ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

GESTIONNAIRE DE LA SECURITE DES DONNEES, DES RESEAUX ET DES SYSTEMES – N°29445
REFERENTIELS
ÉCOLE HEXAGONE

Article L6113-1 En savoir plus sur cet article... Créé par LOI n°2018-771 du 5 septembre 2018 - art. 31 (V)
« *Les certifications professionnelles enregistrées au répertoire national des certifications professionnelles permettent une validation des compétences et des connaissances acquises nécessaires à l'exercice d'activités professionnelles. Elles sont définies notamment par un* ***référentiel d'activités*** *qui décrit les situations de travail et les activités exercées, les métiers ou emplois visés, un* ***référentiel de compétences*** *qui identifie les compétences et les connaissances, y compris transversales, qui en découlent et un* ***référentiel d'évaluation*** *qui définit les critères et les modalités d'évaluation des acquis.* »

La formation et la certification sont accessibles aux candidats en situation de handicap. En ce sens, des aménagements dans le cadre des modalités d'évaluation sont possibles et seront définies au cas par cas auprès du Réfèrent Handicap. À titre d'exemple, voici une liste non-exhaustive des points pouvant être aménagés :

- Supports de travail matériels et/ou logiciels (mobilier, conditions de travail à distance, etc.)
- Dates et lieux des évaluations
- Durée des évaluations

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

<table>
<tr><th rowspan="2">RÉFÉRENTIEL D'ACTIVITÉS
décrit les situations de travail et les activités exercées, les métiers ou emplois visés</th><th rowspan="2">RÉFÉRENTIEL DE COMPÉTENCES
identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</th><th colspan="2">RÉFÉRENTIEL D'ÉVALUATION
définit les critères et les modalités d'évaluation des acquis</th></tr>
<tr><th>MODALITÉS D'ÉVALUATION</th><th>CRITÈRES D'ÉVALUATION</th></tr>
<tr><td rowspan="2">1. Formuler et formaliser la politique de la sécurité des systèmes d'information d'une organisation en adéquation avec son environnement et les risques auxquels elle doit faire face

A.1. Étude du contexte de l'organisation
- Application des textes juridiques de la cyberdéfense, de la législation liée à la cybercriminalité, des normes et des textes règlementaires (Loi Godfrain, CNIL, ANSSI, LPM, RGPD, DSA, DMA, ARCEP, etc.)
- Application des normes liées aux situations de handicap
- Lecture des normes et procédures internes
- Utilisation du vocabulaire métier propre à l'organisation
- Gestion de la coordination entre les parties prenantes (directions, métiers, RSSI, DSI, communication, etc.)
- Prise en compte des principes d'intelligence économique (veille, protection de l'information et influence)
- Prise en compte du contexte géopolitique et concurrentiel dans lequel l'organisation évolue
- Définition d'un objectif de plan de recherche</td><td>C.1. Identifier les enjeux stratégiques de la cyberdéfense d'une organisation en s'appuyant sur la lecture des normes et procédures internes, des textes législatif, règlementaires et normatifs, en communiquant avec les parties prenantes et en utilisant le vocabulaire propre à l'organisation afin d'acquérir une vision d'ensemble des activités de l'organisation.</td><td rowspan="2">M.1. - Étude de cas :
Analyse de l'environnement d'une organisation

Le candidat doit analyser l'environnement juridique, économique et géopolitique d'une organisation et rédiger, à partir d'un dossier d'analyse et individuellement, une cartographie et une note de synthèse.
Le candidat doit s'approprier le contexte cyber de l'organisation, les procédures et normes internes, le vocabulaire propre au secteur d'activité et les besoins métiers. (C1)
Le candidat doit témoigner d'un esprit synthétique, d'une méthode de recherche de l'information à l'aide d'outils et analyser le contexte géopolitique et concurrentiel au regard des activités de l'organisation. (C2)
Les supports et ressources documentaires portant sur l'organisation, sa situation et ses activités sont fournis par l'organisme de formation. Le candidat doit alimenter son travail de ses recherches personnelles.
Cet examen se déroule à domicile.</td><td>• Le cadre législatif, normatif et règlementaire est appliqué.
• Les besoins des services de l'entreprise (usages métiers) sont identifiés et mentionnés au travers d'enquêtes et de témoignages cités.
• Les enjeux cyber de l'organisation sont identifiés.
• Le vocabulaire spécifique au secteur d'activité est utilisé.
• La rédaction témoigne d'un esprit d'analyse de documents.
• Le support ne contient pas de faute d'orthographe.</td></tr>
<tr><td>C.2. Évaluer l'environnement dans lequel évolue une organisation par l'application d'une méthodologie de sélection, de recherche, de collecte et d'analyse d'informations, en identifiant les priorités stratégiques de la cybersécurité dans une synthèse afin d'anticiper la stratégie cyber et garantir la protection des intérêts de l'organisation.</td><td>• L'objectif du plan de recherche est correctement formulé.
• Les informations sont identifiées avant d'être collectées.
• Les informations sont correctement sourcées et authentifiées.
• Le choix des outils de la méthodologie de recherche et d'analyse de l'information est justifié et pertinent.
• La rédaction témoigne d'un esprit de synthèse.
• Des recommandations sont rédigées et justifiées.</td></tr>
</table>

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

- Collecte d'informations au regard de l'objectif établi à partir de différentes sources ouvertes (application de l'OSINT) - Analyse et comparaison des informations collectées - Identification des priorités stratégiques de la cybersécurité de l'organisation - Rédaction d'une synthèse du contexte cyber interne et concurrentiel de l'organisation			
A.2. Analyse du risque numérique d'une organisation en suivant la norme ISO 27005 et en appliquant la méthode d'analyse EBIOS *Risk Manager* (ANSSI) - Application des lignes directrices définies par la norme ISO 27005 tout au long de l'analyse - Organisation d'ateliers de travail avec les différents acteurs (direction, métiers, DSI, RSSI). - Utilisation du guide et des outils de la méthode EBIOS *Risk Manager* - Identification de l'objet d'étude, des participants et du cadre temporel - Recensement des missions, des valeurs métiers (procédures, services, fonctions, informations) - Identification des failles et vulnérabilités - Déduction en événements redoutés et estimation de leur niveau de gravité (mineur, significatif, grave, critique) - Définition du socle de sécurité adapté au contexte : identification des mesures liées aux principes de base et à l'hygiène et des mesures relatives au cadre règlementaire et normatif	C.3. Mettre en œuvre une méthode d'analyse du risque numérique en établissant l'objet d'étude, en mettant en lumière les parties prenantes (partenaires, filiales, sous-traitants, etc.), en analysant les procédures métiers et en catégorisant ces vulnérabilités par niveau de gravité, tout en appliquant le cadre normatif et règlementaire afin de déceler les failles et les vulnérabilités de l'organisation.	**M.2. - Mise en situation professionnelle reconstituée :** Analyse de risque à l'occasion de l'étude préalable à la mise en place d'un outil numérique sur le système d'information d'une organisation. Le candidat doit appliquer, individuellement, une méthode reconnue d'analyse de risque pour évaluer les conséquences sur la cybersécurité de la mise en place du nouvel outil. (C3) Le candidat doit proposer des recommandations et interpréter les risques identifiés au regard des pertes potentielles et de la mise en place du nouvel outil dans un rapport d'analyse du risque. (C4) Les supports et ressources documentaires portant sur l'organisation, sa situation et ses activités ainsi que sur la méthode	• La méthode d'analyse est appliquée rigoureusement. • L'objet d'étude est correctement identifié. • Chaque étape de l'analyse est définie et documentée. • Les parties prenantes sont correctement définies. • L'engagement des parties prenantes est identifié et pris en compte. • Les missions et valeurs métiers sont listés et prises en compte. • L'environnement de l'organisation (contexte, procédures métiers, etc.) est pris en compte et assimilé. • Les failles, vulnérabilités et risques principaux sont correctement identifiés et décrits. • Le cadre législatif, normatif et règlementaire est appliqué.
	C.4. Déterminer des mesures de sécurité idoines au contexte d'une organisation en réalisant une cartographie des sources de risque, des menaces numériques, des scénarios d'attaque, par la prise en		• L'analyse est pertinente. • Les sources de risque et menaces sont correctement identifiées et exhaustives. • Les scénarios et événements redoutés sont cohérents vis-à-

