

Analyste en cybersécurité dans le secteur aéronautique

RNCP36929 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Code(s) NSF	326n, 326p
Formacode(s)	31045
Code(s) ROME	M1804, M1802, M1810, M1801, M1805
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	29/09/2022
Date d'échéance	29/09/2025

Certificateur(s)

AIRBUS OPERATIONS · SIRET : 42091691800048

Résumé de la certification

OBJECTIFS ET CONTEXTE

L'Analyste cybersécurité est le garant de l'intégrité et de la confidentialité des données informatiques de l'entreprise, il lutte notamment contre la cybercriminalité et les menaces qui y sont associées.

ACTIVITÉS VISÉES

Etude des métiers l'industrie aéronautique

Exploitation des systèmes, des logiciels de cybersécurité sur les produits aéronautique

Administration et adaptation d'outils informatiques de sécurité au milieu aéronautique

Participation à la sécurité du système d'information grâce à une veille technologique et réglementaire

Pratique d'audits informatiques

Mise en place des corrections des vulnérabilités

Préconisations d'amélioration de la politique de sécurité

administration et sécurisation des de composants cybersécurité constituant le système d'information

Déploiement des éléments de sécurité dans le système d'information

Génération de rapports de sécurité

Analyse des risques et des vulnérabilités du système d'information

Mise en place des éléments de sécurité du système d'information

Collecte des preuves numériques selon les procédures en vigueur

Sécurisation des réseaux et des accès distants

Utilisation de la gestion de projet dans le cadre du déploiement de la cybersécurité

Sensibilisation et accompagnement des utilisateurs finaux

Accompagnement des utilisateurs lors d'une crise de cybersécurité

COMPÉTENCES ATTESTÉES

Mesurer les risques encourus par les éléments IT d'un environnement aéronautique par une veille active afin d'identifier les points de sensibilité de l'industrie à la cybersécurité.

Participer et améliorer la veille sur la réglementation de la cybersécurité dans le domaine aéronautique en utilisant les informations mises à disposition (newsletter, plateforme de partage, plateforme de veille active,...) afin de garantir la conformité du système d'information

Interagir avec les spécialistes industriels (responsables méthodes et outils, responsables de production) en identifiant les processus clés de la production aéronautique en pour appliquer les principes de la cybersécurité.

Exécuter un test d'intrusion à l'aide d'un ou plusieurs logiciels de cybersécurité sur un système embarqué aéronautique ou aérospatial pour tester sa sécurité

Mettre à jour et connecter des logiciels en développant des codes informatiques afin d'analyser l'activité d'un système d'information en milieu aéronautique

Vérifier la conformité du système d'information en utilisant les outils de veille mis à disposition (rapports du CERT, plateforme de partage, virus total, outils de veille légale, newsletters,...) afin de garantir le respect des règles légales.

Faire des analyses d'éléments du système d'information (poste de travail, serveurs, réseau local) en utilisant les guides à disposition afin de vérifier la cybersécurité des éléments.

Corriger des programmes informatiques en modifiant le code existant afin de supprimer des vulnérabilités le système d'information, Bash pour l'administration système dans les environnements Unix, Python pour l'intégration avec l'écosystème sécurité, SQL pour la connaissance de manipulations de données, Powershell pour l'intégration dans les environnements Windows

Rédiger des rapports proposant des modifications des process de déploiement des outils informatiques afin d'améliorer la sécurité lors de leur mise en place

Analyser le fonctionnement de programmes et de composants en effectuant des tests de sécurité informatiques et en se basant les outils d'administration et de détection type SIEM, IDS/IPS, les outils de manipulation de fichiers de logs et savoir analyser des logs pour détecter des anomalies et comportement anormaux, des outils de test d'intrusion réseau/système pour repérer des potentielles attaques et détecter les points faibles du système d'information

Déployer des éléments de sécurité (Patches, Mises à jour, changement de protocoles de communication, ...) en appliquant les guides appropriés pour sécuriser des systèmes et logiciels.

Automatiser l'analyse du système d'information (journal de bord du système,) par le développement de programmes afin de s'assurer de l'intégrité du système d'information d'une entreprise

Identifier les risques d'éléments du système d'information en appliquant la méthode EBIOS RM afin d'éviter les vulnérabilités.

