

REFERENTIEL DE COMPETENCES ET DE CERTIFICATIONS METIER
INTITULE DU METIER : EXPERT CYBERSECURITE ET CYBERDEFENSE

Candidat en situation de handicap : Tout candidat peut saisir le référent handicap du certificateur pour aménager les modalités d'évaluation et obtenir l'assistance d'un tiers lors de l'évaluation. Les supports et le matériel nécessaires à la réalisation des évaluations pourront être adaptés. Sur le conseil du référent Handicap et dans le respect des spécifications du référentiel, le format de la modalité pourra être adaptée. En fonction du handicap et des besoins spécifiques du candidat, le référent handicap pourra également s'appuyer sur une expertise externe.

Ces possibilités d'aménagement seront fixées dès l'entrée en formation et communiquées au futur candidat, afin que celui-ci puisse être informé des solutions en compensation.

Le métier s'articule autour des 4 blocs de compétences suivants :

Bloc 1 : Elaborer une stratégie de sécurité des systèmes d'information d'une organisation en adéquation avec son environnement et ses risques

Bloc 2 : Mettre en place les outils techniques nécessaires à la sécurisation du système d'information d'une organisation

Bloc 3 : Suivre l'évolution du niveau de sécurité du système d'information d'une organisation

Bloc 4 : Organiser une réponse adaptée en cas de crise impactant une organisation

Prérequis à l'entrée en formation :

Être titulaire d'un diplôme de niveau 6 ou équivalent dans le domaine du numérique (informatique, systèmes d'information, réseaux et systèmes, etc.). Un test de positionnement et un entretien d'admission sont effectués pour chaque candidat.

Toute candidature de candidats ayant un niveau inférieur à celui requis pourront être étudiées, dans ce cas des tests techniques plus poussés seront imposés.

Vérification du prérequis lors de l'inscription :

- Étude du dossier académique du candidat (diplômes obtenus) afin de confirmer la détention d'un diplôme de niveau 6 ou équivalent dans le domaine du numérique (informatique, systèmes d'information, réseaux et systèmes, etc.).
- Analyse du parcours professionnel le cas échéant, notamment des expériences en lien avec l'informatique et la cybersécurité.
- Test de positionnement visant à déterminer le niveau du candidat.
- Entretien d'admission visant à évaluer la motivation, l'adéquation du projet professionnel du candidat avec les objectifs de la certification, ainsi que ses connaissances générales dans le domaine.

REFERENTIEL D'ACTIVITES	REFERENTIEL DE COMPETENCES METIER	REFERENTIEL D'EVALUATION	
		MODALITES D'ÉVALUATION	CRITERES D'ÉVALUATION
1. Elaboration d'une politique de sécurité des systèmes d'information d'une organisation en adéquation avec son environnement et ses risques			
<p>A1.1 Étude du contexte de l'organisation (A1.1.C1 et A1.1.C2)</p> <ul style="list-style-type: none"> - 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.), des normes, politiques et procédures internes, notamment celles liées aux situations de handicap et à la RSE - 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, sociétal et 	<p>A1.1.C1. Identifier les enjeux stratégiques de la cyberdéfense d'une organisation, en s'appuyant sur l'appréhension des normes et procédures internes, des textes législatifs, 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.</p> <p>A1.1.C2. 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/cyberdéfense, afin d'anticiper la stratégie cyber et garantir la protection des intérêts de l'organisation dans son contexte propre.</p>	<p>Type d'évaluation : Mise en situation professionnelle portant sur l'élaboration d'une politique de sécurité du SI d'une organisation</p> <p>Il est remis au candidat un dossier technique présentant le contexte d'une organisation fictive confrontée à des besoins de structuration et de sécurisation de son système d'information.</p> <p>Le candidat, en tant qu'expert, est chargé de proposer une politique de sécurité adaptée à l'environnement, aux risques et aux objectifs de l'organisation.</p> <p>La mise en situation professionnelle donne lieu à la production des livrables suivants :</p> <ul style="list-style-type: none"> • Une note d'analyse de l'environnement et des enjeux cyber de l'organisation, présentant les éléments utiles à la 	<p>Pour A1.1.C1</p> <p>Cr1. La note présente au moins 3 obligations ou normes explicitement rattachées aux activités critiques de l'organisation, avec une analyse de leur impact sur le SI</p> <p>Cr2. Les enjeux cybersécurité sont qualifiés par niveau d'impact (stratégique, opérationnel, juridique...) et contextualisés selon les objectifs de l'organisation.</p> <p>Cr3. Les interactions entre acteurs internes et externes sont décrites de manière structurée, avec identification des zones de responsabilité ou de dépendance en matière de sécurité.</p> <p>Cr4. La présentation des enjeux stratégiques distingue les éléments systémiques (long terme) des vulnérabilités conjoncturelles ou spécifiques à</p>

