'intégration des solutions de sécurité en sélectionnant une méthodologie de gestion de projet adaptée, en définissant des critères de performance, en établissant le planning du projet, en allouant les ressources nécessaires, afin d'optimiser la réalisation du projet.

B2.A1.C3.

Piloter l'avancement du projet en coordonnant les parties prenantes, en supervisant l'exécution des tâches et en ajustant les actions si nécessaire, afin de garantir le respect des délais, des coûts et des objectifs de sécurité.

B2.A2.C1. Concevoir une architecture sécurisée du système d'information en analysant les besoins métiers et les risques de sécurité, en intégrant les principes de défense en profondeur, de segmentation et de contrôle d'accès, en sélectionnant des solutions technologiques adaptées afin de protéger les données, les applications et les infrastructures contre les menaces internes et externes.

B2.A2.C2. Gérer les identités et contrôler les accès en mettant en œuvre des processus d'authentification tenant compte des personnes en situation de handicap le cas échéant, d'autorisation et de gestion des droits afin de sécuriser l'accès aux ressources et prévenir les usages non autorisés.

B2.A2.C3. Déployer des solutions cryptographiques en configurant les outils adaptés, en appliquant les protocoles et en assurant leur intégration dans l'environnement existant afin de garantir la confidentialité, l'intégrité et l'authenticité des données.

B2.A3.C1. Organiser un audit technique des solutions de sécurité en définissant un plan d'audit structuré précisant le périmètre d'analyse et les référentiels applicables, afin de permettre l'identification des vulnérabilités, des non-conformités et des axes d'amélioration.

B2.A3.C2. Rédiger un rapport d'audit technique précis et structuré en synthétisant les résultats des analyses, en formulant des actions correctives ou recommandations adaptées, réalisables et conformes aux normes et standards en vigueur afin de documenter l'état de sécurité et les axes d'amélioration de la solution.

B2.A3.C3. Assurer le suivi des actions correctives issues d'un audit technique de sécurité du SI, en coordonnant les parties prenantes, en vérifiant la mise en œuvre des mesures recommandées et en évaluant leur efficacité, afin de garantir la réduction effective des risques identifiés.

B3.A1.C1. Définir une politique de gestion de l'obsolescence et des mises à jour du système d'information en identifiant les composants matériels et logiciels, leur typologie et leur cycle de vie afin d'assurer la sécurité, la performance et la fiabilité du système d'information.

B3.A1.C2. Réaliser les mises à jour ou décommissionnements des actifs du SI en suivant une procédure préalablement établie afin de garantir la sécurité, la compatibilité et la continuité des opérations.

B3.A1.C3. Développer des indicateurs de suivi en s'appuyant sur l'analyse des données historiques, la collecte d'informations en temps réel et l'automatisation des rapports afin de mesurer l'efficacité de la gestion des mises à jour et de l'obsolescence.

B3.A2.C1. Elaborer une politique de contrôle et de surveillance continue en tenant compte des menaces identifiées et de la PSSI, en alignant les objectifs de surveillance sur les exigences réglementaires et les besoins métiers afin d'assurer une supervision efficace du SI.

B3.A2.C2. Intégrer un Security Operations Center (SOC) au sein de l'organisation en définissant les dispositifs de sécurité adéquats, les équipes nécessaires et les indicateurs à suivre, afin de surveiller en temps réel les menaces.

B3.A2.C3. Évaluer l'efficacité du Security Operations Center (SOC) d'une organisation, en utilisant des scénarios de test réalistes afin de s'assurer de la performance du processus de détection et de l'efficacité des équipes.

B3.A3.C1. Documenter les vulnérabilités détectées lors de la surveillance du SI en analysant les alertes générées par les outils de monitoring, en évaluant leur criticité afin de proposer des actions correctives.

B3.A3.C2. Corriger les vulnérabilités identifiées en élaborant un plan d'actions correctives approprié afin de restaurer la sécurité du système concerné.

B4.A1.C1. Concevoir une stratégie de communication de crise, en identifiant les parties prenantes à contacter et les canaux de communication de secours à utiliser, en rédigeant des messages types clés en main afin d'aider l'organisation à communiquer de manière efficace en cas de crise.

