

Manager de la cybersécurité

RNCP40246 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326n
Formacode(s)	31045
Code(s) ROME	M1802
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	28/02/2025
Date d'échéance	28/02/2030

Certificateur(s)

ADE HOLDING · SIRET : 82450453400028

DE VINCI HIGHER EDUCATION (DVHE) · SIRET : 44087031900025

Partenaires habilités

4 organismes habilités, d'après la liste publiée par France compétences : 4 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
COMPETENTIS	94953886200010	Former et organiser l'évaluation
ISCOD	88877726500107	Former et organiser l'évaluation
VISIPLUS	44321186700116	Former et organiser l'évaluation
YNCREA MEDITERRANEE	38338687700039	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

Le management de la cybersécurité repose sur une analyse des risques auxquels sont confrontés les systèmes d'information et les réseaux. Le métier associe la conception d'architectures de sécurité à la mise en œuvre de solutions destinées à assurer une sûreté de fonctionnement maximale de ceux-ci et la protection des bases de données contre tous types d'intrusion à des fins de vol ou de destruction.

ACTIVITÉS VISÉES

Analyse stratégique des cyber-risques

Veille géopolitique sur les cybermenaces et la cybercriminalité

Identification des risques d'intrusion dans les systèmes d'information de l'entreprise

Analyse des risques affectant les données numériques

Mise en œuvre de l'intelligence économique

Conception et organisation de la sécurité des systèmes d'information et des réseaux

Conception d'une architecture de sécurité adaptée au niveau de risque

Rédaction d'un appel d'offres relatif à des architectures et solutions de sécurité

Mise en place d'une protection adaptée au Cloud computing

Veille réglementaire et technologique

Déploiement de la sécurité des systèmes d'information et des réseaux

Evaluation de la sécurité initiale d'un système d'information
Elaboration et mise en place d'une Politique de Sécurité des Systèmes d'Information (PSSI)
Sécurisation des locaux et des infrastructures sensibles
Protection des données et du patrimoine immatériel de l'entreprise
Mise en place de la sûreté de fonctionnement
Développement d'une culture de la cyber sécurité dans l'entreprise
Formation et conseil aux services supports
Conduite de projet et conduite du changement
Anticipation et gestion des crises
Inclusion handicap et multiculturalité
Gestion budgétaire et financière
Elaboration du budget prévisionnel
Mise en place d'un plan de financement complet
Contrôle de gestion et pilotage budgétaire
Suivi et contrôle des sous-traitants

COMPÉTENCES ATTESTÉES

Analyser une situation géopolitique propice aux cyberattaques contre le potentiel économique d'un pays cible, en recensant les cyberattaques passées, dans le but de cartographier les menaces potentielles sur les systèmes d'information d'un pays ou d'une industrie.

Conduire un audit du système d'information et des réseaux de son entreprise, afin d'identifier leurs points de vulnérabilité au regard des menaces d'intrusion inhérentes au cyberspace.

Dresser un état des dommages potentiels devant résulter des attaques au système d'information de son entreprise, en caractérisant les atteintes possibles aux données numériques (altération, captation ou destruction) traitées ou stockées par celui-ci, en vue d'établir un cahier des charges de la cyber sécurité.

Se conformer à la norme ISO 27032, ainsi qu'à la directive NIS2, dans le cadre du budget disponible, afin de répondre aux impératifs de protection de l'activité et des données.

Organiser la surveillance de l'environnement concurrentiel de son entreprise, en collectant les informations économiques et stratégiques utiles, afin d'anticiper sur les intentions des concurrents sur le marché national et international.

Établir le schéma général de la cyber sécurité dans son entreprise, en s'appuyant sur l'audit de vulnérabilité des systèmes d'information et des réseaux, afin de déterminer les caractéristiques d'une nouvelle architecture à mettre en place.

Traduire en spécifications techniques les attentes en matière d'architecture et de solutions de sécurité, en vue de la rédaction du cahier des charges d'un appel d'offres sur le marché des prestataires.

