Certification Expert en cybersécurité

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BLOC 1: Elaborer la stratégie de cybersécurité d'une organisation		**Type d'évaluation :** Mise en situation professionnelle réelle ou fictive **Attendus du candidat :** Le candidat élabore et organise le déploiement d'une stratégie de cybersécurité d'une organisation de son choix. **Livrable attendu** : Le candidat présente lors d'une soutenance orale et à l'aide de support de présentation de son choix remis au jury, les éléments suivants :	
B1.A1. Etude de l'écosystème de l'organisation			
• Audit de l'organisation • Identification des besoins métier, des actifs et des dépendances fonctionnelles.	B1.A1.C1. Auditer l'organisation en identifiant les besoins métiers, les acteurs et les dépendances fonctionnelles, en analysant les processus métiers, en évaluant les interactions entre les systèmes et en recueillant les attentes des parties prenantes afin de garantir une vision exhaustive du fonctionnement opérationnel de l'organisation.	Une présentation de l'organisation comprenant : - l'organigramme, - la liste des parties prenantes externes - la liste des besoins et contraintes métiers, - le schéma fonctionnel	L'ensemble des éléments présentés témoigne d'une compréhension approfondie de l'organisation et de ses enjeux métiers : - L'organigramme fonctionnel identifie les rôles et responsabilités des parties prenantes internes. - Les parties prenantes externes (ex: prestataires d'infogérance, autorités étatiques, assureurs, partenaires technologiques...) et leurs rôles sont identifiés. - Les besoins et contraintes métiers sont identifiés. - Le schéma fonctionnel identifie l'ensemble des processus métier, les environnements (Cloud, sur site, hybride…) et les interactions entre les différentes fonctions, systèmes ou acteurs de l'organisation. - Les dépendances critiques sont recensées et expliquées.

SI : Système d'information

• Elaboration de la cartographie du SI de l'organisation	B1.A1.C2. Etablir la cartographie du système d'information (SI) de l'organisation, en réalisant l'inventaire des services et actifs techniques, en identifiant les liaisons et les flux de données, en choisissant le modèle et l'outil de modélisation le plus adapté afin de disposer d'une représentation détaillée du système d'information de l'organisation.	La cartographie du système d'information (SI)	La cartographie permet une compréhension immédiate du système d'information de l'organisation. La cartographie recense les principaux environnements (Cloud, sur site, hybride…) et principaux composants techniques (matériels, logiciels, serveurs, réseaux). Les liaisons et les flux de données sont précisés.
• Réalisation d'une veille technologique, technique (ex : menace), normative et règlementaire • Identification des obligations et opportunités d'amélioration	B1.A1.C3. Assurer une veille technologique, technique, réglementaire et normative à l'aide d'outils adaptés, en surveillant les innovations technologiques, les évolutions des cadres légaux et des standards applicables, en analysant leurs impacts sur l'organisation afin d'identifier les obligations et les opportunités d'amélioration en matière de sécurité du système d'information.	Un rapport de veille technique, réglementaire et normative	La méthodologie de veille est expliquée . Les outils sont adaptés à la méthodologie de veille (agrégateurs de flux RSS, newsletters, conférences…etc.). La sélection des sources d'informations utilisées est justifiée. Les réglementations et normes applicables à l'organisation sont identifiées. Les menaces techniques sont identifiées et expliquées au regard des activités de l'organisation. Les évolutions technologiques applicables sont identifiées (ex : IA, machine Learning…). Des opportunités d'amélioration sont proposées.
• Analyse des risques de sécurité pesant sur le SI de l'organisation • Evaluation de la maturité du SI en termes de sécurité	B1.A1.C4. Réaliser une analyse des risques en identifiant le type d'évènements pouvant affecter la sécurité du système d'information et leurs sources, en hiérarchisant les risques selon leur gravité et leur impact potentiel afin de mesurer la maturité de l'organisation en matière de sécurité.	La cartographie des risques résultant de l'analyse de risque réalisée sur le SI de l'organisation	Le choix de la méthode d'analyse des risques est justifié (EBIOS, MARION, MEHARI…). La cartographie des risques utilise une structure conforme aux standards établis (par exemple tableau 5x5) et distingue visuellement les niveaux de criticité à l'aide d'un code de niveaux de risque (numérique ou chromatique). La cartographie des risques répertorie les risques identifiables pour le SI et couvre les catégories techniques, organisationnelles, humaines, physiques et environnementales.