B4.A1.C2. Organiser une cellule stratégique de crise en identifiant ses membres, leurs rôles et missions, en définissant les critères et procédures d'activation de la cellule de crise afin d'assurer une bonne coordination et mobilisation des équipes pendant la crise.

B4.A1.C3. Déployer une stratégie d'entraînement de gestion de crise en réalisant des exercices variés testant différents scénarios d'attaque réalistes et adaptés à l'organisation afin de renforcer les compétences de l'équipe.

B4.A2.C1. Réaliser l'analyse initiale de tout incident détecté en vérifiant qu'il ne s'agisse pas d'une fausse alerte, en définissant sa nature, sa portée et sa criticité afin de décider de l'activation de la cellule stratégique de crise.

B4.A2.C2. Mettre en place des mesures d'endiguement appropriées en protégeant les actifs essentiels du SI à l'aide d'outils et techniques adaptés afin de limiter la propagation de l'incident.

B4.A2.C3. Réaliser une analyse forensique de l'incident en collectant et corrélant les preuves numériques à l'aide des outils adaptés afin de préparer une réponse et remédiation adaptées.

B4.A3.C1. Déployer des actions d'éviction et d'éradication en mobilisant des experts et des outils de sécurité adaptés, en vérifiant l'efficacité de ces actions afin d'éliminer la menace.

B4.A3.C2. Mettre en œuvre le plan de restauration du SI en utilisant des solutions techniques afin de rétablir les capacités du système d'information (SI).

B4.A3.C3. Capitaliser sur les enseignements de la crise en réalisant une analyse post mortem de l'incident afin d'améliorer la gestion future de crise.

Blocs de compétences

RNCP40897BC01 — Elaborer la stratégie de cybersécurité d'une organisation

LISTE DE COMPÉTENCES

Auditer l'organisation en identifiant les besoins métiers, les acteurs et les dépendances fonctionnelles, en analysant les processus métiers, en évaluant les interactions entre les systèmes et en recueillant les attentes des parties prenantes afin de garantir une vision exhaustive du fonctionnement opérationnel de l'organisation.

Etablir la cartographie du système d'information (SI) de l'organisation, en réalisant l'inventaire des services et actifs techniques, en identifiant les liaisons et les flux de données, en choisissant le modèle et l'outil de modélisation le plus adapté afin de disposer d'une représentation détaillée du système d'information de l'organisation.

Assurer une veille technologique, technique, réglementaire et normative à l'aide d'outils adaptés, en surveillant les innovations technologiques, les évolutions des cadres légaux et des standards applicables, en analysant leurs impacts sur l'organisation afin d'identifier les obligations et les opportunités d'amélioration en matière de sécurité du système d'information.

Réaliser une analyse des risques en identifiant le type d'évènements pouvant affecter la sécurité du système d'information et leurs sources, en hiérarchisant les risques selon leur gravité et leur impact potentiel afin de mesurer la maturité de l'organisation en matière de sécurité.

Définir la politique de sécurité du système d'information (PSSI) d'une organisation en tenant compte de l'étude de l'écosystème réalisée, en intégrant les référentiels normatifs et réglementation applicables, les modèles de sécurité choisis, en précisant l'homologation visée le cas échéant afin de formaliser un cadre stratégique de sécurité du SI aligné sur l'organisation.

Réaliser une analyse des écarts entre l'état actuel du système d'information et les objectifs de la politique de sécurité du système d'information en classant les écarts selon leur criticité afin de prioriser les actions de sécurité à déployer.

Définir un plan d'actions de sécurité en tenant compte du rapport d'analyse des écarts, de l'impact économique des actions proposées, en définissant les besoins et moyens techniques et humains nécessaires, en estimant les coûts associés afin de valider le déploiement du plan d'actions de sécurité avec les décideurs de l'organisation.

Elaborer le corpus documentaire de sécurité du SI de l'organisation en tenant compte de la politique de sécurité du système d'information (PSSI), en veillant à l'accessibilité des supports pour les personnes en situation de handicap afin d'encadrer l'utilisation du système d'information (SI).