<p>concurrentiel dans lequel l'organisation évolue</p> <ul style="list-style-type: none"> - Définition d'un objectif de plan de recherche -Collecte d'informations au regard de l'objectif défini 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 - Elaboration de rapports d'analyse en lien avec le contexte cyber interne et concurrentiel de l'organisation <p>A1.1.2 Analyse du risque numérique d'une organisation (A1.2.C1 et A1.2.C2)</p> <ul style="list-style-type: none"> - Application des lignes directrices des normes applicables tout au long de l'analyse, notamment la norme ISO 27005 - Utilisation de guides et outils spécifiques, notamment issus de la méthode EBIOS Risk Manager - Organisation d'ateliers de travail avec les différents acteurs (direction, métiers, DSI, RSSI) 	<p>A1.2.C1. Mettre en œuvre une méthode d'analyse du risque numérique, en déterminant l'objet d'étude et les parties prenantes (partenaires, filiales, sous-traitants...), en analysant les usages (notamment l'IA) et les procédures métiers et en catégorisant ces vulnérabilités par niveau de gravité (par rapport au cadre normatif et réglementaire applicable, à l'éthique...), afin de déceler les failles et les vulnérabilités de l'organisation.</p> <p>A1.2.C2. 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 et par la prise en compte de ses moyens (financiers, humains...), afin de permettre l'adoption d'une politique cyber adaptée à l'organisation et à ses activités.</p>	<p>compréhension du contexte (en lien avec A1.1.C1 et A1.1.C2),</p> <ul style="list-style-type: none"> • Un rapport d'analyse de risque numérique, structuré selon une méthode reconnue intégrant une proposition de mesures de sécurité adaptées au contexte de l'organisation (en lien avec A1.2.C1 et A1.2.C2), • La formulation d'une proposition de politique de sécurité du SI de l'organisation (en lien avec A1.3.C1) <p>A l'oral, le candidat soutient son rapport sous la forme d'un pitch à destination de décideurs de l'entreprise, représentés par les membres du jury. Il est attendu du candidat qu'il justifie la politique proposée et ses recommandations, au regard du contexte et des enjeux spécifiques de l'entreprise (en lien avec A1.3.C2).</p> <p>Le candidat échange ensuite avec le jury et répond à ses questions, notamment sur la prise en compte des enjeux sociétaux dans les analyses réalisées et la politique de sécurité définie.</p>	<p>l'organisation, avec des critères de hiérarchisation argumentés.</p> <p>Pour A1.1.C2</p> <p>Cr1. La méthodologie de collecte et d'analyse est formalisée (étapes, outils, sources...). Elle mobilise au minimum 3 sources distinctes, croisées.</p> <p>Cr2. Les éléments de contexte (risques géopolitiques, pression concurrentielle, exposition médiatique, dépendances technologiques...) sont mis en lien avec les vulnérabilités ou menaces identifiées.</p> <p>Cr3. Les priorités stratégiques en matière de cybersécurité sont formulées en cohérence avec les orientations de l'organisation (développement, innovation, conformité...) et justifiées à partir des risques et des capacités internes.</p> <p>Cr4. L'analyse de l'environnement met en lumière au moins un facteur d'évolution (réglementaire, technologique, sociétal...) susceptible d'impacter la stratégie de sécurisation à court ou moyen terme.</p>
--	---	---	---

- 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 sur l'organisation, ses collaborateurs et ses partenaires/clients
- 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 réglementaire et normatif
- 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 cyberattaquants, chemins d'attaque

Pour A1.2.C1

Cr1. L'analyse de risque suit une méthode formalisée et en respecte les étapes.

Cr2. Les vulnérabilités identifiées couvrent au moins 3 dimensions : technique, organisationnelle et humaine.

Cr3. Les scénarios d'attaque proposés sont contextualisés et chacun est associé à un événement redouté avec un niveau de gravité argumenté.

Cr4. Au moins un risque lié à des usages innovants (comme l'IA) est intégré à l'analyse.

Pour A1.2.C2

Cr1. Les mesures de sécurité proposées sont reliées de manière directe aux risques identifiés et sont décrites de façon opérationnelle

Cr2. La cartographie des menaces comprend au moins 2 scénarios distincts.

Cr3. Les risques résiduels sont qualifiés par niveau et accompagnés d'un arbitrage

<p>qu'une source de risque peut emprunter) et opérationnels</p> <ul style="list-style-type: none"> - Elaboration de rapports d'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 et de l'environnement - Apport d'éléments d'arbitrage quant à l'acceptation ou non des risques résiduels <p>A1.3. Élaboration d'une politique et d'une organisation cyber adaptées au contexte de l'organisation (A1.3.C1 et A1.3.C2)</p> <ul style="list-style-type: none"> - 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 	<p>A1.3.C1. 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, notamment en matière environnementale, 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 SI.</p> <p>A1.3.C2. Communiquer régulièrement auprès de l'ensemble des acteurs d'une organisation sur les enjeux cyber, 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.</p>		<p>justifié au regard des contraintes de l'organisation.</p> <p>Cr4. Au moins une mesure prend explicitement en compte les enjeux sociétaux (accessibilité, protection des personnes, RSE...).</p> <p>Pour A1.3.C1</p> <p>Cr1. La politique formalisée comprend au moins : objectifs, périmètre, responsabilités, règles de sécurité, modalités de suivi.</p> <p>Cr2. Les responsabilités sont affectées par niveau (direction, DSI, métiers, prestataires...) et accompagnées d'indicateurs de contrôle.</p> <p>Cr3. Le cadre de suivi proposé (audit, indicateurs, fréquence...) est structuré et exploitable.</p> <p>Cr4. La politique comporte au moins une mesure visant à intégrer des enjeux de transition écologique, d'accessibilité et de sécurité des personnes.</p> <p>Pour A1.3.C2</p> <p>Cr1. Les choix formulés dans la politique de sécurité sont mis en</p>
--	---	--	--

normes s'y rattachant (référentiel général d'amélioration de l'accessibilité (RGAA), 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 SI
- 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

lien direct avec les enjeux de cybersécurité propres à l'organisation, en justifiant les mesures par les risques identifiés et les priorités stratégiques.

Cr2. Au moins un exemple illustrant les impacts concrets de la politique de sécurité sur les activités ou usages de l'organisation est mobilisé.

Cr3. Les messages délivrés dans le pitch sont structurés selon les besoins spécifiques des profils représentés (décisionnels, opérationnels, métiers, situation de handicap...) et de leur niveau de compréhension technique.