SI : Système d'information

			L'impact, la probabilité et le seuil d'acceptabilité sont définis l'aide d'une matrice des risques. Pour chaque risque critique identifié, au moins une mesure de traitement spécifique est associée (réduction, transfert, acceptation ou évitement) avec un ordre de priorité établi. La cartographie permet de révéler la maturité du SI de l'organisation en termes de sécurité.
B1.A2. Conception de la stratégie de sécurité du système d'information de l'organisation			
• Définition de la Politique de sécurité du système d'information (PSSI) de l'organisation • Intégration des référentiels normatifs et règlementation applicables	B1.A2.C1. Définir la politique de sécurité du système d'information (PSSI) d'une organisation en tenant compte de l'étude de l'écosystème réalisée, en intégrant les référentiels normatifs et règlementation applicables, les modèles de sécurité choisis, en précisant l'homologation visée le cas échéant afin de formaliser un cadre stratégique de sécurité du SI aligné sur l'organisation.	La note de cadrage de la politique de sécurité du système d'information (PSSI)	Le candidat présente la note de cadrage établie pour la PSSI en utilisant un vocabulaire adapté à un public de décisionnaires. Le périmètre couvert par la politique de sécurité est défini et justifié au regard de l'analyse des risques réalisée. Les priorités métiers et les besoins spécifiques de l'organisation sont correctement identifiés et intégrés. Les objectifs de sécurité (confidentialité, intégrité, disponibilité, traçabilité) sont pris en compte. Les référentiels, réglementations applicables ou homologations visées (ex : RGPD, ISO 27001, NIS2, SecNumCloud…) sont explicitement mentionnés et intégrés. Le ou les modèles de sécurité choisis sont précisés. (ex: zero Trust, sécurité périmétrique, défense en profondeur, ...). Les orientations stratégiques proposées sont adaptées aux capacités techniques, humaines et financières de l'organisation.
• Analyse des écarts entre la PSSI et le SI • Priorisation des actions de sécurité à déployer	B1.A2.C2. Réaliser une analyse des écarts entre l'état actuel du système d'information et les objectifs de la politique de sécurité du système d'information en classant les écarts selon leur criticité afin de prioriser les actions de sécurité à déployer.	Une synthèse du rapport d'analyse des écarts (Gap Analysis Report)	La synthèse de l'analyse est présentée de manière organisée, concise et compréhensible. Les écarts entre l'état actuel du SI et les objectifs de la PSSI sont identifiées et classées par thématiques (sécurité des données, contrôle d'accès, gestion des incidents, continuité d'activité, actifs, gestion des ressources humaines …etc.).

SI : Système d'information

			Les écarts sont priorisés selon leur criticité. Des actions de sécurité adaptées sont associées à chaque écart. Les actions prioritaires à déployer sont identifiées et justifiées au regard des objectifs de la politique de sécurité du SI (PSSI).
• Elaboration d'un plan d'actions de sécurité • Estimation des ressources nécessaires (moyens et coût) • Présentation du plan d'actions pour validation par les décisionnaires de l'organisation	B1.A2.C3. Définir un plan d'actions de sécurité en tenant compte du rapport d'analyse des écarts, de l'impact écologique des actions proposées, en définissant les besoins et moyens techniques et humains nécessaires, en estimant les coûts associés afin de valider le déploiement du plan d'actions de sécurité avec les décisionnaires de l'organisation.	Le plan d'actions de sécurité défini	Le plan d'actions de sécurité est structuré et synthétique (ex : tableaux, graphiques) . Les ressources humaines, techniques et organisationnelles requises pour chaque action sont identifiées et adaptées. Le plan d'actions de sécurité tient compte de l'impact écologique. Les coûts directs et indirects ventilés par action sont estimés et justifiés par des données fiables. Les arguments/explications du plan d'actions sont adaptés à un public décisionnaire et mettent en avant les bénéfices stratégiques et financiers. Les besoins sont réalistes et adaptés aux capacités de l'organisation.
B1.A3. Préparation du déploiement de la stratégie de sécurité au sein de l'organisation			
• Elaboration du corpus documentaire de sécurité du SI de l'organisation	B1.A3.C1. Elaborer le corpus documentaire de sécurité du SI de l'organisation en tenant compte de la politique de sécurité du système d'information (PSSI), en veillant à l'accessibilité des supports pour les personnes en situation de handicap afin d'encadrer l'utilisation du système d'information (SI).	La liste des documents clés encadrant la sécurité du SI	Les différents types de documents sont listés et pour chaque document sont précisés : - L'objectif au regard de la PSSI - Le périmètre de diffusion - La cible visée - Le niveau de criticité au regard des enjeux sécuritaires Les documents listés répondent aux enjeux stratégiques, opérationnels et réglementaires de l'organisation. Les documents sont adaptés aux spécificités de l'organisation (taille, secteur d'activité, maturité en cybersécurité). Les supports respectent les bonnes pratiques d'accessibilité (RGAA, WCAG, FALC…)

