

Expert en Cybersécurité

RNCP36122 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	31045
Code(s) ROME	M1802, M1810, M1801, M1805, M1806
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	26/01/2022
Date d'échéance	26/01/2025

Certificateur(s)

IKAI · SIRET : 90005795100031

IKAI · SIRET : 90005795100023

Partenaires habilités

1 organisme habilité, d'après la liste publiée par France compétences : 1 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
IKAI	90005795100031	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

Au cœur de la transformation numérique, la cybersécurité est essentielle au bon fonctionnement de nos entreprises, de nos institutions et plus largement, de nos sociétés. Un grand panel de métiers est nécessaire pour couvrir l'ensemble des enjeux stratégiques, techniques, opérationnels et managériaux du secteur.

La certifie atteste de l'acquisition à la fois des compétences globales essentielles pour travailler en cybersécurité et de certaines compétences spécifiques en fonction du métier visé. La spécialisation est clé pour atteindre le niveau requis pour devenir expert en cybersécurité. Cette certification d'expert en cybersécurité propose 3 spécialisations : en développement ou en sécurité opérationnelle & Ethical Hacking ou encore en gouvernance et conseil.

ACTIVITÉS VISÉES

Bloc n°1 – Identifier les solutions techniques de sécurité d'un SI face à la menace

- Protection des composants physiques d'un système d'information
- Protection des composants logiques d'un système d'information
- Protection des réseaux
- Protection des données personnelles et des informations
- Protection des systèmes embarqués
- La veille en cybersécurité

Bloc n°2 – Opérer et surveiller les mesures de sécurité d'un SI

- Gestion des événements et les incidents de sécurité de l'information
- Réalisation d'une enquête technico légale (Forensic)
- Réalisation d'un test d'intrusion

Bloc n°3 – Auditer la maturité de la cybersécurité d'un système d'information

- Mise en place un système de management de la sécurité de l'information (SMSI)
- Analyse de risque
- Audit de maturité des mesures de sécurité déployées par l'organisation Conception d'une roadmap d'amélioration de la sécurité du système d'information

Bloc n°4 – Piloter un projet et communiquer en cybersécurité

- Réalisation d'un business case et d'un plan de gestion de projet de sécurisation de l'information
- Pilotage du changement
- Communication d'une démarche de cybersécurité
- Communication de crise
- Management d'équipe

(option) Bloc de spécialisation n°1 – Concevoir et déployer un système d'information sécurisé avec une approche DevSecOps

- Projet de Transformation numérique
- Architecture technique hardware
- Architecture logicielle
- La gestion d'un projet de développement sécurisé

(option) Bloc de spécialisation n°2 – Préparer un audit de certification en sécurité et continuité de l'information

- Audit d'un système d'information en sécurité de l'information
- Audit d'une entreprise et du système d'information en résilience, continuité, gestion de crise et plan de secours
- Gouvernance des systèmes d'information

(option) Bloc de spécialisation n°3 – Détecter et traiter les incidents techniques à l'aide de l'intelligence artificielle

- Installer un outil de SIEM (Security Incident & Event Management)
- Analyse et recherche d'anomalies de sécurité
- Paramétrage d'un outil de SIEM et recherches avancées
- Reporting à une équipe technique et à la direction du suivi de la sécurité

COMPÉTENCES ATTESTÉES

Bloc n°1 – Identifier les solutions techniques de sécurité d'un SI face à la menace

- Renforcer la sécurité des 5 composants d'un ordinateur en vue de protéger le système matériel par une analyse de leur périmètre et de leur rôle, ainsi que des risques associés
- Renforcer la sécurité des systèmes d'exploitation, la terminologie et les fonctions de la virtualisation et des containers, en vue de protéger la sécurité des composants logiques d'un système d'information, par une analyse de leur périmètre et de leur rôle, ainsi que des risques associés.
- Renforcer

la sécurité des 7 couches du modèle OSI de description des réseaux, en déterminant les risques associés à chacune des couches, par la reconnaissance

des différents types d'attaque sur chacune des couches du modèle OSI

- Appliquer aux réseaux TCP/IP les principes de la démarche de protection des 7 couches du modèle OSI
- Cartographier les données personnelles déterminer leur criticité et leur valeur selon les exigences du RGPD et d'ISO 27701
- Appliquer à la sécurité des données les mesures techniques de protection adéquates en fonction de leur valeur : chiffrement symétrique et asymétrique, anonymisation, pseudonymisation
- Identifier les systèmes embarqués, les PLC (Programmable Logic Controller) et les RTU (Remote Terminal Unit), identifier les protocoles sous-jacents et les systèmes de supervision, pour déterminer leurs vulnérabilités et appliquer les mesures de sécurité techniques pour renforcer la sécurité des systèmes embarqués
- Suivre les flux d'information en cybersécurité pour être informé des dernières menaces et des solutions à déployer par la mise en place d'un système de veille en cyber sécurité

