Titre de Niveau 7 : Expert en développement de solutions de Cybersécurité

RÉFÉRENTIEL D'ACTIVITÉS	RÉFÉRENTIEL DE COMPÉTENCES	RÉFÉRENTIEL D'ÉVALUATION *définit les critères et les modalités d'évaluation des acquis*	
Décrit les situations de travail et les activités exercées, les métiers ou emplois visés	*Identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
BLOC n°1 Mettre en place une stratégie de cybersécurité dans une démarche de développement de solutions			
		Deux modalités d'évaluation pour la totalité des blocs de compétences sont mises en œuvre : - Des **évaluations par bloc** (études de cas, mise en situation professionnelles, etc…) et décrites ci-après. Elles sont sous la responsabilité de l'enseignant en charge des compétences visées - La **rédaction** d'un **mémoire professionnel.** Le mémoire, visant à reprendre l'ensemble des compétences abordées, fait l'objet d'une **soutenance devant un jury**.	
A1.1 : Implantation de la stratégie en termes de cybersécurité au travers de solutions performantes ○ Introduction de l'importance de la cybersécurité auprès de la Direction ○ Argumentation des différents enjeux et risques encourus si non prise en compte ○ Présentation d'une stratégie cybersécurité à cout, moyen et long terme incluant les budgets impactés et les retours sur investissement ○ Adaptation du système de présentation et communication en fonction des personnes présentes en prenant en compte celles présentant un potentiel handicap ;	**C1.1 : Proposer une stratégie globale de protection en termes de cybersécurité en tenant compte des enjeux, du développement et de l'environnement de l'entreprise**	**E1 Étude de cas pratique** Dans le cadre d'un cas pratique il est demandé au candidat de présenter une stratégie globale de sécurité informatique pour une entreprise donnée Le cas s'articule autour de la simulation d'une entreprise fictive de mise en relation se services BtoC H24 et 7j/7. Selon les préconisations de l'ANSSI le candidat devra convaincre de la nécessité d'adapter le site et le système d'information afin de respecter les contraintes de sécurité, protection des données, les réglementations RGPD et PCI DSS, selon une stratégie définie	**Pertinence de la présentation stratégique :** ○ Tous les critères impactant l'approche stratégique sont pris en compte ○ Le choix des outils d'analyse stratégique est pertinent ○ 80% des préconisations sont pertinentes et en adéquation avec la politique générale de l'entreprise ○ L'adéquation, la qualité des outils de communication et de présentation pour la facilité de compréhension du public concerné

		Sera fourni au candidat l'ensemble des éléments de l'entreprise Le candidat présentera son analyse et la proposition argumentée lors d'un oral soutenu par une synthèse écrite de son choix Lieu de l'évaluation : centre de formation Méthodologie : écrit et présentation orale	
A1.2 : Organisation de la mise en œuvre de la stratégie de cybersécurité ○ Organisation d'un diagnostic stratégique externe et interne ○ Analyse des performances, compétences et connaissances internes ○ Validation et priorisation des besoins et des risques ○ Définition des objectifs en fonctions des besoins préalablement énoncés ○ Proposition d'une stratégie opérationnelle à partir des ressources à dispositions ○ Organisation et orchestration du déploiement ○ Validation des évolutions et réajustements de la stratégie appliquée, si nécessaire	**C1.2 : Définir une stratégie de sécurisation en tenant compte du contexte technique, organisationnel, opérationnel 'et légal de l'entreprise afin d'apporter une réponse adaptée au regard des risques identifiés**	**E2 Étude de cas** Dans le cadre de l'étude proposée précédemment, le candidat décline la stratégie globale en stratégie opérationnelle et fonctionnelle de l'environnement. En fonction des directives le candidat organise une analyse stratégique afin d'identifier les forces-faiblesses-opportunités-menaces de l'écosystème de la cybersécurité de l'entreprise dans le but d'établir un diagnostic macro-environnement. Il choisit, met en place et fait appliquer les outils de veille les plus adaptés en indiquant les objectifs visés et résultats attendus Sera fourni au candidat le résultat de l'audit cybersécurité de l'entreprise. Lieu de l'évaluation : centre de formation	**Pertinence de l'analyse stratégique :** ○ L'analyse est approfondie et exhaustive (enjeux, coût, risques, bénéfices) ○ Le choix des outils d'analyse stratégique est pertinent, maîtrisé et argumenté ○ Les besoins et les risques associés sont identifiés ○ Les objectifs stratégiques sont décrits et priorisés en fonction des besoins identifiés ○ Les solutions proposées permettent de répondre aux problèmes rencontrés ○ La Justification du travail et de la réflexion sont argumentées et concises ○ La priorisation des actions à mener est cohérente
