Titre d'ingénieur : spécialité informatique et cybersécurité

Référentiel d'activité, de compétences et référentiel d'évaluation

Référentiel d'activité	Référentiel de compétences	Référentiel d'évaluation : modalités d'évaluation et critères d'évaluation	
		Modalités d'évaluation	Critères d'évaluation
Activité 1 : Concevoir l'architecture de sécurité Il s'assure que les choix techniques et technologiques des projets et métiers respectent les exigences de sécurité de l'organisation. Il constitue l'autorité technique sur les architectures de sécurité, définit les modèles de sécurité et accompagne le développement des architectures de sécurité au sein du SI, en cohérence avec la stratégie IT et les politiques de sécurité de l'organisation. **Activité 2** : Assurer un développement orienté sécurité Il intervient en appui des équipes de développement afin d'accompagner les développeurs dans la prise en compte des exigences de	**Compétences professionnelles du socle commun ingénieur ENSIBS :** • Identifier les codes et les besoins de son écosystème professionnel et les prendre en compte pour la mise en place de solutions techniques ou organisationnelles (pour résoudre des problèmes techniques ou organisationnels) ; • Appliquer et promouvoir la culture sécurité et cybersécurité par des pratiques managériales respectueuses pour garantir la sécurité des biens et des personnes • Coordonner, fédérer et faire collaborer les équipes ainsi que les parties prenantes ; • Gérer les compétences, former les collaborateurs pour un management efficient, dans un contexte pluridisciplinaire et multiculturel ; • Communiquer en mobilisant le bon	**En contexte académique :** • Examens écrits et oraux : Évaluation de la compréhension des fondamentaux, de leur application pratique, et de la capacité à résoudre des problèmes techniques complexes. • Travaux pratiques et projets : Mini-projets, études de cas, et travaux collaboratifs, incluant des partenariats avec entreprises ou laboratoires, évalués sur la qualité des productions écrites (rapports, posters) et orales (présentations, soutenances). • Participation à des événements : Hackathons, European Cyber Week, ou manifestations entrepreneuriales, évalués sur la créativité des solutions, la qualité des présentations et l'efficacité du travail en équipe. **Mise en situation professionnelle :** • Projets semestriels : incluant des partenariats avec des entreprises ou des	**En contexte académique :** Les enseignements académiques sont évalués à l'aide de grilles spécifiques, élaborées à partir des objectifs d'apprentissage validés par l'établissement. **En situation ou contexte professionnel :** • L'efficacité de l'action de management considérée par l'atteinte aux objectifs fixés (qualité des résultats) • La pertinence des méthodes déployées dans les différentes phases et dimensions du projet (qualité de la démarche) • La pertinence des méthodes et outils utilisés au regard des objectifs fixés • La cohérence des actions par la régulation de la démarche et la prise en compte des parties prenantes, la

sécurité. Il teste la sécurité des développements et suit la correction des vulnérabilités identifiées. **Activité 3** : Développer des solutions de sécurité Le développeur de solutions de sécurité intervient au sein de sociétés d'éditions de produits informatiques. Il assure les spécifications et la conception de solutions et de produits de sécurité adaptés au contexte des menaces de cybersécurité. **Activité 4** : Intégrer des solutions de sécurité Il contribue au choix de l'architecture de la solution de sécurité et en assure l'assemblage au sein du SI. Il intègre dans l'environnement de production la solution de sécurité et en assure le déploiement. Il peut également assurer l'exploitation et le maintien en conditions opérationnelles dans la durée à travers la fourniture d'un service de sécurité managé.	registre de communication selon l'interlocuteur pour atteindre ses objectifs ; • Critiquer, remettre en cause ses décisions et anticiper pour assurer l'agilité de l'organisation ; • Adapter sa pratique pour répondre aux enjeux et besoins de la société, en intégrant le développement durable et l'éthique dans ses actions. • Piloter des projets complexes en appliquant les approches agiles : de l'analyse du besoin à sa recette, en passant par la rédaction du cahier des charges, l'allocation des ressources, la planification, et le retour d'expérience, contribuant ainsi à la réalisation de la stratégie de l'entreprise. • Intégrer systématiquement la dimension économique dans l'ensemble de ses missions • Assurer la communication, à tous les niveaux de l'organisation, y compris institutionnelle, en français et en anglais pour être compris sans ambiguïté • Identifier la démarche entrepreneuriale. **Compétences spécifiques du spécialiste en Informatique et Cybersécurité :** • Réaliser des études bibliographiques ; • Construire des expérimentations respectant les règles de l'art ;	laboratoires, évalués sur la qualité des résultats (produit réalisé), des productions écrites (rapports, posters) et orales (présentations, soutenances). • Exercice de synthèse : durant la dernière semaine de l'école, les élèves travaillent dans une entreprise simulée, avec des objectifs de production et des évènements, liés à des attaques cybernétiques, pour garantir le maintien en condition opérationnelle du système. **En contexte professionnel :** • Alternance (Apprentis) : Suivi des apprentis via des rapports d'activité périodiques et des fiches mission validées par le tuteur entreprise. • Stages (Etudiants) : Validation par un rapport final, une soutenance orale, et une fiche d'évaluation remplie par le tuteur professionnel. • Projet de fin d'études (PFE) : Validation par un rapport final, une soutenance orale, et une fiche d'évaluation remplie par le tuteur professionnel. **Compétences linguistiques et internationales :** • Validation des compétences linguistiques : Niveau B2 du CECRL en anglais (via une certification reconnue) et maîtrise professionnelle de l'orthographe française (certification reconnue). • Validation des compétences interculturelles : Collaboration et adaptation dans des environnements multiculturels, démontrées par une	critique des résultats • La Cohérence des indicateurs mis en place pour le suivi du projet et de ses résultats • L'impact de la solution retenue et déployée : acceptation par les parties prenantes, réplicabilité et adaptation. • L'impact du projet par l'identification des causes, des enjeux, des parties prenantes et l'intégration des facteurs économiques, sociaux et environnementaux • L'efficacité des actions par la qualité des résultats obtenus au regard des objectifs • L'efficience du projet examinée dans la relation des résultats obtenus au regard des moyens mobilisés • La pertinence de l'étude bibliographique pour le problème à traiter et de l'expérimentation vis-à vis des résultats attendus ; • L'efficience des résultats obtenus au vu des moyens utilisés (ressources bibliographiques, outils pour l'expérimentation) ; • L'impact des résultats obtenus en termes d'innovation et d'avancée technologique ; • La pertinence des solutions techniques choisies au vu des propriétés de sécurités recherchées ; • La cohérence des solutions conçues vis-à-vis des réglementations en vigueur des normes et des exigences liées au domaine