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

- Identification des écarts observés entre l'attendu et l'existant - Caractérisation des sources de risque et de leurs objectifs visés (SR/OV) - Formalisation d'une cartographie des sources de risque et d'une cartographie de menace numérique - Élaboration des scénarios stratégiques (modes opératoires des cyber attaquants, chemins d'attaque qu'une source de risque peut emprunter) et élaboration des scénarios opérationnels - Formalisation d'une synthèse de l'analyse des risques comprenant des recommandations et les risques résiduels - Rédaction d'une proposition de prise en compte du risque (suppression, couverture, diminution, acceptation) en fonction des objectifs - Apport d'éléments d'arbitrage quant à l'acceptation ou non des risques résiduels	compte de ses moyens (financiers, humains, etc.) et en synthétisant ces informations afin de permettre l'adoption d'une politique cyber adaptée à l'organisation et à ses activités.	d'analyse du risque sont fournis par l'organisme de formation. Cet examen se déroule en centre d'examen.	vis du contexte de l'organisation. • Les recommandations visant à réduire le risque sont pertinentes et réalistes. • Les ressources de l'organisation sont prises en compte dans la formulation des recommandations. • Le cadre législatif, règlementaire et normatif est appliqué dans la formalisation des risques et des recommandations. • Les risques résiduels sont acceptables dans le contexte de l'organisation. • Le rapport d'analyse est bien rédigé et synthétique. • Les propos sont vulgarisés (compréhensible par un décideur non technique). • Le support ne contient pas de faute d'orthographe.
A.3. Élaboration d'une politique et d'une organisation cyber adaptées au contexte de l'organisation - Application du guide PSSI (ANSSI) - Prise en compte des ressources humaines et financières - Prise en compte des usages métiers - Prise en compte des critères de la norme de management de la qualité (ISO 9001) - Prise en compte des situations de handicap et des normes s'y rattachant (référentiel général d'amélioration de l'accessibilité (RGAA),	C.5. Formuler la politique de sécurité d'une organisation à partir du guide PSSI de l'ANSSI, en tenant compte de l'existant et des usages, en intégrant une démarche qualité, en définissant les objectifs, les orientations et les responsabilités de chacun et en intégrant un cadre de suivi afin de garantir l'usage sécurisé et efficace de l'ensemble du système d'information.	**M.3. - Mise en situation professionnelle reconstituée :** Formalisation d'une politique de sécurité d'une organisation Dans le cadre d'un projet fictif portant sur une organisation souhaitant mettre à jour une politique de sécurité de son système d'information, le candidat doit formaliser la politique à l'écrit et la présenter à l'oral.	**Partie 1** • Le référentiel PASSI est correctement utilisé. • La politique prend en compte le contexte et les ressources. • Les objectifs de la politique sont pertinents. • Le champ d'application de la politique est identifié et cohérent. • L'orientation de la politique de sécurité est claire et approprié au contexte. • Les responsabilités et usages des utilisateurs sont définis et

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

<table>
<tr>
<td rowspan="2">norme internationale WCAG 2.1 (Web Content Accessibility Guidelines))
- Énonciation des objectifs de la politique de sécurité
- Caractérisation du champ d'application de la politique dans le système d'information
- Orientation de la politique de sécurité (principes, généralités, directives, conséquences en cas de non-respect)
- Définition des responsabilités et usages des utilisateurs en termes de contrôle et d'accessibilité aux données, aux services et à l'infrastructure
- Définition d'un cadre de suivi (reporting, période et fréquence d'audit
- Rédaction d'un plan d'amélioration continue (mesures de sécurités)
- Coordination entre les acteurs de l'organisation (direction, métiers, DSI, RSSI)
- Mise en place d'un dispositif lié à la sensibilisation des acteurs de l'organisation aux pratiques recommandées par l'ANSSI et au risque cyber
- Organisation d'ateliers, de réunion pour promouvoir la politique de sécurité
- Communication écrite sur la politique et son intérêt
- Communication immersive en utilisant l'oral, en français et en anglais</td>
<td></td>
<td rowspan="2">Ce projet se déroule en deux parties.

Partie 1 : rédaction de la politique
Le candidat doit rédiger, individuellement, la politique de sécurité en se basant sur le guide PASSI relatif à la politique de sécurité d'un système d'information.
Cette partie se déroule à domicile.

Partie 2 : présentation à une équipe non technique
Le candidat doit, individuellement, présenter au personnel technique et non technique, à l'oral, sa politique et sa pertinence.
Cette partie se déroule en centre d'examen.

Les supports et ressources documentaires portant sur le cas d'étude sont fournis par l'organisme de formation.</td>
<td>justifiés au regard des activités de l'organisation et des métiers.
• Un cadre de suivi est prévu.
• La démarche qualité est prise en compte dans l'ensemble de la politique (ISO 9001).
• Le support ne contient pas de faute d'orthographe.</td>
</tr>
<tr>
<td>C.6. Communiquer régulièrement auprès de l'ensemble des acteurs d'une organisation, à l'écrit et à l'oral, en français et en anglais, en adoptant un langage et/ou des outils inclusifs adaptés aux éventuelles situations de handicap et à la multiculturalité, par l'organisation d'ateliers, réunions ou actions de sensibilisation afin de les impliquer dans la prévention et la gestion du risque cyber.</td>
<td>Partie 2
• Un plan de communication et de sensibilisation à la politique auprès des services est prévu.
• Le plan d'accompagnement est bien fait.
• Les écarts et similitudes culturelles et les éventuelles situations de handicap sont considérées (langue parlée, usages et coutumes propres à la culture du pays, habitudes et horaires de travail, impératifs liés aux convictions religieuses, handicap sensoriel, moteur, cognitif, etc).
• Le candidat est convaincant : Les choix sont justifiés et argumentés en tenant compte de l'environnement de l'organisation.
• Une posture professionnelle est adoptée :
• Le vocabulaire utilisé est précis.
• Le discours est organisé.
• Le langage non-verbal favorise l'attention de son auditoire (voix audible, débit adapté, regarde son auditoire durant l'échange, se tient droit, etc.).</td>
</tr>
</table>