A1.3: Mise en place d'un processus de veille en sécurité ○ Organisation de la mise en place d'une veille règlementaire et technologique	**C1.3 : Mettre en œuvre une veille sur les dernières innovations technologiques applicables à l'entreprise afin de comprendre les technologies en évolution et**		**Qualité de la veille qui regroupe des notions multiples : technologique, règlementaire, normes :** ○ Des outils et des méthodes de veille sont mis en œuvre

○ Validation des propositions de nouvelles tendances, évolutions et des innovations en matière de sécurité ○ Contrôle du respect de la loi Informatique et Libertés, du RGPD, des normes ISO31000 (gestion des risques), ISO 27005 (gestion des risques appliqués au SI), ISO 27037 (collecte de le preuve numérique en cas d'intrusion), etc.	**envisager des solutions pour le futur (cybersécurité, cyber-robotique, intelligence artificielle, ML…)**	Méthodologie : écrit et présentation orale	○ Les domaines à analyser sont identifiés et connus. ○ Les sources d'information collectées sont larges et pertinentes selon une grille ○ Les sources sont analysées au regard de la stratégie d'entreprise
A1.4: intégration des spécificités et besoins du client ○ Intégration des besoins et du niveau de vulnérabilité et de sécurisation du client ○ Validation des risques et menaces de sécurité pour chacune des technologies ○ Argumentation de solutions à mettre en œuvre ○ Contrôle des risques (gravité, coût, probabilité d'occurrence…) et validation de l'impact de la menace et des vulnérabilités ○ Validation du tableau des exigences techniques et de sécurité	**C1.4 : Analyser les besoins de sécurité et le contexte des menaces propres à chacune des technologies afin d'élaborer des solutions en cohérence avec les priorités stratégiques et les besoins du client et formuler le tableau des exigences techniques**	**E3 Étude de cas pratique** Dans le cadre d'un cas pratique il est demandé au candidat d'identifier, analyser et de prendre en compte les menaces et vulnérabilités de toutes les technologies présentes au sein d'une entreprise Le cas s'articule autour de « l'école de l'usine du futur 4.0 » qui fournira au candidat l'ensemble des informations requises. Le candidat présentera la méthodologie déployée, son analyse et le résultat obtenu lors d'un oral soutenu par une synthèse écrite de son choix Il tiendra compte du niveau de compréhension du public et adaptera son intervention en fonction des personnes soumises à un handicap Lieu de l'évaluation : l'école de l'usine du futur 4.0 Méthodologie : écrit et présentation orale	**Les besoins et exigences techniques et de sécurité du client ont intégrées et justifiées de façon pertinente et argumentée** ○ Les besoins, les risques et menaces sont identifiés et présentés ○ L'impact des vulnérabilités et les exigences sont regroupés par thème et les propositions technologiques répondent aux besoins recensés et aux contraintes de sécurité du client ○ Le tableau des exigences techniques et de sécurité est précis, exhaustif et explicite ○ Le vocabulaire technique est maitrisé et employé à bon escient avec un effort de compréhension vis-à-vis du public, handicap compris

A1.5 : Mise en œuvre d'un projet de développement de solution orientée sécurité ○ Choix argumenté d'une méthodologie de travail (classique, agile) avec les parties prenantes (MOA, MOE, chef de projet…) ○ Organisation du plan d'action de déploiement de la solution ○ Contrôle des indicateurs de suivi (qualité, coût, délai, …)	**C1.5 : Appliquer une méthodologie de gestion de projet et une organisation adaptée afin de garantir un résultat respectant les exigences techniques et fonctionnelles du cahier des charges.**	**E4. Étude de cas** Sur la base du cas précédent dédié à « l'école de l'usine du futur 4.0 »,le candidat propose la démarche projet la plus adaptée avec un planning, une organisation et des indicateurs de suivi. Il évalue la concordance des moyens (ressources, compétences, etc…) et propose un dispositif d'accompagnement des parties prenantes (feuille de route, plan de communication…) Lieu de l'évaluation : école de l'usine du futur 4.0 Méthodologie : écrit et présentation orale	**La démarche projet est adaptée par rapport à la nature du projet :** ○ La méthode projet choisie est pertinente, adaptée et argumentée (exemple : projet en mode agile de type SCRUM, méthode DevOps, cycle en V…) ○ La méthode est alignée avec les pratiques des parties prenantes ○ Le plan d'action est cohérent par rapport aux résultats attendus (planification, organisation, revue de projet) ○ Les indicateurs proposés sont pertinents et mesurables