Bloc n°2 – Opérer

et surveiller les mesures de sécurité d'un SI

- Déployer un système de monitoring de l'activité en sécurité de l'information pour repérer les événements et les incidents de sécurité, afin de les traiter
- Concevoir un processus et un flux de traitement des événements et des incidents en s'appuyant sur la norme ISO 27035, pour automatiser le traitement des événements et des incidents
- Mener une enquête technico légale (Forensic) en s'appuyant sur la norme ISO27037, afin d'identifier la cause des incidents de cyber sécurité et d'y apporter des solutions

- Réaliser un test d'intrusion selon les standards du marché (planification, reconnaissance, test de vulnérabilité, exploitation, effacement des traces, rapport) pour identifier les vulnérabilités d'un système d'information et ainsi renforcer sa sécurité

Bloc n°3 – Auditer la maturité de la cybersécurité d'un système d'information

- Déployer un SMSI pour apporter un cadre de gouvernance et de gestion de la sécurité d'un système d'information en s'appuyant sur les meilleures pratiques d'ISO
- Evaluer la maturité du SMSI pour renforcer la sécurité du système d'information en s'appuyant sur la norme ISO 15504
- Réaliser une analyse de risque pour identifier les vulnérabilités et menaces potentielles en sécurité du système d'information et s'appuyant sur ISO 27005 et Ebios
- Proposer des mesures de traitement pour renforcer la sécurité du système d'information en s'appuyant sur l'analyse de risques, ainsi que les meilleures pratiques de l'OWASP, du MITRE
- Analyser l'efficacité et l'efficience des mesures de sécurité mises en place par l'organisation, pour identifier les plus faibles et les moins pertinentes, afin de renforcer la sécurité du système d'information
- Préparer un plan de projet comprenant l'ensemble des mesures de sécurité manquantes ou à renforcer, sur à l'audit de maturité, pour renforcer la sécurité du système d'information

Bloc n°4 – Piloter un projet et communiquer en cybersécurité

- Concevoir un projet de cybersécurité, afin de planifier les différentes activités à réaliser, par l'application d'une méthode de gestion de projet
 - Piloter le plan de gestion de projet, afin de l'adapter aux évolutions, par l'application de processus de gestion des changements, de monitoring et de reporting
 - Piloter une démarche de conduite du changement, en vue d'optimiser la démarche de sécurité de l'information et de lever les freins humains, par l'application d'une méthode de type Kotter et les modèles de communication de type PCM, PNL et analyse transactionnel
 - Communiquer avec la direction générale et le conseil d'administration, afin de les impliquer dans la démarche de sécurité de l'information, par la compréhension de leurs enjeux et la présentation de rapports en sécurité de l'information adaptés à leurs fonctions
 - Aligner la culture de cybersécurité sur la stratégie de l'entreprise, afin de concevoir la meilleure feuille de route, par l'utilisation des frameworks et outils les plus appropriés et pertinents
 - Motiver les équipes, afin d'atteindre les objectifs de sécurité de l'information, par l'acquisition de connaissances et de compétences en leadership
 - Gérer les conflits afin de renforcer le climat de confiance des équipes et d'optimiser les talents, par l'application de techniques de leadership
 - Accompagner une personne en situation de handicap afin de faciliter son intégration dans l'équipe et dans son environnement de travail
 - Créer un plan d'actions pour le déploiement et la gestion des outils de communication digitaux en s'appuyant sur ISO 22301
 - Créer le contenu de communication accessible au grand public en concertation avec les professionnels concernés et en préservant l'e-reputation en s'appuyant sur ISO 22361 (Crisis & resilience)
- (option) Bloc de spécialisation n°1 – Concevoir et déployer un système d'information sécurisé avec une approche DevSecOps
- Faire évoluer le système d'information afin de répondre aux attentes du métier en termes de sécurité, par une démarche de cartographie et d'urbanisation du système d'information
 - Concevoir une roadmap de transformation dans l'entreprise afin de répondre aux exigences de sécurité de l'information, par l'application des méthodes de modélisation et de simulation
 - Concevoir et déployer une architecture technique sécurisée, afin de renforcer la sécurité lors de la conception et la maintenance des composants d'un système d'information par l'application des meilleures pratiques dans ce domaine
 - Appliquer un référentiel Devops, afin de pouvoir immédiatement travailler avec les professionnels du marché, par l'application de cette méthodologie à une étude de cas
 - Concevoir et déployer une architecture logicielle sécurisée, afin de renforcer la sécurité lors de la conception et la maintenance des composants d'une application et de ses composants par l'apprentissage et l'application des meilleures pratiques dans ce domaine
 - Gérer un projet de développement sécurisé pour minimiser attaques sur les logiciels en fonctionnement afin de garantir la sécurité des programmes et des systèmes d'information
 - Appliquer les meilleures pratiques de DevSecOps par des cycles de développement rapides et fréquents en

