

Gestionnaire de la sécurité des données, des réseaux et des systèmes

RNCP37346 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Code(s) NSF	326
Formacode(s)	31006
Code(s) ROME	M1802, M1801, M1806
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	17/02/2023
Date d'échéance	17/02/2026

Certificateur(s)

B2H 83 LA VALETTE · SIRET : 81839222700026

Partenaires habilités

6 organismes habilités, d'après la liste publiée par France compétences : 5 à former et organiser l'évaluation et 1 à former.

Organisme	SIRET	Habilitation
ASSOCIATION ECOLE TECHNIQUE PRIVEE HERMES	40977134200048	Former et organiser l'évaluation
B2H 13 AIX	81946418100018	Former et organiser l'évaluation
B2H13 MARSEILLE	81839227600015	Former et organiser l'évaluation
B2H83 FREJUS	85151781300016	Former et organiser l'évaluation
B2H 83 LA VALETTE	81839222700018	Former et organiser l'évaluation
INSTITUT DU MARAIS - CHARLEMAGNE - POLLES	52840171400019	Former

Résumé de la certification

OBJECTIFS ET CONTEXTE

La société dans laquelle nous vivons, à l'ère du numérique, est envahie de datas, de réseaux et de systèmes informatiques. Dans ce contexte mondial ultra-connecté, l'ensemble des technologies de l'information et des communications constitue un des vecteurs majeurs de la croissance économique. Cette utilisation accrue des systèmes complexes des technologies numériques par les citoyens et toutes formes d'organisations à travers des produits, des services et des dispositifs connectés, augmente drastiquement les risques liés à la cybersécurité.

Selon l'Insee, un tiers des grandes sociétés a vécu un incident de sécurité informatique en 2018. Nadège Pradines (division enquêtes thématiques et études transversales, Insee) précise que « 16 % des sociétés de 10 personnes ou plus implantées en France déclarent avoir vécu un incident de sécurité informatique en 2018. Les sociétés de 250 personnes ou plus sont deux fois plus touchées. » Majoritairement, ces cyber-attaques rendent indisponible les services informatiques des sociétés, détruisent ou altèrent les données et divulguent des datas confidentielles.

La récente étude McAfee révèle que le coût de la cybercriminalité représente un billion de dollars pour l'économie mondiale en 2020 contre 600 milliards en 2018 soit une augmentation de presque 50% en deux ans. Les attaques informatiques sont désormais susceptibles de porter gravement atteinte à notre économie, aux intérêts de notre

défense et de notre sécurité nationale mais il existe des coûts cachés, plus délicats à chiffrer, pour les organisations : « Cybercrime has many hidden costs—from opportunity costs, time and money spent on cybersecurity decision-making, the effect of downtime, loss of productivity, and damage to brand and image ».

Dans ce contexte de menace croissante, la sécurisation des données, des réseaux et des systèmes informatiques devient une priorité stratégique pour les entreprises. Pour faire face à la hausse du risque cyber, un des défis et des enjeux à venir pour les professionnels de la cybersécurité est notamment de résoudre l'équation des ressources humaines : recruter, former et fidéliser afin d'assurer le développement de l'activité. En France, comme à l'international, le secteur est confronté à une pénurie constante de compétences. Selon l'étude du cabinet de conseil Wavestone « plus de 15 000 postes sont disponibles mais non couverts » sur le territoire. Les besoins en main d'œuvre qualifiée se font de plus en plus ressentir.

De ce fait, afin de répondre à la forte demande de ce marché en pénurie de compétences, la certification est structurée autour de l'exercice d'activités et de compétences réparties entre les quatre blocs de compétences suivants :

- Cartographier les systèmes d'information.
- Sécuriser les données, les réseaux et les systèmes.
- Gérer le risque numérique.
- Diffuser des informations relatives à la sécurité des données, des réseaux et des systèmes.

ACTIVITÉS VISÉES

Dans le cadre de sa fonction, le Gestionnaire de la sécurité des données, des réseaux et des systèmes a pour principales activités :