SI : Système d'information

• Conception des plans de résilience du SI de l'organisation (plans de sauvegarde, de secours informatique, de reprise d'activité et de continuité d'activité)	B1.A3.C2. Concevoir les plans de sauvegarde, de secours informatique, de reprise d'activité et de continuité d'activité en s'assurant de la capacité de l'organisation à les mettre en œuvre via des tests et simulations d'incidents, en indiquant leur impact écologique afin d'assurer la résilience globale du système d'information face aux incidents et crises.	Le Plan de sauvegarde **ou** Plan de Secours Informatique **ou** un Plan de Reprise d'Activité **ou** Plan de continuité d'activité du SI	Le plan présenté est structuré avec des sections distinctes et comprend tous les éléments essentiels : - Les objectifs du plan - le périmètre - les scénarios envisagés - les étapes détaillées et les ressources nécessaires associées Les indicateurs fixés pour le plan sélectionné sont définis (ex : RTO Recovery Time Objective, RPO Recovery Point objective, consommation énergétique…) et tiennent compte le cas échéant des accords de niveau de service (SLA des hébergements Cloud, des services Cloud, et autres prestataires de service…). Les actions à entreprendre sont précisées, ordonnées chronologiquement et les rôles et responsabilités des intervenants sont définis. Le bon déroulé du plan est couvert par les tests. Les objectifs fixés dans le plan font l'objet d'une vérification pendant les tests.
• Elaboration du plan de sensibilisation et de formation des utilisateurs à la sécurité du SI • Identification des besoins spécifique des utilisateurs du SI • Conception des contenus et support de formation et sensibilisation	B1.A3.C3. Élaborer un plan de sensibilisation et de formation à la sécurité pour les utilisateurs du SI en identifiant les besoins spécifiques selon les profils d'utilisateurs, en fournissant des contenus adaptés en utilisant des supports pédagogiques variés et adaptés aux personnes en situation de handicap afin de renforcer la culture de la sécurité et réduire les risques liés aux erreurs humaines.	Le plan de sensibilisation et de formation des utilisateurs à la sécurité du SI	Le plan de sensibilisation et de formation identifie les profils utilisateurs au sein de l'organisation et les besoins associés. Les objectifs pédagogiques pour chaque profil cible (utilisateurs standards, administrateurs, managers, etc.) sont précisés. Le programme de sensibilisation et de formation tient compte de l'analyse des risques et de l'utilisation des nouvelles technologies (IA, deepfake…). Les moyens mis en œuvre (cours en ligne, support de présentation, simulations d'hameçonnage…) sont décrits et adaptés aux personnes en situation de handicap. Les moyens d'évaluation des actions de sensibilisation et de formation sont déterminés et tiennent compte des personnes en situation de handicap. Le candidat préconise une fréquence de renouvellement des actions de sensibilisation et de formation adaptée à l'écosystème de l'organisation.

SI : Système d'information

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BLOC 2 : Piloter le cycle de conception, d'intégration et d'évaluation de solutions de sécurité du système d'information		**Type d'évaluation :** Mise en situation professionnelle réelle ou fictive **Attendus du candidat :** A partir de la stratégie de cybersécurité d'une organisation de son choix, le candidat pilote la conception, l'intégration et l'évaluation de solutions de sécurité. **Livrable attendu :** Le candidat remet au jury un dossier écrit comprenant les éléments suivants :	
B2.A1. Pilotage des projets d'intégration de solutions de sécurité du SI			
• Rédaction des spécifications techniques et fonctionnelles des solutions de sécurité	B2.A1.C1. Rédiger les spécifications techniques et fonctionnelles des solutions de sécurité en analysant les besoins métiers, les contraintes réglementaires et les enjeux opérationnels afin de répondre aux exigences de sécurité de la politique de sécurité du SI (PSSI).	Les spécifications techniques et fonctionnelles d'une solution de sécurité (au choix du candidat)	Les spécifications détaillent les objectifs fonctionnels et techniques de la solution conformément aux exigences de la PSSI. Les spécifications techniques tiennent compte des situations de handicap Les contraintes métiers et réglementaires telles que la conformité au règlement général de protection des données (RGPD) ou aux normes de sécurité applicables sont explicitement intégrées dans la spécification. Les diagrammes, schémas ou tableaux fournis sont précis et facilitent la compréhension technique de la solution. Les indicateurs de performance et de succès de la solution sont définis, mesurables et alignés sur les objectifs de sécurité.

