

Responsable en cybersécurité

RNCP37300 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Sigle	Autre — Autre certification professionnelle de droit
Code(s) NSF	326
Formacode(s)	42802, 31045, 14297
Code(s) ROME	M1801, M1810, M1805, M1802, M1807
Type d'enregistrement	Enregistrement de droit
Date d'échéance	26/08/2027

Certificateur(s)

MINISTERE DES ARMEES · SIRET : 11009001600053

MINISTERE DES ARMEES · SIRET : 11009001600046

Partenaires habilités

3 organismes habilités, d'après la liste publiée par France compétences : 2 à former et organiser l'évaluation et 1 à organiser l'évaluation.

Organisme	SIRET	Habilitation
Commandement des systèmes d'information et de communication / Ecole des transmissions (COMSIC/ETRS)	—	Former et organiser l'évaluation
Ecole de formation des sous-officiers de l'Armée de l'air et de l'espace (EFSOAAE)	—	Organiser l'évaluation
Pôle Ecoles Méditerranée (PEM)	—	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

Le besoin des armées

- La cybersécurité

La cybercriminalité qui constitue dans la sphère civile une menace bien réelle, représente aussi pour les forces armées une menace de plus en plus pressante.

La sécurisation des systèmes d'information des unités combattantes et non combattantes est aujourd'hui un enjeu stratégique majeur. Le cyberspace est devenu un terrain d'affrontement stratégique, un nouvel espace de combat dans lequel l'espionnage, l'appropriation de données confidentielles ou encore l'interruption de services des unités de peut altérer les capacités opérationnelles des forces armées.

La certification de Responsable en cybersécurité répond au besoin du ministère des armées de disposer de personnels qualifiés dans le domaine de la cybersécurité pour identifier les vulnérabilités des systèmes d'information et renforcer la cybersécurité, détecter les attaques cyber, alerter rapidement les utilisateurs et élaborer des parades, sensibiliser et former les utilisateurs au risque cyber.

Le besoin du secteur civil

Chaque jour des attaques informatiques menacent le fonctionnement des organisations qui doivent s'en protéger parfois pour survivre. La recrudescence des cyberattaques durant la crise sanitaire de 2020 a encore amplifié le

phénomène.

Conscientes de ce nouveau danger, les entreprises cherchent à recruter. Or, les experts sont rares. Ce secteur nouveau et vaste souffre de pénurie.

Encore méconnus, les métiers liés à la cybersécurité sont très divers et couvrent un large champ d'activités et de compétences. Ils sont aujourd'hui structurés en 5 grandes familles :

1. Pilote, organisation de la sécurité et gestion des risques
2. Management de projets de sécurité et cycle de vie de la sécurité
3. Maintien en condition opérationnelle de la sécurité
4. Support et gestion des incidents de sécurité
5. Conseil, audit et expertise en sécurité

La cybersécurité constitue à l'évidence une filière d'avenir.

Source : ANSSI - Panorama des métiers de la cybersécurité Edition 2020

ACTIVITÉS VISÉES

Le Responsable en cybersécurité conduit des actions défensives ou offensives dans le cyberspace pour soutenir l'action des forces armées et garantir la continuité et l'efficacité des opérations militaires. Il prépare les unités pour qu'elles soient en mesure d'intervenir en cas d'incident.

Le Responsable en cybersécurité audite les systèmes d'information militaires et met en place des tests d'intrusion pour détecter les éventuelles failles et renforcer la sécurité en profondeur. Il recherche, effectue une veille et mène les investigations numériques qui vous permettent d'anticiper les risques.

Enfin, le Responsable en cybersécurité sensibilise et forme les utilisateurs à la reconnaissance de ces menaces et à la mise en œuvre des meilleures pratiques pour les éviter et les neutraliser.

COMPÉTENCES ATTESTÉES

Le Responsable en cybersécurité est capable de :

1- Piloter la cyberprotection des systèmes et réseaux informatiques

- Appuyer le responsable de la sécurité des systèmes d'information (RSSI) ou le directeur des systèmes d'information (DSI)

- Contribuer à l'amélioration de la sécurité technique du système d'information

- Administrer la sécurité des systèmes et des éléments actifs réseau

2- Contrôler et auditer le niveau de cybersécurité d'un système d'information

- Évaluer le niveau de conformité d'un système d'information

- Éprouver le niveau de sécurité d'un système d'information

- Proposer un plan d'action à l'issue d'un audit

3- Superviser la cybersécurité des systèmes d'information

- Diriger l'action d'une équipe de techniciens au sein d'un centre de supervision