- Identification des risques de sécurité des systèmes d'information :
 - o Réalisation de l'inventaire des systèmes d'information
 - o Elaboration des vues cartographiques
 - o Anticipation des risques de traitement.
- Contrôle des accès aux systèmes d'information :
 - o Authentification des utilisateurs,
 - o Contrôle des habilitations,
 - o Qualification des accès critiques.
- Amélioration continue du processus de cartographie des systèmes d'information :
 - o Actualisation régulière et structurée de la cartographie,
 - o Respect du cadre juridique et légal.
 - o Organisation de la veille.
- Protection des données, des réseaux et des systèmes :
 - o Homologation de sécurité,
 - o Gestion de la sécurité des postes de travail,
 - o Protection des locaux,
 - o Fiabilisation de l'administration,
 - o Sécurisation des serveurs et réseaux internes,
 - o Protection des réseaux externes,
 - o Sauvegarde et archivage de manière sécurisé.
- Maintien en condition de sécurité les données, les réseaux et les systèmes :
 - o Mise en œuvre d'une procédure de maintien en condition de sécurité des ressources matérielles et logicielles des systèmes d'information,
 - o Amélioration continue.
- Participation à la définition de la stratégie de sécurité des données, des réseaux et des systèmes :
 - o Collaboration à l'élaboration stratégique,
 - o Mise en œuvre de la sécurisation du système d'information.
- Management du risque numérique au sein de l'organisation :
 - o Gestion des accès aux locaux,
 - o Fiabilisation des actions de maintenance,
 - o Sécurisation des développements informatiques,
 - o Supervision des journaux,
 - o Contrôle des actions de sous-traitance,
 - o Evaluation des dispositifs de sécurité.

- Traitement de cyberattaques :
 - o Gestion de cybercrise,
 - o Investigation,
 - o Remédiation,
 - o Stabilisation.
- Information, formation et assistance :
 - o Diffusion de la politique de protection du système d'information,
 - o Conseil et accompagnement,
 - o Sensibilisation et formation.
- o Communication d'alertes : Transmission d'informations à la Direction,
- o Information et conseil auprès des parties prenantes.

COMPÉTENCES ATTESTÉES

Les compétences attestées sont au nombre de 32. Elles sont structurées au sein de 4 blocs de compétences.

Bloc 1 – Cartographier les systèmes d'information :

- Définir les objectifs et les enjeux du projet de cartographie pour répondre aux besoins opérationnels de sécurité numérique de l'organisation.
- Réaliser un listing exhaustif des composantes du système d'information incluant notamment l'écosystème qui gravite autour du SI, les processus métiers de l'organisme avec les acteurs qui y participent, les périmètres et les niveaux de privilèges des utilisateurs/administrateurs, les logiciels et les équipements physiques utilisés, pour appréhender les risques potentiellement encourus par les systèmes d'information.
- Réaliser une revue des droits d'accès pour identifier les accès obsolètes, incomplets ou non autorisés.
- Déterminer par degré de criticité les accès sensibles, cibles privilégiées par les cyberattaquants, de sorte à prioriser les actions en matière de gestion des risques et de s'assurer que les accès aux éléments sensibles soient maîtrisés.
- Evaluer les risques engendrés par chaque traitement pour mesurer l'impact relatif que pourraient avoir ces menaces sur l'organisation.
- Elaborer la cartographie des systèmes d'information dans une démarche d'amélioration continue, à la fois incrémentale (enrichissement par de nouvelles vues) et itérative (affinement des vues déjà constituées), pour identifier les systèmes les plus critiques et les plus exposés, anticiper les chemins d'attaque possibles sur ces systèmes et mettre en place des mesures adéquates pour assurer leur protection, réagir plus efficacement en cas d'incident, identifier les activités clés de l'organisme afin de définir un plan de continuité d'activité.
- Maintenir la cartographie à jour pour garantir une synchronisation entre les évolutions du système d'information et leur représentation dans l'inventaire et les vues tout en veillant à la bonne conformité de l'organisation avec les nouvelles exigences en matière de sécurité numérique.
- Mettre en œuvre les exigences réglementaires relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, aux mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union Européenne, pour inscrire la sécurisation des données, des réseaux et des systèmes de l'entreprise dans le cadre légal et juridique.
- Utiliser les outils de veille cybersécurité, juridique, technique, concurrentielle, stratégique et mobiliser les ressources expertes (ANSSI) pour maintenir à l'état de l'art sa connaissance relative à la sécurité des systèmes d'information.

Bloc 2 – Sécuriser les données, les réseaux et les systèmes :

- Mesurer le niveau de maîtrise des risques atteint en prenant en compte la sécurité numérique des services proposés afin d'adapter le niveau de risque résiduel accepté à un contexte donné.
- Déployer le niveau de sécurité, défini par la Direction, sur l'ensemble du parc informatique et des locaux techniques de l'entreprise afin d'homogénéiser les politiques de sécurité s'appliquant à l'ensemble du parc pour sécuriser le système d'information.
- Mettre en œuvre les mesures techniques (configuration de matériels et de logiciels, installation de micro-codes, de systèmes d'exploitation...) sur le système d'information d'administration et son écosystème pour protéger le SI d'administration de toutes tentatives d'intrusions et compromissions.
- Cloisonner le système d'information par la mise en place de dispositifs de filtrage entre les différentes zones réseaux plus ou moins critiques pour minimiser la propagation d'informations infectieuses sur l'ensemble des systèmes de l'entreprise.
- Contrôler les accès internet par la mise en place d'une passerelle internet sécurisée permettant de bloquer les flux illégitimes avec des relais applicatifs incontournables implémentant des fonctions de sécurité pour réduire les risques

de sécurité.