Coordonner la rédaction du cahier des charges et de l'appel d'offres, conformément au schéma général de la cyber sécurité préalablement établi, en vue de la sélection des prestataires et sous-traitants.

Concevoir et organiser les systèmes de sauvegarde en cohérence avec la stratégie cloud de l'entreprise et les différentes catégories d'utilisateurs, afin de sécuriser le stockage des données.

Définir les contenus de formation des utilisateurs aux bonnes pratiques de sécurité en matière de cloud computing, quel que soit le mode de cloud choisi : Paas, Iaas ou Saas, afin d'optimiser l'efficacité du système et sa rentabilité.

Concevoir et utiliser un système de veille sur l'actualité des contraintes légales et réglementaires, à l'aide des outils numériques de recherche sur les sites des organismes spécialisés en matière de cyber sécurité et les bases de données juridiques du domaine, afin d'assurer la conformité légale des dispositifs de sécurité mis en place.

Établir le catalogue des risques d'intrusion et failles de sécurité d'un système d'information, sur la base d'un audit des systèmes et selon les principes du hacking éthique, en vue de planifier le déploiement des solutions de cyber sécurité.

Définir une politique de sécurité des systèmes d'information, en s'appuyant sur les recommandations de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), en vue de sa diffusion auprès des parties prenantes internes et externes à l'entreprise.

Évaluer les potentialités de l'intelligence artificielle en matière de cyber sécurité, dans la perspective d'une mise en œuvre offensive et défensive.

Identifier les risques d'atteinte aux infrastructures physiques en vue de placer les alertes et protections à même d'anticiper sur toutes tentatives d'intrusion dans les locaux.

Optimiser les solutions de fourniture d'énergie et les dispositifs de secours en cas de défaillance, afin d'assurer

l'alimentation permanente des systèmes d'information et des réseaux de l'entreprise.

Protéger l'accès aux espaces de stockage et aux données par des systèmes de codes d'accès et de cryptage adaptés aux menaces, afin d'assurer la conservation du patrimoine immatériel de l'entreprise.

Établir le schéma général de la sûreté de fonctionnement à l'intention des services internes à l'entreprise, en vue de garantir la continuité de l'activité quelles que soient les attaques sur le système d'information.

Analyser les compétences du personnel de son entreprise en matière de cyber sécurité, au moyen de questionnaires et d'entretiens, en vue de concevoir et mettre en place un plan de formation des personnels et de conseil aux services supports.

Utiliser une méthode de gestion de projet pour la mise en place d'une nouvelle organisation de la cyber sécurité dans l'entreprise.

Accompagner le changement nécessité par les dispositions locales et internationales en matière de cyber sécurité, au plus près des postes de travail, afin d'assurer le bon fonctionnement de l'organisation mise en place.

Concevoir et déployer dans l'entreprise une communication destinée à anticiper sur la gestion des crises occasionnées par les tentatives d'intrusion cyber.

Prendre en compte le référentiel général d'amélioration de l'accessibilité (RGAA) et les recommandations de la norme internationale WCAG 2.1 (Web Content Accessibility Guidelines) à un niveau aaa, dans le but d'adapter le management interne de la cyber sécurité aux personnes handicapées.

Prendre en compte la multiculturalité des personnels de son organisation, dans le but d'adapter le management interne de la cyber sécurité aux modes particuliers d'appréhension des directives.

Estimer les investissements (coûts et calendrier), afin de déterminer les besoins de financement du projet de cyber sécurité.

Négocier les conditions de financement en tenant compte des évolutions probables des technologies de la cyber sécurité, en vue de construire un budget fiable à moyen terme.

Choisir des indicateurs de suivi budgétaire adaptés au contexte de la cyber sécurité, en vue de constituer les tableaux de bord de gestion conformes aux principes de son entreprise.

Analyser en continu les écarts budgétaires, afin de décider la mise en place des mesures correctives et d'assurer la réalisation des projets dans le cadre imparti.