SI : Système d'information

• Planification du projet d'intégration des solutions de sécurité • Allocation des ressources nécessaires • Définition des échéances liées à l'intégration de la solution	B2.A1.C2. Organiser le projet d'intégration des solutions de sécurité en sélectionnant une méthodologie de gestion de projet adaptée, en définissant des critères de performance, en établissant le planning du projet, en allouant les ressources nécessaires, afin d'optimiser la réalisation du projet.	Une note explicative de la gestion du projet d'intégration d'une solution de sécurité comprenant : - La méthodologie suivie - le planning d'intégration - une liste de la répartition des ressources nécessaires - les critères de performance	Le choix de méthodologie de gestion du projet (Agile, Lean…) est justifié. Le planning est construit au moyen d'outils adaptés (ex : diagramme de Gantt, PERT retroplanning...) Le planning permet de visualiser les différentes étapes d'intégration (préparation, déploiement, tests validation de la solution). Le planning proposé inclut des jalons pour suivre l'avancement de l'intégration de la solution. Les ressources nécessaires (humaines, matérielles, financières) sont allouées et alignées avec les exigences de la solution. Les critères de performance et de sécurité sont mesurables, définis et alignés sur les objectifs de la solution.
• Suivi du projet d'intégration de la solution de sécurité • Coordination des parties prenantes • Supervision de l'exécution des tâches	B2.A1.C3. Piloter l'avancement du projet en coordonnant les parties prenantes, en supervisant l'exécution des tâches et en ajustant les actions si nécessaire, afin de garantir le respect des délais, des coûts et des objectifs de sécurité.	Le rapport d'intégration de la solution comprenant le tableau de suivi des tâches et le tableau des indicateurs clés de performance	Le rapport d'intégration inclut un tableau de bord détaillant : - l'état d'avancement des tâches, - les responsabilités des parties prenantes - les échéances respectées ou ajustées. - les indicateurs clés (KPI) choisis pour suivre la performance et le respect des délais, des coûts et des objectifs de sécurité Les éventuels écarts (temps, coûts, ou performances) sont expliqués, des actions correctives appropriées ont été menées. La communication entre les parties prenantes est décrite (ex : comptes-rendus de réunions, canaux utilisés) et adaptée au contexte.

SI : Système d'information

B2.A2. Conception et intégration de solutions de sécurité du SI de l'organisation			
• Conception d'une architecture sécurisée du SI	B2.A2.C1. Concevoir une architecture sécurisée du système d'information en analysant les besoins métiers et les risques de sécurité, en intégrant les principes de défense en profondeur, de segmentation et de contrôle d'accès, en sélectionnant des solutions technologiques adaptées afin de protéger les données, les applications et les infrastructures contre les menaces internes et externes.	Le schéma d'architecture initiale du SI et le schéma d'architecture sécurisée du SI	Le schéma d'architecture initial du SI est établi et permet de servir de base de comparaison avec le schéma d'architecture sécurisée. La conception de l'architecture sécurisée présentée tient compte des vulnérabilités identifiées dans l'architecture initiale. La conception de l'architecture sécurisée respecte au moins 2 recommandations de l'ANSSI. Les réseaux, flux de données, points de contrôle de sécurité et interactions entre les composants fonctionnels sont représentés visuellement et de manière accessible.
• Gestion des identités, des mécanismes d'authentification et contrôle des accès	B2.A2.C2. Gérer les identités et contrôler les accès en mettant en œuvre des processus d'authentification tenant compte des personnes en situation de handicap le cas échéant, d'autorisation et de gestion des droits afin de sécuriser l'accès aux ressources et prévenir les usages non autorisés.	Une note décrivant la gestion des identités et contrôle d'accès	Les moyens organisationnels et techniques mis en œuvre pour authentifier les utilisateurs sont détaillés (ex : authentification multi facteur, reconnaissance faciale, capteurs biométriques compatible, gestion et contrôle des mots de passe...) et tiennent compte de la PSSI. Les droits et niveaux d'autorisation sont déterminés en fonction des profils des utilisateurs. Les ressources auxquelles les utilisateurs ont accès en fonction de leurs droits sont répertoriées. Les moyens d'attribution des droits sont décrits. Les moyens de contrôle et d'alerte permettent d'identifier les failles sécuritaires.
• Déploiement de solutions cryptographiques pour protéger les données	B2.A2.C3. Déployer des solutions cryptographiques en configurant les outils adaptés, en appliquant les protocoles et en assurant leur intégration dans l'environnement existant afin de garantir la confidentialité, l'intégrité et l'authenticité des données.	Un exemple de solution cryptographique mise en place	La solution cryptographique est décrite en précisant les algorithmes utilisés (chiffrement, signature, hachage) et leurs paramètres (taille des clés, modes d'opération). Les cas d'usage spécifiques de la solution sont justifiés au regard de leur adéquation aux besoins identifiés. La robustesse de la solution est évaluée en tenant compte des meilleures pratiques actuelles et des recommandations des standards (e.g., NIST, ANSSI). Les points faibles potentiels ou limites de la solution sont identifiés avec des recommandations pour minimiser les risques associés.