- Appliquer une politique de sauvegarde des composants critiques (liste des données jugées vitales pour l'organisme et les serveurs concernés, différents types de sauvegarde, fréquence des sauvegardes, procédure d'administration et d'exécution des sauvegardes, informations de stockage et restrictions d'accès aux sauvegardes, procédures de test de restauration, destruction des supports ayant contenu les sauvegardes) pour poursuivre l'activité en cas d'incident.
- Maintenir le niveau de sécurité des systèmes d'information tout au long de leur cycle de vie, conformément à la politique de sécurité des réseaux et systèmes d'information de l'organisation, en raccourcissant le délai entre la publication d'une vulnérabilité et la mise en œuvre de mesures techniques ou organisationnelles pour la contrer.
- Mettre en œuvre un plan d'amélioration continue de la sécurité pour garantir la montée en puissance et en maturité de la sécurité de l'entreprise et permettre une gestion dynamique des risques résiduels selon leur criticité.

Bloc 3 – Gérer le risque numérique :

- Contribuer à la définition du modèle de gouvernance de la politique de sécurité du système d'information afin que la Direction puisse élaborer la stratégie de protection des données, des réseaux et des systèmes.
- Déployer la stratégie de sécurité numérique de l'entreprise, préalablement définie par la Direction, dans le respect du cadre juridique et réglementaire, pour protéger le système d'information contre une large gamme de menaces.
- Contrôler l'accès aux salles serveurs et aux locaux techniques afin de s'assurer que les mécanismes de sécurité physique ne puissent pas être contournés aisément par un attaquant.
- Gérer la maintenance des données en garantissant la sécurité de ces dernières, à tout moment du cycle de vie des matériels et des logiciels, pour maîtriser l'accès aux données.
- Encadrer les développements informatiques pour s'assurer et attester que le développement est effectué conformément aux exigences réglementaires et sécuritaires de l'organisation.
- Mettre en place une supervision des incidents de sécurité informatique par une politique de journalisation sur les différentes ressources du système d'information afin de détecter une éventuelle compromission.
- Gérer la sous-traitance en prenant et documentant les moyens (contrôle de sécurité, visite des installations...), tout en tenant compte des situations de handicap le cas échéant, pour s'assurer l'effectivité des garanties offertes par le sous-traitant.
- Déployer la stratégie de réponse aux cyberattaques associée au dispositif de gestion de crise, définie par anticipation par la Direction, en s'appuyant sur le contexte dans lequel s'inscrit l'attaque pour manager l'impact de cette dernière sur l'organisation et assurer la continuité d'activité puis son retour à un état normal.
- Collecter et analyser les éléments techniques permettant de comprendre le chemin d'attaque utilisé par les cyberattaquants et les actions de ces derniers sur les systèmes infectés, restaurer les systèmes dans leur état initial en éjectant l'attaquant du système et améliorer la sécurité pour éviter une attaque similaire par l'application de mesures d'assainissement, améliorer la sécurité à plus long terme par la définition et l'application de mesures de sécurisation et l'amélioration de la supervision, afin de faire cesser les effets de la cyberattaque et éjecter l'attaquant en dehors des systèmes d'information infectés.
- Procéder à des contrôles des dispositifs de sécurité en évaluant concrètement l'efficacité des mesures mises en œuvre et leur maintien dans le temps pour assurer la protection des données, des systèmes et des réseaux de l'entreprise.

Bloc 4 – Diffuser des informations relatives à la sécurité des données, des réseaux et des systèmes :

- Mener des actions de communication et de sensibilisation, en collaboration avec les éventuels services de l'organisation en charge de la communication et en tenant compte des situations de handicap le cas échéant, permettant au personnel de l'entreprise de développer une culture de protection des données en prenant appui sur les recommandations des autorités nationales (ANSSI, CNIL...).
- Dispenser des conseils et assister les acteurs de l'entreprise sur les problématiques relatives à la protection des données, des réseaux et des systèmes, en adaptant sa posture aux besoins des personnes ayant un handicap, pour éviter toute sortie du cadre juridique et réglementaire tout en les invitant à signaler au service informatique de l'organisation des éléments suspects pour lutter contre la cybermenace.
- Mettre en œuvre des programmes de formation du personnel, pouvant être suivi par tout public quel que soit son handicap, pour sensibiliser aux bonnes pratiques de sécurité numérique, faire naître ou renforcer certains réflexes, renforcer la responsabilité et la transparence de chacun.
- Informer la Direction d'un risque de compromission du système d'information et rédiger un rapport d'analyse associé afin de leur permettre d'appréhender les menaces pesantes sur l'environnement et de prendre les décisions adéquates.
- Alerter les parties prenantes (clients, fournisseurs, médias, autorités, etc.), en adaptant si nécessaire sa communication à un public

ayant un handicap, d'un comportement inhabituel de la part d'un poste de travail ou d'un serveur, synonyme d'une potentielle intrusion, en spécifiant l'état de la compréhension de la menace, les hypothèses d'évolution de cette dernière et en préconisant des actions simples à mener dans l'attente de la réalisation d'opérations techniques pour limiter ou stopper la cybermenace.