Déployer les outils de sécurité (firewall, antivirus) en se basant sur les process de l'entreprise afin de garantir la sécurité du système d'information

Réaliser la collecte de preuves numériques de façon technico-légale à l'aide d'outils de collecte dédiés fournis par la sécurité informatique de l'entreprise afin de préserver les preuves numériques.

Configurer de façon sécurisée les protocoles de bases (BGP, OSPF, VRRP, etc) en s'appuyant sur les standards en vigueur afin d'augmenter la sécurité d'un réseau

Participer au déploiement du système d'information (sur divers environnements techniques : partie du réseau, ensemble de serveurs etc) via les méthodes de gestion de projet (AGILE, SAFE) pour mettre à niveau les différents éléments du système dans une structure complexe.

Sensibiliser les utilisateurs finaux à avoir recours aux bonnes pratiques en diffusant les recommandations de cybersécurité pour améliorer la culture de sécurité.

Accompagner les utilisateurs à la résolution d'une crise suite à un incident de cybersécurité en analysant correctement les informations mises à disposition par les utilisateurs ainsi que par les différents outils d'analyse du système d'information pour garantir la confidentialité et l'intégrité de l'entreprise.

Blocs de compétences

RNCP36929BC01 — Appliquer la cybersécurité au secteur spécifique de l'aéronautique

LISTE DE COMPÉTENCES

Mesurer les risques encourus par les éléments IT d'un environnement aéronautique par une veille active afin d'identifier les points de sensibilité de l'industrie à la cybersécurité.

Participer et améliorer la veille sur la réglementation de la cybersécurité dans le domaine aéronautique en utilisant les informations mises à disposition (newsletter, plateforme de partage, plateforme de veille active,...) afin de garantir la conformité du système d'information

Interagir avec les spécialistes industriels (responsables méthodes et outils, responsables de production) en identifiant les processus clés de la production aéronautique en pour appliquer les principes de la cybersécurité.

Exécuter un test d'intrusion à l'aide d'un ou plusieurs logiciels de cybersécurité sur un système embarqué aéronautique ou aérospatial pour tester sa sécurité

Mettre à jour et connecter des logiciels en développant des codes informatiques afin d'analyser l'activité d'un système d'information en milieu aéronautique

MODALITÉS D'ÉVALUATION

A partir d'un cas basé sur les métiers et processus de l'entreprise ou élaboré par un groupe de professeurs, le candidat répond à un QCM portant sur les principaux éléments sensibles à la cybersécurité dans un environnement aérospatial ainsi que sur les éléments de la réglementation s'y rattachant.

A partir d'un cas fictif ou réel, le candidat accompagner les spécialistes industriels et les sensibiliser aux problématiques de la cybersécurité. Par la suite, il doit faire une présentation orale à un jury composé des professeurs experts de la matière. La présentation orale s'appuie sur un support visuel (diaporama) qui devra comprendre à minima le contexte industriel du cas, la présentation et l'analyse des composants du cas, les processus clés liés aux composants du cas, les éléments de cybersécurité à prendre en compte

A partir d'un cas fictif ou réel, le candidat doit mettre en place une procédure de test d'intrusion et l'exécuter. A l'issue de cette exécution, le candidat effectuera une présentation à l'oral au jury expliquant : le choix des outils et logiciels adéquats pour le test d'intrusion Les éléments démontrant la réussite de l'intrusion le cas échéant, les propositions d'amélioration ou de modification de programmation s'il y a lieu (pour renforcer le système d'information de l'entreprise contre l'intrusion)

A partir d'un cas réel ou fictif, le candidat doit produire un dossier contenant le code informatique, les preuves de l'exécution correcte de ce code, des propositions d'amélioration le cas échéant, le guide d'utilisation, les rapports d'analyses

Le dossier sera fourni sous la forme de fichiers sources (code informatique lisible et commenté) et de fiches explicatives sur les anomalies, les propositions d'amélioration et les rapports d'analyse.

RNCP36929BC02 — Participer à une politique de sécurité

LISTE DE COMPÉTENCES

Vérifier la conformité du système d'information en utilisant les outils de veille mis à disposition (rapports du CERT, plateforme de partage, virus total, outils de veille légale, newsletters,...) afin de garantir le respect des règles légales. Faire des analyses d'éléments du système d'information (poste de travail, serveurs, réseau local) en utilisant les guides à disposition afin de vérifier la cybersécurité des éléments.