A1.6: Communication en interne et en externe autour du projet de développement de la solution technique ○ Pilotage de réunions de travail, de points d'informations réguliers selon un planning préétabli avec le client et les équipes internes, avec délégation quand cela est possible ○ Contrôle du respect de la feuille de route et du traitement des informations destinées à la hiérarchie ○ Maintien d'une communication transparente et adaptée avec l'ensemble des interlocuteurs ○ Sur l'ensemble des étapes, adaptation de sa posture et de ses pratiques relationnelles avec les personnes en situation de handicap. ○ Choix des supports de communication adaptés en fonction des situations de handicap rencontrées, chez le client et/ou sein de l'équipe projet à piloter	**C1.6 : Communiquer auprès de l'équipe et le commanditaire en organisant des réunions de travail et des comités de suivi afin de garantir des prises de décision et faciliter le déroulement du projet**		**Une communication est mise en œuvre et adaptée pour accompagner les parties prenantes du projet :** ○ Des revues de projet et des réunions de travail sont proposées et organisées ○ Les supports et les outils de communication sont adaptés aux parties prenantes ○ Le candidat est capable d'élaborer un glossaire adapté ○ Les informations à remonter à la hiérarchie sont collectées ○ La posture du candidat démontre ses qualités en communication et sa capacité d'ajuster ses pratiques relationnelles en fonction de ses interlocuteurs ○ Le candidat démontre sa capacité à intégrer l'anglais technique dans ses échanges avec les parties prenantes
BLOC n°2 : Construire des solutions de cybersécurité en utilisant les technologies émergentes			

A2.1 : Organisation et contrôler l'audit sur les solutions existantes ○ Validation de l'analyse des risques et des vulnérabilités répertoriés (exemple Ebios RM…) ○ Pilotage d'un audit de code ciblé sur la solution de sécurité ○ Pilotage d'un audit d'architecture logicielle et de configuration ○ Analyse des vulnérabilités logicielles/web (top 10 owasp) issues du scanner de vulnérabilité mettant en exergue les failles potentielles des solutions existantes	**C2.1 : Réaliser un audit de sécurité sur les solutions existantes en listant leurs forces et leurs vulnérabilités afin de définir un plan de remise en conformité des équipements sensibles et vulnérables**	**E5. Étude de cas** Sur la base d'une étude de cas portant sur un audit de sécurité d'une entreprise fictive, Le cas s'articule autour de la simulation d'une entreprise fictive de mise en relation se services BtoC H24 et 7j/7 pour laquelle le candidat propose la mise en œuvre de l'audit de cybersécurité Il établit le programme d'audit prenant en compte les référentiels de sécurité agréés. Le candidat formule différents scénarii de développement. Il présente le programme d'audit lors d'un entretien oral et argumente ses choix par rapport aux préconisations définies en lien avec les exigences du client. Lieu de l'évaluation : centre de formation	**La démarche d'audit est cohérente et en accord avec les référentiels de sécurité en vigueur et agréés :** ○ Les périmètres à risques, les vulnérabilités, les vecteurs d'attaques potentiels sont identifiés et analysés ○ Le candidat vérifie que le code source est sécurisé (utilisation d'outils automatisés) ○ Les architectures logicielles et de configuration sont identifiés selon les bonnes pratiques de cybersécurité ○ Les vulnérabilités de la solution sont identifiées ○ Une recommandation de remédiation (correction) est proposée et argumentée selon leur niveau de complexité