SI : Système d'information

B2.A3. Evaluation de l'efficacité des solutions de sécurité du SI mises en place			
• Réalisation d'audits techniques de sécurité	B2.A3.C1. Organiser un audit technique des solutions de sécurité en définissant un plan d'audit structuré précisant le périmètre d'analyse et les référentiels applicables, afin de permettre l'identification des vulnérabilités, des non-conformités et des axes d'amélioration.	Le plan d'audit technique d'une solution de sécurité	Le plan d'audit définit : - les objectifs et le périmètre de l'audit technique - les critères d'évaluation en lien avec les enjeux de sécurité identifiés. Les étapes de l'audit sont structurées de manière méthodique et couvrent les principales phases (préparation, collecte de données, analyse, rapport). Les outils et méthodologies proposés pour les tests techniques (e.g., scans de vulnérabilités, tests d'intrusion, analyse de configuration…) sont justifiés.
• Rédaction d'un rapport d'audit technique	B2.A3.C2. Rédiger un rapport d'audit technique précis et structuré en synthétisant les résultats des analyses, en formulant des actions correctives ou recommandations adaptées, réalisables et conformes aux normes et standards en vigueur afin de documenter l'état de sécurité et les axes d'amélioration de la solution.	Le rapport d'audit technique de la solution de sécurité	Le rapport est structuré de manière méthodique et professionnelle avec une distinction entre les observations, les impacts et les recommandations. La méthodologie suivie est décrite. Les analyses présentées dans le rapport sont basées sur des preuves et conformes aux standards de la cybersécurité. Le rapport met en évidence des actions correctives ou recommandations spécifiques, réalisables et alignées sur le contexte technique et opérationnel de l'organisation auditée. Les actions correctives ou recommandations formulées respectent les normes et standards en vigueur (ex : ISO 27001, NIST, OWASP, …). Le rapport respecte les règles de confidentialité et de sensibilité des informations.
• Suivi des actions correctives	B2.A3.C3. Assurer le suivi des actions correctives issues d'un audit technique de sécurité du SI, en coordonnant les parties prenantes, en vérifiant la mise en œuvre des mesures recommandées et en évaluant leur efficacité, afin de garantir la réduction effective des risques identifiés.	Le rapport de suivi des actions correctives identifiées lors de l'audit	Le rapport de suivi comprend un état détaillé et actualisé de toutes les actions correctives identifiées lors de l'audit. Les preuves de mise en œuvre des mesures correctives sont fournies et démontrent la réduction effective des risques identifiés. L'évaluation de l'efficacité des mesures appliquées est basée sur des indicateurs objectifs mesurables.