Corriger des programmes informatiques en modifiant le code existant afin de supprimer des vulnérabilités le système d'information, Bash pour l'administration système dans les environnements Unix, Python pour l'intégration avec l'écosystème sécurité, SQL pour la connaissance de manipulations de données, Powershell pour l'intégration dans les environnements Windows

Rédiger des rapports proposant des modifications des process de déploiement des outils informatique afin d'améliorer la sécurité lors de leur mise en place

MODALITÉS D'ÉVALUATION

Vérifier la conformité du système d'information en utilisant les outils de veille mis à disposition (rapports du CERT, plateforme de partage, virus total, outils de veille légale, newsletters,...) afin de garantir le respect des règles légales.
R

épondre à un questionnaire de connaissance sur les règles et normes de cybersécurité

Cas pratique de système d'information d'entreprise

Rédiger d'un rapport des non conformités de sécurité identifiés sur le cas pratique

Le rapport prend la forme d'un manuscrit synthétique.

A partir d'un cas réel ou fictif, le candidat doit produire un rapport d'analyses établissant un état des lieux de la configuration d'éléments du réseau (postes, serveurs, etc.) comprenant les failles et les propositions de traitement.

Le rapport prend la forme d'un manuscrit synthétique.

Cas réels ou fictifs avec rendu de livrables

RNCP36929BC03 — Administrer un système d'information sécurisé

LISTE DE COMPÉTENCES

Analyser le fonctionnement de programmes et de composants en effectuant des tests de sécurité informatiques et en se basant les outils d'administration et de détection type SIEM, IDS/IPS, les outils de manipulation de fichiers de logs et savoir analyser des logs pour détecter des anomalies et comportement anormaux, des outils de test d'intrusion réseau/système pour repérer des potentielles attaques et détecter les points faibles du système d'information

Déployer des éléments de sécurité (Patches, Mises à jour, changement de protocoles de communication, ...) en appliquant les guides appropriés pour sécuriser des systèmes et logiciels.

Automatiser l'analyse du système d'information (journal de bord du système,) par le développement de programmes afin de s'assurer de l'intégrité du système d'information d'une entreprise

MODALITÉS D'ÉVALUATION

A partir d'un cas réel ou fictif, le candidat doit produire un dossier contenant les codes informatiques ou les logiciels utilisés pour faire les analyses, les preuves d'identification des menaces, les corrections des codes informatiques effectuées, les preuves de mise du fonctionnement des corrections le cas échéant

Le dossier sera fourni sous la forme de fichiers sources (code informatique lisible et commenté) et de fiches explicatives synthétiques des logiciels choisis, des menaces identifiées et corrections apportées.

A partir d'un cas réel ou fictif, le candidat doit installer et mettre à jour des éléments du réseau et produire un dossier contenant les éléments de sécurité installés ou mis à jour, la liste des guides utilisés pour déployer ces éléments, les preuves du bon fonctionnement du réseau après ces mis à jour

A partir d'un cas réel ou fictif, le candidat doit automatiser une production de rapport de cybersécurité et produire un dossier contenant le code sources des programmes permettant l'automatisation de rapport, les rapports automatisés émis par le ou les programmes, les éléments démontrant la cohérence des rapports en fonction des informations recueillies lors de l'analyse du système d'information

RNCP36929BC04 — Garantir la sécurité d'un SI

LISTE DE COMPÉTENCES

Identifier les risques d'éléments du système d'information en appliquant la méthode EBIOS RM afin d'éviter les vulnérabilités.

Déployer les outils de sécurité (firewall, antivirus) en se basant sur les process de l'entreprise afin de garantir la sécurité du système d'information

Réaliser la collecte de preuves numériques de façon technico-légale à l'aide d'outils de collecte dédiés fournis par la sécurité informatique de l'entreprise afin de préserver les preuves numériques.

Configurer de façon sécurisée les protocoles de bases (BGP, OSPF, VRRP, etc) en s'appuyant sur les standards en vigueur afin d'augmenter la sécurité d'un réseau

MODALITÉS D'ÉVALUATION

A partir d'un cas réel ou fictif, le candidat doit produire une présentation du cas qu'il aura analysée suivant la méthode EBIOS RM contenant les différents ateliers de la méthode EBIOS, les hypothèses choisis pour l'application de la méthode EBIOS, les conclusions concernant les risques, les préconisations pour limiter l'impact des risques s'il y a lieu

La présentation sera évaluée par un jury composé de certificateurs.