A2.2 : Choix de scénario de développement de solution : ○ Choix du scenario parmi différents des critères validés, dans le respect des exigences du client (délais, qualité, coût…) ○ Validation de l'étude de faisabilité technique de la solution choisie (limite hardware, coût, développement, délais, etc…)	**C2.2 : Sélectionner des scénarii de développement de solutions potentielles en s'appuyant sur une étude de faisabilité et selon des critères bien définis afin de retenir la solution la plus adaptée par rapport aux exigences exprimées par le client**		**La sélection des scénarii préférentiels est pertinente et prend en compte les exigences du client :** ○ Les scénarii sont sélectionnés par rapport à des critères de choix (souveraineté, fiabilité, qualité, normes RGPD…) ○ Les choix sont cohérents avec les exigences exprimées par le client et la faisabilité technique ○ Une étude de faisabilité est proposée et appuyée par des recommandations (proof of concept) ○ Les exigences du client sont prises en compte (délais, coût, qualité…)
A2.3 : Application de la loi Informatique et libertés, RGPD et des normes ISO (ISO 27001/ISO 27002) ○ Faire appliquer le cadre législatif dans le développement de la solution	**C2.3 : Développer une solution sécurité en appliquant les bonnes pratiques de cybersécurité afin de garantir un résultat**	**E6. Questionnaire à visée professionnelle** Le candidat répond aux différentes questions posées portant sur sa	**Le candidat maîtrise les bonnes pratiques en matière de cybersécurité et la législation en vigueur** ○ Les procédures utilisées (sécurité organisationnelle, cyberdéfense, normes

○ Faire respecter les procédures et les normes en vigueur (ISO 27001/27002) ○ Contrôle et validation des outils utilisés (librairie, composant) vis-à-vis des critères de sécurité minimum.	**respectant les normes et réglementation en vigueur**	maîtrise professionnelle en matière de législation et des normes sécurité. Lieu de l'évaluation : centre de formation sur plateforme en ligne	27001/27002) sont maîtrisées au regard des bonnes pratiques de cybersécurité ○ La législation informatique (CNIL, RGPD) est connue et maîtrisée ○ Les norme en vigueur (ISO27001/27002) sont connues et maîtrisées ○ Des outils de librairie ou composants proposés sont connus et maîtrisés
A2.4 : Mise en place d'un modèle de Machine Learning ○ Validation du Data Set (jeu de données) proposé selon les consignes de construction données ○ Manipulation de données pour contrôle du bon fonctionnement de ce jeu de données (mise en forme, effacement des données, ajustement, etc…) ○ Choix et validation du modèle de Machine Learning (algorithme) ○ Organisation de la phase d'apprentissage du modèle d'algorithme choisi avec le jeu de données en adaptant sa communication au public concerné y compris les personnes en situation de handicap (choix du support et de la méthodologie adaptée)	**C2.4 : Mettre en place un modèle de Machine Learning en s'appuyant sur un jeu de données pertinent afin d'augmenter la performance de la solution de sécurité**	**E7. Mise en situation** Sur la base d'une mise en situation portant sur la mise en place d'un modèle de Machine Learning, au sein de l'Usine du futur 4.0 le candidat développe un jeu de données à partir d'une solution déjà sécurisée. Il réalise des tests techniques et fonctionnels qui permettent de démontrer l'efficacité du modèle d'apprentissage. Lieu de l'évaluation : centre de formation et École de l'usine du futur 4.0	**Des algorithmes d'apprentissage automatique (Machine Learning) sont utilisés :** ○ Les données utilisées sont de qualité et pertinentes (sélection) ○ Le processus de création de jeu de données est connu et maîtrisé ○ Les techniques de manipulation de données sont connues et appliquées ○ Les modèles d'algorithme sont connus et proposés
A2.5 : Développement du logiciel algorithme ○ Choix argumenté des technologies adaptées (exemple Python, R, TensorFlow, Julia, Handoop, Spark, ...) ○ Organisation et pilotage du développement (fonctionnalités nécessaires (interface, script, API, modularité, etc…) et développement) ○ Contrôle des résultats de tests unitaires (composants, fonctions, etc…) ○ Correction et validation de la documentation technique proposée (choix techniques,	**C2.5 : Développer le logiciel permettant de mettre en place l'algorithme d'intelligence artificielle en s'appuyant sur une analyse des fonctionnalités afin d'évaluer sa pertinence par rapport au projet**	**E8. Mise en situation** Sur la base d'une mise en situation professionnelle portant sur le développement d'un logiciel, le candidat développe, implémente et teste l'algorithme et rédige la notice inhérente. Lieu de l'évaluation : centre de formation	**Le logiciel développé et implémenté est fonctionnel :** ○ Le choix du langage ou des plateformes de programmation en intelligence artificielle est pertinent par rapport au projet ○ Une analyse des fonctionnalités est réalisée et répond aux caractéristiques du projet (coût, qualité, délai…) ○ La solution développée répond aux exigences du cahier des charges

