EPHEC
HAUTE ÉCOLE

Structure du profil d'enseignement et programme d'études

BACHELIER EN INFORMATIQUE
Orientation « sécurité des systèmes »

Haute Ecole EPHEC – Avenue Konrad Adenauer, 3 – 1200 Bruxelles.	
DOMAINE	17 - Sciences
DEPARTEMENT	Informatique, Orientation « Sécurité des systèmes »
IMPLANTATION	Louvain-La-Neuve
ANNEE ACADEMIQUE	2026-2027

TABLE DES MATIERES

I. ADN pédagogique de la HE EPHEC

Notre ADN pédagogique se décline selon cinq axes : les fondements de notre formation, notre vision à horizon 2026, les valeurs de notre institution, le positionnement pédagogique et l'esprit d'entreprendre.

1.1. Les fondements

Depuis sa création en 1969, l'EPHEC se fonde sur la conviction que le premier cycle d'études supérieures peut être organisé en abordant de plain-pied la formation spécialisée, que partir de problèmes concrets motive fortement jeunes et adultes, les aide à se structurer l'esprit et les forme en peu de temps.

Notre enseignement supérieur de type court

- est axé sur des formations à contenus pratiques centrées sur le développement de compétences propres à un profil professionnel déterminé ;
- favorise le développement d'un savoir-être «social »;
- favorise la prise de responsabilité dans l'organisation du travail;
- implique une participation active aux processus d'apprentissage;
- vise une efficience opérationnelle immédiate des diplômés

1.2. Notre vision

Notre vision à 2026 pour l'ASBL EPHEC-Galilée est définie comme suit : *« L'employabilité durable par la révélation de talents et le développement des compétences professionnelles. Par ses formations, ses projets de recherche appliquée et ses services à la collectivité, en s'appuyant sur ses valeurs et sa culture, l'EPHEC assure à ses partenaires une approche professionnalisante et entrepreneuriale, un écosystème d'expérimentation, une communauté de partage et un environnement favorisant la reconnaissance et l'épanouissement professionnel. »*

1.3. Les valeurs

Les valeurs sont essentielles pour assurer une culture d'entreprise privilégiant l'autonomie et le développement des compétences individuelles et collectives. Cinq valeurs essentielles guident les choix et décisions de l'ASBL EPHEC-Galilée : l'imagination, la responsabilité, l'ambition, l'intégrité et la bienveillance.

1.4. Positionnement pédagogique

Depuis sa création, l'ASBL EPHEC-Galilée fonde sa pédagogie sur sa volonté de proposer des formations pratiques, professionnalisantes et de proximité. La pédagogie comprend le volet « enseignement » et le volet « apprentissage », tous deux en interaction. De nouveaux rôles sont dévolus à l'enseignant, pour accompagner l'étudiant dans son parcours de plus en plus individualisé. Pour les remplir, il faut miser sur une **pédagogie ouverte, différenciée** et qui développe chez l'étudiant **son esprit d'entreprendre**. Nous voulons soutenir le

développement professionnel des enseignants et promouvoir l'innovation pédagogique, notamment grâce à l'exploitation du potentiel lié aux technologies numériques, mais aussi encourager les équipes à évaluer régulièrement l'impact de ces nouvelles méthodes sur la progression de l'apprentissage des étudiants.

1.5. L'esprit d'entreprendre

Par sa conception de la formation supérieure et ses orientations professionnalisantes et pratiques, l'esprit d'entreprendre fait partie de l'ADN de l'EPHEC.

En insufflant à tous nos étudiants tout au long de leurs études cet esprit d'entreprendre, fait de persévérance, de créativité, d'optimisme, d'esprit d'équipe et d'autonomie, nous les incitons à se mettre en projet, ce qui favorise leur future employabilité.

Depuis décembre 2015, la Haute Ecole EPHEC reconnaît le statut académique d'étudiant entrepreneur, afin de soutenir les jeunes qui, parallèlement à leur parcours de formation, désirent se lancer dans le monde de l'entrepreneuriat. Ce statut d'étudiant entrepreneur, accordé sur dossier, donne la possibilité aux étudiants concernés de concilier plus facilement leurs études et la création d'une entreprise : aménagements horaires, motivation de certaines absences liées à leurs activités entrepreneuriales, accès à une série de formules d'accompagnement, à des conférences, échanges avec entrepreneurs et études de cas.