A partir d'un cas réel ou fictif, le candidat doit déployer des outils de sécurité et produire une présentation contenant les différents outils de sécurité à déployer les choix de configurations des différents éléments, les preuves du bon fonctionnement du réseau après l'installation des éléments

La présentation sera évaluée lors d'un oral.

A partir d'un cas réel ou fictif, le candidat doit réaliser une collecte de façon technico légale et produire un rapport contenant la liste des éléments pris en compte dans l'analyse technico légale (des copies de disques durs, des copies de smartphones, log, etc), le choix des outils pour faire l'analyse technico légale, les scénarios d'analyse et les résultats associés

A partir d'un cas réel ou fictif, le candidat doit configurer des protocoles de base et produire un dossier contenant la liste des protocoles à configurer, les configurations choisies, les explications concernant les choix de configurations

RNCP36929BC05 — Participer à l'encadrement et à la coordination d'un projet de sécurisation

LISTE DE COMPÉTENCES

Participer au déploiement du système d'information (sur divers environnements techniques : partie du réseau, ensemble de serveurs etc) via les méthodes de gestion de projet (AGILE, SAFE) pour mettre à niveau les différents éléments du système dans une structure complexe.

Sensibiliser les utilisateurs finaux à avoir recours aux bonnes pratiques en diffusant les recommandations de cybersécurité pour améliorer la culture de sécurité.

Accompagner les utilisateurs à la résolution d'une crise suite à un incident de cybersécurité en analysant correctement les informations mises à disposition par les utilisateurs ainsi que par les différents outils d'analyse du système d'information pour garantir la confidentialité et l'intégrité de l'entreprise.

MODALITÉS D'ÉVALUATION

A partir d'un cas réel ou fictif, le candidat participe à un déploiement d'éléments sur le système d'information. Il doit établir un document décrivant l'utilisation de la méthode de gestion de projet (AGILE, SAFE etc et le vocabulaire associé épopée, use case etc...), les éléments garantissant la structure de l'équipe projet (workpackage, SWOT

analyse de risque etc....), la description du découpage du projet: tâches, itérations, planning, la prise en compte des situations de handicap le cas échéant

Le rapport prend la forme d'un manuscrit synthétique.

A partir d'un cas réel ou fictif, le candidat sensibilise les utilisateurs aux problématiques de la cybersécurité lors de la sélection d'outils informatiques. Il recueille leur besoin et explique les éléments de cybersécurité à prendre en compte. Il doit ensuite produire un dossier contenant une liste de critères justificatifs des logiciels sélectionnés pour adresser les problèmes identifiés dans le cas étudié, un guide d'installation des logiciels retenus, le guide de mise en œuvre des solutions

Le dossier sera fourni sous la forme de liste des logiciels accompagnés de la raison de leur sélection, du séquençage de leur installation ainsi que de celui de leur exécution.

A partir d'un cas réel ou fictif, le candidat accompagne les utilisateurs lors d'une crise de cybersécurité en recueillant leurs informations et leurs besoins. Il doit à partir de cet accompagnement produire un dossier contenant les rapports d'analyse des types d'attaque de cybersécurité associés aux cas étudiés, une liste de recommandations de cybersécurité à mettre en œuvre, le guide de mise en œuvre des recommandations proposées

Le dossier sera fourni sous la forme de listes d'anomalies et de fiches explicatives sur les anomalies, les propositions d'amélioration et les rapports d'analyse.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

L'analyste en cybersécurité peut être recruté dans des entreprises de tailles différentes allant de la TPE à l'entreprise du CAC 40 en passant par la PME. Ses missions seront dès lors adaptées à l'environnement dans lequel il exercera son métier. Les structures peuvent ou non être spécialisées en cybersécurité.