<ul style="list-style-type: none"> - 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 (français et anglais) 			
---	--	--	--

2. Mise en place des outils nécessaires à la sécurisation du système d'information d'une organisation

<p>A2.1. Définition d'architectures sécurisées (A2.1.C1 à A2.1.C3)</p> <ul style="list-style-type: none"> - Application des textes juridiques de la cyberdéfense, de la législation liée à la cybercriminalité, des normes et des textes réglementaires (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 SI - Identification des besoins en cybersécurité - Identification du matériel sécurisé en termes de 	<p>A2.1.C1. Identifier les équipements (logiciels, solutions d'IA, 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 événements ou à automatiser les actions, afin de constituer un catalogue d'éléments de sécurisation adaptés aux capacités, moyens et enjeux de l'organisation.</p> <p>A2.1.C2. Rédiger un cahier des charges fonctionnel portant sur un projet de sécurisation du SI, en tenant compte de l'existant, des besoins métiers et des priorités de l'organisation (politique RSE, de responsabilité/hygiène numérique...), en formulant des préconisations de matériels et logiciels conformes à l'état de l'art, à la réglementation et aux normes, afin de traduire les enjeux de l'organisation et des exigences en termes de sécurité, de façon adaptée et pérenne.</p>	<p>E1 – Type d'évaluation : Mise en situation professionnelle portant sur la conception d'une architecture de sécurisation du SI d'une organisation et la planification de son déploiement</p> <p>Il est présenté au candidat un cas portant sur une organisation fictive ou réelle souhaitant structurer la sécurisation de son SI. Le candidat, mobilisé dès la phase de cadrage du projet, est chargé de concevoir l'architecture de sécurisation cible et d'élaborer le plan de pilotage associé.</p> <p>Dans ce cadre, il est demandé au candidat de produire un dossier technique comprenant :</p> <ul style="list-style-type: none"> • Une analyse comparative d'équipements, outils logiciels et matériels permettant de répondre 	<p>Pour A2.1.C1</p> <p>Cr1. L'analyse comparative retient au moins 3 solutions logicielles, matérielles ou mixtes, avec des critères de sélection définis (performance, certification, intégrabilité...).</p> <p>Cr2. Les vulnérabilités identifiées pour chaque solution sont documentées à partir de sources vérifiables.</p> <p>Cr3. Les solutions préconisées sont compatibles avec les capacités opérationnelles de l'organisation (ressources humaines, infrastructure, budget...).</p> <p>Cr4. Les solutions proposées s'intègrent dans une architecture</p>
--	--	---	--

<p>connectivité, de sécurité réseau, de sécurité des systèmes d'exploitation et de stockage, en fonction des qualifications (CSPN de l'ANSSI, EAL, Critères communs)</p> <ul style="list-style-type: none"> - 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.) dans le respect des normes et politiques internes, notamment en matière environnementale - Déploiement d'une architecture logicielle - Rédaction de documentation liée à l'usage des outils - Présentation du projet aux parties prenantes <p>A2.2. Utilisation de la cryptologie et des outils cryptographiques pour</p>	<p>A2.1.C3. 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 SI, afin d'établir la cartographie de l'architecture de sécurisation du SI à mettre en place.</p> <p>A2.2.C1. Déterminer les différentes solutions de chiffrements symétriques et asymétriques par l'étude de la cryptologie et 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).</p>	<p>aux besoins de sécurisation identifiés (en lien avec A2.1.C1),</p> <ul style="list-style-type: none"> • Un cahier des charges fonctionnel de sécurisation, tenant compte des ressources existantes, des priorités métiers, de la réglementation en vigueur, des politiques internes/normes (RSE, accessibilité, sobriété numérique...) et des exigences techniques et organisationnelles (en lien avec A2.1.C2), • Une modélisation des flux d'information et des traitements du SI, formalisée sous forme de cartographie d'architecture technique cible, décrivant les interactions entre briques logicielles et matérielles de sécurisation (en lien avec A2.1.C3). <p>En complément, le candidat élabore un plan de pilotage du projet de sécurisation, composé :</p> <ul style="list-style-type: none"> • Du plan de gestion de projet précisant : jalons, ressources humaines et techniques, méthode de pilotage, outils de suivi, indicateurs de performance et modalités d'ajustement envisagés 	<p>de supervision cohérente explicitement décrite.</p> <p>Pour A2.1.C2</p> <p>Cr1. Le cahier des charges précise les exigences de sécurité en lien avec les besoins métiers, avec au moins 4 exigences exprimées en termes mesurables (taux de disponibilité, chiffrement, authentification, supervision...).</p> <p>Cr2. Les contraintes réglementaires, RSE et d'accessibilité sont prises en compte.</p> <p>Cr3. Les recommandations techniques sont conformes à l'état de l'art et alignées sur les normes et bonnes pratiques (ISO, ANSSI, etc.).</p> <p>Cr4. Les scénarios d'usage sont exploitables et liés à des profils d'utilisateurs ou de services dans l'organisation.</p> <p>Pour A2.1.C3</p> <p>Cr1. La modélisation représente les échanges entre les briques du SI (matérielles ou logicielles), avec une légende lisible et une cohérence d'ensemble.</p>
---	--	---	---

