Bachelier en Informatique, orientation sécurité des systèmes

PRESENTATION DE LA FORMATION ET DU PROFIL D'ENSEIGNEMENT

Année académique 2026-2027

1. Identification de la Haute Ecole

1. Nom de la Haute Ecole : **Haute Ecole Libre Mosane (HELMo)**
2. Adresse du siège social : **Mont St-Martin 45 - 4000 Liège**
3. Réseau : **Libre Confessionnel**

2. Identification de la formation

1. Intitulé de la section concernée : **Section « Informatique » - Orientation « sécurité des systèmes »**
2. Localisation de la formation : **HELMo Campus Guillemins, rue de Harlez 35 à 4000 Liège**
3. Classement de la formation :
   a) Enseignement supérieur de type **court**
   b) Catégorie d'enseignement supérieur : **Technique**
   c) Secteur : **Sciences et techniques**
   d) Domaine : **Sciences**
   e) Grade académique : **Bachelier** (niveau 6)

3. Présentation générale de la formation et du profil d'enseignement

La formation de bachelier en informatique, orientation sécurité des systèmes se réfère au niveau 6 du cadre des certifications.

La formation débouchant sur le grade de bachelier en informatique, orientation sécurité des systèmes (les autres orientations sont : informatique industrielle, réseaux et télécommunications, développement d'applications, technologies de l'informatique, intelligence artificielle) est organisée dans le cadre du Décret du 7 novembre 2013 définissant le paysage de l'enseignement supérieur et l'organisation académique des études. Elle s'inscrit donc dans les objectifs généraux de ce décret dont notamment « garantir une formation au plus haut niveau, tant générale que spécialisée, tant fondamentale et conceptuelle que pratique, en vue de permettre aux étudiants et étudiantes de jouer un rôle actif dans la vie professionnelle, sociale, économique et culturelle, et de leur ouvrir des chances égales d'émancipation sociale ».

La formation de bachelier en informatique, orientation sécurité des systèmes organisée par l'enseignement supérieur de type court correspond au niveau 6 du cadre européen de certification. Le grade de bachelier est décerné aux étudiants et étudiantes qui :

- ont acquis des connaissances approfondies et des compétences dans un domaine de travail ou d'études qui fait suite à, et se fonde sur, une formation de niveau d'enseignement secondaire supérieur. Ce domaine se situe à un haut niveau de formation basé, entre autres, sur des publications scientifiques ou des productions artistiques, ainsi que sur des savoirs issus de la recherche et de l'expérience ;
- sont capables d'appliquer, de mobiliser, d'articuler et de valoriser ces connaissances et ces compétences dans le cadre d'une activité socioprofessionnelle ou de la poursuite d'études et ont prouvé leur aptitude à élaborer et à développer dans leur domaine d'études des raisonnements, des argumentations et des solutions à des problématiques ;
- sont capables de collecter, d'analyser et d'interpréter, de façon pertinente, des données, généralement dans leur domaine d'études, en vue de formuler des opinions, des jugements critiques ou des propositions artistiques qui intègrent une réflexion sur des questions sociétales, scientifiques, techniques, artistiques ou éthiques ;
- sont capables de communiquer, de façon claire et structurée, à des publics avertis ou non, des informations, des idées, des problèmes et des solutions, selon les standards de communication spécifiques au contexte ;
- ont développé des stratégies d'apprentissage qui sont nécessaires pour poursuivre leur formation avec un fort degré d'autonomie.

En outre, les détenteurs et détentrices d'un bachelier en informatique, toutes orientations devront pouvoir :

- gérer des activités ou des projets techniques ou professionnels complexes, en faisant preuve de responsabilité dans la prise de décisions dans des contextes professionnels ou d'études imprévisibles ;
- prendre des responsabilités en matière de développement professionnel individuel et collectif ;
- sensibiliser, par la nature de leur formation, aux valeurs sociétales et surtout aux principes du développement durable et à la responsabilité, dans ces matières, les entreprises qui les emploient ;
- assimiler les évolutions rapides des technologies utilisées dans ses domaines de compétences.

Quelle que soit son orientation, il ou elle :

- maîtrise le développement, le déploiement, la maintenance et la sécurité du flux quotidien de l'information numérique d'une entreprise ;
- analyse, développe et documente des solutions ICT en réponse à des besoins spécifiques ;
- installe et maintient des systèmes et des réseaux de communication de tous types ainsi que des applications, qu'elles soient locales ou distantes ;
- assure la mise en place et la maintenance des équipements matériels et des applications aux utilisateurs.