Blocs de compétences

RNCP37346BC01 — Cartographier les systèmes d'information

LISTE DE COMPÉTENCES

Définir les objectifs et les enjeux du projet de cartographie pour répondre aux besoins opérationnels de sécurité numérique de l'organisation.

Réaliser un listing exhaustif des composantes du système d'information incluant notamment l'écosystème qui gravite autour du SI, les processus métiers de l'organisme avec les acteurs qui y participent, les périmètres et les niveaux de privilèges des utilisateurs/administrateurs, les logiciels et les équipements physiques utilisés, pour appréhender les risques potentiellement encourus par les systèmes d'information.

Réaliser une revue des droits d'accès pour identifier les accès obsolètes, incomplets ou non autorisés.

Déterminer par degré de criticité les accès sensibles, cibles privilégiées par les cyberattaquants, de sorte à prioriser les actions en matière de gestion des risques et de s'assurer que les accès aux éléments sensibles soient maîtrisés.

Evaluer les risques engendrés par chaque traitement pour mesurer l'impact relatif que pourraient avoir ces menaces sur l'organisation.

Elaborer la cartographie des systèmes d'information dans une démarche d'amélioration continue, à la fois incrémentale (enrichissement par de nouvelles vues) et itérative (affinement des vues déjà constituées), pour identifier les systèmes les plus critiques et les plus exposés, anticiper les chemins d'attaque possibles sur ces systèmes et mettre en place des mesures adéquates pour assurer leur protection, réagir plus efficacement en cas d'incident, identifier les activités clés de l'organisme afin de définir un plan de continuité d'activité.

Maintenir la cartographie à jour pour garantir une synchronisation entre les évolutions du système d'information et leur représentation dans l'inventaire et les vues tout en veillant à la bonne conformité de l'organisation avec les nouvelles exigences en matière de sécurité numérique.

Mettre en œuvre les exigences réglementaires relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, aux mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union Européenne, pour inscrire la sécurisation des données, des réseaux et des systèmes de l'entreprise dans le cadre légal et juridique.

Utiliser les outils de veille cybersécuritaire, juridique, technique, concurrentielle, stratégique et mobiliser les ressources expertes (ANSSI) pour maintenir à l'état de l'art sa connaissance relative à la sécurité des systèmes d'information.

MODALITÉS D'ÉVALUATION

Etude de cas réel d'entreprise. Cartographie des SI. Production écrite.

Le candidat a, à sa disposition, une présentation littéraire et chiffrée de l'entreprise, de ses activités, des méthodes utilisées pour sécuriser les systèmes d'information ainsi, que des comptes rendus d'entretien des salariés de l'entreprise impliqués dans les services informatiques.

Dans le respect du cadre juridique et légal relatif à la protection des systèmes d'information, le candidat doit à partir de ces informations :

1. Identifier les objectifs pour l'entreprise et analyser les besoins de sécurité,
2. Etablir une liste des ressources du système et identifier chaque partie prenante pouvant accéder à ce dernier.
3. Elaborer une cartographie du système d'information afin de recenser les vulnérabilités.
4. Identifier les scénarii de risques et leurs impacts sur l'organisation.
5. Classer par criticité les événements redoutés.
6. Définir les mesures de sécurité permettant de limiter les risques.

RNCP37346BC02 — Sécuriser les données, les réseaux et les systèmes

LISTE DE COMPÉTENCES

Mesurer le niveau de maîtrise des risques atteint en prenant en compte la sécurité numérique des services proposés afin d'adapter le niveau de risque résiduel accepté à un contexte donné.

Déployer le niveau de sécurité, défini par la Direction, sur l'ensemble du parc informatique et des locaux techniques

de l'entreprise afin d'homogénéiser les politiques de sécurité s'appliquant à l'ensemble du parc pour sécuriser le système d'information.

Mettre en œuvre les mesures techniques (configuration de matériels et de logiciels, installation de micro-codes, de systèmes d'exploitation...) sur le système d'information d'administration et son écosystème pour protéger le SI d'administration de toutes tentatives d'intrusions et compromissions.