<p>A2.3. Sécurisation des développements DevSecOps¹ et des infrastructures (A2.3.C1 et A2.3.C2)</p> <ul style="list-style-type: none"> - 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 - 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 face à différents types d'attaques (dépassements mémoire, 	<p>d'outils logiciels conformes à la politique de sécurité de l'organisation.</p> <p>A2.3.C2. Organiser des tests de sécurité, au travers de simulations d'attaques et de réponses (dépassements mémoire, injections, bruteforce...), avec et sans recours à l'IA, à l'encontre des infrastructures de développement (usine de développement), d'hébergement en production et des interfaces des solutions du SI pour identifier des faiblesses et vulnérabilités, anticiper les réponses possibles et garantir le maintien au niveau de sécurité attendu de l'organisation.</p> <p>A2.4.C1. Déployer des outils méthodologiques dans un cadre de projet de sécurisation d'un SI, grâce à la sélection d'une méthode de gestion de projet (Agile, cycle en V) et à la mobilisation responsable des outils d'organisation, de suivi et d'IA, en prenant en compte les normes applicables</p>	<p>Dans ce cadre, il est attendu qu'il :</p> <ul style="list-style-type: none"> • Justifie la solution de chiffrement symétrique et asymétrique retenue au regard des besoins de confidentialité, d'intégrité et d'authenticité de l'organisation (en lien avec A2.2.C1), • Décrit le déploiement de l'infrastructure de gestion de clés, les outils utilisés et leur intégration dans l'environnement de l'organisation (en lien avec A2.2.C2), • Décrit la chaîne de développement sécurisé mise en œuvre : pipeline CI/CD utilisé, outils de test de sécurité intégrés, bonnes pratiques appliquées, intégration d'outils exploitant l'IA pour l'analyse de code ou détection de vulnérabilités (en lien avec A2.3.C1), • Présente une synthèse du rapport d'analyse des tests de sécurité réalisés avec et sans recours à l'IA : scénarios simulés, résultats obtenus, vulnérabilités identifiées, recommandations (en lien avec A2.3.C2). 	<p>conformité, avec des seuils de déclenchement d'alerte définis.</p> <p>Cr4. La planification intègre des marges d'ajustement pour aléas techniques ou humains, en cohérence avec le degré d'incertitude du projet.</p> <p>Cr5. Les normes mobilisées (qualité, sécurité, environnement) sont contextualisées et appliquées dans la définition des livrables ou des étapes clés.</p> <p>Pour A2.4.C2</p> <p>Cr1. Le dispositif de suivi permet d'identifier les signaux faibles de dérive (retard, surcharge, défaut de qualité), à partir de données quantitatives et qualitatives croisées.</p> <p>Cr2. Les outils d'évaluation mobilisés permettent une lecture différenciée par profil d'intervenant (technicien, responsable sécurité...) et s'inscrivent dans un rythme d'analyse adapté aux jalons du projet.</p> <p>Cr3. Les ajustements proposés sont fondés sur une analyse</p>
--	---	--	---

<p>injections, etc.) et simulation des réponses associées</p> <p>A2.4. Management d'un projet portant sur la sécurisation d'un système d'information (SI) (A2.4.C1 et A2.4.C2)</p> <ul style="list-style-type: none"> - 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 - Organisation et distribution des tâches au sein des équipes techniques - Prise en compte des critères de la norme de management environnemental (ISO 14001) - - Prise en compte des situations de handicap et des normes s'y rattachant (référentiel général 	<p>(ISO 9001, 14001...), afin de garantir les conditions les plus favorables à son orchestration.</p> <p>A2.4.C2. Faciliter la résolution des difficultés pouvant mettre en péril la réussite du projet, en mettant en œuvre un suivi régulier des réalisations des équipes à chaque étape/jalon, via des entretiens individuels, des outils numériques (planification, automatisation, suivi général de type Gantt...) et des grilles d'évaluation, pour assurer le déroulement du projet dans le respect du cahier des charges/du rétroplanning défini et des exigences spécifiques aux profils des acteurs mobilisés (situations de handicap, limites/interdépendances de compétences, risques de RPS...).</p>	<p>La soutenance permettra également d'évaluer la capacité du candidat à articuler les aspects techniques et réglementaires tout en prenant en compte les enjeux sociétaux, et à restituer ses travaux de façon exploitable.</p>	<p>explicite des causes des écarts observés (et non seulement sur une réaction automatique à des indicateurs).</p> <p>Cr4. Les modalités d'adaptation pour les profils spécifiques (PSH, profils à expertise limitée, profils à forte dépendance interfonctionnelle...) sont adaptées au contexte et réalistes.</p> <p>Pour A2.2.C1</p> <p>Cr1. L'analyse comparative justifie le choix de l'algorithme en fonction des objectifs de sécurité visés, des contraintes de l'organisation et du contexte technique.</p> <p>Cr2. Les critères de sélection incluent des éléments de robustesse, de performance, de conformité réglementaire et de soutenabilité (écosystème, maintenance, coût énergétique...).</p> <p>Cr3. Les solutions non retenues sont évaluées de manière critique, avec une explicitation des cas où elles pourraient être préférables dans un autre contexte.</p>
--	--	--	--

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 (DSI, DG, équipes techniques)
- Réalisation d'entretiens individuels avec les membres des équipes techniques
- Élaboration de grilles d'évaluation du projet

Pour A2.2.C2

Cr1. L'architecture de gestion de clés déployée permet une intégration fluide avec les services et processus identifiés dans le SI cible. Au moins 2 points d'usage sont couverts (signature, chiffrement de données, authentification...).

Cr2. Le niveau de sécurité de l'AC mise en œuvre est évalué par rapport aux standards actuels. Les mécanismes de renouvellement, révocation et journalisation sont décrits.

Cr3. La prise en compte des exigences sociétales est intégrée dans la configuration (niveau d'accessibilité des outils, sobriété énergétique, facilité d'usage pour les utilisateurs finaux...).

Pour A2.3.C1

Cr1. Le pipeline mis en œuvre assure une chaîne de traitement complète (build, test, intégration, livraison), dans laquelle les actions de sécurité sont visibles, documentées et déclenchées automatiquement.

			<p>Cr2. Les outils de sécurité intégrés sont pertinents au regard des risques projetés et positionnés dans le bon segment de la chaîne.</p> <p>Cr3. L'intégration de composants basés sur l'IA est justifiée par une valeur ajoutée mesurable (réduction des faux positifs, priorisation, optimisation de code...).</p> <p>Cr4. La configuration de la chaîne CI/CD garantit la traçabilité des actions et la reproductibilité des déploiements sécurisés.</p> <p>Pour A2.3.C2</p> <p>Cr1. Les scénarios de tests mettent en œuvre des vecteurs d'attaque variés, incluant au moins une simulation exploitant un comportement non trivial</p> <p>Cr2. Les vulnérabilités détectées sont classées selon leur gravité, leur exploitabilité et leur exposition réelle, avec une méthode reconnue.</p> <p>Cr3. Les recommandations issues des tests sont formulées</p>
--	--	--	---

en fonction de leur faisabilité, de leur impact sur la continuité métier et de leur capacité à prévenir une ré-exploitation future.

