Référentiel RNCP – Niveau 6 « Bachelor en Sciences et Ingénierie - cybersécurité défensive »

Article L6113-1 En savoir plus sur cet article... Créé par LOI n°2018-771 du 5 septembre 2018 - art. 31 (V) « *Les certifications professionnelles enregistrées au répertoire national des certifications professionnelles permettent une validation des compétences et des connaissances acquises nécessaires à l'exercice d'activités professionnelles. Elles sont définies notamment par un* ***référentiel d'activités*** *qui décrit les situations de travail et les activités exercées, les métiers ou emplois visés, un* ***référentiel de compétences*** *qui identifie les compétences et les connaissances, y compris transversales, qui en découlent et un* ***référentiel d'évaluation*** *qui définit les critères et les modalités d'évaluation des acquis.* »

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*	**RÉFÉRENTIEL D'ÉVALUATION** *Définit les critères et les modalités d'évaluation des acquis*	
		MODALITES D'EVALUATION	**CRITÈRES D'ÉVALUATION**
Bloc de compétences 1 : Mobiliser des connaissances et des logiques issues des mathématiques et des sciences physiques pour participer à la conception de systèmes de défense de réseaux informatiques			
A1.1 Langages de programmation et algorithmique, variables, structures de contrôle, fonctions et passage de paramètres. A1.2 Compréhension des principes généraux du traitement de données par des machines binaires et des mécanismes et concepts fondamentaux propres aux traitements informatiques. A1.3 Manipulation d'expressions algébriques A1.4 Intégration des relations interpersonnelles et gestion de conflits A1.5 Prise en compte de l'obsolescence numérique	BC 1.1 Appliquer des concepts mathématiques BC 1.2 Mobiliser des connaissances scientifiques et techniques élevées BC 1.3 Intégrer des modèles pour modéliser un problème donné BC 1.4 Résoudre des problèmes en utilisant les mathématiques BC 1.5 Choisir l'outil le plus adapté pour répondre à une problématique bien identifiée BC 1.6 Savoir utiliser une large variété d'outils complexes BC 1.7. Employer des langages de programmation de référence BC 1.8 Intégrer la programmation frugale et les problèmes d'obsolescence numérique en utilisant des outils adaptés	L'évaluation des acquis s'effectue dans le cadre d'un contrôle continu des connaissances par semestre. Chaque évaluation conduit à une note sur 20. **Devoirs écrits individuels** **Examens de travaux pratiques individuels en laboratoires** **Projets individuels ou en équipe**	Critère 1 : Les productions individuelles du candidat permettent d'évaluer l'acquisition de ces compétences. Critère 2 : Le candidat démontre la mise en pratique de ses connaissances durant des séances de travaux pratiques. Critère 3 : Le candidat met en œuvre et applique ses concepts mathématiques lors de ses travaux en projet (Ex : Start Up Week Critère 4 : Le Candidat présente des exemples d'outils et les mets en application : Business Plan.

Bloc de compétences 2 : Mobiliser des connaissances en informatique et réseaux pour collaborer à la mise en place des systèmes de défense contre les attaques informatique			
A2.1 Maitrise de du “hardware” (ordinateurs, réseaux, IOT…) A2.2 Connaissance des systèmes d’exploitation et des réseaux informatiques dans leur globalité A2.3 Maitrise de plusieurs langages de développement A2.4 Sécurisation du système d’information d’une entreprise A2.5 Sensibilisation à l’informatique durable (Green IT)	BC 2.1 Connaitre l’architecture d’un ordinateur, celle des réseaux et les blocs composant les objets connectés BC 2.2 Administrer un environnement système, réseaux et cloud computing BC 2.3 Optimiser les données d'un système d'information BC 2.4 Concevoir, sécuriser et actualiser des infrastructures et réseaux en prenant compte l’impact environnementale de l’ensemble BC 2.5 Concevoir et développer la couche applicative d'un système d'information BC 2.6 Réaliser et développer une solution logicielle sécurisée en évitant les fonctionnalités superflues à l’impact écologique certain	L’évaluation des acquis s’effectue dans le cadre d’un contrôle continu des connaissances par semestre. Chaque évaluation conduit à une note sur 20. Devoirs écrits individuels Examens de travaux pratiques individuels en laboratoires Projets individuels ou en équipe Soutenance devant un jury	Critère 1 : Dans le cadre d'un projet, le candidat est capable de construire une architecture SI, en s'appuyant sur un schéma conceptuelCritère 2 : Le candidat sait décrire les fonctionnalités de chaque composant d'une architecture et mettre en place des éléments de sécurisation de l'architecture Critère 3 : Le candidat développe et utilise des applications / outils afin de permettre un déploiement et une mise en production plus rapide de l'architecture (Infrastructure As Code) Critère 4 : Le candidat manipule des systèmes d'exploitation et de réseaux, dans une infrastructure locale ou dans le cloud en respectant les bonnes pratiques d'administration Critère 5 : Le candidat installe une solution applicative en l'interconnectant avec sa base de données

