La certification *Développeur de solutions numériques sécurisées* est composée de 4 blocs de compétences dont la validation cumulative est exigée pour son obtention. Ces 4 blocs de compétences sont :

- Bloc de compétences n° 1, compétences C.1.1 à C.1.7 :

Concevoir une solution numérique sécurisée.

- Bloc de compétences n° 2, compétences C.2.1 à C.2.6 :

Développer une solution numérique sécurisée.

- Bloc de compétences n° 3, compétences C.3.1 à C.3.6 :

Déployer et maintenir en conditions sécurisées une solution numérique et son infrastructure associée.

- Bloc de compétences n° 4, compétences C.4.1 à C.4.6 :

Mettre en œuvre des projets de développement, de modernisation et de sécurisation des solutions numériques intégrant des innovations technologiques.

Outre la validation de ces 4 blocs de compétences, l'obtention de la certification est conditionnée à la rédaction et la présentation d'un mémoire professionnel, constituant une modalité d'évaluation transversale, permettant d'évaluer la mise en œuvre coordonnée des compétences.
Ce mémoire professionnel est centré sur une problématique professionnelle généralement choisie à l'issue de la période en entreprise et en fonction des centres d'intérêt du candidat et d'un besoin réel d'entreprise.
Le mémoire professionnel est présenté devant un jury de professionnels, incluant un représentant de l'ESIEE IT. Le candidat présente son travail au jury (environ 30 minutes) et cette présentation est suivie d'une session de questions/réponses. A l'issue de cette séance, le jury délibère en prenant en compte la qualité du livrable écrit ainsi que de la présentation orale selon une grille d'évaluation préétablie.

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**
1. Analyse des besoins et des risques de sécurité associés à la solution numérique *<u>Tâches réalisées</u>* - Clarification du besoin et du contexte d'usage/exploitation, incluant contraintes techniques, dépendances, parties prenantes et responsabilités. - Cartographie des actifs, du périmètre et des flux, avec classification/criticité, frontières de confiance, interfaces et points d'exposition. - Modélisation des menaces et évaluation/hiérarchisation des risques (scénarios d'attaque, impacts, probabilité, risques résiduels et priorités de traitement). - Formalisation des exigences fonctionnelles et de sécurité, critères d'acceptation et décisions de traitement du risque.	C.1.1 Organiser un système de veille en termes juridique, technique, concurrentiel, écologique, et de sécurité, en identifiant les ressources et les bonnes pratiques, afin d'être force de proposition et d'anticiper les opportunités de développement et de sécurisation des projets.	Toutes les compétences associées (C.1.1 à C.1.7) sont évaluées sur la base de la production suivante : Dans le cadre d'une mise en situation professionnelle reconstituée, à partir d'une étude de cas réel ou fictif, le candidat assure la conception d'une solution logicielle, restituée par : - L'analyse des besoins fonctionnelles associés à la solution. - L'identification et l'analyse des risques associés à la solution logicielle. - Le prototype de la solution logicielle. - Les choix d'architecture et de technologies pour la réalisation de la solution logicielle. - Le plan de développement de la solution logicielle. *Les livrables sont réalisés individuellement et présentés oralement devant un jury d'évaluation.*	- Les objectifs, le périmètre et les priorités de la veille sont définis de manière explicite, en lien avec le contexte de l'organisation et ses projets. - Les ressources mobilisées sont sélectionnées au vu de leur fiabilité et de leur actualité. - Les informations collectées intègrent les enjeux de sécurité, de performance/efficience, d'utilisabilité/accessibilité et d'impact environnemental. - Les signaux relatifs à la sécurité sont analysés en priorité et traduits en propositions argumentées en lien avec la solution projetée.
	C.1.2 Analyser les besoins des parties prenantes du projet, en les traduisant en exigences fonctionnelles et en intégrant les contraintes d'accessibilité conformément au RGAA, afin d'élaborer ou de valider un cahier des charges fonctionnel et technique de la solution numérique à développer.		- Les besoins des parties prenantes sont recueillis et clarifiés, y compris contraintes d'usage, d'exploitation et de conformité. - Les exigences fonctionnelles sont formulées de manière compréhensible, testable et priorisée. - Les exigences techniques (interfaces, données, performance/efficience, environnement d'exécution) et contraintes sont identifiées et cohérentes avec le besoin. - Les exigences et contraintes d'accessibilité et d'utilisation de la solution par les personnes en situation de handicap sont identifiées et prises en compte conformément au RGAA. - Le cahier des charges fonctionnel et technique est complet, structuré et validable.
	C.1.3 Modéliser les menaces et qualifier les exigences de sécurité de la solution numérique à développer, en analysant les actifs, flux, surfaces d'attaque et scénarios d'abus à partir du besoin		- Les actifs, flux, points d'exposition et surfaces d'attaque de la solution projetée sont identifiés. - Les scénarios d'abus/menaces sont modélisés et hiérarchisés (impacts, vraisemblance, risques résiduels). - Les exigences de sécurité en découlant sont explicites, priorisées et testables (contrôles attendus, critères de vérification).