3. Suivi de l'évolution du niveau de sécurité d'un système d'information d'une organisation

A3.1. Mise en œuvre d'audits organisationnels et techniques (A3.1.C1 à A3.1.C3)

- Prise en compte du référentiel PASSI²
- 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 SI interne à l'organisation
- Vérification de la conformité des pratiques de sécurité et de la corrélation avec les règles internes de la configuration des divers outils (équipements réseau, OS, applications, etc.)
- Analyse du code source
- Réalisation de tests d'intrusion
- Respect du SI audité (maîtrise des règles d'engagement, utilisation d'outils techniques)

A3.1.C1. Réaliser un audit des SI 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 SI.

A3.1.C2. Présenter les conclusions d'un audit des SI 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 réglementaire applicable (RSE...), en identifiant des axes d'amélioration réalistes afin de proposer des recommandations contribuant à l'élévation du niveau de sécurité de l'organisation ou permettant d'obtenir son homologation de sécurité.

A3.1.C3. Intégrer la conduite de changement du SI de l'organisation par l'établissement d'une veille sur les modifications à venir, la conduite d'audit sur les nouveaux outils et processus à mettre en place, pour garantir l'adoption et l'application continue de la politique de sécurisation du SI dans le contexte

Type d'évaluation : Mise en situation professionnelle portant sur l'audit, la supervision et l'amélioration continue de la cybersécurité d'un SI

Il est présenté au candidat un cas dans lequel une organisation fictive ou réelle souhaite évaluer la maturité de la sécurité de son SI, mettre en place un dispositif de supervision adapté et structurer une démarche de maintien en condition de sécurité et d'amélioration continue.

Le candidat est chargé de produire un audit technique et organisationnel, d'identifier les vulnérabilités et les écarts, de proposer des outils et indicateurs de supervision et de formaliser une démarche d'anticipation stratégique des évolutions du SI.

Dans ce cadre, il produit un dossier écrit comprenant :

Pour A3.1.C1

Cr1. Le plan d'audit définit une méthode cohérente avec les objectifs fixés, en s'appuyant sur un référentiel reconnu et couvre l'ensemble du périmètre identifié.

Cr2. Les éléments audités (architecture, configurations, pratiques, code source, processus...) sont choisis en fonction de leur criticité et de leur exposition au risque.

Cr3. Les outils et techniques d'audit (scanning, intrusion simulée, revue de code, observation terrain...) sont mobilisés à bon escient et documentés.

Cr4. Les règles d'engagement et de respect du SI audité sont

<p>maîtrisés) - Identification des axes d'amélioration, des failles de sécurité</p> <ul style="list-style-type: none"> - Proposition et recommandation d'éléments d'amélioration - Elaboration d'un rapport d'audit et présentation des résultats aux parties prenantes (en fonction de l'audit) <p>A3.2. Mise en place d'une organisation pour la supervision des systèmes d'information (SI) (A3.2.C1 et A3.2.C2)</p> <ul style="list-style-type: none"> - Intégration d'un SIEM au sein du SOC³ - Exploitation de sondes de sécurité - Surveillance de pare-feu - Exploitation d'une solution EDR⁴ - Établissement de règles de corrélations - Analyse et corrélation des logs à l'aide d'outils - Utilisation de l'IA 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 	<p>évolutif de l'organisation (nouveaux usages de l'IA, nouveaux profils de collaborateurs, nouveaux équipements pour les PSH...).</p> <p>A3.2.C1 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, EDRs, 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 SI.</p> <p>A3.2.C2. 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'IA 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 adaptés à l'incident.</p>	<ul style="list-style-type: none"> • Un plan d'audit : méthode utilisée, objectifs, éléments audités et points de contrôle sélectionnés (en lien avec A3.1.C1), • Un rapport d'audit technique et organisationnel : écarts par rapport aux référentiels internes ou normatifs, vulnérabilités détectées, axes d'amélioration identifiés et préconisations associées (en lien avec A3.1.C2), • Des préconisations visant à garantir l'adoption et l'application continue de la politique de sécurité dans le contexte d'évolution de l'entreprise (en lien avec A3.1.C3), • Une proposition de dispositif de supervision du SI (en lien avec A3.2.C1), • Une fiche d'analyse d'un incident simulé, basée sur un jeu de logs ou d'alertes fourni : origines probables, éléments techniques observés, parties impliquées, gravité évaluée et mesures correctives proposées (en lien avec A3.2.C2), • La description des actions à mettre en œuvre pour assurer la 	<p>formalisées et respectées à chaque étape de l'audit.</p> <p>Pour A3.1.C2</p> <p>Cr1. Le rapport d'audit présente des constats étayés, croisant données techniques, observations organisationnelles et indicateurs de conformité.</p> <p>Cr2. Les écarts identifiés sont reliés à des référentiels ou obligations précises (normes, politiques internes, exigences réglementaires...), avec une qualification du niveau de gravité.</p> <p>Cr3. Les recommandations proposées sont classées selon leur impact sur la sécurité globale, leur urgence et leur faisabilité.</p> <p>Pour A3.1.C3</p> <p>Cr1. Les évolutions du SI à venir sont identifiées à partir d'éléments concrets (plan de transformation, innovations, profils utilisateurs, contraintes légales...).</p> <p>Cr2. Au moins 3 préconisations pertinentes sont formulées pour accompagner ces évolutions</p>
---	--	--	---