Pratiquement, deux structures sont organisées localement, une à Louvain-la-Neuve- et une à Bruxelles. Cet ancrage local permet également de collaborer plus aisément avec les acteurs locaux. Ces cellules, bénéficiant de subsides régionaux, ont pour objectif d'accompagner, de mettre en lumière et en réseau les étudiants et les anciens à profil entrepreneur.

II. ADN du Bachelier en Informatique de l'EPHEC (Sécurité des systèmes)

2.1. Valeurs

- La responsabilité
- L'intégrité
- L'imagination

Le bachelier en Informatique, orientation Sécurité des systèmes, adopte des valeurs qui prônent la responsabilité, l'intégrité et l'imagination dans toutes les actions qu'il est amené à entreprendre.

2.2. Compétences

- Le bachelier est capable d'autonomie et de proactivité face aux situations rencontrées dans la vie professionnelle, il a le sens des responsabilités vis-à-vis des objectifs à atteindre et de la qualité de son travail.
- Les compétences vues ci-avant doivent s'appuyer sur une approche méthodologique, rigoureuse et méticuleuse, tout en faisant preuve de cohérence et d'éthique.
- La formation s'inscrit dans une pluridisciplinarité bien nécessaire face aux multiples facettes du métier et à la polyvalence des problématiques rencontrées.
- La résolution de problèmes pratiques s'appuie sur une capacité d'abstraction propre à la pédagogie inductive proposée, il est capable d'imaginer les bonnes solutions.

2.3. Accents particuliers dans la formation

- La formation familiarise l'étudiant à la résolution de problèmes qui n'est possible que dans le cadre de l'acquis de techniques précises et approfondies.
- La résolution d'un problème n'est possible qui si l'on a su poser un diagnostic clair et complet.
- La formation assure une approche adaptée pour permettre d'intégrer et faire communiquer différents composants software et hardware dans un environnement hétérogène, en offrant l'acquisition de nombreuses compétences en informatique (Administration systèmes, Réseaux, Développement, Electronique, Télécommunication, …) Elle privilégie une approche pratique et par projets.

III. Référentiel de compétences du Bachelier en Informatique, Orientation Sécurité des systèmes

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, sécurité des systèmes, 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

3.1. 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 à caractère technique : développeur ou développeuse, programmeur ou programmeuse, gestionnaire de réseau, consultant·e en informatique, web développeur ou développeuse, helpdesk …

Le bachelier ou la bachelière en informatique, orientation sécurité des systèmes fait partie du personnel technicien supérieur capable d'intégrer et de faire communiquer différents composants software et hardware dans un environnement hétérogène.

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.

3.2. Compétences

Compétences communes à toutes les orientations

1. Communiquer et informer

1. Choisir et utiliser les moyens d'informations et de communication adaptés
2. Mener une discussion, argumenter et convaincre de manière constructive
3. Assurer la diffusion vers les différents niveaux de la hiérarchie (interface entre les collaborateurs, la hiérarchie et/ou les clients)
4. Utiliser le vocabulaire adéquat
5. Présenter des prototypes de solution et d'application techniques
6. Utiliser une langue étrangère

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

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

3. S'engager dans une démarche de développement professionnel

1. Prendre en compte les aspects éthiques et déontologiques
2. S'informer et s'inscrire dans une démarche de formation permanente
3. Développer une pensée critique
4. 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

1. Participer à la démarche qualité
2. Respecter les normes, les procédures et les codes de bonne pratique
3. 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

1. Évaluer le risque informatique au sein d'un système ICT en respectant une norme d'analyse

2. Identifier les composantes de la sécurité
3. Identifier les faiblesses des dispositifs de sécurité implémentés, concernant l'infrastructure, les applicatifs et les systèmes
4. Prendre en considération les défaillances matérielles, humaines, prévisibles ou non
5. Proposer une solution technique répondant à une analyse en prenant en considération les aspects juridiques, organisationnels, éthiques et économiques
6. 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