Cloisonner le système d'information par la mise en place de dispositifs de filtrage entre les différentes zones réseaux plus ou moins critiques pour minimiser la propagation d'informations infectieuses sur l'ensemble des systèmes de l'entreprise.

Contrôler les accès internet par la mise en place d'une passerelle internet sécurisée permettant de bloquer les flux illégitimes avec des relais applicatifs incontournables implémentant des fonctions de sécurité pour réduire les risques de sécurité.

Appliquer une politique de sauvegarde des composants critiques (liste des données jugées vitales pour l'organisme et les serveurs concernés, différents types de sauvegarde, fréquence des sauvegardes, procédure d'administration et d'exécution des sauvegardes, informations de stockage et restrictions d'accès aux sauvegardes, procédures de test de restauration, destruction des supports ayant contenu les sauvegardes) pour poursuivre l'activité en cas d'incident.

Maintenir le niveau de sécurité des systèmes d'information tout au long de leur cycle de vie, conformément à la politique de sécurité des réseaux et systèmes d'information de l'organisation, en raccourcissant le délai entre la publication d'une vulnérabilité et la mise en œuvre de mesures techniques ou organisationnelles pour la contrer.

Mettre en œuvre un plan d'amélioration continue de la sécurité pour garantir la montée en puissance et en maturité de la sécurité de l'entreprise et permettre une gestion dynamique des risques résiduels selon leur criticité.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle en groupe de maximum quatre personnes. Serious Game. Production numérique / informatique.

Les équipes ont pour mission d'administrer deux machines qui hébergent des services de messagerie, des applications web et du partage de fichiers. Les serveurs ont vingt vulnérabilités (ex : un mot de passe faible, un problème de droits, etc). Chaque équipe gère un couple de machines et peut intervenir sur n'importe quelle partie du système, mais les services doivent rester accessibles, sous peine de pénalité.

Les groupes ont à disposition une cartographie répertoriant les menaces, vulnérabilités et risques potentiels.

En s'appuyant sur les différentes vues cartographiques, les équipes doivent mettre en œuvre un plan d'action pour :

- Sécuriser les postes de travail,
- Sécuriser l'administration,
- Sécuriser le serveur,
- Protéger le réseau interne,
- Protéger le réseau externe,
- Sauvegarder et archiver les composants critiques.

L'exercice est hébergé sur une plateforme, type infrastructure de virtualisation, conçue à cet effet.

RNCP37346BC03 — Gérer le risque numérique

LISTE DE COMPÉTENCES

Contribuer à la définition du modèle de gouvernance de la politique de sécurité du système d'information afin que la Direction puisse élaborer la stratégie de protection des données, des réseaux et des systèmes.

Déployer la stratégie de sécurité numérique de l'entreprise, préalablement définie par la Direction, dans le respect du cadre juridique et réglementaire, pour protéger le système d'information contre une large gamme de menaces.

Contrôler l'accès aux salles serveurs et aux locaux techniques afin de s'assurer que les mécanismes de sécurité physique ne puissent pas être contournés aisément par un attaquant.

Gérer la maintenance des données en garantissant la sécurité de ces dernières, à tout moment du cycle de vie des matériels et des logiciels, pour maîtriser l'accès aux données.

Encadrer les développements informatiques pour s'assurer et attester que le développement est effectué conformément aux exigences réglementaires et sécuritaires de l'organisation.

Mettre en place une supervision des incidents de sécurité informatique par une politique de journalisation sur les différentes ressources du système d'information afin de détecter une éventuelle compromission.

Gérer la sous-traitance en prenant et documentant les moyens (contrôle de sécurité, visite des installations...), tout en tenant compte des situations de handicap le cas échéant, pour s'assurer l'effectivité des garanties offertes par le sous-traitant.

Déployer la stratégie de réponse aux cyberattaques associée au dispositif de gestion de crise, définie par anticipation

par la Direction, en s'appuyant sur le contexte dans lequel s'inscrit l'attaque pour manager l'impact de cette dernière sur l'organisation et assurer la continuité d'activité puis son retour à un état normal.

Collecter et analyser les éléments techniques permettant de comprendre le chemin d'attaque utilisé par les cyberattaquants et les actions de ces derniers sur les systèmes infectés, restaurer les systèmes dans leur état initial en éjectant l'attaquant du système et améliorer la sécurité pour éviter une attaque similaire par l'application de mesures d'assainissement, améliorer la sécurité à plus long terme par la définition et l'application de mesures de sécurisation et l'amélioration de la supervision, afin de faire cesser les effets de la cyberattaque et éjecter l'attaquant en dehors des systèmes d'information infectés.

Procéder à des contrôles des dispositifs de sécurité en évaluant concrètement l'efficacité des mesures mises en œuvre et leur maintien dans le temps pour assurer la protection des données, des systèmes et des réseaux de l'entreprise.