<p>- Surveillance de l'état de la menace cyber en appliquant une CTI (Cyber Threat Intelligence) adaptée au contexte de l'entreprise</p> <p>A3.3. Maintien en condition de sécurité du système d'information (SI) (A3.3.C1 et A3.3.C2)</p> <p>- 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, du portefeuille applicatif et des utilisations faites par les parties prenantes - Veille technologique sur les outils d'attaque et d'audits utilisant l'IA</p> <p>A3.4. Mise en place d'une veille concurrentielle,</p>	<p>A3.3.C1. Assurer la mise à jour des outils matériels et logiciels au regard des processus métiers, des profils des utilisateurs (situations de handicap...) et des contraintes de l'organisation (liées à une politique économique, environnementale ...), en appliquant les nouvelles versions de logiciels, en renouvelant le parc matériel et logiciel selon les 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 SI et la protection de son utilisation/de ses utilisateurs.</p> <p>A3.3.C2. Établir un suivi actif des vulnérabilités des briques du SI, 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 SI.</p> <p>A3.4.C1. Réaliser une veille technologique, économique et sociale dans un contexte international en définissant les thèmes critiques,</p>	<p>mise à jour régulière des outils, le suivi des vulnérabilités, l'adaptation des systèmes aux usages réels et aux contraintes réglementaires (en lien avec A3.3.C1 et A3.3.C2),</p> <ul style="list-style-type: none"> • Une note de veille : thématiques critiques à surveiller, sources sélectionnées, signaux faibles analysés et impacts potentiels identifiés sur la sécurité du SI de l'organisation, dans un contexte international (en lien avec A3.4.C1 et A3.4.C2). <p>Lors d'une soutenance orale, le candidat présente ses travaux et répond aux questions du jury, notamment s'agissant de la prise en compte des enjeux sociétaux (situations de handicap, transition écologique, santé-sécurité) et de la dimension éthique dans l'utilisation de l'IA.</p>	<p>(audits préalables, mises à jour de politique, actions de communication ou de formation ciblées...).</p> <p>Cr3. Les adaptations nécessaires sont justifiées en lien avec la soutenabilité de la politique de sécurité (charge des équipes, usage d'outils, sensibilisation à la conformité...).</p> <p>Cr4. Au moins un enjeu lié à la diversité des usages (PSH, IA, profils non techniques) est intégré dans les propositions d'adaptation de la politique cyber.</p> <p>Pour A3.2.C1</p> <p>Cr1. Le dispositif proposé comprend les composants indispensables à un SOC fonctionnel : sondes, collecteurs, plateforme de supervision (SIEM), référentiel d'alertes.</p> <p>Cr2. Les signaux remontés par les outils de sécurité sont traités via des règles de corrélation pertinentes, classées selon leur criticité.</p> <p>Cr3. Les indicateurs sélectionnés</p>
--	--	---	--

<p>technologique, économique et sociale dans un contexte international (A3.3.C1 et A3.3.C2)</p> <ul style="list-style-type: none"> - Identification des thèmes et obligations à maintenir en veille - Identification de la véracité des sources - Sélection de sources d'information (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 - Analyse des signaux faibles indiquant une mutation technologique 	<p>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.</p> <p>A3.4.C2. Identifier les mutations et innovations technologiques impactant la cybersécurité et la cyberdéfense, 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 SI et participer à la défense des intérêts de l'organisation (avantage concurrentiel, protection de la propriété intellectuelle, protection des données stratégiques/sensibles des clients/des collaborateurs ...).</p>		<p>(taux d'alerte, détection, faux positifs, MTTR...) permettent un suivi opérationnel de la performance du dispositif.</p> <p>Cr4. L'intégration de l'IA est justifiée par des cas d'usage réels (détection de comportements anormaux, priorisation automatisée...).</p> <p>Pour A3.2.C2 :</p> <p>Cr1. L'analyse d'incident identifie les causes racines, les signaux précoces et la chaîne de propagation à partir d'un jeu de logs ou de données simulées.</p> <p>Cr2. Les critères de qualification des incidents sont définis (fréquence, origine, gravité, impact métier...) et appliqués de manière cohérente.</p> <p>Cr3. Le plan d'action proposé est réaliste, séquencé et adapté au niveau d'urgence évalué.</p> <p>Cr4. Le suivi de l'incident inclut la traçabilité des décisions, les interactions entre équipes et les outils de communication utilisés.</p> <p>Pour A3.3.C1</p>
---	--	--	---

			<p>Cr1. Le processus de mise à jour proposé couvre les aspects techniques et contractuels</p> <p>Cr2. Les contraintes métiers (disponibilité, compatibilité, continuité de service...) sont prises en compte dans la priorisation des mises à jour.</p> <p>Cr3. Les spécificités des profils utilisateurs, y compris en situation de handicap, sont prises en compte dans l'analyse des impacts ou des contraintes liées à l'évolution des outils.</p> <p>Cr4. La stratégie de mise à jour est articulée avec les politiques de sécurité, d'accessibilité et d'écoresponsabilité de l'organisation.</p> <p>Pour A3.3.C2</p> <p>Cr1. Le dispositif de veille sur les vulnérabilités couvre plusieurs sources (éditeurs, CERT, plateformes de sécurité...) et permet l'identification rapide des failles critiques.</p> <p>Cr2. Le processus de traitement différencie les cas nécessitant une mise à jour immédiate de</p>
--	--	--	--

			<p>ceux pouvant faire l'objet d'un arbitrage ou d'un report.</p> <p>Cr3. Les outils d'inventaire et de scoring de vulnérabilités sont mobilisés, et les niveaux de risque associés sont cohérents avec l'exposition réelle du SI.</p> <p>Pour A3.4.C1</p> <p>Cr1. La veille mobilise des sources qualifiées.</p> <p>Cr2. Les données collectées sont triées, structurées et mises en lien avec des enjeux concrets de l'organisation (menaces, opportunités, contraintes...).</p> <p>Pour A3.4.C2</p> <p>Cr1. L'analyse des signaux faibles permet d'identifier au moins 2 tendances émergentes ayant un impact potentiel sur la stratégie cyber de l'organisation.</p> <p>Cr2. Les mutations identifiées sont contextualisées par secteur, activité ou type d'acteur, avec des exemples d'applications ou de risques induits.</p> <p>Cr3. Les recommandations proposées s'appuient sur les résultats concrets de veille et</p>
--	--	--	---

anticipent les évolutions à court et moyen terme.