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

IV. Acquis d'apprentissage Terminaux (AAT) en Informatique, orientation Sécurité des systèmes de l'EPHEC

Au terme du cursus de Bachelier en Informatique, orientation Sécurité des systèmes, les bacheliers :

- 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 et sécurité 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 :

- identifie et d'explique des vulnérabilités courantes qui s'appliquent au système logiciel sélectionné, ainsi que les contres mesures et pratiques de développement sécurisé adéquates pour ces vulnérabilités ;
- conçoit, modifie ou étend, sur base d'une analyse des besoins, un système logiciel dans le respect de l'état de l'art des pratiques du développement sécurisé ;
- identifie et d'explique les enjeux, les technologies, les risques et les principes essentiels à la fonction de détection dans un processus de CyberSécurité ;
- sélectionne le processus (les méthodes, outils, procédures, paramètres et technologies) appropriés à la fonction de détection ;
- réalise des démarches sur base d'un scénario donné ;
- identifie et d'explique les enjeux, les technologies, les risques et les principes essentiels en CyberSécurité matérielle (hardware security), physique ou logique ;
- explique différents concepts, modèles, pratiques et principes liés à la sécurisation des réseaux des systèmes d'information ;
- analyse et explique les aspects des protocoles réseaux et des protocoles de sécurités faisant usage des réseaux, dont les faiblesses, les vulnérabilités et leurs traces de communications ;
- conçoit et met en pratique des attaques sur des protocoles réseaux ou faisant usage de ces réseaux ;
- identifie des outils et des technologies de sécurisation des réseaux systèmes d'information et de communication appropriés.

V. Architecture du Bachelier en Informatique, Orientation Sécurité des systèmes

Programme de cours du Bachelier en Informatique orientation Sécurité des systèmes

Ouverture de la formation prévue en septembre 2026, en attente de la décision finale de la Ministre de l'Enseignement Supérieur

AGENCEMENT PAR UNITÉS D'ENSEIGNEMENT (UE) ET PAR ACTIVITÉS D'APPRENTISSAGE (ACTA)

UE DU BLOC 1

TECHNOLOGIE DES ORDINATEURS	5
ÉLECTRICITÉ I	5
ÉLECTRONIQUE I	5
TÉLÉCOMMUNICATIONS I	5
MATHÉMATIQUE	5
ANGLAIS I	5
RÉSEAUX I	5
SYSTÈMES D'EXPLOITATION I	5
LOGIQUE ET PROGRAMMATION ORIENTÉE WEB	7
STRUCTURE ET DONNÉES	8
INTRODUCTION À LA SÉCURITÉ INFORMATIQUE	5

UE DU BLOC 2

DÉVELOPPEMENT INFORMATIQUE II	5
RÉSEAUX II	5
RÉSEAUX III	5
SYSTÈMES D'EXPLOITATION II ET ADMIN. SYSTÈME ET RÉSEAUX I	5
CRYPTOGRAPHIE CONCEPTS ET USAGES	3
SÉCURISATION DES SYSTÈMES D'EXPLOITATION	5
ÉLECTRONIQUE II	2
SÉCURITÉ DES SYSTÈMES EMBARQUÉS ET IOT	5
TÉLÉCOMMUNICATIONS II	5
ANGLAIS II	5
APPROCHE ÉTHIQUE DE L'ENTREPRISE	5
SÉCURITÉ APPLICATIVE	5
GESTION DES DONNÉES I ET SEMAINE INTERNATIONALE	5

UE DU BLOC 3

ADMINISTRATION ET SÉCURISATION DES RÉSEAUX	5
IA DÉTECTION DE MENACE ET AUTOMATISATION	5
SÉCURITÉ DES TÉLÉCOMMUNICATIONS SATELLITAIRES	5
GESTION ET RÉPONSES AUX INCIDENTS	3
RED TEAM VS BLUE TEAM	5
VEILLE TECHNOLOGIQUE	2
DÉONTOLOGIE, RSE ET DROIT LIÉ À L'INFORMATIQUE	3
COMMUNICATION	2

STAGE & PORTFOLIO	14
TFE	16

5.1. Unités d'enseignements (UE) réparties sur le quadrimestre 1 et le quadrimestre 2

UE – BLOC 1	UE – BLOC 2
Anglais I	Anglais II

Les UE sont réparties sur 2 quadrimestres car elles constituent des fondements de la formation et nécessitent un apprentissage progressif.