MODALITÉS D'ÉVALUATION

Etude de cas réel d'entreprise. Stratégie et plan d'action. Production écrite.

Le candidat dispose d'un rapport d'analyse, sous forme de cartographie, des systèmes d'informations de l'entreprise ainsi qu'un compte rendu de réunion de la Direction précisant la stratégie de sécurité numérique de l'organisation privilégiée.

En s'appuyant sur ces deux documents, le Gestionnaire de la sécurité des données, des réseaux et des systèmes a pour mission d'apporter des préconisations à sa Direction afin de parfaire la stratégie de sécurité numérique.

Dans un second temps, il rédige un plan d'action relatif au déploiement de la stratégie de sécurisation du système d'information préalablement préconisée.

Mise en situation professionnelle en groupe de maximum quatre personnes. Cyberattaque. Production écrite et présentation orale.

Les groupes sont réunis dans une pièce. Le formateur leur fait part des événements majeurs de la cyberattaque :

- Une attaque touchant le réseau bureautique provenant d'un vecteur logiciel lié à une faille propre à un sous-traitant et d'un vecteur physique provenant des locaux de la société.
- Sa propagation sur au moins un autre site.
- La médiatisation de l'attaque.
- La publication par un groupe d'attaquants d'une partie des données exfiltrées afin de faire pression en vue du paiement d'une rançon.

Le formateur leur transmet également la stratégie de réponse aux cyberattaques définie par la Direction.

A partir de l'ensemble des éléments communiqués, les candidats analysent les données permettant de comprendre les chemins d'attaque utilisés puis mettent en œuvre des actions pour gérer la crise et assurer la continuité d'activité de l'entreprise puis son retour à l'état normal.

Les groupes exposent en suite leurs actions et justifient leurs choix auprès d'un jury composé de deux membres qui joueront les rôles de :

- Directeur Général ;
- Responsable de la sécurité des systèmes d'information.

Mise en situation professionnelle. Contrôle de sécurité. Production numérique / informatique et écrite.

Le candidat se connecte à un espace informatique, conçu spécifiquement pour cette mise en situation, où il a la visibilité sur l'ensemble des dispositifs de sécurité de l'entreprise.

Il contrôle que les règles pour assurer le maintien en conditions de sécurité sont mises en œuvre, respectées et efficaces.

Il identifie les vulnérabilités et effectue des actions de remédiation.

Dans un second temps, une fois avoir techniquement opéré, il rédige un compte rendu des actions menées à sa Direction.

RNCP37346BC04 — Diffuser des informations relatives à la sécurité des données, des réseaux et des systèmes

LISTE DE COMPÉTENCES

Mener des actions de communication et de sensibilisation, en collaboration avec les éventuels services de l'organisation en charge de la communication et en tenant compte des situations de handicap le cas échéant, permettant au personnel de l'entreprise de développer une culture de protection des données en prenant appui sur les recommandations des autorités nationales (ANSSI, CNIL...).

Dispenser des conseils et assister les acteurs de l'entreprise sur les problématiques relatives à la protection des données, des réseaux et des systèmes, en adaptant sa posture aux besoins des personnes ayant un handicap, pour

éviter toute sortie du cadre juridique et réglementaire tout en les invitant à signaler au service informatique de l'organisation des éléments suspects pour lutter contre la cybermenace.

Mettre en œuvre des programmes de formation du personnel, pouvant être suivi par tout public quel que soit son handicap, pour sensibiliser aux bonnes pratiques de sécurité numérique, faire naître ou renforcer certains réflexes, renforcer la responsabilité et la transparence de chacun.

Informar la Direction d'un risque de compromission du système d'information et rédiger un rapport d'analyse associé afin de leur permettre d'appréhender les menaces pesantes sur l'environnement et de prendre les décisions adéquates.

Alerter les parties prenantes (clients, fournisseurs, médias, autorités, etc.), en adaptant si nécessaire sa communication à un public

ayant un handicap, d'un comportement inhabituel de la part d'un poste de travail ou d'un serveur, synonyme d'une potentielle intrusion, en spécifiant l'état de la compréhension de la menace, les hypothèses d'évolution de cette dernière et en préconisant des actions simples à mener dans l'attente de la réalisation d'opérations techniques pour limiter ou stopper la cybermenace.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle. Note de vigilance et proposition d'accompagnement. Production écrite.

La Direction de l'entreprise a confié la mission au candidat d'adresser, via le système de messagerie interne de l'organisation, une note de vigilance à l'ensemble des collaborateurs sur une potentielle cybermenace (exemple : type rançongiciel).

En retour, un membre de l'entreprise signale au Gestionnaire de la sécurité des données, des réseaux et des systèmes qu'il remarque une anomalie technique sur son ordinateur.