fonctionnement général, caractéristiques, etc…) ; vérification de la prise en compte du handicap potentiel et des adaptation nécessaires			○ Des tests unitaires sont intégrés au logiciel pour vérifier l'opérationnalité de la solution ○ Une documentation technique est définie
A2.6 : Consolidation de la sécurité des systèmes embarqués ○ Contrôle des protocoles proposés (IP, Lora, 5G, Bluetooth, FIP, blockchain, …) adaptés aux technologies de sécurité embarquée (IoT, trains, voitures, drones, satellites, objets connectés, bâtiment, robots) ○ Contrôle de leur configuration pour sécuriser les systèmes embarqués. ○ Organisation et contrôle Cde l'installation des outils et configuration des équipements embarqués (durcissement des OS, Contrôle d'intégrité, …)	**C2.6 : Sélectionner et configurer les différents équipements en appliquant les bonnes pratiques cyber sécurité afin de renforcer la sécurité des systèmes embarqués**	**E9. Mise en situation** Sur la base d'une mise en situation portant sur la sécurisation d'un système embarqué aéronautique proposé par un partenaire ou d'un objet connecté, le candidat configure, implémente et teste la sécurité du système. Il présente lors d'un entretien oral sa sélection et le résultat obtenu Lieu de l'évaluation : centre de formation	**Le système embarqué est sécurisé :** ○ Les différents protocoles sont connus et maitrisés ○ Le choix des systèmes de sécurité défensifs est pertinent par rapport au projet ○ Le système est bien configuré et bien protégé, DICP appliqués (Disponibilité, intégrité, confidentialité, preuve) ○ L'OS de l'objet est bien durci et sécurisé selon les bonnes pratiques
BLOC n° 3 : Intégrer des solutions de cybersécurité dans le système d'information			
A3.1 : Prototypage d'une solution sécurisée ○ Validation du prototype réalisé selon le cahier de charge intégrant : ○ Les besoins client ○ Le plan de test technique et fonctionnel ○ Les politiques de protection des données choisies par l'architecte de la solution. ○ Le monitoring de supervision	**C3.1 : Valider la solution sur les aspects de sécurité en construisant un prototype afin de garantir la faisabilité de l'architecture dans les systèmes réseaux avant sa mise en œuvre.**	**E10. Mise en situation** Le cas s'articule autour de la simulation d'une entreprise fictive de mise en relation se services BtoC H24 et 7j/7. Est mis à disposition du candida, le résultat de l'audit révélant ○ les failles sur site transactionnel et au sein même du SI interne ○ la préconisation de mise en place de Vlans, Firewalls Deep inspection, contrôle AD,	**Le prototype et le plan de tests prennent en compte tous les critères de validation :** ○ Les critères de validation ont été définis dans le respect des exigences de sécurité. ○ Un plan de test technique et fonctionnel est proposé (tests unitaires couvrant l'ensemble des fonctionnalités, cas d'erreur, etc…) ○ Les politiques de protection sont respectés (choix techniques, niveau de protection, choix des bons outils, etc…) ○ Les cas de défaillance de la solution sont identifiés et surveillés (niveau de criticité)

A3.2 : Exploitation du plan de tests techniques ○ Analyse des écarts techniques constatés et expliqués ○ Présentation de d'un plan d'actions correctives ○ Contrôle du monitoring, du PCA (Plan de continuité d'activité) PRA (Plan de reprise d'activité), si applicable.	**C3.2 : Conduire un plan de tests techniques en déployant des méthodologies de tests afin de contrôler la qualité du code, la performance et la sécurité de la solution.**	○ redéveloppement de manière sécurisée le site BtoC pour éviter les attaques par SQL injection Le candidat réalise un prototype respectueux des règles imposées. Il présente lors d'un entretien oral le prototype et le plan de test technique à mettre en œuvre afin de confirmer la pertinence de la solution envisagée. Lieu de l'évaluation : centre de formation	**Le plan de test est conforme :** ○ Les écarts techniques sont identifiés et catégorisés par niveau de criticité (critiques, haut, moyens ou bas) ○ Le candidat identifie la limite de la capacité de traitement de la solution et son régime d'utilisation ○ Des actions correctives et évolutives sont proposées, le cas échéant ○ Des pannes sont simulées et bien remontées dans les outils de supervision existants (solution monitoring)