5.2. Cohérence de la formation

Les unités d'enseignement du bloc 1 constituent les fondements essentiels nécessaires à la poursuite du cursus, l'étudiant y acquerra les bases des ordinateurs, des réseaux, des télécoms, de la programmation, de l'électronique, de l'électricité et des systèmes d'exploitation. L'étudiant acquerra la capacité à communiquer en anglais autour des thématiques de la vie courante.

Dans le bloc 2, l'étudiant renforcera et développera ses compétences en programmation, base de données, réseaux, systèmes d'exploitation, télécommunications et électronique. L'accent est également mis sur la communication et la gestion de projet et sur la préparation des étudiants au monde de l'entreprise. L'étudiant aura également l'occasion d'améliorer ses compétences techniques et humaines dans le cadre d'une semaine internationale.

Le bloc 3 sera consacré à l'intégration des compétences. L'étudiant renforcera et développera ses compétences en administration et sécurisation des réseaux, en base de données, en traitement de signal. L'accent sera mis sur l'entreprise avec des cours tels que la déontologie, la responsabilité sociétale des entreprises et la communication. On y développera l'autonomie, la responsabilisation et l'analyse réflexive des étudiants notamment au travers des activités d'intégration que sont le projet d'intégration, le stage et le travail de fin d'études.

VI. Programme en ECTS

Bloc	Intitulé		ects
1	**CY101 - Technologie des ordinateurs**		**5**
1	CY1011 - Technologie des ordinateurs (Théorie)	3,5	
1	CY1012 - Technologie des ordinateurs (Pratique)	1,5	
1	**CY104 - Electricité**		**5**
1	**CY107 - Electronique I**		**5**
1	CY1071 - Electronique analogique (Théorie)	2	
1	CY1072 - Electronique analogique (Pratique)	3	
1	**CY109 - Mathématique**		**5**
1	**CY110 - Anglais I**		**5**
1	**CY111 - Réseaux I**		**5**
1	CY1111 - Réseaux I (Théorie)	2	
1	CY1112 - Réseaux I (Pratique)	3	
1	**CY112 - Systèmes d'exploitation I**		**5**
1	CY1121 - Systèmes d'exploitation I (Théorie)	2	
1	CY1122 - Systèmes d'exploitation I (Pratique)	3	
1	**CY113 - Développement informatique I : Logique et programmation orientée web**		**7**
1	CY1131 - Logique et programmation orientée web (Théorie)	3	
1	CY1132 - Logique et programmation orientée web (Pratique)	4	
1	**CY114 - Développement informatique I : Structures et données et projet transversal**		**8**
1	CY1141 - Structures et données (Théorie)	3	
1	CY1142 - Structures et données (Pratique)	4	
1	CY1143 – Projet transversal	1	
1	**CY115 – Signaux I : Canaux de communication**		**5**
1	CY1151 - Signaux I : Canaux de communication (Théorie)	2,5	
1	CY1152 - Signaux I : Canaux de communication (Pratique)	2,5	
1	**CY116 Introduction à la cybersécurité**		**5**
1	CY1161 - Introduction à la cybersécurité (Théorie)	3	
1	CY1162 - Introduction à la cybersécurité (Pratique)	2	
			60

Bloc	Intitulé	ects	
2	**CY201 - Développement informatique II**	**5**	
2	**CY203 - Réseaux II**	**5**	
2	**CY204 - Réseaux III**	**5**	
2	**CY205 - Administration système et réseaux I**	**5**	
2	CY2051 - Systèmes d'exploitation II (Théorie)		1
2	CY2052 - Systèmes d'exploitation II (Pratique)		1,5
2	CY2053 - Administration systèmes et réseaux I (Théorie)		1
2	CY2054 - Administration systèmes et réseaux I (Pratique)		1,5
2	**CY207 - Electronique II**	**2**	
2	**CY208 - Télécommunications II**	**5**	
2	**CY209 - Anglais II**	**5**	
2	**CY210 - Approche éthique de l'entreprise**	**5**	
2	CY2101 - Anthropologie		1
2	CY2102 - Communication		1,5
2	CY2103 - Approche de l'entreprise		1
2	CY2104 - Gestion de projet		1,5
2	**CY212 - Gestion des données I et semaine internationale ou interdisciplinaire**	**5**	
2	CY2121 - Gestion des données I		3
2	CY2122 - Semaine internationale ou interdisciplinaire		2
2	**CY213 - Sécurité des systèmes d'exploitation**	**5**	
2	**CY214 - Sécurité des systèmes embarqués et IoT**	**5**	
2	**CY215 - Sécurité applicative**	**5**	
2	**CY216 - Cryptographie, concepts et usages**	**3**	