Le candidat précise, en réponse, les actions à mettre en œuvre pour parer à la menace éventuelle.

Mise en situation professionnelle. Conception de formation. Production écrite et présentation orale.

Le candidat reçoit un mail du Responsable Formation de l'entreprise indiquant un besoin en formation interne, pour huit collaborateurs, relatif à la sécurité des données, des réseaux et des systèmes.

Il conçoit un programme de formation de deux jours (quatorze heures).

Mise en situation professionnelle. Communication d'alerte. Production écrite.

En pleine action de contrôle des dispositifs de sécurité, le candidat observe, sur son ordinateur portable, un risque de compromission du système d'information. Il informe alors sa direction, via un rapport d'analyse.

Puis, dans un second temps, le candidat constate sur son PC un comportement inhabituel (connexion impossible, activité importante, activités inhabituelles, services ouverts non autorisés, fichiers créés, modifiés ou supprimés sans autorisation, multiples alertes de l'antivirus, etc.). Il rédige alors une note à l'ensemble des parties prenantes indiquant l'état de la compréhension de la menace, les hypothèses d'évolution de cette dernière et en préconisant des actions simples à mener.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Les cyberattaques, de plus en plus fréquentes et virulentes, menacent les ambitions économiques et sociales de tous types d'organisations usant du numérique dans ses activités. L'étude menée par Splunk précise que « 57 % des entreprises françaises ont déclaré être confrontées à une augmentation des cyberattaques » et que « 38 % des entreprises françaises déclarent avoir été victimes d'au moins une violation de données au cours des deux dernières années ». L'ANSSI souligne, dans son panorama de la menace informatique 2021, cette hausse significative et indique avoir eu connaissance de « 1082 intrusions avérées dans des systèmes d'information en 2021, pour 786 en 2020 ». Soit une augmentation de 37% que l'ANSSI explique par « l'évolution et l'amélioration constante des capacités des acteurs malveillants dont les principales intentions restent le gain financier, l'espionnage et la déstabilisation ». La répartition des entités victimes d'attaques, recensés par l'ANSSI en 2021 dans le cadre des incidents traités, démontre que des entreprises de toutes tailles sont visées par des cyberattaques.

Le Gestionnaire de la sécurité des données, des réseaux et des systèmes peut donc travailler dans des entreprises de toutes tailles et de tous secteurs mais également, puisque 67% des sociétés ont recours à des prestataires pour réaliser des activités de sécurité informatique comme précisé par l'INSEE, dans des entreprises spécialisées dans la cybersécurité.

TYPE D'EMPLOIS ACCESSIBLES

- Gestionnaire de la sécurité des données, des réseaux et des systèmes

- Gestionnaire cybersécurité
- Administrateur sécurité informatique
- Administrateur cybersécurité
- Chargé de gestion de crise cyber
- Analyste en surveillance des données, des réseaux et des systèmes
- Analyste cybersécurité

RÈGLEMENTATIONS D'ACTIVITÉ

L'exercice du métier de Gestionnaire de la sécurité des données, des réseaux et des systèmes n'est pas spécifiquement réglementé mais ce professionnel travaille dans un cadre réglementaire précis :

- Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Il constitue le texte de référence en matière de protection des données personnelles. Ses dispositions sont directement applicables dans l'ensemble des États membres à compter du 25 mai 2018.
- Le Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité).
- Le Règlement (UE) « eIDAS » n°910/2014 du 23 juillet 2014 relatif aux transactions électroniques au sein du marché intérieur permettant d'établir un socle commun pour les interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques.
- Directive (UE) 2016/1148 du Parlement Européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.
- La loi " Informatique et Libertés " du 6 janvier 1978 et la loi du 20 juin 2018 relative à la protection des données personnelles.
- La loi n°2018-607 relative à la programmation militaire pour les années 2019 - 2025 promulguée par la Président de la République le 13 juillet 2018. Elle comporte, dans son article 34, des dispositions relatives au renforcement des capacités de détection des attaques informatiques, aujourd'hui indispensables pour élever le niveau de sécurité de la Nation.
- L'article 22 de la loi de programmation militaire (loi n° 2013-1168 du 18 décembre 2013) qui impose aux opérateurs d'importance vitale le renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent : les systèmes d'information d'importance vitale (SIIV).
- Le décret n°2015-351 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale.
- Le décret n°2015-350 relatif à la qualification des produits de sécurité et des prestataires de services de confiance pour les besoins de la sécurité nationale.
- Le décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.
- L'instruction générale interministérielle n°1300 du 9 août 2021 sur la protection du secret de la défense nationale.
- L'instruction générale interministérielle n°2100 du 1er décembre 1975 pour l'application en France du système de sécurité de l'Organisation du traité de l'Atlantique nord.
- L'instruction générale interministérielle n°2102 du 12 juillet 2013 sur la protection en France des informations classifiées de l'Union européenne.
- L'instruction interministérielle n°920 du 12 janvier 2005 relative aux systèmes traitant des informations classifiées de défense de niveau Confidentiel-défense.
- L'instruction interministérielle n° 300 du 23 juin 2014 relative à la protection contre les signaux compromettants.
- L'instruction interministérielle n° 901 du 28 janvier 2015 relative à la protection des systèmes d'information sensibles, notamment ceux traitant des informations portant la mention Diffusion Restreinte.
- Le référentiel général de sécurité est pris en application du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives. La version initiale du RGS (v.1.0) a été rendue officielle par arrêté du Premier ministre en date du 6 mai 2010. Une version 2.0 a été publiée par arrêté du Premier ministre du 13 juin 2014. Ses mesures de transitions ont été étendues par arrêté du Premier ministre du 10 juin 2015. Elle est applicable depuis le 1er juillet 2014. La version 2.0 du RGS constitue un référentiel de transition entre une première version liée à la mise en œuvre de l'administration électronique et une troisième version qui se fondera sur la réglementation européenne en cours d'évolution.
- La circulaire du Premier ministre n° 5725/SG du 17 juillet 2014 relative à la politique de sécurité des systèmes