Spécifiquement à l'orientation en sécurité des systèmes, il ou elle :

- analyse et met en œuvre un système informatique sécurisé ;

- assure la sécurité des systèmes informatiques, en adoptant une démarche de sécurisation suivant une méthodologie.

Le diplômé ou la diplômée d'un bachelier en informatique, toutes orientations exerce son activité professionnelle dans tout type d'organisation ou d'entreprise publique ou privée, marchande ou non marchande, nationale ou internationale, de petite, moyenne ou grande taille.

À ce titre, l'informaticien ou l'informaticienne dispose de compétences générales en informatique et se spécialise dans son orientation.

Profil professionnel

Professionnellement, le détenteur ou la détentrice d'un bachelier en informatique, orientation sécurité des systèmes fait partie des « ICT workers ». Ce concept regroupe un ensemble étendu de profils métiers essentiellement centrés sur le développement, le déploiement et la maintenance du flux quotidien de l'information numérique d'une entreprise.

Sans que cette liste ne soit exhaustive et définitive, il ou elle est capable d'exercer les métiers ICT en sécurité des systèmes : consultant ou consultante en intrusion informatique, analyste SOC, ingénieur sécurité réseau, analyste en risques et conformité (RGPD, ISO 27001…), pentester, expert en forensique numérique, responsable sécurité des systèmes d'information (RSSI), …

Le bachelier ou la bachelière en informatique, orientation sécurité des systèmes fait partie du personnel technicien supérieur capable d'assurer la sécurité et l'intégrité des systèmes, des applications, des logiciels et des réseaux informatiques, en adoptant une démarche de sécurisation suivant une méthodologie.

Il ou elle travaille seul ou en équipe et est en contact avec des client·es et/ou des utilisateurs·trices.

Vu l'évolution constante du marché du travail, il ou elle s'adapte et se forme afin d'être efficient·e tout au long de sa carrière.

Il ou elle développe une communication efficace au travers de la documentation de son travail et de l'utilisation de techniques écrites et orales vis-à-vis d'interlocuteurs·trices informaticien·nes ou non.

4. Acquis d'apprentissage terminaux et Référentiel de compétences

Au terme de sa formation, l'étudiant sera capable de :

1. Communiquer et informer :

- Choisir et utiliser les moyens d'informations et de communication adaptés
- Mener une discussion, argumenter et convaincre de manière constructive
- Assurer la diffusion vers les différents niveaux de la hiérarchie (interface)
- Utiliser le vocabulaire adéquat
- Présenter des prototypes de solution et d'application techniques
- Utiliser une langue étrangère

2. Collaborer à la conception, à l'amélioration et au développement de projets:

- Élaborer une méthodologie de travail
- Planifier des activités et évaluer la charge et la durée de travail liées à une tâche
- Analyser une situation donnée sous ses aspects techniques et scientifiques
- Rechercher et utiliser les ressources adéquates
- Proposer des solutions qui tiennent compte des contraintes
- Documenter son travail afin d'en permettre la traçabilité et le cycle de vie

3. S'engager dans une démarche de développement professionnel :

- Prendre en compte les aspects éthiques et déontologiques
- S'informer et s'inscrire dans une démarche de formation permanente
- Développer une pensée critique
- Travailler tant en autonomie qu'en équipe dans le respect de la structure de l'environnement professionnel

4. S'inscrire dans une démarche de respect des réglementations :

- Participer à la démarche qualité
- Respecter les normes, les procédures et les codes de bonne pratique
- Respecter les prescrits légaux en vigueur relatifs au contexte dans lequel s'exerce l'activité (exemple code du bien-être au travail, RGPD, le droit à l'image, licences logicielles…)

Orientation : sécurité des systèmes

5. Collaborer à l'analyse et à la mise en œuvre d'un système informatique sécurisé

- Évaluer le risque informatique au sein d'un système ICT en respectant une norme d'analyse
- Identifier les composantes de la sécurité
- Identifier les faiblesses des dispositifs de sécurité implémentés, concernant l'infrastructure, les applicatifs et les systèmes
- Prendre en considération les défaillances matérielles, humaines, prévisibles ou non
- Proposer une solution technique répondant à une analyse en prenant en considération les aspects juridiques, organisationnels, éthiques et économiques
- Identifier les zones de risques juridiques et déterminer les mesures à prendre pour y répondre adéquatement

6. Assurer la sécurité des systèmes informatiques, en adoptant une démarche de sécurisation suivant une méthodologie

- Respecter les normes, méthodologies, et standards de sécurité
- Évaluer la sécurité des systèmes, en identifiant les faiblesses, et adapter les solutions implémentées
- Configurer et déployer de manière efficace, les dispositifs de sécurité, et en assurer la maintenance
- Assurer la performance et la disponibilité des systèmes, ainsi que l'intégrité et la confidentialité des données