	et du contexte d'usage, afin d'orienter les choix de conception et de réduire le risque dès l'amont.		- Les arbitrages et décisions amont (mesures retenues, risques acceptés, dérogations) sont justifiés et tracés.
	C.1.4 Participer au prototypage de la solution envisagée, en respectant le cahier des charges afin de répondre aux besoins des parties prenantes et prendre en compte les exigences légales et de sécurité (respect de la vie privée sécurisation des interfaces en limitant la surface d'attaques possibles).		- Le prototype respecte le cahier des charges (fonctionnalités visées, parcours, contraintes techniques) et permet la validation avec les parties prenantes. - Les exigences légales et de protection de la vie privée sont prises en compte dans le prototype. - Les interfaces et échanges du prototype intègrent des mesures de sécurisation adaptées. - Les limites du prototype, les écarts et les conditions de passage vers une version industrialisable sont identifiés et documentés.
2. Conception d'une solution logicielle sécurisée *Tâches réalisées* - Définition de l'architecture cible et des choix de conception, intégrant les exigences de sécurité, les contraintes d'exploitation et les dépendances. - Conception des mécanismes de sécurité "by design", incluant gestion des identités et des accès, contrôle d'accès, chiffrement, protections applicatives… - Elaboration d'un plan de sécurisation, incluant schémas d'architecture, spécifications techniques, modèles de données et flux, critères de sécurité testables dans une logique DevSecOps.	C.1.5 Sélectionner les technologies et les données adaptées à la réalisation de la solution numérique, en prenant en compte l'infrastructure nécessaire et les enjeux liés à la sécurité, afin de répondre aux exigences des parties prenantes et de la solution à développer.		- Les technologies retenues (langages, frameworks, services) répondent aux exigences fonctionnelles et aux contraintes d'exploitation identifiées. - Les choix sont justifiés au regard de la sécurité (maturité, correctifs, dépendances, configuration, risques) et de la conformité. - Les données nécessaires sont qualifiées et les modalités de traitement/stockage sont cohérentes avec les exigences. - Les besoins d'infrastructure associés (environnements, intégration, déploiement, exploitation) sont identifiés et compatibles avec la solution visée.
	C.1.6 Concevoir l'architecture et les composants de la solution numérique projetée, en intégrant les exigences de protection, de sécurisation des données et d'accessibilité imposées par le RGAA dans les choix d'architecture, de fonctionnalité et de technologies, afin d'assurer sa résilience, sa maintenabilité et sa sécurisation durable.		- L'architecture et le découpage en composants sont définis en cohérence avec les exigences fonctionnelles et les contraintes d'exploitation. - Les choix d'architecture intègrent la protection des données et réduisent les risques majeurs. - Les propriétés de résilience, de maintenabilité et d'évolutivité sont prises en compte. - L'efficacité énergétique est intégrée comme critère de qualité. - La conception de la solution comprend des modalités techniques conformes au référentiel général d'amélioration de l'accessibilité (RGAA).