Bloc de compétences 3 : Appliquer les bonnes pratiques pour analyser et tester les outils de détection d'anomalies d'un système d'information			
A3.1 Veille professionnelle sur l'actualité liée à la sécurité A3.2 Connaissances des solutions proposées au niveau de la sécurité des systèmes d'informations : pare-feu, antivirus A3.3 Connaissances des méthodes de test d'intrusion (Pentest) A3.4 Accompagnement des équipes dans la sécurisation du SI	BC 3.1 Se tenir à jour sur les failles, malwares et toute autres menaces existantes BC 3.2 Installer et mettre à jour les outils de protection de base (pare-feu, antivirus) BC 3.3 Effectuer des tests d'intrusion de manière éthique BC 3.4 Déterminer les failles d'un système d'information pour les résorber BC 3.5 Proposer des solutions dans une optique de sécurisation optimale BC 3.6 Gérer les vulnérabilités et les risques pour éviter tout futur incident	L'évaluation des acquis s'effectue dans le cadre d'un contrôle continu des connaissances par semestre. Chaque évaluation conduit à une note sur 20. **Devoirs écrits individuels** **Examens de travaux pratiques individuels en laboratoires** **Projets individuels ou en équipe**	Critère 1 : Le candidat présente un outil de veille informatique (outil de curation) afin de centraliser sa veille et s'informer de manière efficace Critère 2 : Le candidat installe des outils de sécurité en les paramétrant de manières optimisées en accord avec les besoins d'un cahier des charges Critère 3 : Le candidat respecte un protocole d'hacking éthique et sait décrire les comportements d'hacking à risques Critère 4 : Le candidat est capable de s'introduire dans un système d'information au cours d'un TP Critère 5 : Le candidat est capable de s'introduire dans un système d'information au cours d'un TP

Bloc de compétences 4 : Poser un diagnostic et mettre en œuvre un système de réponses à incidents performant pour optimiser la mise en place d'actions correctives			
A4.1 Analyse du risque et de l'impact de l'incident A4.2 Recherche de preuves sur des supports numériques (analyse forensic) A4.3 Mise en place d'un plan de restauration A4.4 Rédaction d'un retour d'expérience de l'incident (REx) A4.5 Mise en place de nouvelles mesures de défense	BC 4.1 Identifier les menaces sur l'informatique d'une société lors d'une attaque BC 4.2 Identifier les ressources non touchées par l'incident et qui vont permettre une poursuite d'activité BC 4.3 Mettre en place des mesures d'atténuations de l'incident BC 4.3 Comprendre l'origine de l'incident pour le contrecarrer le plus efficacement possible BC 4.4 Rétablir les activités une fois l'incident maitrisé BC 4.5 Analyser l'incident et ses conséquences pour corriger les failles utilisées et améliorer le SI BC 4.6 Implémenter de nouveaux mécanismes de défense pour se protéger de manière plus efficace	L'évaluation des acquis s'effectue dans le cadre d'un contrôle continu des connaissances par semestre. Chaque évaluation conduit à une note sur 20. **Devoirs écrits individuels** **Examens de travaux pratiques individuels en laboratoires** **Projets individuels ou en équipe**	Critère 1 : Le candidat sait reconnaitre les actifs critiques d'une entreprise en se basant sur des données fournies dans une étude de cas Critère 2 : Le candidat installe et met en œuvre une centralisation des journaux d'événements systèmes afin de faciliter ses recherches lors d'une attaque informatique. Critère 3 : A l'aide de lectures des journaux systèmes, le candidat sait faire état d'une éventuelle attaque sur les systèmes et proposer des solutions pour bloquer l'attaque Critère 4 : Au vu des connaissances, le candidat implémente de nouveaux mécanismes pour diminuer les surfaces d'attaques des systèmes Critère 5 : Le candidat propose au jury un moyen de sauvegarde des données, en local ou dans le cloud, et présente leurs restaurations afin de lutter contre les attaques de types ransomware

Bloc de compétences 5 : Maitriser les règlementation nationales et internationales de la sécurité des réseaux et systèmes d'information pour éclairer les prises de décisions liées à la sécurité informatique en collaboration avec des ingénieurs et non ingénieurs dans un contexte international			
A5.1 Veille sur les législations liées à la sécurité au niveau d'un pays ou d'un groupe d'états (UE) A5.2 Connaissance des normes ISO A5.3 Pédagogie auprès d'interlocuteurs non formés à l'aspect technique de la sécurité informatique A5.4 Collaborer avec des équipes internationales	BC5.1 Répondre à toutes les situations liées à la sécurité informatique quel que soit le contexte géographique BC5.2 Accompagner un client (interne ou externe) à travers un plan d'actions d'amélioration du niveau de sécurité en respectant les obligations réglementaires et normatives BC5.3 Expliquer de manière claire, en français et/ou en anglais, les tenants et aboutissants des choix stratégiques effectués BC5.4 Être capable de manager des équipes multiculturelles BC5.5 Savoir s'adapter dans toutes les situations	L'évaluation des acquis s'effectue dans le cadre d'un contrôle continu des connaissances par semestre. Chaque évaluation conduit à une note sur 20. **Devoirs écrits individuels** **Examens de travaux pratiques individuels en laboratoires** **Projets individuels ou en équipe** **Evaluation TOEIC**	Critère 1 : Lors d'une étude de cas, le candidat met en avant les différences législatives réglementaires en matière de sécurité informatique selon le contexte géographique où l'on se trouve Critère 2 : Le candidat est capable de mener une étude de risques, en classifiant les risques selon une échelle de criticité, et proposer des contre-mesures aux risques exprimées Critère 3 : Le candidat arrive à prendre la parole en public afin d'animer une présentation, et proposer un planning prévisionnel en obtenant la compréhension de tous sur les sujets présentés Critère 4 : Le candidat sait présenter un projet en anglais tout en étant capable de répondre aux questions à bon escient

