

Analyste opérationnel de renseignement

RNCP37912 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Sigle	Autre — Autre certification professionnelle de droit
Code(s) NSF	344t
Formacode(s)	42802, 42803
Code(s) ROME	K2502, M1403
Type d'enregistrement	Enregistrement de droit
Date d'échéance	17/05/2028

Certificateur(s)

MINISTERE DE L' INTERIEUR ET DES OUTRE-MER · SIRET : 11001401600015<https://www.interieur.gouv.fr/Accueil>

Résumé de la certification

OBJECTIFS ET CONTEXTE

Les Analystes Opérationnels de Renseignement (AOR) exercent au sein des services spécialisés de la communauté du renseignement et notamment au sein du ministère de l'intérieur et des outre-mer. Cette certification professionnelle vient attester de compétences rares, transposables dans le secteur du renseignement, le secteur public ou privé. Son obtention est conditionnée à la validation d'un parcours de formation exigeant, ou à la validation des acquis de l'expérience.

ACTIVITÉS VISÉES

L'analyste opérationnel du renseignement est en charge de la recherche, la collecte, l'exploitation et la valorisation du renseignement recueilli sur l'ensemble du territoire français, ce afin d'évaluer ou d'anticiper les risques d'atteinte aux institutions ou à la sécurité nationale, et de permettre la mise en œuvre d'actions de mitigations du risque, voire d'entrave administrative ou judiciaire.

L'analyste opérationnel du renseignement traite des informations sensibles dans un environnement complexe. En charge du suivi d'un portefeuille de dossiers, il évalue des menaces et analyse des risques en évolution constante. Il intervient à plusieurs étapes du cycle du renseignement (collecte, exploitation, diffusion), en interaction avec des experts techniques ou juridiques, dans une perspective d'information et d'aide à la décision.

- Piloter son activité de recherche de renseignement ;
- Concevoir et mettre en œuvre la collecte du renseignement,
- Structurer et exploiter les données de renseignement,
- Contribuer à l'anticipation et à la prévention des risques.

COMPÉTENCES ATTESTÉES

1.1 - Organiser ses activités de recherche de renseignement :

- Appliquer le cadre légal, réglementaire et déontologique de recherche du renseignement applicable à son entité afin de garantir la conformité de son action ;
- Orienter son activité en fonction des priorités déterminées au niveau stratégique de son entité ;
- Assurer une veille informationnelle sur les menaces identifiées
- Détecter et analyser les signaux faibles de menaces émergentes ;
- Suivre son portefeuille de dossiers selon leur degré d'urgence et les contraintes opérationnelles et techniques ;
- Alimenter les bases de données légales et réglementaires en s'assurant de l'intégrité et de la fiabilité des

informations.

1.2

- Gérer l'information et communiquer dans un environnement sensible ;
- Gérer l'information sensible selon les règles de confidentialité en vigueur ;
- Diffuser les informations requises dans le respect des procédures de communication de son entité ;
- Rendre compte à sa hiérarchie et communiquer à ses collaborateurs concernés l'avancée de ses recherches ;
- Coopérer avec les experts thématiques, juridiques et techniques de son entité en fonction des besoins opérationnels ;
- Coopérer et partager des informations auprès de partenaires, sur le territoire national ou à l'étranger.

2.1

- Concevoir une stratégie d'enquête et un plan de collecte de données ;
- Réaliser une primo-évaluation des menaces en interrogeant les systèmes d'information de son entité (bases de données légales, sources ouvertes,...)
- Élaborer et mettre en œuvre une stratégie d'enquête en vue de procéder à une analyse des risques ;
- Définir les axes de recherche permettant de caractériser la menace ;
- Déterminer l'ensemble des informations à obtenir et identifier les sources de données idoines ;
- Établir les différentes opérations à réaliser et inventorier les ressources à mobiliser ;
- Planifier la collecte du renseignement en fonction de l'urgence de la situation et des contraintes opérationnelles et techniques.

2.2 - Mettre en œuvre le recueil des données :

- Activer l'ensemble des capteurs d'informations arrêtés dans le plan de collecte ;
- Identifier les contacts externes pour préparer et mener les entretiens utiles ;
- Exprimer un besoin de renseignement auprès des prestataires techniques autorisés par l'entité ;
- Étudier la faisabilité technique des opérations avec les experts techniques autorisés par l'entité ;
- Évaluer le ratio bénéfice/risque des opérations techniques demandées ;
- Motiver la demande de prestation en fonction des règles en vigueur dans son entité.

3.1 Structurer des données de nature hétérogènes :

- Évaluer l'intégrité des données collectées au regard de leur conditions de recueil (direct, indirect,...) ;
- Ordonner les données recueillies dans un système documentaire et numérique ;
- Valider ou enrichir les liens entre les données (objets, propriétés) intégrées au système documentaire et numérique.