Assurer le suivi des contrats de sous-traitance en vérifiant régulièrement la solidité des garanties financières, afin d'éviter les ruptures dans la fourniture et la maintenance des systèmes de sécurité mis en place.

Blocs de compétences

RNCP40246BC01 — Mener une analyse stratégique des cyber-risques

LISTE DE COMPÉTENCES

Analyser une situation géopolitique propice aux cyberattaques contre le potentiel économique d'un pays cible, en recensant les cyberattaques passées, dans le but de cartographier les menaces potentielles sur les systèmes d'information d'un pays ou d'une industrie.

Conduire un audit du système d'information et des réseaux de son entreprise, afin d'identifier leurs points de vulnérabilité au regard des menaces d'intrusion inhérentes au cyberspace.

Dresser un état des dommages potentiels devant résulter des attaques au système d'information de son entreprise, en caractérisant les atteintes possibles aux données numériques (altération, captation ou destruction) traitées ou stockées par celui-ci, en vue d'établir un cahier des charges de la cyber sécurité.

Se conformer à la norme ISO 27032, ainsi qu'à la directive NIS2, dans le cadre du budget disponible, afin de répondre aux impératifs de protection de l'activité et des données.

Organiser la surveillance de l'environnement concurrentiel de son entreprise, en collectant les informations économiques et stratégiques utiles, afin d'anticiper sur les intentions des concurrents sur le marché national et international.

MODALITÉS D'ÉVALUATION

Travaux écrits : notes de synthèse relatives aux études de cas, rapports d'activité

Etude de cas (supports des évaluations proposés par les entreprises partenaires de DVHE)

Mise en situation professionnelle (durant les périodes en entreprise)

Présentation orale individuelle devant le jury

RNCP40246BC02 — Concevoir et organiser la sécurité des SI et des réseaux

LISTE DE COMPÉTENCES

Établir le schéma général de la cyber sécurité dans son entreprise, en s'appuyant sur l'audit de vulnérabilité des systèmes d'information et des réseaux, afin de déterminer les caractéristiques d'une nouvelle architecture à mettre en place.

Traduire en spécifications techniques les attentes en matière d'architecture et de solutions de sécurité, en vue de la rédaction du cahier des charges d'un appel d'offres sur le marché des prestataires.

Coordonner la rédaction du cahier de charges et de l'appel d'offres, conformément au schéma général de la cyber sécurité préalablement établi, en vue de la sélection des prestataires et sous-traitants.

Concevoir et organiser les systèmes de sauvegarde en cohérence avec la stratégie cloud de l'entreprise et les différentes catégories d'utilisateurs, afin de sécuriser le stockage des données.

Définir les contenus de formation des utilisateurs aux bonnes pratiques de sécurité en matière de cloud computing, quel que soit le mode de cloud choisi : Paas, Iaas ou Saas, afin d'optimiser l'efficacité du système et sa rentabilité.

Concevoir et utiliser un système de veille sur l'actualité des contraintes légales et réglementaires, à l'aide des outils numériques de recherche sur les sites des organismes spécialisés en matière de cyber sécurité et les bases de données juridiques du domaine, afin d'assurer la conformité légale des dispositifs de sécurité mis en place.

MODALITÉS D'ÉVALUATION

Questionnaire

Travaux écrits : notes de synthèse relatives aux études de cas, rapports d'activité

Mise en situation professionnelle (durant les périodes en entreprise)

Présentation orale individuelle devant le jury

RNCP40246BC03 — Déployer la sécurité des SI et des réseaux

LISTE DE COMPÉTENCES

Établir le catalogue des risques d'intrusion et failles de sécurité d'un système d'information, sur la base d'un audit des systèmes et selon les principes du hacking éthique, en vue de planifier le déploiement des solutions de cyber sécurité.