intégrant la sécurité du code dès la conception des applications

(option) Bloc de spécialisation n°2 – Préparer un audit de certification en sécurité et continuité de l'information

- Préparer un plan de test (les preuves d'audit à analyser), un plan d'audit et des entretiens pour effectuer un audit de certification en s'appuyant sur ISO 19011
- Effectuer des revues de preuves d'audit pour déterminer la conformité de l'organisation en s'appuyant ISO 19011
- Évaluer la performance des mesures de sécurité en place, afin d'optimiser la sécurité du système d'information en s'appuyant sur le NIST SP 800 53
- Rédiger un rapport d'audit, pour déterminer le plan d'action afin de renforcer la sécurité du système d'information, par l'application d'une méthodologie d'audit comme ISO 19 011
- Proposer un ensemble de mesures de sécurité, afin de renforcer la sécurité des systèmes d'information, en s'inspirant d'une démarche de type Cycle de Deming
- Préparer l'entreprise à une certification en sécurité de l'information, en vue de rassurer les clients et les partenaires, par une démarche d'accréditation à partir d'une norme de certification
- Préparer un plan de test (les preuves d'audit à analyser), un plan d'audit et des entretiens pour effectuer un audit en résilience, continuité, gestion de crise et plan de secours en s'appuyant sur ISO 19011
- Auditer la maturité d'une organisation en termes de continuité et de résilience de l'information pour déterminer les vulnérabilités du système d'information, par l'application d'un ensemble de critères d'audit comme 22301.
- Effectuer des revues de preuves d'audit (orale & entretiens, documentaire, d'observation, technique, statistique) pour déterminer la conformité de l'organisation en s'appuyant sur ISO 19011.
- Évaluer la performance des mesures de sécurité en place, afin d'optimiser la sécurité du système d'information en s'appuyant sur le NIST SP 800 53
- Rédiger un rapport d'audit, pour déterminer le plan d'action afin de renforcer la sécurité du système d'information, par l'application d'une méthodologie d'audit comme ISO 19 011
- Proposer un ensemble de mesures de sécurité, afin de renforcer la sécurité des systèmes d'information, en s'inspirant d'une démarche de type Cycle de Deming
- Préparer l'entreprise à une certification en sécurité de l'information, en vue de rassurer les clients et les partenaires, par une démarche d'accréditation à partir d'une norme de certification
- Mettre en place une gouvernance de la sécurité des systèmes d'information, afin de déployer une démarche cohérente au niveau stratégique, tactique et opérationnel, par le déploiement de meilleures pratiques comme Cobit
- Évaluer la conformité légale et réglementaires de l'organisation par rapport aux exigences légales et réglementaires en termes de sécurité de l'information et de protection des données personnelles (RGPD), afin d'éviter toute non-conformité et sanctions financières en résultant

(option) Bloc de spécialisation n°3 – Détecter et traiter les incidents techniques à l'aide de l'intelligence artificielle