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

RÉFÉRENTIEL D'ACTIVITÉS *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**RÉFÉRENTIEL DE COMPÉTENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**RÉFÉRENTIEL D'ÉVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
2. Mettre en place les outils techniques nécessaires à la sécurisation du système d'information d'une organisation A.4. Définition d'architectures sécurisées - Application des textes juridiques de la cyberdéfense, de la législation liée à la cybercriminalité, des normes et des textes règlementaires (Loi Godfrain, CNIL, ANSSI, LPM, RGPD, DSA, DMA, ARCEP, etc.) - Analyse de l'existant technique - Recensement des ressources disponibles et des infrastructures existantes - Représentation de l'activité opérationnelle du système d'information - Identification des besoins en cybersécurité - Identification du matériel sécurisé en termes de connectivité, de sécurité réseau, de sécurité des systèmes d'exploitation et de stockage, en	C.7. Identifier les équipements (logiciels et matériels) présents sur le marché apportant performance, confidentialité, intégrité et/ou disponibilité, grâce à l'étude de leurs qualifications (CSPN de l'ANSSI, EAL, Critères communs), le recueil de leurs vulnérabilités connues et leur capacité à s'intégrer à une solution de supervision et journalisation des évènements afin de constituer un catalogue d'éléments de sécurisation adaptés aux capacités, moyens et enjeux de l'organisation.	**M.4. - Étude de cas et comptes-rendus écrits :** Équiper le système d'information d'un hôpital Dans un contexte de projet de sécurisation d'un système d'information d'un hôpital (opérateur d'importance vitale), le candidat doit établir un cahier des charges fonctionnel et identifier les équipements nécessaires. Ce projet se déroule en deux parties. **Partie 1 :** identification de l'architecture technique (C7) Le candidat doit, en groupe de 3 à 4 personnes, produire un dossier écrit contenant un inventaire de l'ensemble des ressources, une synthèse des	**Partie 1** • L'inventaire des ressources est exhaustif. • Le rapport rédigé met en lumière les forces et faiblesses des équipements présents. • Les contraintes techniques, humaines et économiques liées à l'entreprise sont prises en compte. • Des préconisations liées à l'amélioration technique et humaine sont apportées. • Le choix des équipements préconisés est justifié en termes de performance, confidentialité, intégrité et disponibilité. • Les vulnérabilités des équipements préconisés sont listées. • Le travail réalisé vérifie de manière exhaustive les points de vigilance en s'appuyant sur une littérature existante.

fonction des qualifications (CSPN de l'ANSSI, EAL, Critères communs) - Prise en compte des vulnérabilités des produits utilisés - Identification des points de supervision, de vigilance - Élaboration d'un cahier des charges fonctionnel - Modélisation d'une base de données, des flux d'informations et des traitements - Représentation d'une architecture technique complète (cloud, serveurs, dimensionnement, interconnexion, etc.) - Déploiement d'une architecture logicielle - Rédaction de documentation liée à l'usage des outils - Présentation du projet aux parties prenantes	C.8. Rédiger un cahier des charges fonctionnel portant sur un projet de sécurisation du système d'information, en tenant compte de l'existant, des besoins métiers et des priorités de l'organisation, en formulant des préconisations de matériels et logiciels conformes à l'état de l'art, à la règlementation et aux normes, afin de proposer une traduction des enjeux de l'organisation et des exigences en termes de sécurité adaptée et pérenne.	différents services/outils et leur agencement logique sous forme de documentation technique et un rapport d'analyse sur les forces et faiblesses des solutions en place ainsi que des pistes d'amélioration. Les supports et ressources documentaires portant sur l'entreprise et sa situation sont fournis au candidat. Cette partie se déroule en centre d'examen. **Partie 2 :** rédaction d'un cahier des charges fonctionnel (C8) Le candidat doit réaliser, individuellement, un cahier des charges fonctionnel dans le cadre d'un projet de sécurisation d'un système d'information. Le candidat doit se baser sur le dossier établi en partie 1. Cette partie se déroule à domicile.	**Partie 2** • Le périmètre du projet est défini dans le cahier des charges. • Les exigences des usages métiers sont prises en compte. • Les aspects techniques et fonctionnels sont précisément définis. • Les besoins en ressources et délais sont précisés. • Les contraintes du projet sont anticipées. • Le besoin en ressources est correctement formulé (temps, humaines, financières, etc.). • Le support ne contient pas de faute d'orthographe. • Le vocabulaire utilisé est précis et cohérent vis-à-vis du contexte.
	C.9. Modéliser une base de données, des flux d'information et traitements, à l'aide du relevé des échanges d'informations existants ou nécessaires entre les différentes briques (logicielles et matérielles) de sécurisation du système d'information afin d'établir la cartographie de l'architecture de sécurisation du système d'information à mettre en place.	**M.5. - Étude de cas/Travaux pratiques :** Modélisation d'une base de données À partir d'un dossier technique, le candidat doit réaliser, individuellement, une cartographie d'une base de données. Les supports et ressources documentaires nécessaires sont fournis par l'organisme de formation. Cet examen se déroule en centre d'examen.	• Les activités opérationnelles sont prises en compte dans la représentation de la base de données, des flux d'information et de traitements. • Le travail de préparation sur les données est anticipé, construit de façon logique pour pouvoir les exploiter correctement pour la suite (suppression de données non pertinentes, suppression des valeurs nulles). • L'architecture matérielle et logicielle est représentée de manière exhaustive. • Les outils utilisés sont justifiés et permettent de répondre aux

			besoins en fonction des contraintes.
A.5. Management d'un projet portant sur la sécurisation d'un système d'information - Sélection d'un mode de gestion de projet - Prise en compte des critères de la norme de management de la qualité (ISO 9001) - Prise en compte des critères de la norme de management de la sécurité informatique pour la mise en place d'un SMSI (ISO 27000) - Création d'outils d'organisation paramétrables (tableaux, simulateurs, etc.) - Planification des tâches avec ces outils organisationnels - Définition d'indicateurs de suivi - Ajustement des outils créés - Distribution des tâches au sein des équipes techniques - Prise en compte des critères de la norme de management environnemental (ISO 14001)	C.10. Déployer des outils méthodologiques dans un cadre de projet de sécurisation d'un système d'information grâce à la sélection d'une méthode de gestion de projet (Agile, cycle en V) et à des outils de suivi, en prenant en compte es normes ISO (9001, 14001), afin de garantir les conditions les plus favorables à son orchestration.	**M.6. - Mise en situation professionnelle reconstituée :** Gestion d'un projet de sécurisation d'un système d'information d'une organisation Le candidat doit réaliser, individuellement un dossier écrit présentant le plan d'action du projet, les méthodes et les outils qui seront utilisées, dans le cadre d'un projet fictif d'une organisation témoin souhaitant sécuriser son système d'information dans un contexte international. Le candidat doit élaborer un planning, prévoir une méthode et des outils de gestion et de suivi du projet et des	• Le choix de la méthode de gestion de projet est cohérent et justifié vis-à-vis des besoins, contraintes et ressources. • La méthode sélectionnée est correctement appliquée. • Le planning et l'organisation permettent d'identifier les priorités et les étapes du projet et sont cohérents vis-à-vis des objectifs. • Les tâches sont correctement distribuées (en fonction des normes de sécurité, du niveau de responsabilité de chaque acteur, des compétences, etc.). • Les outils et indicateurs de suivi du projet sont définis. • Les outils sont ajustés en suivant le rythme d'exécution, la difficulté du travail et en respectant les objectifs.