A3.3 : Pilotage du déploiement de la solution dans un environnement de production ○ Construction du kit d'utilisation à destination des personnes en charge de l'exploitation et de la maintenance, comprenant : ○ La procédure d'installation et de déploiement ○ Les procédures de maintenance ○ Adaptation du support au handicap potentiel des personnes concernées par le déploiement	**C3.3 : Orchestrer le déploiement de la solution en communiquant tous les protocoles nécessaires aux équipes d'exploitation et de maintenance afin de garantir la réalisation des bénéfices attendus de la solution**	**E11. Étude de cas** Sur la base du cas précédent portant sur la rédaction d'un plan de déploiement, le candidat rédige une fiche technique et propose un dispositif pour assurer le transfert de connaissance aux personnes en charge de l'exploitation et de la maintenance. Lieu de l'évaluation : centre de formation	**Le plan de déploiement de la solution proposé par le candidat est exhaustif :** ○ Des actions de formation sont proposées ○ Le plan de transfert de connaissance est clair et explicité ○ Le plan de transfert de connaissance est approprié pour les personnes en situation de handicap ○ Des procédures d'installation et de maintenance sont établies ○ Le vocabulaire métier est respecté et adapté à l'auditoire

A3.4 : Encadrement et organisation de l'assistance auprès des équipes support ○ Priorisation argumentée ses incidents selon l'impact de la crise et l'urgence pour l'organisation ○ Analyse des causes racines et validation des des résolutions des incidents de sécurité	**C3.4 : Superviser l'assistance auprès des parties prenantes en charge de l'installation de la solution en production afin de résoudre les dysfonctionnements de la solution**	**E12. Mise en situation professionnelle** Sur la base d'une simulation d'un incident de sécurité provoqué au sein du Lab interne, le candidat devra proposer une méthodologie pour traiter l'incident en coordination avec les équipes supports Le candidat sera évalué sur : ○ la qualité de l'analyse des causes racines ○ sa capacité à proposer et orchestrer le solutionnement de l'incident ○ la qualité du plan d'action pour la mise en œuvre du correctif Lieu de l'évaluation : centre de formation	**Le candidat propose une méthodologie d'assistance technique pertinente et structurée (ticketing, échelle de gravité des incidents de sécurité, monitoring) :** ○ Une solution de gestion de ticket est proposée ○ Un plan de réponse aux incidents est élaboré en fonction du niveau de dégradation du service rendu par la solution. ○ Une échelle de niveau de gravité des incidents est proposée (impacts et degré d'urgence sur l'organisation) ○ Une analyse des causes racines est réalisée (défaillance matérielle, configuration, actions administrateurs, erreur de conception dans le code…) ○ Une correction du programme est proposée
A3.5 : Maintenance évolutive de la solution de sécurité ○ Choix d'évolutions de la solution (nouvelles fonctionnalités, changement d'architectures, interfaces vers d'autres produits, etc…) incluant : ○ Le respect des besoins clients (avantages, risques, coût, …) ○ L'impact de l'évolution	**C3.5 : Élaborer des scénarii d'évolution de la solution en tenant compte des retours des équipes d'exploitation et du client afin de garantir la cohérence globale de la solution**	**E13. Étude de cas** Le cas s'articule autour de la simulation d'une entreprise fictive de mise en relation se services BtoC H24 et 7j/7 pour laquelle le candidat instruit une demande d'évolution d'une solution et établit des préconisations. Il présente lors d'un entretien oral un plan de maintenance argumenté et sera évalué sur : ○ La pertinence des propositions d'évolution et le choix des options ○ La qualité écrite du plan de maintenance ○ L'analyse des impacts sur la solution	**Les scénarii d'évolution de la solution s'appuient sur plusieurs critères (avantages, inconvénients, risques, coûts, délais, exigences clients…) :** ○ Les propositions d'évolution de la solution sont pertinentes ○ Une analyse des impacts des évolutions est établie (changements à opérer/refonte complète, performance de la solution) ○ Les exigences du client sont respectées ○ Les recommandations formulées sont optimales quant aux modifications à apporter dans la solution.