TYPE D'EMPLOIS ACCESSIBLES

Analyste en cybersécurité

Opérateur Security Operation Center (SOC)

Administrateur sécurité systèmes et réseaux

Pentester junior

Opérateur de rapport d'audit en cybersécurité

Coordinateur sécurité

RÉGLEMENTATIONS D'ACTIVITÉ

Pour faire face aux nouvelles menaces cyber, l'article 22 de la loi de programmation militaire

(loi n° 2013-1168 du 18 décembre 2013), qui fait suite aux préconisations du Livre blanc sur la défense et la sécurité nationale

(LPM) (loi n° 2013-1168 du 18 décembre 2013) imposent aux Opérateurs d'Importance Vitale (OIV) le renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent. Dans ce cadre, les OIV doivent être en mesure d'obtenir en interne et en externe une certaine compétence en cybersécurité afin d'assurer cette obligation légale pionnière en Europe encadrant la cybersécurité de ces infrastructures critiques.

Pour faire face aux nouvelles menaces cyber, l'article 22 de cette loi vient définir les responsabilités et les obligations des OIV en termes de protection de leurs systèmes d'information critiques. Il oblige ainsi les OIV à faire auditer leurs SIIV (Systèmes d'Information d'Importance Vitale) par des organismes qualifiés PASSI (Prestataires d'Audit SSI) ainsi qu'à mettre en œuvre les mesures de sécurité des systèmes d'informations (SSI) et des systèmes de détection qualifiés. Plus encore, l'article contraint les OIV à déclarer de façon immédiate des incidents SSI affectant de manière significative leurs SIIV.

L'écosystème aéronautique et spatial est particulier car les entreprises le composant sont souvent des OIV (Opérateurs d'Importance Vitale). Leur sécurité doit donc être maintenue au plus haut niveau d'exigence. Dans ce cadre, l'activité des analystes en cybersécurité est soumise aux décrets n°2015-351 et n°2015-350 relatif à la sécurité des systèmes d'information des Opérateurs d'Importance Vitale et à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information.

De plus, les autorités européennes ont publié la norme PART IS. Par cette nouvelle norme, l'autorité de certification aéronautique, l'EASA, demande depuis 2020 aux acteurs de l'écosystème aéronautique de garantir la sécurité des données liés aux produits tels que les avions et les hélicoptères, des services associés aux produits mais aussi la sécurité de l'environnement dans lequel elles sont utilisées (aéroports, chaînes d'approvisionnement etc...).

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

PRÉREQUIS À L'ENTRÉE EN FORMATION

Peuvent accéder à la certification des candidats disposant de :

Diplôme de niveau 5 tels que DUT Réseaux & Télécommunication, DUT Informatique, BTS Services Informatiques aux Organisations (SIO) (options : Solutions d'Infrastructure, Systèmes et Réseaux, BTS Systèmes Numériques (SN) (option : Informatique et Réseaux, L2 Informatique, Autres diplômes Bac + 2 de la spécialité cybersécurité, Étudiants en 3eme année de cycle ingénieur IT souhaitant changer de cursus
ou d'un diplôme de niveau 4 avec minimum 5 ans d'expérience professionnelle en informatique

COMPOSITION DU JURY — FORMATION CONTINUE, APPRENTISSAGE

Le jury est composé de 4 membres:

Un responsable de Airbus Cybersecurity School ou son représentant (formateur référent ou personne déléguée dans le cadre de l'encadrement des formations sous Licence)

Le responsable pédagogique à l'Airbus Cybersecurity School assurant la cohésion des enseignements délivrant les compétences nécessaires.

Un professionnel (non salarié d'Airbus) expert de la cybersécurité depuis au moins 3 ans

Un représentant des salariés : personne exerçant l'un des métiers visés par la certification depuis au moins 3 ans

COMPOSITION DU JURY — VAE

Le jury est composé de 3 membres:

Un responsable de Airbus Cybersecurity School ou son représentant (formateur référent ou personne déléguée dans le cadre de l'encadrement des formations sous Licence)

Un représentant des employeurs : chef d'entreprise ou élu d'une organisation professionnelle

Un représentant des salariés : personne exerçant l'un des métiers visés par la certification depuis au moins 3 ans

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	7 541 €
Selon la branche	7 124 € – 8 000 €
Prise en charge	Branches concernées
7 541 €	Valeur par défaut · 210 branches
8 000 €	CPNE chimie
7 500 €	CPNEFP de la métallurgie
7 124 €	CPNEFP de la blanchisserie, laverie, location de linge, nettoyage à sec, pressing et teinturerie

Base légale

Date de décision	29/09/2022
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	29/09/2025

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/36929/>