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

- Prise en compte des situations de handicap et des normes s'y rattachant (référentiel général d'amélioration de l'accessibilité (RGAA), norme internationale WCAG 2.1 (*Web Content Accessibility Guidelines*)) - Coordination avec les différents acteurs - Communication immersive en utilisant l'oral comme l'écrit, en français et en anglais, avec les différentes parties prenantes (direction des systèmes d'information, direction générale, équipes techniques) - Organisation d'entretiens individuels avec les membres des équipes techniques - Élaboration de grilles d'évaluation du projet	C.11. Identifier les difficultés pouvant mettre en péril la réussite du projet à l'aide du suivi régulier des étapes du projet, des réalisations de chaque équipe via des entretiens individuels, d'outils de planification et de suivi général (Gantt) et des grilles d'évaluation pour assurer le déroulement du projet dans le respect du cahier des charges/du *rétroplanning* défini.	équipes. (C10) Le candidat doit également identifier et anticiper les éventuelles difficultés et les possibles remédiations. (C11) Les supports et ressources documentaires portant sur l'entreprise et nécessaires à la définition des objectifs du projet sont fournis par l'organisme de formation. L'examen est réalisé à domicile.	• La phase de communication avec les équipes techniques (interrogations, dialogues, discussions) est décrite en amont de la distribution des tâches. • Des ajustements des outils sont proposés et tiennent compte du rythme d'exécution, de la difficulté du travail. • Les ajustements proposés sont cohérents vis-à-vis des objectifs. • Les éventuels conflits et risques sont identifiés. • Des pistes de remédiation sont présentées.
A.6. Utilisation de la cryptologie et des outils cryptographiques pour sécuriser un système d'information - Prise en compte du contexte de l'organisation - Définition du besoin de l'organisation - Étude des différentes solutions présentes sur le marché - Analyse des forces et faiblesses de chaque solution - Sélection d'une solution chiffrée symétrique ou asymétrique - Sélection de l'algorithme de chiffrement adapté aux besoins de sécurité	C.12. Maîtriser les différentes solutions de chiffrements symétriques et asymétriques par l'étude de la cryptologie et par l'analyse des forces et faiblesses de chacune des solutions afin d'opter pour la solution la plus adaptée en fonction des besoins de l'organisation (recherche de confidentialité et/ou d'intégrité et/ou d'authenticité).	**M.7. - Mise en situation professionnelle reconstituée :** Sécurisation d'un système d'information À partir d'éléments de contextualisation d'une organisation et de différents cas d'utilisation supposés d'une messagerie chiffrée, le candidat doit, individuellement, définir les outils répondant aux besoins la solution de cryptologie la	• Les objectifs sont identifiés. • La solution cryptographique retenue est décrite et justifiée. • Le contexte de l'organisation est pris en compte. • La solution cryptographique est pertinente au regard du contexte. • Le support ne contient pas de faute d'orthographe. • Le vocabulaire utilisé est précis et cohérent vis-à-vis du contexte. • La modularité et l'évolutivité ont été prises en compte dans l'étude.

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

- Application à la confidentialité - Application à l'intégrité - Application à l'authenticité - Sélection d'un outil de signature électronique adaptée au besoin de sécurité - Mise en place d'une autorité de certification - Sélection et installation d'une infrastructure de gestion de clés - Choix d'un chiffreur - Choix des mécanismes de chiffrement pour les couches applicatives - Évaluation de la solidité d'un algorithme de chiffrement, d'une clé de chiffrement	C.13. Déployer une infrastructure de gestion de clés par la mise en place d'une autorité de certification répondant aux objectifs (niveau de résistance, facilité d'utilisation, intégration aux chiffreurs matériels) afin de permettre la mise en place du chiffrement et de la signature au sein des échanges/outils de l'organisation.	plus judicieuse et conforme au contexte. (C12) Le candidat doit déployer une solution technique dans un environnement mis à sa disposition. Il doit tester des scénarios potentiels pour vérifier la pertinence et la robustesse de ses choix techniques (C13). Le candidat doit livrer un PoC (*Proof of Concept*) de la solution sous forme de code et présenter et défendre ses propositions à l'écrit. La documentation et l'environnement simulé sont fournis par le centre d'examen. Cet examen se déroule en centre d'examen.	• Le déploiement de la solution cryptographique est correctement mis en œuvre et sécurisé. • La solution cryptographique intégrée dans l'environnement fonctionne. • Le choix des scénarios de test est précisé et justifié. • Les scénarios permettent de couvrir 90% des possibilités. • La solution retenue est robuste et en adéquation avec les objectifs.
A.7. Utilisation du développement sécurisé DevSecOps[1] - Prise en compte de la cybersécurité à chaque phase du cycle de vie du logiciel (conception initiale, intégration, tests, déploiement, maintenance, retrait de service) - Prise en compte de la cybersécurité dans la méthode agile - Utilisation d'une pile logicielle de développement sur un modèle de *Digital Factory* (usine à produits) - Création d'un organigramme de l'utilisation de la *digital factory*	C.14. Mettre en place une usine de développement sécurisé par l'utilisation de pipeline d'intégration et de déploiement continus (CI/CD), par l'intégration de tests unitaires/non-régression tournés vers la sécurité, par l'exploitation d'une pile logicielle (bibliothèque d'outils éprouvés) afin d'assurer la production d'outils logiciels conformes à la politique de sécurité de l'organisation.	**M.8. - Étude de cas :** Développement d'une *digital factory* Dans le cadre du développement d'une *digital factory* pour une organisation, le candidat doit proposer une sélection d'outils permettant de prendre en compte la sécurité lors du développement d'applications et lors de leur déploiement. Le candidat doit proposer également un organigramme avec les différentes équipes de la *digital factory*.	• Les outils utilisés pour développer le programme et le faire fonctionner sont exhaustifs. • Le schéma est conçu de sorte à rester exploitable par un tier • Le choix des composants est cohérent et justifié. • L'organigramme de la *digital factory* est complet et l'organisation prend bien en compte la fonction de sécurité.

[1] Le processus DevSecOps pour *Development, Security and Operations* permet d'intégrer la sécurité des données dans chaque étape du cycle d'un projet de développement.