3.2 Exploiter les données collectées :

- Recouper les données collectées afin de les consolider ;
- Visualiser les informations et les mettre en forme pour préparer leur analyse ;
- Analyser les informations recueillies au regard des axes de recherche afin de caractériser la menace et d'établir la réalité des risques ;
- Identifier le cas échéant des axes de recherche complémentaires ;
- Produire un renseignement à partir d'informations fiables, recoupées, enrichies ;
- Capitaliser le renseignement au sein des bases de données légales et réglementaires de son entité ;
- Mettre en place des indicateurs d'alerte et savoir les adapter en fonction des événements.

4.1 Informer les décideurs sur les risques caractérisés :

- Restituer le renseignement aux autorités compétentes par des briefings oraux ;
- Restituer le renseignement aux autorités compétentes par la production de comptes-rendus écrits et de notes selon les procédures et le formalisme en vigueur ;
- Identifier les partenaires pertinents et leur diffuser les renseignements collectés ;
- Sécuriser la transmission du renseignement.

4.2 Proposer des mesures répondant au risque établi et à la menace caractérisée :

- Déterminer les mesures préventives et mobiliser les acteurs adéquats en fonction de la stratégie établie ;
- Sensibiliser les acteurs susceptibles de présenter une vulnérabilité ;
- Proposer la saisine des autorités administratives ou judiciaires compétentes en cas de détection d'une menace avérée.

Blocs de compétences

RNCP37912BC01 — Piloter son activité de recherche de renseignement

LISTE DE COMPÉTENCES

1.1 - Organiser ses activités de recherche de renseignement :

- Appliquer le cadre légal, réglementaire et déontologique de recherche du renseignement applicable à son entité afin de garantir la conformité de son action ;
- Orienter son activité en fonction des priorités déterminées au niveau stratégique de son entité ;
- Assurer une veille informationnelle sur les menaces identifiées
- Détecter et analyser les signaux faibles de menaces émergentes ;
- Suivre son portefeuille de dossiers selon leur degré d'urgence et les contraintes opérationnelles et techniques ;
- Alimenter les bases de données légales et réglementaires en s'assurant de l'intégrité et de la fiabilité des informations.

1.2 - Gérer l'information et communiquer dans un environnement sensible :

- Gérer l'information sensible selon les règles de confidentialité en vigueur ;
- Diffuser les informations requises dans le respect des procédures de communication de son entité ;
- Rendre compte à sa hiérarchie et communiquer à ses collaborateurs concernés l'avancée de ses recherches ;
- Coopérer avec les experts thématiques, juridiques et techniques de son entité en fonction des besoins opérationnels ,
- Coopérer et partager des informations auprès de partenaires, sur le territoire national ou à l'étranger.

MODALITÉS D'ÉVALUATION

- Contrôle de connaissances ;
- Mise en situation contextualisées ;
- Étude de cas et/ou de restitutions technico-opérationnelles.

RNCP37912BC02 — Concevoir et mettre en œuvre la collecte du renseignement

LISTE DE COMPÉTENCES

2.1 Concevoir une stratégie d'enquête et un plan de collecte de données :

- Réaliser une primo-évaluation des menaces en interrogeant les systèmes d'information de son entité (bases de données légales, sources ouvertes,...)
- Élaborer et mettre en œuvre une stratégie d'enquête en vue de procéder à une analyse des risques ;
- Définir les axes de recherche permettant de caractériser la menace ;
- Déterminer l'ensemble des informations à obtenir et identifier les sources de données idoines ;
- Établir les différentes opérations à réaliser et inventorier les ressources à mobiliser ;
- Planifier la collecte du renseignement en fonction de l'urgence de la situation et des contraintes opérationnelles et techniques.

2.2 Mettre en œuvre le recueil des données :

- Activer l'ensemble des capteurs d'informations arrêtés dans le plan de collecte ;
- Identifier les contacts externes pour préparer et mener les entretiens utiles ;
- Exprimer un besoin de renseignement auprès des prestataires techniques autorisés par l'entité ;
- Étudier la faisabilité technique des opérations avec les experts techniques autorisés par l'entité ;
- Évaluer le ratio bénéfice/risque des opérations techniques demandées ;
- Motiver la demande de prestation en fonction des règles en vigueur dans son entité.

MODALITÉS D'ÉVALUATION

- Contrôle de connaissances ;
- Mise en situation contextualisées ;
- Étude de cas et/ou de restitutions technico-opérationnelles.

RNCP37912BC03 — Structurer et exploiter les données de renseignement

LISTE DE COMPÉTENCES

3.1 Structurer des données de nature hétérogènes :

- Évaluer l'intégrité des données collectées au regard de leurs conditions de recueil (direct, indirect,...) ;
- Ordonner les données recueillies dans un système documentaire et numérique ;
- Valider ou enrichir les liens entre les données (objets, propriétés) intégrées au système documentaire et numérique.