SI : Système d'information

Certification Expert en cybersécurité

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	REFERENTIEL DE COMPETENCES *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	REFERENTIEL D'EVALUATION *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BLOC 3 : Maintenir en condition de sécurité le système d'information (SI) d'une organisation		**Type d'évaluation :** Mise en situation professionnelle réelle ou fictive **Attendus du candidat :** Sur la base d'une analyse du système d'information d'une organisation de son choix, le candidat présente les éléments permettant de maintenir la sécurité du système d'information **Livrable attendu :** le candidat remet au jury un dossier écrit comprenant les éléments suivants :	
B3.A1.Gestion de l'obsolescence et des mises à jour du SI			
• Définition d'une politique de gestion de l'obsolescence et des mises à jour du système d'information	B3.A1.C1. Définir une politique de gestion de l'obsolescence et des mises à jour du système d'information en identifiant les composants matériels et logiciels, leur typologie et leur cycle de vie afin d'assurer la sécurité, la performance et la fiabilité du système d'information.	La politique de gestion de l'obsolescence et des mises à jour du système d'information	La politique de gestion de l'obsolescence et des mises à jour du SI définit les processus pour identifier, inventorier et prioriser les actifs obsolescents ou nécessitant des mises à jour. Les parties prenantes et leurs responsabilités pour la mise en œuvre de la politique sont identifiées. La typologie des composants matériels et logiciels sont identifiés. Les cycles de mises à jour et les échéances de gestion des obsolescences sont alignés sur les exigences réglementaires, les besoins métiers et les bonnes pratiques de sécurité.

SI : Système d'information

• Réalisation des mises à jour ou des décommissionnements des actifs du SI	B3.A1.C2. Réaliser les mises à jour ou décommissionnements des actifs du SI en suivant une procédure préalablement établie afin de garantir la sécurité, la compatibilité et la continuité des opérations.	Une procédure de mise à jour d'un actif du SI	La procédure est détaillée et couvre l'ensemble des étapes nécessaires, de l'identification de l'actif à la mise en production ou à la mise hors service. Les actions respectent les bonnes pratiques et normes de sécurité. La procédure comprend des tests préalables pour garantir la fiabilité et la continuité des opérations. L'indisponibilité éventuelle de l'actif liée à l'application de la procédure est justifiée.
• Suivi des mises à jour et de l'obsolescence par la mise en place d'un tableau de bord et d'indicateurs	B3.A1.C3. Développer des indicateurs de suivi en s'appuyant sur l'analyse des données historiques, la collecte d'informations en temps réel et l'automatisation des rapports afin de mesurer l'efficacité de la gestion des mises à jour et de l'obsolescence.	Un tableau de bord de suivi des mises à jour et de l'obsolescence	Le tableau de bord présente les indicateurs sous une forme visuelle facilitant leur compréhension. Les indicateurs sont mesurables et alignés avec la politique de gestion de l'obsolescence et des mises à jour. Les indicateurs sont calculés avec des méthodologies explicites, basées sur des données fiables et actualisées.
B3.A2. Contrôle et surveillance continue de la sécurité du SI de l'organisation			
• Elaboration d'une politique de contrôle et de surveillance continue	B3.A2.C1. Elaborer une politique de contrôle et de surveillance continue en tenant compte des menaces identifiées et de la PSSI, en alignant les objectifs de surveillance sur les exigences règlementaires et les besoins métiers afin d'assurer une supervision efficace du SI.	La note de cadrage de la politique de contrôle et surveillance	La politique est alignée avec les objectifs stratégiques de la PSSI et les besoins métiers identifiés. Une liste des composants du SI à surveiller est établie et justifiée. Les dispositifs permettant de surveiller la sécurité du SI sont déterminés (journalisation, système SIEM…). Les menaces identifiées sont prises en compte dans la politique de contrôle et surveillance