Concevoir les plans de sauvegarde, de secours informatique, de reprise d'activité et de continuité d'activité en s'assurant de la capacité de l'organisation à les mettre en œuvre via des tests et simulations d'incidents, en indiquant leur impact économique afin d'assurer la résilience globale du système d'information face aux incidents et crises.

Élaborer un plan de sensibilisation et de formation à la sécurité pour les utilisateurs du SI en identifiant les besoins

spécifiques selon les profils d'utilisateurs, en fournissant des contenus adaptés en utilisant des supports pédagogiques variés et adaptés aux personnes en situation de handicap afin de renforcer la culture de la sécurité et réduire les risques liés aux erreurs humaines.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle réelle ou fictive donnant lieu à une soutenance orale avec une remise au jury du support de présentation.

RNCP40897BC02 — Piloter le cycle de conception, d'intégration et d'évaluation de solutions de sécurité du système d'information

LISTE DE COMPÉTENCES

Rédiger les spécifications techniques et fonctionnelles des solutions de sécurité en analysant les besoins métiers, les contraintes réglementaires et les enjeux opérationnels afin de répondre aux exigences de sécurité de la politique de sécurité du SI (PSSI).

Organiser le projet d'intégration des solutions de sécurité en sélectionnant une méthodologie de gestion de projet adaptée, en définissant des critères de performance, en établissant le planning du projet, en allouant les ressources nécessaires, afin d'optimiser la réalisation du projet.

Piloter l'avancement du projet en coordonnant les parties prenantes, en supervisant l'exécution des tâches et en ajustant les actions si nécessaire, afin de garantir le respect des délais, des coûts et des objectifs de sécurité.

Concevoir une architecture sécurisée du système d'information en analysant les besoins métiers et les risques de sécurité, en intégrant les principes de défense en profondeur, de segmentation et de contrôle d'accès, en sélectionnant des solutions technologiques adaptées afin de protéger les données, les applications et les infrastructures contre les menaces internes et externes.

Gérer les identités et contrôler les accès en mettant en œuvre des processus d'authentification tenant compte des personnes en situation de handicap le cas échéant, d'autorisation et de gestion des droits afin de sécuriser l'accès aux ressources et prévenir les usages non autorisés.

Déployer des solutions cryptographiques en configurant les outils adaptés, en appliquant les protocoles et en assurant leur intégration dans l'environnement existant afin de garantir la confidentialité, l'intégrité et l'authenticité des données.

Organiser un audit technique des solutions de sécurité en définissant un plan d'audit structuré précisant le périmètre d'analyse et les référentiels applicables, afin de permettre l'identification des vulnérabilités, des non-conformités et des axes d'amélioration.

Rédiger un rapport d'audit technique précis et structuré en synthétisant les résultats des analyses, en formulant des actions correctives ou recommandations adaptées, réalisables et conformes aux normes et standards en vigueur afin de documenter l'état de sécurité et les axes d'amélioration de la solution.

Assurer le suivi des actions correctives issues d'un audit technique de sécurité du SI, en coordonnant les parties prenantes, en vérifiant la mise en œuvre des mesures recommandées et en évaluant leur efficacité, afin de garantir la réduction effective des risques identifiés.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle réelle ou fictive donnant lieu à un dossier écrit.

RNCP40897BC03 — Maintenir en condition de sécurité le système d'information (SI) d'une organisation

LISTE DE COMPÉTENCES

Définir une politique de gestion de l'obsolescence et des mises à jour du système d'information en identifiant les composants matériels et logiciels, leur typologie et leur cycle de vie afin d'assurer la sécurité, la performance et la fiabilité du système d'information.

Réaliser les mises à jour ou décommissionnements des actifs du SI en suivant une procédure préalablement établie afin de garantir la sécurité, la compatibilité et la continuité des opérations.

Développer des indicateurs de suivi en s'appuyant sur l'analyse des données historiques, la collecte d'informations en temps réel et l'automatisation des rapports afin de mesurer l'efficacité de la gestion des mises à jour et de l'obsolescence.