		○ La prise en compte des exigences du client ○ La clarté de la restitution technique Lieu de l'évaluation : centre de formation	
BLOC n° 4 : Assurer la mise en exploitation et la maintenance des solutions de cybersécurité développées			
A4.1: Supervision et amélioration de la solution ○ Proposition d'amélioration de la solution en fonction des remontées terrain ○ Supervision et contrôle de la mise en œuvre ; interface, ergonomie de la solution, traçabilité des modifications de codes , mise à jour de la documentation techniques et des procédure	**C4.1 : Mettre en exploitation la solution en veillant à son adaptation au regard des besoins utilisateurs afin de faciliter son appropriation et son utilisation.**	**E14. Mise en situation professionnelle** Sur la base d'une simulation d'un incident de sécurité grave et complexe, le candidat devra proposer une procédure de maintenance afin de résoudre l'incident. Il élabore un plan d'amélioration de la solution qui intègre la traçabilité et l'évolution des modifications et la prise en compte des publics-utilisateurs. Lieu de l'évaluation : centre de formation	**Les adaptations proposées sont pertinentes au regard des exigences du client :** ○ Les améliorations proposées sont adaptées par rapport aux besoins utilisateurs ○ Les évolutions répondent aux contraintes de coûts dans le respect de l'analyse de risques courante. ○ La solution répond aux standards ergonomiques ○ Le code source est versionné (traçabilité du code) ○ Le manuel d'exploitation et les fiches de procédures sont mis à jour
A4.2 : Résolution d'incidents complexes liés à des vulnérabilités de la solution ○ Suivi des journaux d'évènements pour diagnostic et analyse des incidents ○ Intégration des correctifs de mise à jour du cycle de vie produit et prise en compte des éventuels effets de bord liés aux correctifs. ○ Pilotage de la gestion de crise majeure (activation et suivi du plan de continuité en cas d'incidents graves), le cas échéant.	**C4.2 : Résoudre des opérations de maintenance complexes en effectuant une analyse des causes afin d'évaluer les vulnérabilités et les menaces et les corriger**		**Le traitement des incidents est maîtrisé :** ○ L'impact de l'incident de sécurité est identifié. ○ L'incident est enregistré dans un journal d'évènement ○ Une analyse des causes racines concernant la nature et l'origine de l'incident est explicitée. ○ Les effets de bords sont maîtrisés. ○ La posture du candidat est adéquate et maîtrisée et permet la coordination de la gestion de crise et de la réponse à l'incident, le cas échéant.

A4.3 : Mise en place d'un dispositif d'amélioration continue pour la solution ○ Rédaction et présentation explicitée des incidents et des propositions d'amélioration, dans le logiciel de suivi (ex. Jira) sur les évènements, retours utilisateurs, anomalies, etc… ○ Adaptation du vocabulaire technique pour prise en compte des parties prenantes et s'assurer de la compréhension ○ Animation des revues qualité (ou Sprint si gestion de projet agiles) ○ Préconisation d'améliorations de la solution tout au long de son cycle de vie.	**C4.3 : Rendre compte des incidents et dysfonctionnements de la solution dans le logiciel de suivi à disposition afin de contribuer à l'amélioration continue de la solution tout au long de son cycle de vie.**		**Les incidents sont tracés dans un rapport d'incident de cybersécurité :** ○ Les éléments liés à l'incident sont enregistrés dans un logiciel de suivi tout au long de la crise ○ L'impact de la crise est explicité de manière factuelle ○ Le vocabulaire technique est maîtrisé et utilisé à bon escient ○ La restitution écrite du rapport d'incident est de qualité
BLOC n° 5 : Animer et encadrer une équipe au quotidien et en mode projet			
A5.1: Pilotage l'équipe projet : ○ Recrutement du personnel de l'équipe ○ Orchestration des missions et fixation des objectifs ○ Mise en place des outils et outils de management (réunions, outils de gestion/outils collaboratifs, reporting, entretien individuel) ○ Mise en œuvre de la communication et du leadership nécessaire au pilotage d'un service et/ou d'un projet ○ Prise en compte des différents handicaps présents pour adapter en conséquence l'organisation des tâches et missions, la gestion du temps de travail et la communication et outils de communication adaptés ○	**C5.1 : Encadrer et animer une équipe p en mettant en œuvre des méthodes et des outils efficients afin de