5. Organisation en unités de formation

BLOC 1

		C	H
C1-B1-Q1-UE1	Réseaux informatiques		
	Réseaux informatiques	4	54
C1-B1-Q1-UE2	Systèmes d'exploitation		
	Systèmes d'exploitation	4	50
C1-B1-Q1-UE3	Programmation de base		
	Programmation de base	6	72
C1-B1-Q1-UE5	Bases de données		
	Bases de données	3	36
C1-B1-Q1-UE6	Technique de communication		
	Technique de communication	2	30
C1-B1-Q2-UE13	Analyse de risques		
	Analyse de risques	3	46
C1-B1-Q1-44	Compétences numériques		
	Compétences numériques	1	10
C1-B1-Q1-Q2-UE7	Mathématiques appliquées		
	Mathématiques appliquées	7	74
C1-B1-Q2-UE8	Anglais		
	Anglais	3	36
C1-B1-Q2-UE9	Techniques web		
	Techniques web	2	22
C1-B1-Q2-UE10	Gestion d'un système de sécurité de l'information		
	Gestion d'un système de sécurité de l'information	3	32
C1-B1-Q2-UE11	Sécurité des réseaux		
	Sécurité des réseaux	4	42
C1-B1-Q2-UE12	Systèmes d'exploitation (avancé)		
	Systèmes d'exploitation (avancé)	3	32
C1-B1-Q2-UE14	Intégration de la sécurité 1		
	Intégration de la sécurité 1	4	42
C1-B1-Q2-45	Aspects organisationnels juridiques et éthiques		
	Aspects organisationnels juridiques et éthiques	1	12
C1-B1-Q2-48	Introduction à l'analyse forensic		
	Introduction à l'analyse forensic	5	54
C1-B1-Q2-47	Scripting		
	Scripting	3	32
C1-B1-Q2-UE60	Fondamentaux IA		
	Fondamentaux IA	2	24

BLOC 2

		C	H
C1-B2-Q1-UE15	Organisation du secteur de l'informatique		
	Organisation du secteur de l'informatique	2	24
C1-B2-Q1-UE16	Aspects éthiques et juridiques		
P : UE10	Aspects éthiques et juridiques	2	22
C1-B2-Q1-UE17	Sécurité des bases de données		
P : UE5	Sécurité des bases de données	3	36
C1-B2-Q1-UE18	Mathématiques et physique appliquées		
P : UE3,7	Mathématiques et physique appliquées	4	48
C1-B2-Q1-UE19	Gestion de la sécurité opérationnelle		
P : UE10	Gestion de la sécurité opérationnelle	5	64
C1-B2-Q1-UE61	Option : Retro-ingénieurie		
P : UE48	Option : Retro-ingénieurie	6	58
C1-B2-Q1-UE62	Option : Introduction à l'analyse forensic		
	Option : Introduction à l'analyse forensic	6	58
C1-B2-Q1-UE21	Architectures sécurisées		
P: UE1,10,11	Architectures sécurisées	4	42
C1-B2-Q1-UE25	Anglais		
P: UE8	Anglais	3	36
C1-B2-Q1-UE23	Sécurité des infrastructures réseaux		
P : UE1, UE11	Sécurité des infrastructures réseaux	2	24
C1-B2-Q2-UE22	Technique de communication		
P : UE6 C : UE29	Technique de communication	3	30
C1-B2-Q2-UE24	Sécurité matérielle		
	Sécurité matérielle	3	36
C1-B2-Q2-UE26	Vulnérabilités: principes & outils		
P : UE1,9	Vulnérabilités: principes & outils	6	72
C1-B2-Q2-UE27	Administration système		
P : UE2,11, 47	Administration système	6	70
C1-B2-Q2-UE28	Monitoring : principes et protocoles		
P : UE1,2, 47 C : UE18	Monitoring : principes et protocoles	6	70
C1-B2-Q2-UE29	Intégration de la sécurité 2		
P : UE3,14 C : UE26,27,28	Intégration de la sécurité 2	5	60