Elaborer une politique de contrôle et de surveillance continue en tenant compte des menaces identifiées et de la PSSI, en alignant les objectifs de surveillance sur les exigences réglementaires et les besoins métiers afin d'assurer une supervision efficace du SI.

Intégrer un Security Operations Center (SOC) au sein de l'organisation en définissant les dispositifs de sécurité adéquats, les équipes nécessaires et les indicateurs à suivre, afin de surveiller en temps réel les menaces.

Évaluer l'efficacité du Security Operations Center (SOC) d'une organisation, en utilisant des scénarios de test réalistes afin de s'assurer de la performance du processus de détection et de l'efficacité des équipes.
Documenter les vulnérabilités détectées lors de la surveillance du SI en analysant les alertes générées par les outils de monitoring, en évaluant leur criticité afin de proposer des actions correctives.
Corriger les vulnérabilités identifiées en élaborant un plan d'actions correctives approprié afin de restaurer la sécurité du système concerné.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle réelle ou fictive donnant lieu à un dossier écrit.

RNCP40897BC04 — Gérer stratégiquement et opérationnellement une crise cyber

LISTE DE COMPÉTENCES

Concevoir une stratégie de communication de crise, en identifiant les parties prenantes à contacter et les canaux de communication de secours à utiliser, en rédigeant des messages types clés en main afin d'aider l'organisation à communiquer de manière efficace en cas de crise.

Organiser une cellule stratégique de crise en identifiant ses membres, leurs rôles et missions, en définissant les critères et procédures d'activation de la cellule de crise afin d'assurer une bonne coordination et mobilisation des équipes pendant la crise.

Déployer une stratégie d'entraînement de gestion de crise en réalisant des exercices variés testant différents scénarios d'attaque réalistes et adaptés à l'organisation afin de renforcer les compétences de l'équipe.

Réaliser l'analyse initiale de tout incident détecté en vérifiant qu'il ne s'agisse pas d'une fausse alerte, en définissant sa nature, sa portée et sa criticité afin de décider de l'activation de la cellule stratégique de crise.

Mettre en place des mesures d'endiguement appropriées en protégeant les actifs essentiels du SI à l'aide d'outils et techniques adaptés afin de limiter la propagation de l'incident.

Réaliser une analyse forensique de l'incident en collectant et corrélant les preuves numériques à l'aide des outils adaptés afin de préparer une réponse et remédiation adaptées.

Déployer des actions d'éviction et d'éradication en mobilisant des experts et des outils de sécurité adaptés, en vérifiant l'efficacité de ces actions afin d'éliminer la menace.

Mettre en œuvre le plan de restauration du SI en utilisant des solutions techniques afin de rétablir les capacités du système d'information (SI).

Capitaliser sur les enseignements de la crise en réalisant une analyse post mortem de l'incident afin d'améliorer la gestion future de crise.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle réelle ou fictive donnant lieu à une soutenance orale avec une remise au jury du support de présentation.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

L'expert en cybersécurité peut exercer au sein de structures de toutes tailles et dans tous les secteurs d'activité, qu'il s'agisse d'entreprises industrielles, de sociétés de services et de conseil, d'organismes publics, d'associations ou encore de prestataires en services informatiques.

TYPE D'EMPLOIS ACCESSIBLES

Expert cybersécurité /Expert sécurité des systèmes d'information

Consultant cybersécurité / Consultant en sécurité des systèmes d'information

Ingénieur cybersécurité/ Ingénieur sécurité des systèmes d'information

Responsable sécurité informatique

Auditeur sécurité des systèmes d'informations

Analyste SOC (Security Operations Center)

Pentester

RÉGLEMENTATIONS D'ACTIVITÉ

Le métier d'expert en cybersécurité n'est pas réglementé, néanmoins les activités de l'expert en cybersécurité s'inscrivent dans un cadre légal et réglementaire en constante évolution, que cela soit de manière globale ou spécifique à certains secteurs, national, européen ou international.