SI : Système d'information

• Mise en place d'un SOC au sein de l'organisation • Déploiement des outils de détection des menaces et d'analyse avancée • Définition des indicateurs clés	B3.A2.C2. Intégrer un Security Operations Center (SOC) au sein de l'organisation en définissant les dispositifs de sécurité adéquats, les équipes nécessaires et les indicateurs à suivre, afin de surveiller en temps réel les menaces.	Une description détaillée du SOC mis en place	Les dispositifs de sécurité (SIEM, EDR…) sont définis et adaptés aux personnes en situation de handicap le cas échéant. Les rôles et responsabilités des différents acteurs sont décrits. Les indicateurs de sécurité à suivre sont définis et permettent une surveillance efficace du SI. Des objectifs de détection et de réponse sont déterminés (MTTD, MTTR, taux de faux positifs). Le processus de traitement des alertes est précisé.
• Vérification du fonctionnement du SOC (test d'intrusion, simulation d'incidents...)	B3.A2.C3. Évaluer l'efficacité du Security Operations Center (SOC) d'une organisation, en utilisant des scénarios de test réalistes afin de s'assurer de la performance du processus de détection et de l'efficacité des équipes.	Le scenario de test permettant d'évaluer l'efficacité du SOC et l'analyse des résultats.	Le scénario de test choisi est justifié au regard de sa capacité et pertinence pour évaluer l'efficacité du SOC. Les données mesurables collectées durant le scénario (MTTD, MTTR) reflètent la performance actuelle du SOC et incluent des comparaisons avec les objectifs de sécurité fixés. Les recommandations proposées sont réalisables et priorisées selon leur impact sur l'amélioration du fonctionnement global du SOC.
B3.A3. Détection et correction des vulnérabilités			
• Détection et documentation des vulnérabilités	B3.A3.C1. Documenter les vulnérabilités détectées lors de la surveillance du SI en analysant les alertes générées par les outils de monitoring, en évaluant leur criticité afin de proposer des actions correctives.	L'étude d'une vulnérabilité détectée	L'étude décrit précisément la vulnérabilité : sa nature, sa source (ex : CVE) ; son type (ex : CWE) et son impact potentiel sur le système d'information. L'évaluation de la criticité de la vulnérabilité est basée sur une méthodologie claire, telle que CVSS (Common Vulnerability Scoring System). Les scénarios d'exploitation possibles sont identifiés et accompagnés d'une estimation des risques associés pour le SI. Des recommandations sont proposées pour corriger ou atténuer la vulnérabilité et tiennent compte des contraintes opérationnelles.

SI : Système d'information

• Traitement des vulnérabilités identifiées	B3.A3.C2. Corriger les vulnérabilités identifiées en élaborant un plan d'actions correctives approprié afin de restaurer la sécurité du système concerné.	La correction d'une vulnérabilité détectée.	Les étapes nécessaires à la correction de la vulnérabilité détectée sont listées. Les délais de réalisation de chaque étape sont justifiés. Un cross check (vérification croisée) permet de s'assurer de la correction effective de la vulnérabilité.

SI : Système d'information

Certification Expert en cybersécurité

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	REFERENTIEL DE COMPETENCES *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	REFERENTIEL D'EVALUATION *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BLOC 4 : Gérer stratégiquement et opérationnellement une crise cyber		**Type d'évaluation :** Mise en situation professionnelle réelle ou fictive **Attendus du candidat :** Le candidat présente sa gestion stratégique et opérationnelle d'une crise de cybersécurité d'une organisation de son choix. **Livrable attendu :** Le candidat présente lors d'une soutenance orale et à l'aide de support de présentation de son choix remis au jury, les éléments suivants :	
B4.A1. Elaboration d'une stratégie de gestion de crise			
• Conception d'une stratégie de communication de crise • Identification des parties prenantes à contacter en cas de crise	B4.A1.C1. Concevoir une stratégie de communication de crise, en identifiant les parties prenantes à contacter et les canaux de communication de secours à utiliser, en rédigeant des messages types clés en main afin d'aider l'organisation à communiquer de manière efficace en cas de crise.	La stratégie de communication de crise et Un exemple de message type	La stratégie de communication de crise identifie toutes les parties prenantes internes et externes à contacter et indique pour chacune des parties les délais à respecter. Des canaux de communication utilisables en cas de crise, y compris en cas d'indisponibilité des outils classiques (mails) sont identifiés et justifiés pour atteindre les différentes cibles. Le message type présenté tient compte d'un scénario cyber identifié.
• Organisation d'une cellule stratégique de crise • Mise en place des critères et des procédures d'activation de la cellule de crise	B4.A1.C2. Organiser une cellule stratégique de crise en identifiant ses membres, leurs rôles et missions, en définissant les critères et procédures d'activation de la cellule de crise afin d'assurer une bonne coordination et mobilisation des équipes pendant la crise.	Le plan d'organisation et de fonctionnement de la cellule de crise	Tous les membres nécessaires (internes et externes) de la cellule de crise sont identifiés avec des rôles et responsabilités définis pour chacun. Les critères déclencheurs de la cellule de crise sont objectifs et adaptés aux types de crises identifiés. Les procédures d'activation sont justifiées et testées.