3.2 Exploiter les données collectées :

- Recouper les données collectées afin de les consolider ;
- Visualiser les informations et les mettre en forme pour préparer leur analyse ;
- Analyser les informations recueillies au regard des axes de recherche afin de caractériser la menace et d'établir la réalité des risques ;
- Identifier le cas échant des axes de recherche complémentaires ;
- Produire un renseignement à partir d'informations fiables, recoupées, enrichies ;
- Capitaliser le renseignement au sein des bases de données légales et réglementaires de son entité ;
- Mettre en place des indicateurs d'alerte et savoir les adapter en fonction des événements.

MODALITÉS D'ÉVALUATION

- Contrôle de connaissances ;
- Mise en situation contextualisées ;
- Étude de cas et/ou de restitutions technico-opérationnelles.

RNCP37912BC04 — Contribuer à l'anticipation et à la prévention des risques

LISTE DE COMPÉTENCES

4.1 Informer les décideurs sur les risques caractérisés :

- Restituer le renseignement aux autorités compétentes par des briefings oraux ;
- Restituer le renseignement aux autorités compétentes par la production de comptes-rendus écrits et de notes selon les procédures et le formalisme en vigueur ;
- Identifier les partenaires pertinents et leur diffuser les renseignements collectés ;
- Sécuriser la transmission du renseignement

4.2 Proposer des mesures répondant au risque établi et à la menace caractérisée :

- Déterminer les mesures préventives et mobiliser les acteurs adéquats en fonction de la stratégie établie ;
- Sensibiliser les acteurs susceptibles de présenter une vulnérabilité ;
- Proposer la saisine des autorités administratives ou judiciaires compétentes en cas de détection d'une menace avérée.

MODALITÉS D'ÉVALUATION

- Contrôle de connaissances ;
- Mise en situation contextualisées ;
- Étude de cas et/ou de restitutions technico-opérationnelles.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Les Analystes Opérationnels de Renseignement évoluent principalement au sein des services de la communauté du renseignement du premier cercle (DGSE, DRM, DRSD, DNRED, Tracfin) ou du second cercle (SCRT, DRPP, SDAO, SNRP).

Dans le service public, les AOR peuvent mettre leurs compétences au profit de services d'investigations habilités à mettre en œuvre des techniques de renseignement dans le cadre des finalités légales qui leur sont propres (DCPJ, DCPAF...), intégrer des services interministériels spécialisés (SGDSN, VIGINUM, GIC,...) voire des organisations internationales d'essence policière ou militaire (Europol, Interpol, OTAN).

Dans le secteur privé, les AOR peuvent évoluer au sein des directions sécurité-sûreté d'entreprise des grands groupes et PME françaises ou de toute autre direction thématique opérant dans la prévention des risques et des menaces, notamment

sur des enjeux liés à la sécurité économique et à la protection des savoir-faire industriels et technologiques essentiels.

TYPE D'EMPLOIS ACCESSIBLES

- Analyste Sécurité-Sûreté Corporate (SSC), chargé de veille-analyse SSC, veilleur stratégique,
- Analyste expert en gestion des risques, sécurité/intelligence économique, lutte contre la fraude.

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 4 sur 5.
Facteurs principaux	Non-attractivité salariale, Intensité d'embauche, Inadéquation géographique
Salaire médian (mensuel)	2 006 €
Familles professionnelles (FAP)	L4X82 — Techniciens et agents de maîtrise chargés d'études socio-économiques · tension 4/5 (Élevée) L5X93 — Chargés d'études socio-économiques · tension 3/5 (Modérée) T3X61 — Agents de sécurité et de surveillance · tension 4/5 (Élevée)
Projets de recrutement (BMO 2026)	26 847
Jugés difficiles à recruter	47 %
Emplois saisonniers	21 %
Familles professionnelles (FAP)	L4X82 — Techniciens et agents de maîtrise chargés d'études socio-économiques L5X93 — Chargés d'études socio-économiques T3X61 — Agents de sécurité et de surveillance

Voies d'accès

MODALITÉS D'ACCÈS

Formation continue, VAE

COMPOSITION DU JURY — FORMATION CONTINUE, VAE

- Président : le directeur général de la sécurité intérieure ou son représentant ;
- Collège employeur : 2 représentants qualifiés en exercice au sein d'un service de la communauté du renseignement ;
- Collège formateur : 1 membre du service de formation de la direction générale de la sécurité intérieure.

Base légale

Date d'échéance de l'enregistrement	17/05/2028
Date de dernière délivrance possible	17/05/2031

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/37912/>