- Améliorer les dispositifs de détection

- Diriger les différentes phases de réponse sur incident dans le périmètre d'un centre de supervision

- Assurer la formation du personnel

4- Conduire une investigation numérique dans le domaine de la cybersécurité

- Mener des investigations en réponse sur incident

- Capitaliser le résultat des investigations

Blocs de compétences

RNCP37300BC01 — Piloter la cyberprotection des systèmes et réseaux informatiques

LISTE DE COMPÉTENCES

Appuyer le responsable de la sécurité des systèmes d'information (RSSI) ou le directeur des systèmes d'information (DSI) :

- contribuer à l'élaboration des moyens et procédures CYBER au profit d'une ou plusieurs autorités qualifiées et autorités d'emploi ;

- concourir à la rédaction des documents réglementaires d'organisation et de conduite de la cybersécurité de l'entité d'emploi ;

- organiser, conduire et contrôler la mise en œuvre des mesures locales CYBER ;

- préparer son unité à une homologation et/ou contrôle d'un système d'information ;

- évaluer et rendre compte du niveau de sécurité organisationnel du périmètre d'emploi ;
- conduire l'analyse des risques pesant sur un périmètre informatique défini ;
- réaliser et animer des séances de sensibilisation au profit des utilisateurs et des administrateurs ;
- conseiller le directeur de l'entité sur les actions de cyberprotection.

Contribuer à l'amélioration de la sécurité technique du système d'information :

- assurer une veille technologique et le suivi des études amont du domaine cyber ;
- anticiper et proposer les nouveaux besoins cyber relatifs à son périmètre de responsabilité ;
- évaluer et rendre compte du niveau de sécurité technique du périmètre d'emploi ;
- développer les compétences en cybersécurité des administrateurs et des utilisateurs des systèmes informatiques ;
- proposer les solutions de chiffrement adaptées au niveau de sécurité attendu.

Administrer la sécurité des systèmes et des éléments actifs réseau :

- proposer ou développer les outils et procédures de sécurisation des architectures réseaux et les services associés ;
- définir et mettre en œuvre les règles et outils d'administration sécurisés ;
- définir et appliquer la politique technique de gestion des droits d'accès aux ressources informatiques ;
- exploiter et préserver les journaux d'événements des systèmes ;
- appliquer les mesures prioritaires de lutte informatique défensive en réaction à un incident de sécurité ;
- établir et diffuser un compte-rendu d'incident précis ;
- apporter un soutien technique aux actions de résolution des incidents de sécurité ;
- concourir aux processus de lutte informatique défensive.

MODALITÉS D'ÉVALUATION

Par la voie de la formation :

- Epreuves écrites et orales ;
- Mises en situation professionnelles ;

Par la voie de la VAE :

- Etude du livret 2 ;
- Entretien avec le jury.

visant à démontrer la capacité du candidat à assurer la gouvernance de la sécurité des systèmes et réseaux informatiques

RNCP37300BC02 — Contrôler et auditer le niveau de cybersécurité d'un système d'information

LISTE DE COMPÉTENCES

Évaluer le niveau de conformité d'un système d'information :

- constituer et maintenir à jour les référentiels techniques et organisationnels à appliquer lors de conduite des audits de sécurité ;
- assurer une veille technologique active sur les risques pesant sur les systèmes informatiques du ministère des armées ;
- mener seul ou en équipe une investigation technique sur un périmètre défini ;
- mener seul ou en équipe une investigation liée à l'environnement technique du système d'information ;
- mener seul ou en équipe une investigation liée à l'environnement organisationnel d'un système d'information ;
- conduire sur plateforme des tests et études de produits de sécurité afférents aux audits techniques ;
- élaborer les synthèses et rédiger les rapports d'audit et contrôle.

Éprouver le niveau de sécurité d'un système d'information :

- réaliser des tests d'intrusion sur un système informatique ;
- rédiger un rapport de test d'intrusion technique.

Proposer un plan d'action à l'issue d'un audit :

- Identifier et formaliser les non-conformités des systèmes et organisations par rapport à un référentiel défini ;
- proposer les évolutions nécessaires à la mise en conformité de l'organisation ou du système d'information contrôlé ;
- concevoir les tableaux de suivi des actions demandées suite à audit ou contrôle ;
- proposer les évolutions de codes informatiques requis pour accroître le niveau de sécurité applicatif ;
- proposer des évolutions techniques sur le paramétrage et la configuration des équipements du système d'information ;
- communiquer et argumenter de manière adaptée selon l'interlocuteur.