Définir une politique de sécurité des systèmes d'information, en s'appuyant sur les recommandations de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), en vue de sa diffusion auprès des parties prenantes internes et externes à l'entreprise.

Évaluer les potentialités de l'intelligence artificielle en matière de cyber sécurité, dans la perspective d'une mise en œuvre offensive et défensive.

Identifier les risques d'atteinte aux infrastructures physiques en vue de placer les alertes et protections à même d'anticiper sur toutes tentatives d'intrusion dans les locaux.

Optimiser les solutions de fourniture d'énergie et les dispositifs de secours en cas de défaillance, afin d'assurer l'alimentation permanente des systèmes d'information et des réseaux de l'entreprise.

Protéger l'accès aux espaces de stockage et aux données par des systèmes de codes d'accès et de cryptage adaptés aux menaces, afin d'assurer la conservation du patrimoine immatériel de l'entreprise.

Établir le schéma général de la sûreté de fonctionnement à l'intention des services internes à l'entreprise, en vue de garantir la continuité de l'activité quelles que soient les attaques sur le système d'information.

MODALITÉS D'ÉVALUATION

Travaux écrits : notes de synthèse relatives aux études de cas, rapports d'activité

Mise en situation professionnelle (durant les périodes en entreprise)

Présentation orale individuelle devant le jury

RNCP40246BC04 — Développer une culture de la cybersécurité dans l'entreprise

LISTE DE COMPÉTENCES

Analyser les compétences du personnel de son entreprise en matière de cyber sécurité, au moyen de questionnaires et d'entretiens, en vue de concevoir et mettre en place un plan de formation des personnels et de conseil aux services supports.

Utiliser une méthode de gestion de projet pour la mise en place d'une nouvelle organisation de la cyber sécurité dans l'entreprise.

Accompagner le changement nécessité par les dispositions locales et internationales en matière de cyber sécurité, au plus près des postes de travail, afin d'assurer le bon fonctionnement de l'organisation mise en place.

Concevoir et déployer dans l'entreprise une communication destinée à anticiper sur la gestion des crises occasionnées par les tentatives d'intrusion cyber.

Prendre en compte le référentiel général d'amélioration de l'accessibilité (RGAA) et les recommandations de la norme internationale WCAG 2.1 (Web Content Accessibility Guidelines) à un niveau aaa, dans le but d'adapter le management interne de la cyber sécurité aux personnes handicapées.

Prendre en compte la multiculturalité des personnels de son organisation, dans le but d'adapter le management interne de la cyber sécurité aux modes particuliers d'appréhension des directives.

MODALITÉS D'ÉVALUATION

Travaux écrits : notes de synthèse relatives aux études de cas, rapports d'activité

Mise en situation professionnelle (durant les périodes en entreprise)

Présentation orale individuelle devant le jury

RNCP40246BC05 — Gérer les aspects budgétaires et financiers de la cyber sécurité

LISTE DE COMPÉTENCES

Estimer les investissements (coûts et calendrier), afin de déterminer les besoins de financement du projet de cyber sécurité.

Négocier les conditions de financement en tenant compte des évolutions probables des technologies de la cyber sécurité, en vue de construire un budget fiable à moyen terme.

Choisir des indicateurs de suivi budgétaire adaptés au contexte de la cyber sécurité, en vue de constituer les tableaux de bord de gestion conformes aux principes de son entreprise.

Analyser en continu les écarts budgétaires, afin de décider la mise en place des mesures correctives et d'assurer la réalisation des projets dans le cadre imparti.

Assurer le suivi des contrats de sous-traitance en vérifiant régulièrement la solidité des garanties financières, afin d'éviter les ruptures dans la fourniture et la maintenance des systèmes de sécurité mis en place.

MODALITÉS D'ÉVALUATION

Travaux écrits : notes de synthèse relatives aux études de cas, rapports d'activité

Mise en situation professionnelle (durant les périodes en entreprise)

Présentation orale individuelle devant le jury

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Toutes entreprises et organisations publiques et privées dotées d'un système d'information. Toutes entreprises de services numériques et organismes spécialisés en cyber sécurité.