- Appliquer les meilleurs pratiques de réponse aux incidents, pour pouvoir intégrer une équipe de SOC (Security Operation Center) ou un CERT (Computer Emergency Response Team) et gérer tout incident de sécurité de l'information (y compris les fuites de données ou DLP Data Leakage Prevention), en appliquant des normes comme ISO 27 035 (gestion des incidents) ou de réponse à gestion de crise
- Utiliser un outil de SIEM (Security Incident & Event Management) du marché, pour repérer une fuite de données, afin de prévenir celle-ci et d'en limiter les conséquences
- Utiliser un outil de type Splunk pour effectuer des corrélations statistiques et des index de données agrégées, pour repérer une série d'incidents de sécurité, ou une fuite de donnée, afin d'y remédier au plus vite
- Créer des règles pour examiner de façon précise les infractions de sécurité, et utiliser le langage AQL (Ariel Query Language) pour des recherches avancées, pour des analyses de sécurité plus poussées afin d'anticiper les risques de cybersécurité
- Présenter un rapport de suivi de la sécurité de l'information à une équipe technique et à la direction, pour informer en temps réel du suivi de la sécurité, de mesures mises en place et des risques

Blocs de compétences

RNCP36122BC01 — Identifier les solutions techniques de sécurité d'un SI face à la menace

LISTE DE COMPÉTENCES

- Renforcer la sécurité des 5 composants d'un ordinateur en vue de protéger le système matériel par une analyse de leur périmètre et de leur rôle, ainsi que des risques associés

- Renforcer la sécurité des systèmes d'exploitation, la terminologie et les fonctions de la virtualisation et des containers, en vue de protéger la sécurité des composants logiques d'un système d'information, par une analyse de leur périmètre et de leur rôle, ainsi que des risques associés.
- Renforcer la sécurité des 7 couches du modèle OSI de description des réseaux, en déterminant les risques associés à chacune des couches, par la reconnaissance des différents types d'attaque sur chacune des couches du modèle OSI
- Appliquer aux réseaux TCP/IP les principes de la démarche de protection des 7 couches du modèle OSI
- Cartographier les données personnelles déterminer leur criticité et leur valeur selon les exigences du RGPD et d'ISO 27701
- Appliquer à la sécurité des données les mesures techniques de protection adéquates en fonction de leur valeur : chiffrement symétrique et asymétrique, anonymisation, pseudonymisation
- Identifier les systèmes embarqués, les PLC (Programmable Logic Controller) et les RTU (Remote Terminal Unit), identifier les protocoles sous-jacents et les systèmes de supervision, pour déterminer leurs vulnérabilités et appliquer les mesures de sécurité techniques pour renforcer la sécurité des systèmes embarqués
- Suivre les flux d'information en cybersécurité pour être informé des dernières menaces et des solutions à déployer par la mise en place d'un système de veille en cyber sécurité

MODALITÉS D'ÉVALUATION

Etude de cas : Renforcer la sécurité technique d'un SI.

RNCP36122BC02 — Opérer et surveiller les mesures de sécurité d'un SI

LISTE DE COMPÉTENCES

- Déployer un système de monitoring de l'activité en sécurité de l'information pour repérer les événements et les incidents de sécurité, afin de les traiter
- Concevoir un processus et un flux de traitement des événements et des incidents en s'appuyant sur la norme ISO 27035, pour automatiser le traitement des événements et des incidents
- Mener une enquête technico légale (Forensic) en s'appuyant sur la norme ISO27037, afin d'identifier la cause des incidents de cyber sécurité et d'y apporter des solutions
- Réaliser un test d'intrusion selon les standards du marché (planification, reconnaissance, test de vulnérabilité, exploitation, effacement des traces, rapport) pour identifier les vulnérabilités d'un système d'information et ainsi renforcer sa sécurité

MODALITÉS D'ÉVALUATION

Etude d'un cas : Suite à une série d'incidents de sécurité significatifs, une entreprise décide dans un premier temps de réaliser une enquête technico légale pour comprendre l'origine des incidents, puis de réaliser un pentest pour tester la vulnérabilité du système d'information, et enfin d'automatiser le monitoring et le traitement des incidents de sécurité

RNCP36122BC03 — Auditer la maturité de la cybersécurité d'un système d'information