Activité 5 : Piloter des projets Il assure la formation des utilisateurs et celle des collaborateurs, ainsi que le développement de ces derniers. Il coordonne des équipes pluridisciplinaires dans le cadre de projets de conception ou d'évolution de systèmes d'information sécurisés. Il supervise l'intégration des sous-systèmes en veillant à la compatibilité technique et aux exigences de sécurité. Pour cela, il utilise des outils collaboratifs et adopte approche agile pour améliorer la réactivité et l'innovation. **Activité 6** : Communiquer Il communique efficacement, avec parties prenantes, sur les résultats techniques, la prise en compte des contraintes économiques et réglementaires. Il montre l'adéquation de la conduite des projets avec les exigences environnementales et sociétales.	• Connaître les différentes approches de validations de solutions innovantes ; • Connaître les principes et les méthodes de la veille technologique ; • Connaître les outils qui permettent de préserver la propriété intellectuelle ; • Connaître et promouvoir les techniques nouvelles (innovation, vulgarisation, information, formation) ; • Communiquer et négocier, à l'oral et à l'écrit y compris en anglais et dans un contexte international ; • Adapter sa communication en fonction du contexte socioculturel et du niveau de compétences techniques de ses interlocuteurs ; • Discerner les différents concepts de la sécurité logicielle ; • Respecter les normes de gouvernance des systèmes d'information et de communication ; • Appliquer et maîtriser le maintien en condition opérationnelle et le soutien logistique intégré ; • Appliquer et maîtriser les méthodes statistiques ; • Exploiter les techniques de classification et d'analyse à partir d'un modèle de données ; • Exploiter les techniques de projection et de prédiction à partir d'un modèle de données ; • Appliquer et maîtriser l'ingénierie des tests (fonctionnels et de	mobilité internationale significative.	d'application. • L'efficacité des solutions, de sécurité proposée, face à des attaques connues. • La pertinence des fonctionnalités proposées par rapport aux besoins exprimés par le client. • La cohérence de la conception proposée par rapport aux exigences de sécurité. • L'efficacité de l'équipe de réalisation en mesurant le niveau de réalisation par rapport aux objectifs initiaux. • La durabilité du produit réalisé mesurée en termes de facilité d'évolution et du niveau d'impact sur l'environnement des solution techniques mises en œuvre.

Activité 7 : Réaliser des recherches en sécurité des systèmes d'information Il se consacre à l'expérimentation et au progrès de sa discipline. Il met en œuvre, aux frontières de plusieurs champs scientifiques constitués, ses acquis techniques et académiques au service d'une problématique de sécurité au plus haut niveau scientifique. Il mobilise des connaissances expertes pour contribuer à l'émergence de technologies novatrices et de savoirs inédits. Il participe au développement de produits, de procédés ou de services innovants.	sécurité) ; • Connaître les principes et outils de scan de vulnérabilités logicielles ; • Appliquer et maîtriser l'ingénierie de la qualification ; • Connaître et savoir appliquer les mathématiques et la statistique de base ; • Comprendre les interfaces numériques liées à l'utilisation conjointe de l'informatique avec l'électronique, l'automatique et la mécanique ; • Comprendre et utiliser le matériel, les systèmes d'exploitation et les réseaux ainsi que les techniques de virtualisation ; • Être capable d'utiliser les différents langages de modélisation, d'analyse et de programmation des systèmes ; • Exploiter l'urbanisation et l'architecture des systèmes à logiciel prépondérant ; • Gérer des systèmes d'informations et des données. • Maîtriser les fondamentaux scientifiques et technologiques en informatique et cybersécurité.		