4. Organisation d'une réponse adaptée en cas de crise impactant une organisation

A4.1. Conception d'un plan de gestion de crise et un plan de continuité et de reprise d'activité (A4.1.C1 et A4.1.C2)

- Application du cadre normatif (politiques internes telles la RSE...), réglementaire 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
- Identification des ressources mobilisables
- Évaluation des divers scénarios

A4.1.C1. Elaborer 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 ambitions, moyens et priorités.

A4.1.C2. 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 à la protection de l'organisation et de ses collaborateurs, y compris en situation de handicap, de la part de la cellule de crise.

E1 – Type d'évaluation : Mise en situation professionnelle portant sur la préparation d'un plan de gestion de crise et d'un plan de continuité et de reprise d'activité

Il est présenté au candidat un cas dans lequel une organisation fictive ou réelle souhaite formaliser sa préparation à une éventuelle crise cyber.

Le candidat est chargé d'élaborer les différents plans nécessaires pour structurer la réponse à incident, garantir la continuité de ses activités critiques et organiser la reprise à la suite d'un sinistre, à savoir :

- Un plan de gestion de crise (en lien avec A4.1.C1),
- Un plan de continuité et de reprise d'activité (PCA/PRA) (en lien avec A4.1.C1 et A4.3.C2),
- Un dispositif d'animation et de mise à jour des plans (en lien avec A4.1.C2).

Pour A4.1.C1

Cr1. Le plan de gestion de crise établit une cartographie des fonctions critiques, des ressources et des dépendances avec des indicateurs de priorisation.

Cr2. Les scénarios envisagés permettent de tester différents niveaux de gravité et d'exposition, et sont accompagnés d'hypothèses claires.

Cr3. Les rôles, responsabilités et seuils de déclenchement sont définis, avec des procédures d'activation réalistes et compatibles avec la structure de l'organisation.

Cr4. La stratégie de continuité (PCA/PRA) est formalisée avec des jalons temporels précis et des mesures adaptables à différents contextes de crise.

<p>- Identification de solutions pour maintenir l'activité (logicielles, prestataires, institutionnelles, etc.)</p> <p>- Rédaction d'un plan de gestion de crise, protocole à suivre en cas d'incident (organisation humaine, logistique, matérielle, logicielle, financière, etc.)</p> <p>- Rédaction d'un protocole de communication de crise</p> <p>- Rédaction d'un plan de continuité et de reprise d'activité</p> <p>- Validation auprès de la direction</p> <p>- Conduite d'entraînements</p> <p>- Sensibilisation des membres de l'équipe et la procédure à suivre en cas d'incident et aux signaux faibles pré-crise</p> <p>A4.2. Prise en charge d'un incident (A4.2.C1 et A4.2.C2)</p> <p>- Déploiement des protocoles définis (PGC, PCA, PRA, PCC, etc.)</p> <p>- Recueil de l'ensemble des informations de la crise pour rendre l'organisation plus résiliente</p> <p>- Organisation d'une réunion de crise</p>	<p>A4.2.C1. Appliquer un protocole de réponse à une crise par la mobilisation de tous les acteurs et moyens pouvant participer à l'endiguement de l'incident et/ou la protection et la sauvegarde des fonctions sensibles du SI et des données associées, par la mise en place d'un canal de communication régulier, fluide et contrôlé, ainsi que le partage d'éléments d'information adaptés, afin de permettre la sortie progressive de crise.</p> <p>A4.2.C2. Procéder à la recherche d'éléments de preuve techniques grâce à une méthodologie d'investigation et d'outils d'analyse forensique (Volatility ...), par l'utilisation de la rétro-ingénierie (reverse engineering), l'étude des comportements</p>	<p>Le candidat présente ses travaux lors d'une soutenance orale, sous la forme d'un pitch face au jury représentant une Direction de crise. Il justifie ses choix organisationnels et les mesures prévues au regard des enjeux spécifiques de l'organisation, notamment la protection de ses collaborateurs, y compris en situation de handicap.</p> <p>E2 – Type d'évaluation : Mise en situation professionnelle portant sur la gestion d'un incident cyber et la remédiation post-crise</p> <p>Il est présenté au candidat le cas d'une entreprise réelle ou fictive dans laquelle un incident de sécurité majeur a été détecté.</p> <p>Il est attendu du candidat, chargé de piloter la cellule d'investigation et de remédiation, qu'il :</p> <ul style="list-style-type: none"> • Conduise une investigation technique à l'aide d'outils d'analyse forensique et de reverse engineering, formalisée dans un rapport d'investigation, avec collecte de preuves, hypothèses de compromission, validation et reconstitution du scénario 	<p>Cr5. Le plan respecte les exigences du cadre légal et réglementaire applicable.</p> <p>Pour A4.1.C2</p> <p>Cr1. Le dispositif de mise à jour est structuré autour de cycles d'évaluation, avec des indicateurs de déclenchement, des responsables désignés et une méthode de traçabilité des versions.</p> <p>Cr2. La conduite d'exercices est prévue selon des modalités réalistes et mesurables (objectifs, acteurs, déroulé, indicateurs de performance...).</p> <p>Cr3. Les actions de sensibilisation sont alignées avec les rôles et périmètres des acteurs impliqués dans le dispositif de crise.</p> <p>Cr4. Au moins une modalité de communication ou de participation spécifique est prévue pour les personnels en situation de handicap ou avec des contraintes d'accessibilité.</p> <p>Pour A4.2.C1</p>
---	---	--	--