d'information (PSSIE).

- Instruction interministérielle n° 910 du 22 octobre 2013 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI).

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	Lien formation-emploi, Manque de main-d'œuvre disponible
Salaire médian (mensuel)	2 704 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (35 % des actifs en emploi)
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (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)	14 307
Jugés difficiles à recruter	46 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique 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 initiale, Formation continue, Apprentissage, Contrat de professionnalisation, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

La certification est accessible aux titulaires qui justifient d'un titre ou diplôme de niveau 5 dans les domaines de l'informatique et du numérique ou d'une expérience significative dans le domaine de la cybersécurité.

Le candidat devra réussir des tests d'évaluation des connaissances et un entretien de motivation.

PRÉREQUIS À LA VALIDATION

Chaque bloc de compétences est certifié, il donne lieu à une évaluation spécifique et à une validation. Chaque bloc de compétences est validé si l'ensemble des compétences du bloc est validé. Les blocs de compétences sont complémentaires et capitalisables.

La validation partielle du titre est constituée du ou des blocs dont la totalité des compétences est validée. La certification est acquise si tous les blocs de compétences sont validés.

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

5 personnes au minimum dans le respect de 50 % de membres externes à l'organisme certificateur et n'ayant pas pris part à la formation :

- un président professionnel extérieur à l'établissement,
- trois professionnels du secteur non intervenants dans l'établissement,

- un membre de la direction : directeur pédagogique, responsable de programme...

Parmi les professionnels : 50% de représentants des salariés et 50% de représentants d'employeurs, parité hommes/femmes.

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	9 475 €
Selon la branche	7 000 € – 11 845 €
Prise en charge	Branches concernées
9 475 €	Valeur par défaut · 161 branches
8 540 €	COPANIEF - Fabricant de sucres, CPNE Boulangerie-pâtisserie industrielles, CPNE Branche ITV, CPNE de l'agriculture, CPNE des MFR
11 844 €	CPNE Entreprises des activités du déchet et de la propreté urbaine, CPNE Travail Temporaire, CPNE autoroutes, CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique, CPNEF de la Branche des organismes de formation
9 480 €	CPNE Casinos, CPNE de la branche de la Distribution Directe, CPNEF de l'Exploitation cinématographique et de la Distribution de films, CPNEF de l'audiovisuel
11 055 €	CPNEFP de l'enseignement privé indépendant, CPNEFP de la Restauration rapide
8 990 €	CPNEF branche retraite complémentaire et prévoyance, CPNEFP Mutualité
7 923 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager, CPNEFP du Négoce de l'ameublement
7 500 €	CPNE des industries de santé (CPNEIS), CPNEFP des industries des tuiles et briques
7 000 €	CPNE chimie, CPNEFP de la métallurgie
11 845 €	CPNE des Télécoms
9 027 €	CPNEFP Grands Magasins/ Magasins Populaires
9 000 €	CPNEFP de la branche des prestataires de services du secteur tertiaire
8 500 €	CPNE de l'ingénierie, des services informatiques et du conseil
8 285 €	CPNEFP Commerce à distance
8 057 €	CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
8 036 €	CPNE FP Branche des magasins du Bricolage
8 029 €	CPNEFP des jardineries et graineteries

Base légale

Date de décision	17/02/2023
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	17/02/2026
Date de dernière délivrance possible	17/02/2030

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/37346/>