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

- Mise en place de tests unitaires/non-régression - Automatisation des tâches de sécurité, insertion dans un pipeline CI/CD (Intégration Continue/Déploiement continu) - Prise en compte des infrastructures, du développement d'applications et de la sécurité - Évaluation de la solidité d'un développement face à différents types d'attaques (dépassements mémoire, injections, etc.)		La documentation et l'environnement simulé sont fournis par le centre d'examen. Cet examen se déroule en centre d'examen.	
	C.15. Organiser des tests de sécurité au travers de simulations d'attaques (dépassements mémoire, injections, *bruteforce*, etc.) à l'encontre des infrastructures de développement (usine de développement), d'hébergement en production et des interfaces présentées par les outils pour identifier des faiblesses et vulnérabilités et garantir le maintien au niveau de sécurité attendu des développements logiciels de l'organisation.	**M.9. - Mise en situation professionnelle reconstituée :** Tester la sécurité d'un environnement À partir d'une plateforme de simulation, le candidat doit effectuer des tests de sécurité en suivant une fiche d'audit. Il doit rédige un rapport qui comprend une synthèse écrite des tests réalisés à l'attention des non-techniques et une liste de recommandations. L'environnement technique simulé et la fiche d'audit sont fournis par l'organisme de formation. Cet examen se déroule en centre d'examen.	• Les tests sont correctement réalisés. • Le rapport est pertinent du point de vue technique. • La synthèse est bien écrite et accessible pour un non spécialiste. • Les recommandations formulées dans le rapport sont pertinentes. • Le support ne contient pas de faute d'orthographe.

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

RÉFÉRENTIEL D'ACTIVITÉS *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**RÉFÉRENTIEL DE COMPÉTENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**RÉFÉRENTIEL D'ÉVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
3. Suivre l'évolution du niveau de sécurité d'un système d'information d'une organisation A.8. Mise en œuvre d'audits organisationnels et techniques - Prise en compte du référentiel PASSI[2] - Application de la norme ISO 19011 relative à la conduite d'audit - Vérification du respect des normes et règlements en vigueur et de la politique de sécurité des systèmes d'information interne à l'organisation - Vérification de la conformité des pratiques de sécurité et de la corrélation avec les règles internes de la	C.16. Réaliser un audit des systèmes d'information grâce à la conduite de tests et simulations *in situ* (intrusions), de l'évaluation du code source et de remontées statistiques cadrés par le référentiel PASSI et les règles d'engagement (entre l'auditeur et l'audité) pour acquérir les données nécessaires à l'évaluation du niveau de sécurisation du système d'information.	**M.10. - Étude de cas :** Conduite d'un audit de sécurité Le candidat doit, individuellement, réaliser un audit et produire un rapport. À partir d'une infrastructure technique existante fictive, d'une envergure similaire à celle que l'on retrouve dans une PME de 200 collaborateurs, le candidat doit conduire, individuellement, un audit technique et organisationnel à partir du référentiel PASSI. (C16) Le candidat doit rédiger le rapport de cet audit. Celui-ci doit témoigner du niveau de sécurisation du système d'information évalué et mettre en valeur les axes	• Le référentiel PASSI est respecté et appliqué. • Les recommandations de la norme 19011 sont appliquées. • L'audit est adapté au périmètre. • L'audit d'architecture est correctement réalisé. • L'audit de configuration est correctement réalisé. • L'audit de code source est correctement réalisé. • Les tests d'intrusion sont bien réalisés et concluants. • Les politiques et procédures sont auditées et comparées à l'état de l'art et aux normes.

[2] Référentiel d'exigences publié par l'ANSSI, pour les Prestataires d'Audit de la Sécurité des Systèmes d'Information

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

configuration des divers outils (équipements réseau, OS, applications, etc.) - Analyse du code source - Réalisation de tests d'intrusion - Respect du système d'information audité (maîtriser les règles d'engagement, utilisation d'outils techniques maîtrisés) - Identification des axes d'amélioration, des failles de sécurité - Proposition et recommandation d'éléments d'amélioration - Rédaction d'un rapport d'audit - Élaboration d'un tableau synthétique - Présentation des résultats aux parties prenantes (en fonction de l'audité)	C.17. Présenter les conclusions d'un audit des systèmes d'information par l'analyse des résultats et comportements obtenus (techniques, humains et organisationnels) et leur comparaison avec les référentiels de l'organisation (politique SSI) et le cadre normatif et règlementaire, en identifiant des axes d'amélioration afin de proposer des recommandations qui contribueront à l'élévation du niveau de sécurité de l'organisation ou lui permettront d'obtenir son homologation de sécurité.	d'amélioration, des vulnérabilités, des écarts entre le cadre (légal, normatif interne, etc.) et la réalité observée. (C17) Le candidat doit formuler des recommandations d'évolution et de changement afin que le système d'information évalué respecte l'état de l'art. Il doit réaliser justifier une note à l'attention des parties prenantes leur enjoignant d'appliquer ces recommandations (C18). L'environnement technique, les supports et ressources documentaires portant sur l'organisation, sa situation et ses activités sont fournis par l'organisme de formation. Cet examen se déroule sur plusieurs journées en centre d'examen.	• Les objectifs du commanditaire sont respectés. • Le rapport d'audit est correctement rédigé. • Le rapport d'audit est vulgarisé pour être partagé à un public non technique. • Le contexte et le périmètre sont définis. • Les vulnérabilités techniques et organisationnelles sont identifiées. • Le niveau de sécurité est bien déduit et conforme au périmètre et aux objectifs du commanditaire.
	C.18. Intégrer la conduite de changement du système d'information de l'organisation par l'établissement d'une veille sur les modifications à venir, la conduite d'audit sur les nouveaux outils et processus qui seront mis en place pour garantir l'adoption et l'application continue de la politique de sécurisation du système d'information.		• Des mesures correctives sont proposées pour chaque vulnérabilité. • Les mesures proposées sont sourcées et documentées conformément à l'état de l'art. • Des éléments de poursuite sont mentionnés et relatifs aux contraintes vécues (temps, moyens, etc.). • Le rapport propose un audit de validation et ses objectifs.