- Préparation et organisation du développement de la solution numérique.	C.1.7 Planifier le projet de développement, en ordonnant et en organisant ses étapes, et en répartissant les responsabilités et les tâches en fonction des compétences disponibles, tout en prenant les dispositions favorisant l'inclusion et le maintien dans l'équipe projet des personnes en situation de handicap, afin de répondre aux exigences des parties prenantes en optimisant les délais, les coûts et l'efficacité collective.		- Les étapes du projet sont ordonnancées et structurées avec un plan de suivi. - Les rôles, responsabilités et tâches sont répartis en fonction des compétences et disponibilités, avec des modalités de coordination explicites. - Les dispositions d'accessibilité sont prévues pour permettre la contribution des membres en situation de handicap.
3. Développement sécurisé de la solution numérique *<u>Tâches réalisées</u>* - Mise en œuvre des pratiques de développement, appliquant les standards de code sécurisé, les conventions d'architecture logicielle, et les règles de gestion d'erreurs. - Gestion sécurisée des dépendances et composants, incluant sélection/validation des bibliothèques et configuration sécurisée. - Traçabilité et production des preuves de conformité du développement, incluant documentation technique minimale, enregistrement des décisions/écarts, justification des compromis, et constitution des éléments de preuve nécessaires aux étapes de tests, de validation et d'audit.	C.2.1 Développer les composants applicatifs de la solution numérique selon des pratiques de codage sécurisé, en appliquant les principes secure-by-design/secure-by-default et les référentiels de vulnérabilités usuels (Web/API), afin de prévenir l'introduction de failles dès le développement.	Toutes les compétences associées (C.2.1 à C.2.6) sont évaluées sur la base de la production suivante : Dans le cadre d'une mise en situation professionnelle reconstituée, à partir d'une étude de cas réel ou fictif, le candidat assure le développement d'une solution logicielle, restitué par : - La solution développée. - Le plan de tests de la solution. - La restitution des résultats des tests, incluant les correctifs opérés pour remédier aux vulnérabilités de la solution identifiées. *Les livrables sont réalisés individuellement et présentés oralement devant un jury d'évaluation.*	- Les composants développés respectent des règles de codage sécurisé et évitent les vulnérabilités usuelles. - Les mécanismes "secure-by-design/secure-by-default" sont effectivement appliqués. - Les revues de code et contrôles outillés sont réalisés et les écarts identifiés sont corrigés ou justifiés. - Les éléments de preuve du développement sécurisé sont disponibles.
	C.2.2 Protéger les données sensibles utilisées par la solution numérique, en appliquant les exigences de chiffrement et de gestion des clés et en mettant en œuvre des mesures contre les attaques courantes visant les bases de données, afin d'en préserver la confidentialité et de les prémunir de toute tentative de piratage.		- Les données sensibles sont identifiées et leur traitement est cohérent avec leur niveau de sensibilité. - Les mécanismes de chiffrement et de gestion des clés sont mis en œuvre correctement. - Les protections contre les attaques visant les bases de données sont appliquées.
	C.2.3 Intégrer la maîtrise les dépendances et composants logiciels utilisés par le code, en contrôlant versions, intégrité, provenance, licences et mises à jour, et en traitant les alertes de sécurité associées, afin de limiter l'exposition aux vulnérabilités connues et aux risques de chaîne d'approvisionnement logicielle.		- Les dépendances et composants utilisés sont inventoriés et maîtrisés de manière traçable. - L'intégrité et la provenance des composants sont contrôlées. - Les contraintes de licences sont identifiées et gérées de façon compatible avec le projet et les alertes de sécurité sur dépendances sont traitées.

