

CERTIFICATION PROFESSIONNELLE

Accueil > Trouver une certification > Répertoire national des certifications professionnelles > Expert en cybersécurité

Expert en cybersécurité

Code de la fiche :
RNCP40897

Etat :
Active

 [Télécharger la fiche](#)

 [Aide en ligne](#)

 [Supplément Europass : FR - EN](#)

L'essentiel





**Nomenclature
du niveau de qualification**

Niveau 7



Code(s) NSF

326 : Informatique, traitement de l'information, réseaux de transmission
326n : Analyse informatique, conception d'architecture de réseaux



Formacode(s)

31045 : Cybersécurité
31038 : Audit informatique
31008 : Système information
42881 : Risque criminel entreprise



**Date d'échéance
de l'enregistrement**

25-06-2028

Certificateur(s)

Résumé de la certification

Blocs de compétences

Secteur d'activité et type d'emploi

Voie d'accès

Liens avec d'autres certifications professionnelles, certifications ou habilitations

Base légale

Pour plus d'informations

Certificateur(s)

Nom légal	Siret	Nom commercial	Site internet
YNOV	53056211500101	-	https://www.ynov.com/

Résumé de la certification

Objectifs et contexte de la certification :

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.

Modalités d'évaluation :

Mises en situations professionnelles réelles ou fictives avec remise de livrables (dossiers écrits, soutenances orales)

Blocs de compétences

RNCP40897BC01 - Elaborer la stratégie de cybersécurité d'une organisation

Liste de compétences	Modalités d'évaluation
<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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 décideurs de l'organisation.</p>	<p>Mise en situation professionnelle réelle ou fictive donnant lieu à une soutenance orale avec une remise au jury du support de présentation.</p>

Liste de compétences	Modalités d'évaluation
<p>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).</p> <p>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.</p> <p>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.</p>	

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

Liste de compétences	Modalités d'évaluation
<p>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).</p> <p>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.</p> <p>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.</p>	<p>Mise en situation professionnelle réelle ou fictive donnant lieu à un dossier écrit.</p>

Liste de compétences	Modalités d'évaluation
<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	

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

Liste de compétences	Modalités d'évaluation
<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Corriger les vulnérabilités identifiées en élaborant un plan d'actions correctives approprié afin de restaurer la sécurité du système concerné.</p>	<p>Mise en situation professionnelle réelle ou fictive donnant lieu à un dossier écrit.</p>

Liste de compétences	Modalités d'évaluation
<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Mettre en œuvre le plan de restauration du SI en utilisant des solutions techniques afin de rétablir les capacités du système d'information (SI).</p> <p>Capitaliser sur les enseignements de la crise en réalisant une analyse post mortem de l'incident afin d'améliorer la gestion future de crise.</p>	<p>Mise en situation professionnelle réelle ou fictive donnant lieu à une soutenance orale avec une remise au jury du support de présentation.</p>

Description des modalités d'acquisition de la certification par capitalisation des blocs de compétences et/ou par correspondance :

L'obtention de la certification visée nécessite obligatoirement la validation des 4 blocs de compétences.

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

Code(s) ROME :

M1802 - Expertise et support en systèmes d'information

Références juridiques des 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.

Voie d'accès

Le cas échéant, 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.

Le cas échéant, prérequis à la validation de la certification :

Pré-requis distincts pour les blocs de compétences :

Non

Voie d'accès à la certification	Oui	Non	Composition des jurys	Date de dernière modification
Après un parcours de formation sous statut d'élève ou d'étudiant	X		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.	-

Voie d'accès à la certification	Oui	Non	Composition des jurys	Date de dernière modification
En contrat d'apprentissage	X		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.	-
Après un parcours de formation continue	X		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.	-
En contrat de professionnalisation	X		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.	-
Par candidature individuelle		X	-	-
Par expérience	X		Le jury VAE est composé de 5 membres : 2 représentants du groupe YNOV, 3 professionnels externes exerçant dans le métier	-

Voie d'accès à la certification	Oui	Non	Composition des jurys	Date de dernière modification
			visé ou l'un des métiers visés par la certification ou supervisant des personnes qui l'exercent.	