<ul style="list-style-type: none"> - Communication écrite et orale auprès des membres de la cellule de crise - Alerte des personnels et institutions concernées - Prise en compte des SI - 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, réglementaire et législatif (Loi Godfrain, CNIL, ANSSI, LPM, RGPD, DSA, DMA, ARCEP, etc.) - Rédaction d'un rapport d'investigation 	<p>tracés dans des journaux et la rédaction d'un rapport, afin de déterminer les marqueurs facilitant la détection de l'attaque et son élimination (contre-mesures).</p> <p>A4.3.C1. 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, la</p>	<p>d'attaque (en lien avec A4.2.C1 et A4.2.C2),</p> <ul style="list-style-type: none"> • Propose une stratégie de reprise d'activité opérationnelle, incluant les actions de restauration, les contre-mesures techniques, les étapes de vérification post-redémarrage et les outils de coordination avec les acteurs métiers, techniques et décisionnels (en lien avec A4.3.C1), • Rédige un rapport post-incident synthétisant les constats techniques, les impacts métiers, les pistes de remédiation structurelles, les axes d'amélioration continue et les indicateurs à mettre en place (en lien avec A4.3.C2). 	<p>Cr1. La gestion de la crise suit une chronologie claire et structurée, avec des décisions documentées à chaque étape-clé.</p> <p>Cr2. Les points de bascule et les conditions de passage d'un mode nominal à un mode dégradé sont formalisés, avec des justifications techniques.</p> <p>Cr3. Les outils de communication et de coordination mobilisés (canaux, supports, fréquence...) assurent la fluidité de l'information et la traçabilité des échanges.</p> <p>Cr4. La gestion de la crise prend en compte les fonctions critiques du SI et les mécanismes de protection des données ou des utilisateurs.</p> <p>Pour A4.2.C2</p> <p>Cr1. Le rapport d'investigation présente une chronologie étayée par des preuves techniques (fichiers, logs, artefacts...) collectées selon une méthode rigoureuse.</p> <p>Cr2. Les hypothèses de compromission sont formulées</p>
---	--	--	--

<p>A4.3. Restauration de systèmes en application d'un plan de continuité d'activité et/ou de reprise d'activité (A4.3.C1 et A4.3.C2)</p> <ul style="list-style-type: none"> - 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 - Mise à jour des indicateurs de performance - Mise à jour des protocoles définis (PGC, PCA, PRA, PCC, etc.) 	<p>remise en service des équipements et 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.</p> <p>A4.3.C2. Enrichir les plans de continuité et de reprise d'activité par la consolidation des éléments de preuve et relevés techniques, la mise en perspective de ces éléments avec des référentiels (indicateurs de performance, référentiels et réglementations applicables), l'établissement d'un bilan post-crise et la mise à jour ou le renforcement des procédures et des outils du SI, à l'aide des conclusions tirées de l'analyse post-crise, pour rendre plus réactives et performantes les réponses à incident futurs.</p>		<p>et révisées en fonction de l'analyse des indicateurs de compromission, jusqu'à l'identification d'un scénario final cohérent.</p> <p>Cr3. Les outils d'analyse mobilisés sont justifiés par leur pertinence pour l'environnement étudié.</p> <p>Cr4. La constitution du dossier de preuve est conforme aux règles de protection des données et d'intégrité de la chaîne de traçabilité.</p> <p>Pour A4.3.C1</p> <p>Cr1. La stratégie de reprise est formalisée sous forme de phases, avec des points de vérification, des critères de succès et des actions de restauration cohérentes avec les contraintes du SI.</p> <p>Cr2. Les contre-mesures proposées répondent aux failles ou vulnérabilités exploitées lors de l'incident et sont alignées avec les priorités métiers.</p> <p>Cr3. Les moyens humains, techniques et logistiques nécessaires à la reprise sont</p>
--	---	--	--

			<p>identifiés, chiffrés et mobilisables.</p> <p>Cr4. La cible post-crise est définie en termes de niveau de sécurité restauré, de services fonctionnels et d'exigences de conformité.</p> <p>Pour A4.3.C2</p> <p>Cr1. Le plan comprend des indicateurs de performance post-crise adaptés à l'environnement (taux de reprise, temps de restauration, pertes évitées...).</p> <p>Cr2. Les procédures de révision sont déclenchées par des critères explicites (nouvelles menaces, changements SI, incidents...) et donnent lieu à des mesures concrètes (au moins 3).</p> <p>Cr4. La mise à jour du plan intègre les engagements sociétaux de l'organisation : inclusion, continuité de services critiques, transition écologique.</p>
--	--	--	---

Epreuves transversales :

- 1) **Production d'un rapport écrit** (40 à 60 pages maximum), sur une problématique professionnelle de cybersécurité ou de cyberdéfense (le sujet, choisi par le candidat et validé par l'organisme de formation, peut être en lien avec le contexte ou les enjeux spécifiques du lieu d'accueil de l'alternance ou du stage ou être lié aux problématiques spécifiques explorées/traitées dans le cadre de l'alternance ou du stage)

- 2) **Soutenance orale du rapport devant le jury**

Critères d'évaluation :

A travers les productions du candidat, le jury appréciera :

S'agissant du rapport écrit :

- La prise en compte du cadre méthodologique présenté,
- La prise en compte du cadre légal, réglementaire et normatif applicable ainsi que de l'état de l'art
- La mise en perspective du sujet traité (avec les enjeux sociétaux, avec les évolutions de contexte et d'environnement macro/micro économique et technologique, avec les autres secteurs d'activité...),
- La démarche réflexive, analytique et critique adoptée,
- L'opérationnalité du rapport.

S'agissant de la soutenance orale :

- La capacité du candidat à étayer ses propos et à convaincre son auditoire,
- La capacité du candidat à adopter une méthode de présentation et une terminologie adaptées au profil de ses interlocuteurs.

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.

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

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 événements d'un SI.

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