MODALITÉS D'ÉVALUATION

Par la voie de la formation :

- Epreuves écrites et orales ;
- Mises en situation professionnelles ;

Par la voie de la VAE :

- Etude du livret 2 ;
- Entretien avec le jury.

visant à démontrer la capacité du candidat à évaluer et identifier les non-conformités et les vulnérabilités d'un système d'information et de proposer un plan de remédiation.

RNCP37300BC03 — Superviser la cybersécurité des systèmes d'information

LISTE DE COMPÉTENCES

Diriger l'action d'une équipe de techniciens au sein d'un centre de supervision :

- exploiter des systèmes de cybersurveillance et de détection d'événements de sécurité ;
- conduire une recherche des éléments précurseurs d'une agression informatique ;
- interpréter les détections afin de qualifier un incident ;
- compléter au besoin les travaux des techniciens en cybersécurité ;
- croiser les constats avec d'autres sources ou d'autres informations.

Améliorer les dispositifs de détection :

- réaliser une veille technologique sur les menaces et les vulnérabilités des systèmes ;
- rédiger des règles de détection pour répondre à de nouvelles menaces ;
- maintenir à jour le catalogue des indicateurs de compromission ;
- caractériser la menace en s'appuyant sur une bonne connaissance régulièrement mis à jour des MOA adverses.

Diriger les différentes phases de réponse sur incident dans le périmètre d'un centre de supervision :

- faire appliquer les directives et procédures de réaction prédéfinies, y compris les procédures d'alerte ;
- faire appliquer les ordres techniques de lutte informatique défensive ;
- caractériser la menace cyber ;
- transmettre les éléments pertinents aux organismes tiers participant à la recherche sur événement ;
- préserver les traces et preuves à des fins d'analyse ;
- transmettre les éléments de façon rigoureuse aux analystes.

Assurer la formation du personnel :

- concevoir et rédiger des scénarii d'entraînement adaptés au profits des équipes de supervision ;
- former les techniciens et opérateurs du centre supervision ;
- évaluer les techniciens et opérateurs du centre de supervision.

MODALITÉS D'ÉVALUATION

Par la voie de la formation :

- Epreuves écrites et orales ;
- Mises en situation professionnelles ;

Par la voie de la VAE :

- Etude du livret 2 ;
- Entretien avec le jury

visant à démontrer la capacité du candidat à superviser, détecter et proposer des solutions de résilience suite à incident cyber.

RNCP37300BC04 — Conduire une investigation numérique dans le domaine de la cybersécurité

LISTE DE COMPÉTENCES

Mener des investigations en réponse sur incident :

- exploiter les éléments recueillis par des sondes gouvernementales ou commerciales de supervision des réseaux ;
- collecter les traces, codes informatiques et preuves lors d'un incident de sécurité ;
- réaliser l'analyse post mortem (inforensique) d'un système ayant subi un incident de sécurité ;
- analyser les traces, codes informatiques et preuves collectés ;
- garantir la préservation et l'intégrité des éléments collectés afin d'être juridiquement recevable ;
- réaliser une analyse dynamique d'un code malveillant dans un environnement sécurisé ;
- évaluer les impacts avérés et potentiels d'incidents informatiques et tenant compte de contextes sensibles.

Capitaliser le résultat des investigations :

- étudier les éléments issus des analyses pour déterminer les stratégies d'attaque et de propagation de codes malveillants ;

- construire et capitaliser un référentiel de données pertinentes à partir des informations recueillies à des fins de retour d'expérience ;
- rédiger et transmettre les rapports d'incident et d'analyse ;
- proposer des solutions de renforcement à long terme du niveau de sécurité des systèmes ;
- maintenir les bases de connaissances des indicateurs de compromission.

MODALITÉS D'ÉVALUATION

Par la voie de la formation :

- Epreuves écrites et orales ;
- Mises en situation professionnelles ;

Par la voie de la VAE :

- Etude du livret 2 ;
- Entretien avec le jury

visant à démontrer la capacité du candidat à caractériser une attaque et adapter sa stratégie de gestion de crise en fonction des retours d'expérience.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Le Responsable en cybersécurité exerce essentiellement ses fonctions dans des unités à terre, sur le territoire métropolitain, en outre-mer ou sur un théâtre d'opération extérieur.

Au gré de ses affectations, il peut être amené à travailler dans des centres d'expertises cyber ou au sein des états-majors propres à chaque armée. Dans ce dernier cas il travaillera le plus souvent au profit de la division SI de l'état-major où il est affecté.