	Oui	Non
Inscrite au cadre de la Nouvelle Calédonie		X
Inscrite au cadre de la Polynésie française		X

Liens avec d'autres certifications professionnelles, certifications ou habilitations

Certifications professionnelles enregistrées au RNCP en correspondance partielle :

Bloc(s) de compétences concernés	Code et intitulé de la certification professionnelle reconnue en correspondance partielle	Bloc(s) de compétences en correspondance partielle
RNCP40897BC01 - Elaborer la stratégie de cybersécurité d'une organisation	<u>RNCP36924 - Expert en cybersécurité et sécurité informatique</u>	RNCP36924BC01 - Conception de la stratégie de sécurité du système d'information et conseil à la gouvernance
RNCP40897BC01 - Elaborer la stratégie de cybersécurité d'une organisation	<u>RNCP37989 - Expert en cybersécurité des systèmes d'information (BADGE CGE)</u>	RNCP37989BC03 - Identifier les risques et organiser la cybersécurité
RNCP40897BC01 - Elaborer la stratégie de cybersécurité d'une organisation	<u>RNCP38951 - Expert de la sécurité des données, des réseaux et des systèmes</u>	RNCP38951BC01 - Conseiller une organisation en sécurité des systèmes d'information
RNCP40897BC01 - Elaborer la stratégie de cybersécurité d'une organisation	<u>RNCP39495 - MASTER - Cybersécurité (fiche nationale)</u>	RNCP39495BC05 - Piloter la sécurité des systèmes d'information
RNCP40897BC01 - Elaborer la stratégie de cybersécurité d'une organisation	<u>RNCP39837 - Expert en cybersécurité (MS)</u>	RNCP39837BC01 - Concevoir la sécurité d'un système d'information
RNCP40897BC01 - Elaborer la stratégie de cybersécurité d'une organisation	<u>RNCP39999 - Expert en cybersécurité</u>	RNCP39999BC01 - Gérer les risques liés à la sécurité de l'information ET RNCP39999BC03 - Assurer la conformité du

Bloc(s) de compétences concernés	Code et intitulé de la certification professionnelle reconnue en correspondance partielle	Bloc(s) de compétences en correspondance partielle
		traitement de l'information au cadre réglementaire et normatif en vigueur dans l'organisation
RNCP40897BC02 - Piloter le cycle de conception, d'intégration et d'évaluation de solutions de sécurité du système d'information	<u>RNCP39999 - Expert en cybersécurité</u>	RNCP39999BC02 - Protéger un système d'information face à la cyber-menace ET RNCP39999BC04 - Piloter un projet et communiquer en cybersécurité
RNCP40897BC04 - Gérer stratégiquement et opérationnellement une crise cyber	<u>RNCP37989 - Expert en cybersécurité des systèmes d'information (BADGE CGE)</u>	RNCP37989BC04 - Détecter les incidents de sécurité numérique et y répondre
RNCP40897BC04 - Gérer stratégiquement et opérationnellement une crise cyber	<u>RNCP38951 - Expert de la sécurité des données, des réseaux et des systèmes</u>	RNCP38951BC05 - Gérer une crise cyber

Anciennes versions de la certification professionnelle reconnues en correspondance totale :

Code et intitulé de la certification professionnelle reconnue en correspondance

RNCP37832 - Expert en cybersécurité

Base légale

Date du dernier Journal Officiel ou Bulletin Officiel :

19-07-2023

Date de décision	25-06-2025
Durée de l'enregistrement en années	3
Date d'échéance de l'enregistrement	25-06-2028
Date de dernière délivrance possible de la certification	25-06-2032

Pour plus d'informations

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 %)
2023	7	0	80	80	-
2022	51	0	91	91	92
2021	32	0	93	84	81

Lien internet vers le descriptif de la certification :

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

Liste des organismes préparant à la certification :

Liste des organismes préparant à la certification

Certification(s) antérieure(s) :

Code de la fiche	Intitulé de la certification remplacée
<u>RNCP37832</u>	Expert en cybersécurité

Référentiel d'activité, de compétences et d'évaluation :

Référentiel d'activité, de compétences et d'évaluation