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)
Facteurs principaux	Lien formation-emploi, Manque de main-d'œuvre disponible
Salaire médian (mensuel)	3 115 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (35 % des actifs en emploi)
Familles professionnelles (FAP)	M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	4 758
Jugés difficiles à recruter	45 %
Emplois saisonniers	0 %
Familles professionnelles (FAP)	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

Le dispositif s'adresse aux titulaires d'un baccalauréat ou certification de niveau 4 pour un parcours en 5 ans

Dans le cadre d'admission parallèle:

- Admission en 3ème année : Être titulaire d'un diplôme ou titre de niveau 5 dans le domaine de l'informatique pour un parcours en 3 ans
- Admission en 4ème année : Être titulaire d'un diplôme ou titre de niveau 6 dans le domaine de l'informatique pour un parcours en 2 ans

Toute demande ne répondant pas aux prérequis de la formation est étudiée par une commission placée sous l'autorité du certificateur.

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

Le jury de certification est composé de 5 membres : 2 représentants du groupe YNOV, 3 professionnels externes exerçant dans le métier visé ou l'un des métiers visés par la certification ou supervisant des personnes qui l'exercent.

COMPOSITION DU JURY — VAE

Le jury VAE est composé de 5 membres : 2 représentants du groupe YNOV, 3 professionnels externes exerçant dans le métier visé ou l'un des métiers visés par la certification ou supervisant des personnes qui l'exercent.

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	9 157 €
Selon la branche	8 000 € – 12 000 €
Prise en charge	Branches concernées
9 157 €	Valeur par défaut · 168 branches

12 000 €	CPNE Entreprises des activités du déchet et de la propreté urbaine, CPNE autoroutes, CPNE de l'ingénierie, des services informatiques et du conseil, CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique, CPNE des exploitations frigorifiques
8 740 €	CNPEFP des sociétés d'assistance, CPNEFP de la branche professionnelle des Entreprises du courtage d'assurances et/ou réassurances, CPNFPE des sociétés d'assurances
8 696 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager, CPNEFP des jardineries et graineteries, CPNEFP du Négoce de l'ameublement
11 250 €	CPNE de la branche de la Distribution Directe, CPNEF de l'Exploitation cinématographique et de la Distribution de films
10 683 €	CPNEFP de l'enseignement privé indépendant, CPNEFP de la Restauration rapide
10 000 €	CPNE des industries de santé (CPNEIS), Commission Paritaire Activités de Marchés Financiers
9 992 €	CPNEF branche retraite complémentaire et prévoyance, CPNEFP Mutualité
9 500 €	CPNE Branche Caisse d'Epargne, CPNE de la branche Banque Populaire
9 000 €	CPNE Banque, CPNEFP de la branche des prestataires de services du secteur tertiaire
11 447 €	CPNE des Télécoms
11 446 €	CPNE Travail Temporaire
11 258 €	CPNEFP de la Mutualité Sociale Agricole
10 500 €	CPNEFP des industries des tuiles et briques
10 164 €	CPNE Casinos
9 800 €	CPNEF de l'audiovisuel
9 231 €	CPNEFP Commerce à distance
8 942 €	CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
8 775 €	CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
8 701 €	CPNE FP Branche des magasins du Bricolage
8 520 €	CPNE de la branche des experts comptables et commissaires aux comptes
8 500 €	CPNEFP de la métallurgie
8 000 €	CPNE chimie

Base légale

Date de décision	25/06/2025
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	25/06/2028
Date de dernière délivrance possible	25/06/2032

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2023	7	0	80 %	—
2022	51	0	91 %	92 %

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP37832

CORRESPONDANCES (PAR BLOCS)

RNCP36924, RNCP37832, RNCP37989, RNCP38951, RNCP39495, RNCP39837, RNCP39999

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.ynov.com/>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/40897/>

Se former en apprentissage

Formations en apprentissage	34
Organismes gestionnaires (CFA)	11
Organismes formateurs	26
Régions couvertes	10
Départements couverts	15
Organismes certifiés Qualiopi	26
Formations à distance	4
Sessions	de 09/2025 à 08/2029

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