LISTE DE COMPÉTENCES

- Déployer un SMSI pour apporter un cadre de gouvernance et de gestion de la sécurité d'un système d'information en s'appuyant sur les meilleures pratiques d'ISO
- Evaluer la maturité du SMSI pour renforcer la sécurité du système d'information en s'appuyant sur la norme ISO 15504
- Réaliser une analyse de risque pour identifier les vulnérabilités et menaces potentielles en sécurité du système d'information et s'appuyant sur ISO 27005 et Ebios
- Proposer des mesures de traitement pour renforcer la sécurité du système d'information en s'appuyant sur l'analyse de risques, ainsi que les meilleures pratiques de l'OWASP, du MITRE
- Analyser l'efficacité et l'efficience des mesures de sécurité mises en place par l'organisation, pour identifier les plus faibles et les moins pertinentes, afin de renforcer la sécurité du système d'information
- Préparer un plan de projet comprenant l'ensemble des mesures de sécurité manquantes ou à renforcer, sur à l'audit de maturité, pour renforcer la sécurité du système d'information

MODALITÉS D'ÉVALUATION

Etude de cas : Auditer la sécurité organisationnelle d'une entreprise et déployer une démarche de gouvernance de la sécurité

RNCP36122BC04 — Piloter un projet et communiquer en cybersécurité

LISTE DE COMPÉTENCES

- Concevoir un projet de cybersécurité, afin de planifier les différentes activités à réaliser, par l'application d'une méthode de gestion de projet
- Piloter le plan de gestion de projet, afin de l'adapter aux évolutions, par l'application de processus de gestion des changements, de monitoring et de reporting
- Piloter une démarche de conduite du changement, en vue d'optimiser la démarche de sécurité de l'information et de lever les freins humains, par l'application d'une méthode de type Kotter et les modèles de communication de type PCM, PNL et analyse transactionnel
- Communiquer avec la direction générale et le conseil d'administration, afin de les impliquer dans la démarche de sécurité de l'information, par la compréhension de leurs enjeux et la présentation de rapports en sécurité de l'information adaptés à leurs fonctions
- Aligner la culture de cybersécurité sur la stratégie de l'entreprise, afin de concevoir la meilleure feuille de route, par l'utilisation des frameworks et outils les plus appropriés et pertinents
- Motiver les équipes, afin d'atteindre les objectifs de sécurité de l'information, par l'acquisition de connaissances et de compétences en leadership
- Gérer les conflits afin de renforcer le climat de confiance des équipes et d'optimiser les talents, par l'application de techniques de leadership
- Accompagner une personne en situation de handicap afin de faciliter son intégration dans l'équipe et dans son environnement de travail
- Créer un plan d'actions pour le déploiement et la gestion des outils de communication digitaux en s'appuyant sur ISO 22301
- Créer le contenu de communication accessible au grand public en concertation avec les professionnels concernés et en préservant l'e-réputation en s'appuyant sur ISO 22361 (Crisis & Resilience)

MODALITÉS D'ÉVALUATION

Le candidat est mis en situation réelle ou simulée et prend part à des jeux de rôle. Il doit mettre en place une politique de sécurité au sein d'une organisation donnée, gérer des conflits au sein d'une équipe, proposer un plan de sensibilisation de l'ensemble du personnel, et un plan de communication de crise (une proposition spécifique est formulée pour faciliter la prise en compte d'une personne en situation de handicap)

RNCP36122BC05 — Spécialisation (option): Concevoir et déployer un système d'information sécurisé avec une approche DevSecOps

LISTE DE COMPÉTENCES

- Faire évoluer le système d'information afin de répondre aux attentes du métier en termes de sécurité, par une démarche de cartographie et d'urbanisation du système d'information
- Concevoir une roadmap de transformation dans l'entreprise afin de répondre aux exigences de sécurité de l'information, par l'application des méthodes de modélisation et de simulation
- Concevoir et déployer une architecture technique sécurisée, afin de renforcer la sécurité lors de la conception et la maintenance des composants d'un système d'information par l'application des meilleures pratiques dans ce domaine
- Appliquer un référentiel Devops, afin de pouvoir immédiatement travailler avec les professionnels du marché, par l'application de cette méthodologie à une étude de cas
- Concevoir et déployer une architecture logicielle sécurisée, afin de renforcer la sécurité lors de la conception et la maintenance des composants d'une application et de ses composants par l'apprentissage et l'application des meilleures pratiques dans ce domaine
- Gérer un projet de développement sécurisé pour minimiser attaques sur les logiciels en fonctionnement afin de garantir la sécurité des programmes et des systèmes d'information
- Appliquer les meilleures pratiques de DevSecOps par des cycles de développement rapides et fréquents en intégrant la sécurité du code dès la conception des applications

MODALITÉS D'ÉVALUATION

Etude de cas : Concevoir un système d'information sécurisé. L'étude de cas porte sur une organisation qui décide de migrer l'ensemble de son système d'information vers une solution externalisée de cloud computing.