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

A.9. Mettre en place une organisation pour la supervision des systèmes d'information - Intégration d'un SIEM au sein du SOC[3] - Exploitation de sondes de sécurité - Surveillance de pare-feu - Exploitation d'une solution EDR[4] - Établissement de règles de corrélations - Analyse et corrélation des logs à l'aide d'outils - Utilisation de l'intelligence artificielle à des fins de supervision - Mise en place de processus de gestion des alarmes et incidents de sécurité - Résolution des alarmes de sécurité en collaboration avec la DSI et les métiers - Surveillance de l'état de la menace cyber en appliquant une CTI (*Cyber Threat*	C.19. Développer un SOC (*Security Operating Center*) par la mise en place de la remontée en temps réel des signaux d'états des outils de sécurité (sondes, *EDR*s, pare-feux) au sein d'une plateforme de supervision/*monitoring* (SIEM) afin d'assurer le maintien en fonction et la performance de la détection d'alertes de sécurité liées au système d'information.	**M.11. - Mise en situation professionnelle reconstituée – Jeu de rôle :** Officier en tant que RSSI Le candidat doit réaliser le développement et la mise en place d'un SOC. Pour cela, le candidat doit adopter la posture d'un responsable de la sécurité des systèmes d'information officiant pour une Ambassade française à l'étranger. Celle-ci vient d'emménager dans de nouveaux locaux. Il n'y a pas de reprise de l'existant. Ce travail se matérialise, dans un premier temps, par la conception, l'installation et la configuration de paramètres, de logiciels ou d'équipements sécurisés. (C19)	• La sélection du ou des outils de supervision a été réalisée à l'aide d'une méthodologie adaptée au contexte. • L'ensemble des équipements et services de l'infrastructure simulée a été considéré dans la sélection de l'outil. • La conception des alertes et le canal de remonté a été adaptée en fonction des spécificités de chacun des équipement et services (criticité et impact). • La modularité et l'évolutivité ont été prises en compte dans l'étude.

[3] Le SOC est une plateforme permettant la supervision et l'administration de la sécurité du système d'information au travers d'outils de collecte, de corrélation d'événements et d'intervention à distance. Le SIEM (Security Information Event Management) est l'outil principal du SOC puisqu'il permet de gérer les évènements d'un SI.

[4] Un EDR est une solution de sécurité pour les endpoints (points terminaux) qui désignent les appareils (téléphone, ordinateur).

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

Intelligence) adaptée au contexte de l'entreprise	C.20. Mettre en place un suivi des alarmes de sécurité par la définition de critères d'évaluation (origine, occurrence – fréquence, nature), par l'analyse de comportements suspects au travers de l'intelligence artificielle et par la définition des parties impliquées (départements, victimes), afin d'en déterminer le niveau de gravité et de proposer rapidement un plan d'action et une réponse adaptée à l'incident.	Ce travail se matérialise également par le développement d'outils d'analyse et de suivi en temps réel des signaux d'états des équipements et services, par la définition d'une politique d'alerte correspondante. (C20) Le candidat doit livrer un PoC (*Proof of Concept*) de la solution sous forme de code, machines virtuelles et documentations techniques et présenter et défendre ses propositions de valeur devant un jury et procéder à une démonstration. L'environnement simulé à superviser est fourni par l'organisme de formation. L'examen est réalisé à domicile et en centre d'examen.	• Une posture professionnelle est adoptée : • Le vocabulaire utilisé est précis. • Le discours est organisé. • Le langage non-verbal favorise l'attention de son auditoire (voix audible, débit adapté, regarde son auditoire durant l'échange, se tient droit, etc.). • La démonstration est pertinente et fonctionnelle. • Un support de présentation qualitatif est créé : • Les données présentées sont claires et lisibles. • Le support ne contient pas de faute d'orthographe.
A.10. Assurer le maintien en condition de sécurité du système d'information - Suivi des vulnérabilités - Intégration du *scoring* (niveau/score) des vulnérabilités à l'analyse de risque cyber. - Management des patchs de sécurité - Vérification de la non-régression des services à la suite de l'application d'un patch de sécurité - Gestion des obsolescences de sécurité - Adaptation du dispositif de sécurité informatique à l'évolution du parc informatique et du portefeuille applicatif - Veille technologique sur les outils d'attaque et d'audits utilisant l'Intelligence Artificielle	C.21. Assurer la mise à jour des outils matériels et logiciels au regard des processus métiers et des contraintes de l'organisation, en appliquant les nouvelles versions de logiciels, en renouvelant le parc matériel et logiciel en fonction des nouvelles technologies et des nouveaux besoins, en actualisant la gestion des contrats fournisseurs et de l'organisation afin de maintenir le niveau de sécurisation du système d'information.	**M.12. - Questionnaires à visée professionnelle :** Comment garantir la maintenance de la sécurité d'un système d'information ? Le candidat doit, individuellement, répondre à un questionnaire portant sur sa capacité à mener des actions pour assurer le maintien en condition de sécurité d'un système d'information. Le questionnaire est composé de mini-cas relatifs à la mise à jour des équipements logiciels et matériels, à la gestion et au traitement des vulnérabilités d'un système d'information, à l'anticipation du suivi et de ses mises à jour. Cet examen se déroule en centre d'examen.	• Les obsolescences des contrats sont identifiées. • Le parc matériel et logiciel est correctement contrôlé. • Les mises à jour des versions des logiciels sont détectées et considérées. • Les équipements présentant des failles sont dépréciés et des préconisations sont faites. • Les éléments clés des recommandations de l'ANSSI sont cités, exploités et mis en application dans les contextes fictifs présentés. • Les éléments clés des règlementations territoriales sont cités, exploités et mis en application dans les contextes fictifs présentés.
	C.22. Établir un suivi actif des vulnérabilités des briques du système d'information,		• Les différentes parties prenantes de la politique de sécurité et du

	en surveillant l'obsolescence des produits et les demandes automatiques constructeurs de mise à jour de la version du logiciel en cas de remontée de vulnérabilité pour maintenir les outils à jour et garantir le niveau de sécurisation du système d'information.		maintien en conditions opérationnelles sont identifiées. • Les enjeux et moyens de mise en place de suivi des vulnérabilités des différentes parties prenantes sont cohérents vis-à-vis de la règlementation. • Des préconisations sont faites pour pallier les vulnérabilités.
A.11. Mise en place d'une veille concurrentielle, technologique, économique et sociale dans un contexte international - Listage des thèmes et obligations à maintenir en veille - Identification de la véracité des sources - Sélection de sources d'information (exemple : Legifrance, Techcrunch, Financial Times, CNRS, etc.) - Surveillance des sources d'informations - Assurance d'une veille technologique adaptée à la cyberdéfense - Paramétrage d'une plateforme de veille - Tri de l'information en recoupant plusieurs sources par thème - Identification des thèmes concurrentiels et effets d'annonce - Lecture de documents sur chaque thème	C.23. Réaliser une veille technologique, économique et sociale dans un contexte international en définissant les thèmes critiques, en sélectionnant des sources vérifiées et authentiques, en mettant en place une plateforme centralisée recensant les évolutions en termes d'attaques et de concurrence de l'organisation afin d'anticiper l'apparition de nouvelles menaces.	**M.13. - Mise en situation professionnelle reconstituée :** Conception d'un outil de veille Le candidat doit réaliser, pour une organisation fictive, une plateforme de veille et identifier des signes de mutations et innovations technologiques. **Partie 1 :** création d'une plateforme de veille (C23) Le candidat doit, individuellement, sélectionner un ensemble de sources d'informations adapté au secteur d'activité de l'organisation visée, les intégrer au sein d'un outil de son choix (ou de sa propre création) et constituer une base de données de veille. Le candidat doit remettre son code et un support de son choix présentant son outil.	**Partie 1** • Les sources sélectionnées sont pertinentes et authentiques, leur véracité est vérifiée par recoupement. • La cybersécurité est prise en compte dans la définition des sources. • Une veille qualitative est réalisée : alimentation de son réseau, suivi de conférences, échanges avec les pairs, sites Internet, etc. • Les outils sélectionnés et utilisés sont justifiés. • Une justification des enjeux et mutations supposés est présente.