Bloc	Intitulé	ects	
3	**CY301 - Administration et sécurisation des réseaux**	**5**	
3	CY3011 - Administration des réseaux (Théorie)		1
3	CY3012 - Administration des réseaux (Pratique)		1,5
3	CY3013 - Sécurité des réseaux (Théorie)		1
3	CY3014 - Sécurité des réseaux (Pratique)		1,5
3	**CY305 - Informatique et Société**	**5**	
3	CY3051 - Déontologie et RSE		1,5
3	CY3052 - Droit lié à l'informatique		1,5
3	CY3053 - Communication		2
3	**CY306 - Stage + portfolio**	**14**	
3	**CY307 - TFE**	**16**	
3	**CY308 - IA détection des menaces et automatisation**	**5**	
3	**CY309 - Sécurité des télécommunications**	**5**	
3	**CY310 - Gestion et réponse aux incidents**	**3**	
3	**CY311 - Red team vs Blue team**	**5**	
3	**CY312 - Veille technologique**	**2**	
		60	

VII. Compatibilité avec le référentiel des compétences

Code Secu	Bloc	Intitulé	C1.1.	C1.2.	C1.3.	C1.4.	C1.5.	C1.6.	C2.1.	C2.2.	C2.3.	C2.4.	C2.5.	C2.6	C3.1.	C3.2.	C3.3.	C3.4.	C4.1.	C4.2.	C4.3.	C5.1.	C5.2.	C5.3.	C5.4.	C5.5.	C6.1.	C6.2.	C6.3.	C6.4.
CY101	1	CY101 - Technologie des ordinateurs																												
CY101-CY1011	1	CY1011 - Technologie des ordinateurs (Théorie)					1				1													1						
CY101-CY1012	1	CY1012 - Technologie des ordinateurs (Pratique)														1									1					
CY104-CY1041	1	CY104 - Electricité I								1	1										1									
CY107	1	CY107 - Electronique I																												
CY107-CY1071	1	CY1071 - Electronique analogique (Théorie)									1		1								1									
CY107-CY1072	1	CY1072 - Electronique analogique (Pratique)										1	1								1									
CY108-CY1081	1	CY108 - Télécommunications I				1	1				1	1	1								1									
CY109-CY109	1	CY109 - Mathématique				1							1																	
CY110-CY110	1	CY110 - Anglais I		1		1		1																						
CY111	1	CY111 - Réseaux I																												
CY111-CY1111	1	CY1111 - Réseaux I (Théorie)						1								1											1			
CY111-CY1112	1	CY1112 - Réseaux I (Pratique)						1										1									1			
CY112	1	CY112 - Systèmes d'exploitation I																												
CY112-CY1121	1	CY1121 - Systèmes d'exploitation I (Théorie)				1						1																1		
CY112-CY1122	1	CY1122 - Systèmes d'exploitation I (Pratique)										1																1		
CY113	1	CY113 - Développement informatique I : Logique et programmation orientée web																												
CY113-CY1131	1	CY1131 - Logique et programmation orientée web (Théorie)							1				1									1								
CY113-CY1132	1	CY1132 - Logique et programmation orientée web (Pratique)											1										1							1
CY114	1	CY114 - Développement informatique I : Structures et données																												
CY114-CY1141	1	CY1141 - Structures et données (Théorie)					1															1								
CY114-CY1142	1	CY1142 - Structures et données (Pratique)																					1							1
CY115-CY115	1	CY115 - Introduction à la cyber sécurité	1		1																									