En environnement interarmées, il est amené à travailler dans la majorité des cas au sein de la Direction Interarmées de Réseau d'Infrastructure et des Systèmes d'Information (DIRISI) au sein :

- Du Centre d'Analyse en Lutte Informatique Défensive
- Des Centres de supervision de sécurité régionaux ou nationaux

TYPE D'EMPLOIS ACCESSIBLES

Métier et fonctions accessibles au sein du ministère des armées

- Superviseur cyberdéfense
- Analyste cyberdéfense
- Formateur cybersécurité
- Administrateur cybersécurité
- Officier de systèmes d'information
- Expert SOC(Security Operation Center)
- Administrateur de sécurité
- Auditeur de systèmes d'information
- Contrôleur en cyberprotection
- Analyste en risque des systèmes d'information
- Rédacteur de dossier d'homologation
- Responsable du CSIRT (Computer Security Incident Response Team)
- Spécialiste en cybersécurité

Métier et fonctions accessibles dans le secteur civil

- Responsable de la cybersécurité et de la gestion de crise
- Analyste en cybersécurité
- Responsable du SOC (Security Operation Center)
- Analyste réponse aux incidents de sécurité
- Gestionnaire de crise de cybersécurité
- Analyste de la menace cybersécurité
- Responsable du CSIRT (Computer Security Incident Response Team)
- Spécialiste en cybersécurité

RÈGLEMENTATIONS D'ACTIVITÉ

Sont impérativement exigées pour exercer l'emploi de Responsable en cybersécurité au sein du ministère des

Armées :

- L'habilitation « Secret Défense »[1]
 - L'obtention du statut militaire (sous réserve des conditions de recrutement en vigueur)
- [1]

Le niveau Secret défense (SD) est réservé aux informations ou supports protégés dont la divulgation est de nature à nuire gravement à la défense nationale.

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)	Élevée (4/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 781 €
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) M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom · tension 3/5 (Modérée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	41 765
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 M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

MODALITÉS D'ACCÈS
Formation continue, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Pour l'armée de Terre :

L'admission au stage certifiant de « référent cybersécurité » nécessite de :

1- Détenir les certifications suivantes :

- La certification de Technicien veilleur de cybersécurité enregistrée au RNCP au niveau 5 référencée sous le numéro 36164 ;
- La formation de spécialité 2 « cybersécurité » (FS2 Cyber) ou la Qualification des Acquis Professionnels (QAP 2

CYS) ;

2- Justifier d'au moins 5 années d'expérience après le brevet militaire de 2ème degré à la suite de la FS2 sur un poste du domaine des systèmes d'information et communication (SIC) décrit en cybersécurité ;

3- Justifier d'un niveau en langue anglaise équivalent au niveau B1 du cadre européen commun de référence pour les langues (CECRL) correspondant à un score TOEIC de 550 points ou au profil linguistique standardisé (PLS) 2222.

Pour la Marine nationale

Qu'il s'agisse de la voie alfa ou de la voie bravo (voir infra), l'accès au dispositif de certification nécessite de satisfaire les trois conditions suivantes :

1- Détenir l'une des certifications suivantes :

- le brevet supérieur « systèmes d'informations et de télécommunications » (BS SITEL). Cette certification est enregistrée au RNCP au niveau 5 sous l'intitulé Chef d'équipe d'exploitation et de maintenance des systèmes d'information et de télécommunications et référencée sous le numéro 35239,
- le brevet supérieur « systèmes numériques » (BS SYNUM),
- le brevet supérieur « réseaux et communications » (BS RECOM),
- avoir suivi et réussi la formation de spécialité de 1er niveau (FS1). Cette certification est enregistrée au RNCP au niveau 5 sous l'intitulé de Technicien veilleur de cybersécurité et référencée sous le numéro 36164,
- un brevet supérieur de toute spécialité et être sélectionné ou être titulaire du certificat d'analyste programmeur de système d'information (C CAPSI)

2- Justifier de 2 années d'expérience dans le domaine de la cybersécurité ;

3- Justifier d'un niveau en langue anglaise équivalent au niveau B1 du cadre européen commun de référence pour les langues (CECRL) correspondant à un score TOEIC de 550 points ou au profil linguistique standardisé (PLS) de 2222.

[1] Brevet militaire de 2ème degré délivré à la suite de la FS2.

PRÉREQUIS À LA VALIDATION

Pour l'armée de Terre :

Avoir suivi avec succès le stage « référent cybersécurité », point ultime du parcours professionnel pour attribuer la certification professionnelle de Responsable en cybersécurité de niveau 6.