BLOC 3

		C	H
C1-B3-Q1-UE30	Cloud	2	28
P : UE19	Cloud		28
C1-B3-Q1-UE31	Savoir être et culture d'entreprise	4	58
P : UE15,16,25	Management		22
	Soft skills		36
C1-B3-Q1-UE32	Entrepreneuriat	4	48
P : UE15,16	Entrepreneuriat		36
	Dynamique de groupes		12
C1-B3-Q1-UE63	Sécurité des systèmes IA	2	26
P : UE21,23,26	Sécurité des systèmes IA		26
C1-B3-Q1-UE 46	Sécurité de l'IOT	2	24
P : 21, 23	Sécurité de l'IOT		24
C1-B3-Q1-UE34	Sécurité des infrastructures réseaux 2	2	24
P : UE21,23 C: UE33	Sécurité des infrastructures réseaux 2		24
C1-B3-Q1-UE35	Configurer pour sécuriser	2	20
P: UE27	Configurer pour sécuriser		20
C1-B3-Q1-UE36	Vulnérabilités : Principes et outils 2	2	24
P : UE26	Vulnérabilités : Principes et outils 2		24
C1-B3-Q1-UE37	Monitoring : Principes et outils	2	24
P: UE28	Monitoring : Principes et outils		24
C1-B3-Q1-UE39	Technique de communication	3	30
P : UE22 C : 43	Technique de communication		30
C1-B3-Q1-UE40	Aspects éthiques et juridiques	2	20
P : UE15,16	Aspects éthiques et juridiques		20
C1-B3-Q1-UE41	Conférences - Visites - Séminaires	2	24
P : UE29 C : UE42	Conférences - Visites - Séminaires		24
C1-B3-Q1 et/ou Q2-UE42	Insertion professionnelle	24	0
P : UE 24,26,27,28,29 C : UE30,31,32,34,35, 36, 37,39,40,41, 43, 46,63	Insertion professionnelle		
C1-B3-Q1 et/ou Q2-UE43	Mémoire	7	
C: UE42	Travail écrit		
	Défense orale		
	Communication ecrite et orale en langue française		12

6. Justifications des modifications apportées par rapport à la version de 2025-2026 et des UEs sur 2 quadrimestres

- En Bloc 1
    - UE9 Techniques Web : diminue du nombre de crédits de 3 à 2 crédits pour se recentrer sur la découverte du web (client-serveur, DOM, …) sans aborder ses vulnérabilités.
    - UE47 Scripting : diminue du nombre de crédits de 4 à 3 crédits pour se concentrer sur le scripting à proprement parlé sans aborder des paradigmes de programmation.
    - UE60 Fondamentaux IA : création d'une nouvelle UE de 2 crédits. L'intelligence artificielle s'impose désormais comme une composante incontournable du paysage des menaces et des outils défensifs en cybersécurité. Former nos étudiants dès le B1 à ses fondements — sans en faire des spécialistes — leur permet d'aborder les UEs avancées avec le recul critique nécessaire pour exploiter ces technologies à bon escient et en comprendre les risques intrinsèques.
- En Bloc 2
    - UE16 Aspects éthiques et juridiques : diminue du nombre de crédits de 3 à 2 crédits.
    - UE20 Analyse: est abandonnée. Les acquis d'apprentissage « Interpréter et expliquer des diagrammes documentant des processus métiers » et « Modéliser des processus métiers simples au moyen des mêmes diagrammes » sont entrainés dans l'UE13 Analuse de risques.
    - UE61 Retro-ingénieurie : création d'une nouvelle UE de 6 crédits. Cette UE s'inscrit naturellement dans la continuité de l'introduction à l'analyse forensique dispensée en B1, en approfondissant la capacité des étudiants à disséquer et comprendre le comportement interne des systèmes et des logiciels malveillants. Ce fil conducteur forensique, construit sur deux années, répond directement aux attentes des employeurs dans les domaines du DFIR et de l'analyse de malware.
    - UE62 Introduction à l'analyse forensic : création d'une nouvelle UE optionnelle de 6 crédits. Les étudiants ayant échoué à l'UE20 analyse et n'ayant pas eu l'UE48 Introduction à l'analyse forensic (introduite en 25-26) auront cette UE temporaire dans leur PAE.
- En Bloc 3
    - UE33 Architecture sécurisée 2: est abandonnée afin d'éviter les nombreuses redondances avec l'UE du même nom de B2.
    - UE63 Sécurité des systèmes IA : création d'une nouvelle UE de 2 crédits. Les systèmes d'IA sont désormais déployés au cœur des infrastructures critiques et des outils de sécurité eux-mêmes, créant une surface d'attaque nouvelle que les cyberprofessionnels ne peuvent ignorer. Cette UE en B3 permet aux étudiants, forts

de leur maîtrise technique acquise en B1 et B2, de comprendre et d'anticiper les vulnérabilités spécifiques aux modèles ML et aux LLM — une compétence encore rare sur le marché et fortement différenciante.