faciliter la réalisation du projet et travailler efficacement au quotidien avec l'ensemble des parties prenantes**	**E15. Étude de cas et Mise en situation** Dans le cadre d'une entreprise fictive, le candidat doit : ○ Organiser une adaptation de sécurisation à court terme ○ Organiser une reconception à moyen terme ○ Contrôler la rédaction d'un cahier des charges de spécification dans le respect des contraintes réglementaires ○ Superviser le développement d'un connecteur API (implémentation et pas uniquement spécification) Il doit : ○ Composer, organiser et orchestrer une équipe projet	**L'équipe projet est correctement choisie par rapport à la nature du projet :** ○ Le choix des ressources est conforme aux besoins du projet et tient compte des compétences-cibles. ○ Les supports et les outils de gestion sont adaptés au projet et à l'équipe ○ Une répartition des tâches est proposée ○ L'organisation du projet est alignée avec les pratiques des équipes et prend en compte la diversité des situations de handicap ○ Des outils de pilotage sont proposés

A5.2 : Conduite de réunions et prise de parole ○ Organisation, préparation et animation de tous types de réunions, information ou prise de décision ○ Prise de parole en public ○ Présentation argumentée de stratégie, négociation de moyens et de mise en œuvre opérationnelle ○ Rédaction d'un compte rendu, cahier des charges et contrats	**C5.2 : Conduire des réunions de projet en structurant sa présentation orale et écrite afin de faciliter l'avancement du projet et le partage d'information**	○ Présenter les éléments de fonctionnement ○ Animer une réunion ○ Formalise un plan de communication de sensibilisation et de vulgarisation destiné à l'ensemble des parties prenantes. Lieu de l'évaluation : centre de formation	**La réunion de projet est préparée, organisée et concoure à la mobilisation des équipes :** ○ Les convocations et informations sur la réunion sont établies ○ L'ordre du jour (objectifs, attentes, intervention des parties prenantes…) est choisi avec précision, justesse et stratégie ○ Le support et les techniques d'animation sont adaptés aux parties prenantes ○ La prise de décision est favorisée ○ La rédaction d'un compte rendu de synthèse intégrant un plan de décisions et plan d'actions est proposé
A5.3 : Mise en place d'une approche pédagogique et de vulgarisation de la cybersécurité destiné aux parties-prenantes - Mise en œuvre d'une communication adaptée au niveau technique de compréhension des acteurs, sponsors et utilisateurs du projet - Vulgarisation des éléments complexes en utilisant l'ensemble des outils de communication à disposition Construction et déploiement d'outils de communication et supports de travail adaptés au public relevant de handicap	**C5.3 : Mettre en place une communication adaptée en démocratisant le processus technique cybersécurité afin de faciliter l'adhésion de l'ensemble des parties prenantes**		**Le plan de communication est clair, synthétique et compréhensible par tous** - Le plan de communication est structuré et complet - La cible est déterminée - Un glossaire technique de vulgarisation et compréhension des éléments complexes est transmis - Un lexique du vocabulaire métier est intégré (y compris la terminologie anglaise) Les supports et les outils de communication choisis sont adaptés à la cible
A5.4 : Encadrement d'une équipe ○ Connaissance du cadre légal lié au droit du travail et au droit social en entreprise ○ Prise en compte et contrôle des RPS (Risque Psychosociaux), des situations dégradées, du handicap et des situations discriminantes ○ Déclinaison de la stratégie d'entreprise ○ Conduite des entretiens réglementaires	**C5.4 : Piloter une équipe dans le respect du cadre légal, des droits et devoirs de chacun**	**E16. Questionnaire à visée professionnelle et mises en situations applicatives** Le candidat répond aux différentes questions posées portant sur sa maîtrise du cadre légal lié au droit du travail	**Le pilotage de l'équipe est anticipé et construit selon** ○ Le collaborateur, l'équipe et l'environnement de travail ○ Le respect des droits et devoirs de chacun ○ Le choix des méthodologies et postures comportementales associées à chaque cas

○ Mise à disposition des dispositifs et accompagnement sociaux et ○		Il mène des entretiens ciblés sur scenarii préétablis Lieu de l'évaluation : centre de formation	○ L'adaptation aux personnes relevant d'un handicap quel qu'il soit