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

- Analyse des signaux faibles indiquant une mutation technologique	C.24. Identifier les mutations et innovations technologiques en s'appuyant sur l'analyse des signaux faibles (économiques, politiques, sociaux ou techniques) recensés à partir d'une base de données de veille et des outils associés afin d'orienter la stratégie de sécurisation du système d'information et participer à la défense des intérêts de l'organisation (avantage concurrentiel, protection de la propriété intellectuelle).	Les supports et ressources documentaires portant sur l'entreprise et sa situation sont fournis par l'organisme de formation. Cet examen se déroule à domicile. **Partie 2 :** analyse et interprétation des données de la plateforme (C24) Le candidat doit réaliser, à partir de l'outil déployé dans la partie 1, l'analyse des résultats obtenus pour identifier les signaux faibles indiquant une mutation technologique. Le candidat doit présenter à l'oral et avec un support de présentation son analyse. Cet examen se déroule à domicile (préparation en amont) et en centre d'examen (présentation orale).	**Partie 2** • La veille permet d'identifier les différents outils sur le marché au-delà des plus connus. • La veille réalisée permet d'observer de nouveaux usages numériques ayant une portée économique, ou politique ou sociale ou technologique. • Le candidat est convaincant : Les choix sont justifiés et argumentés en tenant compte de l'environnement économique et sociétal. • Une posture professionnelle est adoptée : • Le vocabulaire utilisé est précis. • Le discours est organisé. • Le langage non-verbal favorise l'attention de son auditoire (voix audible, débit adapté, regarde son auditoire durant l'échange, se tient droit, etc.).

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

RÉFÉRENTIEL D'ACTIVITÉS *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**RÉFÉRENTIEL DE COMPÉTENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**RÉFÉRENTIEL D'ÉVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
4. Organiser une réponse adaptée en cas de crise A.12. Concevoir un plan de gestion de crise et un plan de continuité et de reprise d'activité - Application du cadre normatif, règlementaire et législatif (Loi Godfrain, CNIL, ANSSI, LPM, RGPD, DSA, DMA, ARCEP etc.) dans chacune des actions de préparation - Mise en place d'un niveau adapté de résilience numérique en fonction des priorités - Constitution d'une équipe de cellule de crise en fonction des risques prioritaires - Identification d'une stratégie de continuité et de reprise d'activité - Identification des activités critiques - Listage des ressources - Évaluation des divers scénarios	C.25. Rédiger un plan d'action de gestion de crise, par la collecte des moyens et services essentiels à son fonctionnement, en respectant le cadre normatif, réglementaire et législatif, par l'analyse de la résilience des services selon différents scénarios afin de permettre aux parties prenantes de l'organisation de définir les ressources allouables à l'établissement d'une cellule de crise selon ses moyens et priorités.	**M.14. - Mise en situation professionnelle :** Préparation à une crise cyber Le candidat doit démontrer, individuellement, qu'il est apte à préparer avec efficacité une crise cyber. Une plateforme technique permet de simuler les infrastructures numériques de l'organisation attaquée. Le candidat doit mettre en place des outils avant la crise (niveau de résilience, annuaires, fiches de compte rendu, cartographie du système d'information).	**Partie 1** • Le cadre législatif, normatif et règlementaire est appliqué. • Les ressources sont listées. • Le niveau de résilience défini est adapté au contexte et justifié. • Le choix des outils de gestion de crise est pertinent. • Les outils sélectionnés et utilisés sont justifiés. • Les protocoles rédigés sont adaptés aux enjeux de l'organisation. • Le document rédigé est synthétique, clair et adapté à un public non technique.

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

- Identification de solutions pour maintenir l'activité (logicielles, prestataires, institutionnelles, etc.) - Rédaction d'un plan de gestion de crise, protocole à suivre en cas d'incident (organisation humaine, logistique, matérielle, logicielle, financière, etc.) - Rédaction d'un protocole de communication de crise - Rédaction d'un plan de continuité et de reprise d'activité - Validation auprès de la direction - Conduite d'entraînements - Sensibilisation des membres de l'équipe et la procédure à suivre en cas d'incident et aux signaux faibles pré-crise	C.26. Maintenir à jour le plan de gestion de crise, par l'entretien régulier des moyens (matériels et documentations) participant à la résilience de l'organisation, par la sensibilisation continue des acteurs concernés, et par la conduite d'exercices à grande échelle, pour garantir la fourniture d'une réponse rapide et adaptée de la part de la cellule de crise.	**M.15. - Questionnaires à visée professionnelle :** Prévenir une cyber crise Le candidat doit, individuellement, répondre à un questionnaire portant sur sa capacité à maintenir à jour une stratégie de gestion de crise pour être en mesure de réagir en cas de cyberattaque. Le questionnaire est composé de mini-cas relatifs à une ou des organisations. Cet examen se déroule en centre d'examen.	• Les différentes parties prenantes de la politique de sécurité et du maintien en conditions opérationnelles sont identifiées. • Les enjeux et moyens de sensibilisations des différentes parties prenantes sont cohérents vis-à-vis de la règlementation. • La conduite d'exercice d'entraînement est mentionnée. • Les différents protocoles sont connus et identifiés.

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

<table>
<tr>
<td rowspan="2">A.13. Faire face à un incident
- Déploiement des protocoles définis (PGC, PCA, PRA, PCC, etc.)
- Recueillir l'ensemble des informations de la crise pour rendre l'organisation plus résiliente
- Organisation d'une réunion de crise
- Communication écrite et orale auprès les membres de la cellule de crise
- Alerte des personnels et institutions concernées
- Prise en compte des systèmes d'information
- Prise en compte des procédures métiers
- Saisie du matériel pour obtenir les données à analyser
- Collecte des informations techniques
- Rédaction d'un historique des événements
- Identification d'un scénario hypothétique
- Recherche des indicateurs de compromission
- Analyse des relevés techniques réalisés
- Test du scénario au regard des éléments d'investigation
- Réfutation de l'hypothèse
- Proposition d'une nouvelle hypothèse
- Validation de l'hypothèse (du scénario final)
- Constitution d'un dossier de preuve
- Application du cadre normatif, règlementaire et législatif (Loi Godfrain, CNIL, ANSSI, LPM, RGPD, DSA, DMA, ARCEP, etc.)
- Rédaction du rapport d'investigation</td>
<td>C.27. Appliquer un protocole de réponse à une crise par la mobilisation de tous les acteurs et moyen pouvant participer à l'endiguement de l'incident et/ou la protection et la sauvegarde des fonctions sensibles du système d'information, par la mise en place d'un canal de communication régulier, fluide et contrôlé, le partage d'éléments d'information adaptés, afin de permettre la sortie progressive de crise.</td>
<td rowspan="2">M.16. - Mise en situation professionnelle reconstituée – Jeu de rôle :
Gestion de crise cyber

À l'occasion d'un exercice s'étalant sur cinq jours, le candidat doit démontrer, individuellement, qu'il est apte à conduire avec efficacité une crise cyber.
Une plateforme technique permet de simuler les infrastructures numériques de l'organisation attaquée. Des encadrants jouent le rôle des acteurs de la crise (directions, métiers, média,).