4. Réalisation des tests de sécurité et validation avant mise en production *Tâches réalisées* - Définition de la stratégie de tests de sécurité et des critères de validation de la solution numérique. - Réalisation et automatisation des vérifications de sécurité, incluant tests applicatifs (DAST), tests sur APIs, contrôles des dépendances/containers, validation des configurations et analyses ciblées. - Conduite des investigations et tests approfondis, incluant reproduction des failles, analyse d'impact, priorisation et, le cas échéant, coordination de tests d'intrusion/évaluations externes. - Décision de validation pré-production, incluant *reporting*, mise à jour du backlog sécurité, vérification des correctifs, gestion des dérogations acceptées et constitution des preuves de conformité.	C.2.4 Elaborer un plan de tests de sécurité, en définissant le périmètre, les scénarios et les critères d'acceptation, afin de sécuriser la décision de mise en production.		- Le périmètre, les scénarios et les critères d'acceptation des tests de sécurité sont définis et reliés aux exigences de sécurité de la solution. - Les contrôles de sécurité outillés sont paramétrés et automatisés dans le cycle de livraison, avec des seuils d'acceptation permettant une décision de mise en production. - Les tests d'intrusion/résilience prévus sont planifiés selon le contexte.
	C.2.5 Mettre en œuvre des tests de sécurité outillés, incluant des tests d'intrusion/résilience, en paramétrant et exécutant les contrôles adaptés au contexte, afin d'identifier et de qualifier les vulnérabilités de la solution développée.		- Les outils et paramètres de tests de sécurité sont choisis et configurés en cohérence avec le contexte applicatif. - Les tests (incluant intrusion/résilience) sont exécutés dans des conditions maîtrisées, et les résultats sont collectés de façon exploitable. - Les vulnérabilités identifiées sont qualifiées et priorisées. - La réalisation des tests et leurs résultats sont documentés.
	C.2.6 Corriger les vulnérabilités et vérifier la non-régression des fonctionnalités de la solution numérique, en appliquant des correctifs et en re-testant, afin de réduire le risque résiduel d'atteindre le niveau de sécurité attendu.		- Les correctifs appliqués répondent aux causes identifiées et sont cohérents avec les exigences de sécurité attendues. - Les re-tests de sécurité confirment la correction et l'absence de réapparition de la vulnérabilité. - Les tests fonctionnels et de non-régression démontrent que les correctifs n'altèrent pas les comportements attendus. - Les décisions de clôture et les preuves associées sont tracées.
5. Intégration et déploiement sécurisés de la solution numérique *Tâches réalisées* - Conception et sécurisation de la chaîne d'intégration et de déploiement (CI/CD).	C.3.1 Industrialiser l'intégration et la livraison en sécurisant la chaîne CI/CD, afin de produire des livraisons reproductibles et conformes au niveau de sécurité attendu.	Toutes les compétences associées (C.3.1 à C.3.6) sont évaluées sur la base de la production suivante : Dans le cadre d'une mise en situation professionnelle reconstituée, à partir d'une étude de cas réel ou fictif, le	- La chaîne d'intégration/livraison est configurée et permet de produire des livrables déployables de manière reproductible. - Les contrôles qualité et sécurité intégrés au pipeline sont effectivement exécutés et leurs résultats sont exploitables. - Des seuils/conditions de passage sont définis et appliqués avant production des livrables (critères d'acceptation, blocage en cas d'écarts).

- Industrialisation des configurations et de l'infrastructure de déploiement de façon sécurisée. - Exécution des déploiements et mise en service sécurisée, incluant vérifications post-déploiement, validation de la configuration effective, activation de la journalisation/monitoring et gestion des accès.	C.3.2 Déployer la solution sur des environnements cibles, en appliquant des procédures d'installation/mise à jour, en vérifiant l'état de santé post-déploiement et en assurant la réversibilité, afin de garantir la disponibilité du service et la maîtrise du risque opérationnel.	candidat assure le déploiement d'une solution logicielle et sa maintenance, restitués par : - L'intégration de la solution dans son infrastructure et son environnement d'utilisation. - La configuration applicative et la sécurisation de l'utilisation de la solution. - La réalisation d'une action de maintenance évolutive contribuant au maintien de la sécurité de la solution. - Le traitement d'un incident de sécurité affectant la solution. - L'audit de sécurité de l'infrastructure de la solution.	- Le déploiement et la mise à jour sont réalisés selon une procédure maîtrisée. - L'état de la solution post-déploiement est vérifié à partir d'éléments observables. - Les écarts ou incidents de déploiement sont tracés et traités (diagnostic, correctifs, mesures de prévention).
	C.3.3 Gérer la configuration applicative et les secrets de déploiement, en séparant configuration et code, en utilisant des mécanismes de stockage/rotation sécurisés, et en contrôlant les droits d'accès, afin de limiter les erreurs de configuration et les expositions accidentelles.		- La séparation code / configuration est effective et appliquée de façon cohérente sur les environnements cibles. - Les secrets sont stockés et distribués via des mécanismes adaptés, avec des droits d'accès maîtrisés. - La mise à jour des secrets est prévue et réalisable sans exposition accidentelle. - Les erreurs de configuration et expositions liées aux secrets sont détectées et corrigées.
6. Maintien en conditions opérationnelles sécurisées et gestion des vulnérabilités de la solution numérique <u>*Tâches réalisées*</u> - Maintenance et exploitation de la solution, incluant qualité de service (performance/disponibilité), supervision (observabilité) et sécurité. - Organisation et exécution du processus de gestion des vulnérabilités, incluant veille/alertes, qualification (sévérité, exploitabilité, impact), priorisation, planification des	C.3.4 Mettre en œuvre la maintenance et le traitement continu des vulnérabilités de la solution numérique, en déployant des correctifs et des éléments de sécurité supplémentaires (patchs correctifs, mises à jour, protocoles, …), afin d'en garantir les fonctionnalités en toute sécurité.	*Les livrables sont réalisés individuellement et présentés oralement devant un jury d'évaluation.*	- Les vulnérabilités et mises à jour de sécurité applicables sont identifiées, qualifiées et priorisées dans la durée. - Les correctifs (patchs, mises à jour, ajustements de configuration/protocoles) sont planifiés et déployés selon un processus maîtrisé. - Les vérifications post-correctifs confirment la remédiation et l'absence de régression significative.
	C.3.5 Contribuer au traitement d'un incident de sécurité sur la solution numérique, en collectant les éléments utiles, en appliquant les actions nécessaires et en produisant un retour d'expérience, afin d'en limiter l'impact et de prévenir sa récurrence.		- Les éléments utiles à l'analyse sont collectés et préservés. - Les actions de contribution à la réponse sont appliquées conformément aux consignes et procédures. - La qualification de l'incident est documentée. - Un retour d'expérience exploitable est produit.