Bloc de compétences 6 : Appréhender la complexité des situations économiques et sociales pour entreprendre, innover et apprendre tout au long de sa vie professionnelle			
A6.1 Application d'outils et de méthodes de modélisation et de simulation afin d'optimiser des systèmes complexes sous contraintes multiple A6.2 Intégration de la connaissance des systèmes complexes (interdisciplinarité et approche systémique) afin de concevoir, développer, améliorer et innover dans l'ingénierie des systèmes complexes A6.3 Intervention en recherche, innovation et prospective commerciale A6.4 Identification les avancées technologiques et déployer des solutions créatives	BC6.1 Construire des composants dans le langage d'une base de données. BC6.2 Conceptualiser, transposer un phénomène ou une situation complexe en sujet de recherche et le problématiser BC6.3 Développer selon une démarche de recherche une analyse critique de la production scientifique BC6.4 Faire un bilan objectif et critique des avancées de ses propres travaux, d'identifier la valeur ajoutée par rapport aux travaux antérieurs ; BC6.5 Décrire le processus d'exploitation commerciale de résultats de recherche pour être à même d'identifier les occasions de contribuer à la coopération entre la recherche universitaire, la recherche industrielle et l'ensemble des secteurs de production dans un objectif d'innovation.	L'évaluation des acquis s'effectue dans le cadre d'un contrôle continu des connaissances par semestre. Chaque évaluation conduit à une note sur 20. **Devoirs écrits individuels** **Examens de travaux pratiques individuels en laboratoires** **Projets individuels ou en équipe** **Projet tutoré.** **Soutenance devant un jury professionnel**	Critère 1 : Le choix des composants dans le langage d'une base de données est pertinent Critère 2 : Des indicateurs d'activité sont présentés de façon synthétique et visuelle et permettent d'opérer un bilan objectif Critère 3 : Le candidat propose une structuration des résultats de recherche Critère 4 : Le candidat présente un bilan structuré et critique permettant d'identifier la valeur ajoutée des travaux Critère 5 : le candidat présente les opportunités commerciales de ses résultats de recherche Critère 6 : le candidat présente ses travaux en intégrant des opportunités d'innovation.

Bloc de compétences 7 : Mettre en place une veille technique et des recherches bibliographiques pour recueillir et exploiter des données pertinentes			
A7.1 Organisation et animation d'un système de veille active pour se tenir à jour sur les offres et solutions d'architecture des SI A7.2 Analyse des indicateurs d'activité des solutions choisies pour identifier les besoins de mises à jour ou d'évolutions du SI A7.3 Organisation et animation d'un système de veille active pour se tenir à jour sur les menaces en cyber sécurité et solutions de sécurisation	BC7.1 Déterminer les axes de la veille technologique BC7.2 Sélectionner les outils adéquats (logiciels, moteurs de recherche…) et les paramétrer BC7.3 Sélectionner des services de banques de données adaptés à la recherche BC7.4 Utiliser les critères booléens BC7.5 Pratiquer les techniques de recherche d'informations dans des bases de données scientifiques BC7.6 Exploiter les bilans de veille BC7.7 Constituer une revue de littérature académique et/ou professionnelle sur un sujet BC7.8 Maintenir et développer continuellement ses connaissances et compétences	L'évaluation des acquis s'effectue dans le cadre d'un contrôle continu des connaissances par semestre. Chaque évaluation conduit à une note sur 20. **Devoirs écrits individuels** **Examens de travaux pratiques individuels en laboratoires** **Projets individuels ou en équipe** **Soutenance devant un jury professionnel**	Critère 1 : La veille professionnelle proposée par le candidat sert les enjeux du système d'information et permet d'adapter les solutions techniques. Critère 2 : Des indicateurs d'activité sont présentés de façon synthétique et visuelle et permettent la prise de décision pour un maintien ou une évolution des solutions choisies. Critère 3 : Une structure de revue de littérature est présentée Critère 4 : Le candidat présente au moins une technique de recherche d'information dans les bases de données scientifiques. Critère 5 : le candidat présente un exemple concret permettant d'identifier les techniques utilisées pour l'exploitation de la veille. Critère 6 : Le candidat présente un ou 2 outils lui permettant maintenir ou de développer ses compétences (sites de référence, abonnements, séminaires, webinaires…)

Le cas échéant, description de tout autre document constitutif de la certification professionnelle