La cybersécurité est une dimension stratégique des organisations. Le manager de la cybersécurité porte une responsabilité importante, tant au niveau de la conception des plans de sécurité qu'à celui de leur mise en œuvre opérationnelle face à des dangers de toutes natures. A ces deux niveaux, une large autonomie est indispensable afin de permettre au manager de la cybersécurité de dépasser les contraintes et les résistances des personnes concernées, et de déployer une réactivité maximale face aux risques d'intrusion, de blocage des systèmes et de dégradation des données numériques.

TYPE D'EMPLOIS ACCESSIBLES

Manager de la cyber sécurité

Expert en sécurité des SI

Expert cyber défense

Responsable de la sécurité des systèmes d'information

Ingénieur cyber sécurité

Consultant en sécurité des SI

RÉGLEMENTATIONS D'ACTIVITÉ

Le métier n'est pas réglementé mais l'environnement de travail l'est fortement.

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

PRÉREQUIS À L'ENTRÉE EN FORMATION

Être titulaire d'une certification professionnelle de niveau 6 minimum

Ou être titulaire d'une certification professionnelle de niveau 5 avec une expérience professionnelle, après validation du dossier par la Commission d'autorisation de candidature (CAC)

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

5 membres :

Un président du jury, personnalité extérieure à l'autorité de certification

Le directeur Exécutive Education de DVHE ou son représentant

Le directeur pédagogique de la formation conduisant à la certification

Deux professionnels extérieurs à l'autorité de certification

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	7 748 €
Selon la branche	7 748 € – 8 273 €
Prise en charge	Branches concernées
7 748 €	Valeur par défaut · 204 branches
8 273 €	CPNE de l'ingénierie, des services informatiques et du conseil, CPNEFP ICGV entreprises de la viande, CPNEFP de la Mutualité Sociale Agricole
8 088 €	CPNE Branche Caoutchouc, CPNE des industries de santé (CPNEIS), CPNEFP de la métallurgie
8 245 €	CPNE des Télécoms
8 108 €	CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique
8 062 €	CPNEFP dans les établissements d'enseignement privés sous contrat

Base légale

Date de décision	28/02/2025
Durée de l'enregistrement	5 ans
Date d'échéance de l'enregistrement	28/02/2030
Date de dernière délivrance possible	28/02/2034

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2022	23	0	96 %	94 %
2021	23	0	96 %	80 %

Liens avec d'autres certifications

ANCIENNES VERSIONS
RNCP36595

Pour plus d'informations

LIEN VERS LE DESCRIPTIF
<https://executive.devinci.fr/formation/master-management-cybersecurite/>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/40246/>

Où se former

Formations référencées	3
Organismes	3
Régions couvertes	2
Prix indicatif	9 750 € – 13 900 €
Durée	400 h

Offre de formation — MonCompteFormation (Caisse des Dépôts), licence ouverte.

Se former en apprentissage

Formations en apprentissage	2
Organismes gestionnaires (CFA)	1
Organismes formateurs	1
Régions couvertes	1
Départements couverts	1
Organismes certifiés Qualiopi	1
Formations à distance	2
Sessions	de 01/2026 à 12/2027

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

Entrées et sorties de formation

Entrées en formation	12
Parcours menés à terme	1
Taux d'achèvement	8 %
Période	09/2025 – 09/2026

Entrées et sorties — Caisse des Dépôts (open data), tous organismes confondus.

Demande CPF — formations engagées

Dossiers CPF engagés	13
Montant total engagé	56 947 €
Coût moyen par dossier	4 381 €
Durée moyenne	773 h
Période	07/2025 – 09/2026
France compétences	60 %
OPCO	27 %
Régions	5 %
Reste à charge titulaire	4 %
France Travail	4 %

Formations engagées via le CPF — Caisse des Dépôts (open data), tous organismes confondus.