correctifs et gestion des dépendances. - Réalisation des actions de remédiation et de durcissement continu, et gestion des événements de sécurité.	C.3.6 Réaliser un audit technique de sécurité de la solution et de son infrastructure associée, en vérifiant la configuration, l'exposition, les droits, la gestion des secrets, la journalisation et les composants déployés au moyen de référentiels et d'outils adaptés, afin d'identifier les écarts, de prioriser les actions correctives et de réduire les risques en exploitation.		- Le périmètre de l'audit est défini et couvre configuration, exposition, droits, secrets, journalisation et composants. - Les vérifications sont réalisées à partir de référentiels et d'outils adaptés, avec des preuves exploitables. - Les écarts identifiés sont qualifiés et priorisés. - Les actions correctives proposées sont opérationnelles et tracées.
7. Accompagnement des projets de développement, de modernisation et de sécurisation des outils de l'organisation intégrant les innovations technologiques *<u>Tâches réalisées</u>* - Cadrage et appui à la définition des trajectoires de modernisation incluant une technologie innovante. - Analyse de l'existant, identification des écarts (techniques, sécurité, conformité), priorisation et recommandation de scénarios. - Adaptation de l'architecture de la solution en vue de	C.4.1 Identifier l'opportunité et la pertinence de faire appel à des technologies avancées et innovantes (Cybersécurité, IA, VR, Blockchain…) pour l'évolution de la solution numérique, en étudiant leur faisabilité et en analysant les enjeux de sécurité associés, afin d'apporter de la valeur ajoutée pour le produit ou la partie prenante.	Toutes les compétences associées (C.4.1 à C.4.6) sont évaluées sur la base de la production suivante : Dans le cadre d'une mise en situation professionnelle reconstituée, à partir d'une étude de cas réel ou fictif, le candidat propose l'implémentation d'une solution intégrant une technologie émergente, restituée par : - Une étude de faisabilité de la solution. - Les dispositions assurant la sécurisation de la solution. - Les exigences et risques de sécurité de la solution et la sensibilisation de ses parties prenantes.	- Les cas d'usage et la valeur attendue de la technologie envisagée sont clairement identifiés au regard de l'évolution de la solution. - La faisabilité est étudiée (compatibilité avec l'existant, contraintes d'exploitation, coûts/charges, compétences, dépendances). - Les risques de sécurité associés à l'introduction de la technologie sont analysés et qualifiés. - Une recommandation argumentée est produite.
	C.4.2 Proposer une architecture adéquate, pour intégrer des technologies et des usages innovants en respectant une éthique de développement durable, en analysant et en étudiant les différentes possibilités, afin d'assurer la cohérence de la solution finale au regard des différents modules qui la composent.		- Plusieurs options d'architecture d'intégration sont analysées et comparées. - L'architecture proposée explicite les choix structurants et garantit la cohérence globale de la solution. - Les exigences de sécurité sont intégrées dans les choix d'architecture. - Les principes de développement durable sont pris en compte dans les arbitrages, avec justification des choix.