Pour la Marine nationale

La certification de Responsable en cybersécurité est délivrée à l'issue d'un parcours professionnel repéré par l'attribution du brevet de maîtrise cybersécurité (BM Cyber) accessibles par deux voies : la voie alfa et la voie bravo.

1- Soit la validation totale d'une formation professionnelle (voie alfa),

- dispensée dans une école militaire de spécialité de la marine nationale,
- d'une durée de 10 mois, comprenant un stage d'application,
- sanctionnée par l'obtention du certificat supérieur d'analyste en cybersécurité (CSUP Cyber).

2- Soit la réussite à un examen (voie bravo)

Le niveau d'exigence de l'examen est identique à celui du certificat supérieur d'analyste en cybersécurité (CSUP Cyber) évoqué ci-dessus. Le niveau de compétence est évalué au travers :

- D'une composition écrite (4 heures) sur un thème en lien avec la cybersécurité
- De trois oraux portant sur la sécurité des réseaux, la sécurité des systèmes et la réglementation
- D'un oral devant un grand jury au cours duquel le candidat présente un projet Cyber préparé à l'avance sur le thème communiqué deux mois avant le début des épreuves.
- La réussite à cet examen conduit à l'attribution du brevet de maîtrise cybersécurité (BM Cyber) et à des perspectives d'emplois identiques à la voie alfa.

COMPOSITION DU JURY — FORMATION CONTINUE

Pour l'armée de Terre :

Le jury de certification (hors VAE) pourra comprendre jusqu'à cinq membres avec, si possible, une représentation équilibrée des hommes et des femmes :

Composition du jury comprenant cinq membres :

- le président ;
- deux membres du « collège professionnels » si possible ;
- deux membres du « collège formateurs ».

Composition du jury comprenant trois membres :

Le président ;

- un représentant qualifié de la profession (non formateur, si possible) ;
- un représentant qualifié de la profession (non formateur) ou un formateur.

Des suppléants sont également désignés.

Le président du jury de certification (hors VAE) est soit le commandant de l'école, soit le directeur de l'enseignement ou un officier supérieur cadre de l'enseignement.

Le président et les membres du jury (ainsi que les suppléants) sont désignés par le commandant de l'organisme certificateur pour une période d'un an renouvelable.

Les « professionnels » sont représentés par tout professionnel du secteur hors formateurs, hors organisme certificateur si possible.

Le pourcentage de membres extérieurs à l'autorité délivrant la certification dont professionnels qualifiés est égal à 50 % au moins, dans la mesure du possible, hormis le président.

Pour la Marine nationale

Président du jury :

- Le directeur du Pôle écoles Méditerranée (PEM) ou son représentant.

Membres du jury :

- Le directeur de l'enseignement ou son représentant ;
- Le chef de la division
- Le chef du groupement d'instruction ;
- Le chef de cours
- Un représentant titulaire de la certification.

Le pourcentage de membres extérieurs à l'autorité délivrant la certification dont professionnels qualifiés est égal à zéro (0%)

COMPOSITION DU JURY — VAE

Les membres du jury sont désignés par le commandant de l'organisme certificateur ou son représentant pour une période d'un an renouvelable. Des suppléants sont également désignés.

Les membres du jury sont désignés avec le souci d'assurer une représentation équilibrée entre les femmes et les hommes, en fonction du « vivier » de la spécialité concernée.

- Jurys comprenant cinq membres

Le nombre de membres extérieurs à l'autorité délivrant la certification est égal à deux, si possible. Le nombre de représentants qualifiés de la profession est de trois ou de deux, selon la qualité du président de jury.

Le pourcentage de membres extérieurs à l'autorité délivrant la certification est égal à 40%. Le pourcentage de professionnels qualifiés est égal à 60% ou à 40%, selon la qualité du président de jury.

- Jurys comprenant trois membres

Le nombre de membres extérieurs à l'autorité délivrant la certification est égal, si possible :

- A un, si le président relève du collège « professionnel ». Le pourcentage de membres extérieurs à l'autorité délivrant la certification est de 33%. Le pourcentage de professionnels qualifiés est de 66%.
- A deux, si le président relève du collège « formation ». Le pourcentage de membres extérieurs à l'autorité délivrant la certification est de 66%. Le pourcentage de professionnels qualifiés est également de 66%.

Base légale

Date d'échéance de l'enregistrement 26/08/2027

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2021	5	0	100 %	—
2020	15	0	100 %	—
2019	15	0	100 %	—

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/37300/>