RNCP36122BC06 — Spécialisation (option): Préparer un audit de certification en sécurité et continuité de l'information

LISTE DE COMPÉTENCES

- Préparer un plan de test (les preuves d'audit à analyser), un plan d'audit et des entretiens pour effectuer un audit de certification en s'appuyant sur ISO 19011
- Effectuer des revues de preuves d'audit pour déterminer la conformité de l'organisation en s'appuyant ISO 19011
- Évaluer la performance des mesures de sécurité en place, afin d'optimiser la sécurité du système d'information en s'appuyant sur le NIST SP 800 53
- Rédiger un rapport d'audit, pour déterminer le plan d'action afin de renforcer la sécurité du système d'information, par l'application d'une méthodologie d'audit comme ISO 19 011
- Proposer un ensemble de mesures de sécurité, afin de renforcer la sécurité des systèmes d'information, en s'inspirant d'une démarche de type Cycle de Deming
- Préparer l'entreprise à une certification en sécurité de l'information, en vue de rassurer les clients et les partenaires, par une démarche d'accréditation à partir d'une norme de certification
- Préparer un plan de test (les preuves d'audit à analyser), un plan d'audit et des entretiens pour effectuer un audit en résilience, continuité, gestion de crise et plan de secours en s'appuyant sur ISO 19011
- Auditer la maturité d'une organisation en termes de continuité et de résilience de l'information pour déterminer les vulnérabilités du système d'information, par l'application d'un ensemble de critères d'audit comme 22301.
- Effectuer des revues de preuves d'audit (orale & entretiens, documentaire, d'observation, technique, statistique) pour déterminer la conformité de l'organisation en s'appuyant sur ISO 19011.
- Évaluer la performance des mesures de sécurité en place, afin d'optimiser la sécurité du système d'information en s'appuyant sur le NIST SP 800 53
- Rédiger un rapport d'audit, pour déterminer le plan d'action afin de renforcer la sécurité du système d'information, par l'application d'une méthodologie d'audit comme ISO 19 011
- Proposer un ensemble de mesures de sécurité, afin de renforcer la sécurité des systèmes d'information, en s'inspirant d'une démarche de type Cycle de Deming
- Préparer l'entreprise à une certification en sécurité de l'information, en vue de rassurer les clients et les partenaires, par une démarche d'accréditation à partir d'une norme de certification
- Mettre en place une gouvernance de la sécurité des systèmes d'information, afin de déployer une démarche cohérente au niveau stratégique, tactique et opérationnel, par le déploiement de meilleures pratiques comme Cobit
- Évaluer la conformité légale et réglementaires de l'organisation par rapport aux exigences légales et réglementaires en termes de sécurité de l'information et de protection des données personnelles (RGPD), afin d'éviter toute non-conformité et sanctions financières en résultant

MODALITÉS D'ÉVALUATION

Etude de cas : Le candidat sera évalué sur sa capacité à mener un audit de maturité en sécurité de l'information. L'étude de cas porte sur une véritable entreprise anonymisée, qui souhaite se faire certifier ISO 27001 en sécurité de l'information.

RNCP36122BC07 — Spécialisation (option): Détecter et traiter les incidents techniques à l'aide de l'intelligence artificielle

LISTE DE COMPÉTENCES

- Appliquer les meilleurs pratiques de réponse aux incidents, pour pouvoir intégrer une équipe de SOC (Security Operation Center) ou un CERT (Computer Emergency Response Team) et gérer tout incident de sécurité de l'information (y compris les fuites de données ou DLP Data Leakage Prevention), en appliquant des normes comme ISO 27 035 (gestion des incidents) ou de réponse à gestion de crise
- Utiliser un outil de SIEM (Security Incident & Event Management) du marché, pour repérer une fuite de données, afin de prévenir celle-ci et d'en limiter les conséquences
- Utiliser un outil de type Splunk pour effectuer des corrélations statistiques et des index de données agrégées, pour repérer une série d'incidents de sécurité, ou une fuite de donnée, afin d'y remédier au plus vite
- Créer des règles pour examiner de façon précise les infractions de sécurité, et utiliser le langage AQL (Ariel Query Language) pour des recherches avancées, pour des analyses de sécurité plus poussées afin d'anticiper les risques de cybersécurité
- Présenter un rapport de suivi de la sécurité de l'information à une équipe technique et à la direction, pour informer

en temps réel du suivi de la sécurité, de mesures mises en place et des risques

MODALITÉS D'ÉVALUATION

Le candidat est mis en situation réelle. Il dispose de 72 heures pour traiter une série d'incidents de sécurité est une fuite de données.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