l'intégration des innovations identifiées. - Préconisation des évolutions nécessaires pour maintenir la sécurité de la solution, durant le processus d'intégration de l'innovation.	C.4.3 Faire évoluer la sécurité de la solution au regard des innovations technologiques introduites en améliorant les règles de sécurisation ou en apportant des solutions de sécurisation innovantes, afin de rester en adéquation avec la stratégie de sécurité des parties prenantes.	- La documentation de la solution. *Les livrables sont réalisés individuellement et présentés oralement devant un jury d'évaluation.*	- Les impacts des innovations introduites sur la posture de sécurité sont identifiés. - Les règles de sécurisation sont mises à jour en conséquence et diffusées aux équipes concernées. - Des mesures de sécurisation adaptées sont ajoutées ou renforcées. - L'évolution proposée est cohérente avec la stratégie/exigences de sécurité des parties prenantes, et les arbitrages sont tracés.
8. Sensibilisation des parties prenantes aux enjeux de sécurité *Tâches réalisées* - Analyse des profils de parties prenantes (métiers, IT, produit, direction, prestataires), de leurs interactions avec la solution et les principaux scénarios de risque - Ciblage des messages et des priorités de sensibilisation. - Conception de contenus et de dispositifs de sensibilisation adaptés, incluant supports et formats appropriés. - Animation d'actions de sensibilisation et accompagnement des comportements.	C.4.4 Communiquer les exigences et risques de sécurité du produit, en traduisant les enjeux techniques en messages compréhensibles et actionnables pour les parties prenantes (produit, développement, QA, exploitation), afin d'aligner les décisions de conception, de développement et de déploiement sur un niveau de sécurité attendu.		- Les exigences et risques de sécurité du produit sont synthétisés de façon fidèle et priorisée. - Les messages sont adaptés aux destinataires et traduits en éléments actionnables (décisions, règles, critères). - Les points de décision (arbitrages, dérogations, conditions de passage) sont explicités et compris par les parties prenantes concernées. - Les échanges et décisions sont tracés.
	C.4.5 Documenter les exigences et mécanismes de sécurité de la solution développée, en produisant une documentation technique et d'exploitation (contrôles d'accès, flux, gestion des secrets, règles de validation, journalisation, limites connues) accessible et adaptée aux personnes en situation de handicap, afin de garantir la compréhension des choix de conception et la mise en œuvre correcte des mesures de sécurité par les parties prenantes.		- La documentation produite décrit les exigences et mécanismes de sécurité de manière structurée. - Les informations nécessaires à l'exploitation correcte des mesures de sécurité sont présentes. - La documentation est cohérente avec la solution livrée et maintenable. - Les dispositions permettant l'accessibilité de la documentation aux personnes en situation de handicap sont appliquées.
	C.4.6 Animer des actions de sensibilisation et d'accompagnement intégrant les besoins spécifiques des personnes en situation de handicap, en organisant des ateliers ciblés (revue de risques, démo de vulnérabilités, retour d'expérience d'incidents, revue de code orientée sécurité) et en aidant les équipes à mettre en œuvre les mesures attendues, afin d'améliorer l'appropriation, la conformité et la qualité de réalisation dans la durée.		- Un plan de sensibilisation des parties prenantes est prévu. - Les actions mises en place sont adaptées aux parties prenantes identifiées et aux besoins des personnes en situation de handicap. - Elles comprennent la sensibilisation aux enjeux d'accessibilité aux personnes en situation de handicap, en s'appuyant sur les bonnes pratiques du RGAA et, le cas échéant, en appliquant les normes internationales WCAG. - La sensibilisation des parties prenantes est mesurée avec les outils adaptés (satisfaction, …).