SI : Système d'information

• Déploiement d'une stratégie d'entrainement de gestion de crise	B4.A1.C3. Déployer une stratégie d'entrainement de gestion de crise en réalisant des exercices variés testant différents scénarios d'attaque réalistes et adaptés à l'organisation afin de renforcer les compétences de l'équipe.	Un exercice d'entrainement de gestion de crise	Le candidat présente un exercice d'entrainement de gestion de crise en justifiant : - les objectifs de l'exercice; - le scénario d'attaque choisi ; - le format de l'exercice (exercice sur table, simulation, …); - les indicateurs permettant d'évaluer la performance des équipes et l'efficacité de l'exercice. L'exercice présenté est adapté à l'organisation.
B4.A2. Analyse des incidents détectés et endiguement			
• Qualification et confirmation de l'incident détecté	B4.A2.C1. Réaliser l'analyse initiale de tout incident détecté en vérifiant qu'il ne s'agisse pas d'une fausse alerte, en définissant sa nature, sa portée et sa criticité afin de décider de l'activation de la cellule stratégique de crise.	Le rapport d'analyse initiale d'un incident détecté	Le rapport identifie la nature de l'incident en décrivant les symptômes et les événements déclencheurs. L'analyse de la portée de l'incident inclut une évaluation des systèmes, des données et des utilisateurs potentiellement affectés. La classification de la criticité repose sur des critères objectifs et est accompagnée d'une justification détaillée. Le rapport permet de confirmer le caractère avéré de l'incident et de décider de l'activation de la cellule de crise.
• Endiguement de l'incident	B4.A2.C2. Mettre en place des mesures d'endiguement appropriées en protégeant les actifs essentiels du SI à l'aide d'outils et techniques adaptés afin de limiter la propagation de l'incident.	Les mesures d'endiguement prises face à l'incident	Les mesures d'endiguement définies sont adaptées et tiennent compte de l'impact et de la criticité de l'incident. Les mesures d'endiguement permettent d'éviter la propagation supplémentaire à d'autres systèmes ou réseaux. Les outils et techniques utilisés pour limiter l'incident respectent les bonnes pratiques de sécurité et les spécificités de l'organisation.
• Analyse forensique de l'incident	B4.A2.C3. Réaliser une analyse forensique de l'incident en collectant et corrélant les preuves numériques à l'aide des outils adaptés afin de préparer une réponse et remédiation adaptées.	Le rapport d'analyse forensique de l'incident	Le rapport d'analyse identifie les causes et les vecteurs de l'incident à l'aide d'outils et méthodologies conformes aux standards. Les preuves numériques sont identifiées, collectées et préservées sans altérer leur intégrité. La collecte des preuves numériques respecte les cadres légaux, réglementaires et standards applicables (RGPD, ANSSI, ISO 27037, …) Les preuves collectées permettent de tirer des conclusions et préparer une réponse adaptée.

SI : Système d'information

B4.A3.Pilotage opérationnel de la remédiation de l'incident et capitalisation			
• Mise en œuvre d'actions d'éviction et d'éradication	B4.A3.C1. Déployer des actions d'éviction et d'éradication en mobilisant des experts et des outils de sécurité adaptés, en vérifiant l'efficacité de ces actions afin d'éliminer la menace.	Les actions d'éviction et d'éradication prises au regard de l'incident	Les actions d'éviction et d'éradication effectuées sont décrites et ordonnées selon une logique opérationnelle. Les experts mobilisés et les outils de sécurité utilisés sont adaptés à la nature de la menace. L'efficacité des actions est prouvée au regard de la menace.
• Mise en œuvre des plans de restauration	B4.A3.C2. Mettre en œuvre le plan de restauration du SI en utilisant des solutions techniques afin de rétablir les capacités du système d'information (SI).	La description du plan de restauration du SI	Les actions permettent la restauration des capacités du SI. Les rôles des parties prenantes et les ressources impliquées sont décrits. Le séquençage des actions est justifié.
• Réalisation d'une analyse post mortem • Capitalisation sur la crise	B4.A3.C3. Capitaliser sur les enseignements de la crise en réalisant une analyse post mortem de l'incident afin d'améliorer la gestion future de crise.	Le rapport d'analyse post mortem de l'incident	Le candidat présente le rapport d'analyse post mortem comprenant : - les causes de l'incident ; - les vecteurs d'attaque exploités ; - les impacts ; - un RETEX de la gestion de crise ; - et les actions d'améliorations.

SI : Système d'information