La certification permet de travailler dans de nombreux secteurs d'activités, la cybersécurité étant omniprésente. Il est possible de catégoriser les métiers visés en 3 groupes d'activités:

- Les métiers de la conception de la sécurité:
Au sein de la DSI d'une entreprise ou d'un éditeur de logiciel de sécurité, ces métiers consistent à développer des services ou produits sécurisés ou ayant vocation à sécuriser une organisation
- Les métiers du maintien de la sécurité opérationnelle
Au sein de la DSI ou de prestataire de service en sécurité opérationnelle, ces métiers consistent à maintenir la sécurité d'une organisation et gérer les incidents le cas échéant
- Les métiers du conseil et de l'intégration: Au sein de cabinets indépendants, ces métiers consistent à renforcer la sécurité d'une organisation cliente.

TYPE D'EMPLOIS ACCESSIBLES

Une large multiplicité de métiers existent au sein de la cybersécurité. La certification propose 3 spécialisations métiers afin de couvrir l'ensemble des métiers exerçables.

La spécialisation développement: adresse les métiers de la conception de la sécurité

1. Développeur de produits de sécurité
2. DevSecOps
3. Intégrateur de solutions de sécurité
4. Architecte SSI

La spécialisation Sécurité Opérationnelle & Ethical Hacking: adresse les métiers du maintien de la sécurité et de la gestion des crises

1. Pentester
2. Analyste SOC
3. Analyste en gestion des incidents
4. Analyste CERT/SIEM
5. Administrateur de systèmes sécurisés

Enfin la spécialisation Conseil & Gouvernance: adresse les métiers du conseil et de la gouvernance de la cybersécurité

1. Consultant en cybersécurité
2. Chef de projet en cybersécurité
3. Responsable de la sécurité SI

RÈGLEMENTATIONS D'ACTIVITÉ

Les professionnels de la cybersécurité visés par la certification seront sensibles aux lois et réglementations en vigueur, au niveau français et européen, mais également aux normes, référentiels, et recommandations délivrés par les organes compétents (l'ANSSI, la CNIL, 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

Etre titulaire d'un titre de niveau 5 ou 6 ou encore justifier d'une expérience professionnelle en Informatique

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

- 2 responsables pédagogiques du centre de formation (Directeur pédagogique et enseignant en charge d'un module lié au bloc de compétence évalué)
- 2 professionnels exerçant en entreprise, externes au centre de formation

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	9 000 €
Selon la branche	7 697 € – 9 157 €
Prise en charge	Branches concernées
9 000 €	Valeur par défaut · 186 branches
9 157 €	CPNE Casinos, CPNE autoroutes, CPNE de l'ingénierie, des services informatiques et du conseil, CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique, CPNE des Télécoms
8 696 €	CPNE FP Commerce de Détail de l'Horlogerie Bijouterie, CPNEFP Commerce succursaliste de la Chaussure, CPNEFP Commerce à distance, CPNEFP Grands Magasins/ Magasins Populaires, CPNEFP Import-Export
9 005 €	CPNE FP Branche des magasins du Bricolage

8 813 €	CPNEFP Professions de la Photographie
8 775 €	CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
8 711 €	CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
8 600 €	CPNEFP de l'habillement, mercerie, chaussure et jouet
8 519 €	CPNE Industrie pétrolière
8 500 €	CPNEFP de la métallurgie
7 697 €	CPNEFP de la blanchisserie, laverie, location de linge, nettoyage à sec, pressing et teinturerie

Base légale

Date de décision	26/01/2022
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	26/01/2025

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)
RNCP39999

Pour plus d'informations

LIEN VERS LE DESCRIPTIF
www.oteria.fr

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/36122/>