Partie 1 : jeu de rôle – Wargame (C27)
Dans un environnement adapté (réseaux et parc de machines d'entreprise simulés), le candidat en groupe de 4 à 6 personnes est amené à gérer une situation de crise (scénarios variés : attaques de type ransomware, pannes matérielles, etc.).
Le candidat doit se coordonner avec les membres de son groupe pour élaborer une stratégie dans le but de relancer/maintenir les activités de l'entreprise.
Le candidat doit comprendre la nature technique de la crise et commencer le dialogue avec les acteurs clés de la crise (direction de l'organisation attaquées, personnels représentants les métiers attaqués, médias, clients et sous-traitants).
Lors d'un entretien auprès d'un jury, le candidat doit présenter l'ensemble des modalités à dérouler et justifier son propos au regard de la crise, des enjeux du contexte</td>
<td>Partie 1 :
• Le comportement des candidats (gestion du stress, pragmatisme) est adapté à une situation de crise.
• La situation de crise est abordée avec sang-froid et sérénité dans les échanges avec les acteurs.
• La créativité et la rapidité d'exécution face à un nouveau problème est adaptée au contexte de crise et au milieu professionnel.
• La règlementation et les normes sont prises en compte.
• La communication de crise est adaptée aux enjeux internes et externes de l'organisation.
• Les priorités sont identifiées.
• Une posture professionnelle est adoptée :
• Le vocabulaire utilisé est précis.
• Le discours est organisé.
• Le langage non-verbal favorise l'attention de son auditoire (voix audible, débit adapté, regarde son auditoire durant l'échange, se tient droit, etc.).
• Un support de présentation qualitatif est créé :
• Les données présentées sont claires et lisibles.
• Le support ne contient pas de faute d'orthographe.
• Les indications données aux acteurs sont claires et concises.</td>
</tr>
<tr>
<td>C.28. Procéder à la recherche d'éléments de preuve techniques grâce à une méthodologie</td>
<td>Partie 2 :
• Les prélèvements et l'investigation numériques sont réalisés avec succès.</td>
</tr>
</table>

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

	d'investigation et d'outils d'analyse forensique (Volatility par exemple), par l'utilisation de la rétro-ingénierie (*reverse engineering)* et l'étude des comportements tracés dans des journaux et par la rédaction d'un rapport, afin de déterminer les marqueurs facilitant la détection de l'attaque et son élimination (contre-mesures).	de l'organisation et des priorités afin de limiter les perturbations de l'activité. **Partie 2 :** identification et maîtrise de l'attaque (C28) Le candidat doit, individuellement, identifier l'attaquer et lancer l'analyse à l'aide d'outils. Le candidat doit déterminer les impacts techniques et opérationnels de l'attaque et effectuer des prélèvements numériques et une investigation numérique. Le candidat doit remettre un rapport d'investigation rédigé en fournissant des preuves techniques afin d'engager des poursuites judiciaires, et établir une note sur les impacts liés à cet incident. **Partie 3 :** remédiation de la crise (C29) Le candidat doit, de nouveau en groupe de 4 à 6 personnes, remettre en service le système d'information impacté en déroulant un plan de reprise d'activité. Le candidat doit rédiger un rapport et proposer des mesures techniques et organisationnelles permettant de renforcer la résilience de l'organisation. Il propose d'éventuelles suites judiciaires.	• Les outils techniques et les approches humaines/*social engineering* ont permis la détection et mitigation des attaques. • Le cadre législatif, normatif et règlementaire est appliqué dans le rapport. • Le rapport présente une hypothèse validée • Le rapport technique écrit est complet et la synthèse écrite est précise et intelligible pour du personnel non spécialiste. • Le support ne contient pas de faute d'orthographe.
A.14. Restaurer les systèmes en appliquant un plan de continuité d'activité et/ou de reprise d'activité - Déploiement du plan de reprise - Coordination avec les parties prenantes (direction, métiers, DSI, RSSI, acteurs externes, etc.) - Application de contre-mesures - Remise en service des équipements - Rédaction d'une analyse et d'un bilan sur les impacts de la crise - Préconisation des mesures de contournement et de remédiation de l'incident - Retour d'expérience et amélioration continue	C.29. Déployer une stratégie de reprise d'activité à la suite d'un contexte de crise/d'incident par l'utilisation des mécanismes de restauration des sauvegardes existantes, par la remise en service des équipements et par l'application des contre-mesures déterminées sur l'ensemble du système d'exploitation afin de retrouver un niveau de fonctionnement et de sécurité équivalent ou supérieur au niveau pré-crise.		**Partie 3 :** • La coordination avec l'ensemble des acteurs est prise en compte. • La communication de crise est adaptée. • Les services et équipements sont remis en service correctement. • La remédiation est réussie. • Le retour d'expérience est pertinent. • Le cadre législatif, normatif et règlementaire est appliqué et cité dans le rapport.

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

- Mise à jour des indicateurs de performance - Mise à jour des protocoles définis (PGC, PCA, PRA, PCC, etc.)	C.30. Enrichir les plans de continuité et de reprise d'activité par la consolidation des éléments de preuve et relevés techniques, par la mise en perspective de ces éléments avec des référentiels (indicateurs de performance, référentiels et réglementations applicables), par l'établissement d'un bilan post-crise et la mise à jour et le renforcement des procédures et des outils du système d'information à l'aide des conclusions tirées de l'analyse post-crise pour rendre plus réactives et performantes les réponses à incident futurs.	L'environnement technique simulé et l'ensemble des ressources documentaires est fourni par l'organisme de formation. Cet examen se déroule en centre d'examen. Le candidat est au courant de la période mais pas de la date exacte.	• Les indicateurs de performance sont pertinents ; • Une posture professionnelle est adoptée : • Le vocabulaire utilisé est précis. • Le discours est organisé. • Le langage non-verbal favorise l'attention de son auditoire (voix audible, débit adapté, regarde son auditoire durant l'échange, se tient droit, etc.). • Un support de présentation qualitatif est créé : les données présentées sont claires et lisibles. • Le support ne contient pas de faute d'orthographe. • Les indications données aux acteurs sont claires et concises.

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

Nota Bene : L'évaluation du bloc de compétences est réalisée via des modalités spécifiques d'évaluation détaillées dans le référentiel. La réussite de ce bloc de compétences fait l'objet de la remise d'un certificat.

Le titre de Gestionnaire de la sécurité des données, des réseaux et des systèmes est quant à lui **obtenu si le candidat obtient l'ensemble des blocs de compétences** compris au sein de la certification et qu'il réussit les évaluations transverses ci-dessous :

• Le mémoire de recherche et professionnel de fin d'étude ;
• La soutenance orale relative à son mémoire.