Code Secu	Bloc	Intitulé	C1.1	C1.2	C1.3	C1.4	C1.5	C1.6	C2.1	C2.2	C2.3	C2.4	C2.5	C2.6	C3.1	C3.2	C3.3	C3.4	C4.1	C4.2	C4.3	C5.1	C5.2	C5.3	C5.4	C5.5	C6.1	C6.2	C6.3	C6.4
CY201-CY2011	2	CY201 - Développement informatique II							1													1	1							1
CY203-CY2031	2	CY203 - Réseaux II								1			1									1		1			1			
CY204-CY2041	2	CY204 - Réseaux III																							1		1	1		
CY205-CY2052	2	CY2052 - Systèmes d'exploitation II (Pratique)					1						1										1							
CY205-CY2053	2	CY2053 - Administration systèmes et réseaux I (Théorie)									1																1	1		
CY205-CY2054	2	CY2054 - Administration systèmes et réseaux I (Pratique)									1																1	1		
CY207-CY207.Q1	2	CY207 - Electronique II									1													1					1	
CY208-CY208	2	CY208 - Télécommunications II										1	1								1									
CY209-CY209	2	CY209 - Anglais II		1		1		1																						
CY210	2	CY210 - Approche éthique de l'entreprise																												
CY210-CY2101	2	CY2101 - Anthropologie													1		1													
CY210-CY2102	2	CY2102 - Communication	1	1		1																								
CY210-CY2103	2	CY2103 - Approche de l'entreprise																	1	1										
CY210-CY2104	2	CY2104 - Gestion de projet							1	1				1																
CY212	2	CY212 - Gestion des données I et semaine internationale ou interdisciplinaire																												
CY212-CY2121	2	CY2121 - Gestion des données I									1		1																	
CY212-CY2122	2	CY2122 - Semaine internationale ou interdisciplinaire					1	1										1												
CY213-CY213	2	CY213 - Sécurité des systèmes d'exploitation																		1									1	
CY213-CY213	2	CY213 - Sécurité des systèmes d'exploitation																		1									1	
CY214-CY214	2	CY214 - Sécurité des systèmes embarqués et IoT																		1									1	
CY215-CY215	2	CY215 - Sécurité applicative												1						1										
CY216-CY216	2	CY216 - Cryptographie, concepts et usages				1					1	1								1										

Code Secu	Bloc	Intitulé	C1.1.	C1.2.	C1.3.	C1.4.	C1.5.	C1.6.	C2.1.	C2.2.	C2.3.	C2.4.	C2.5.	C2.6	C3.1.	C3.2.	C3.3.	C3.4.	C4.1.	C4.2.	C4.3.	C5.1.	C5.2.	C5.3.	C5.4.	C5.5.	C6.1.	C6.2.	C6.3.	C6.4.
CY301	3	CY301 - Administration et sécurisation des réseaux																												
CY301-CY3011	3	CY3011 - Administration des réseaux (Théorie)					1																		1		1			
CY301-CY3012	3	CY3012 - Administration des réseaux (Pratique)														1								1		1				
CY301-CY3013	3	CY3013 - Sécurité des réseaux (Théorie)																						1		1				
CY301-CY3014	3	CY3014 - Sécurité des réseaux (Pratique)											1													1	1			
CY305	3	CY305 - Informatique et Société																												
CY305-CY3051	3	CY3051 - Déontologie et RSE													1		1		1											
CY305-CY3052	3	CY3052 - Droit lié à l'informatique	1																1	1										
CY305-CY3053	3	CY3053 - Communication	1	1		1																								
CY306-CY306	3	CY306 - Stage + portfolio	1		1										1			1												
CY307-CY307	3	CY307 - TFE			1		1		1							1	1	1												
CY308-CY308	3	CY308 - IA détection des menaces et automatisation													1		1													
CY309-CY309	3	CY309 - Sécurité des télécommunications																						1				1		
CY310-CY310	3	CY310 - Gestion et réponse aux incidents			1									1						1										
CY311-CY311	3	CY311 - Red team vs Blue team												1				1											1	
CY312-CY312	3	CY312 - Veille technologique																			1				1					

VIII. Respect des contenus minimaux

Sécurité des systèmes Contenus minimaux	CY101 - Technologie des ordinateurs	CY104 - Electricité I	CY107 - Electronique I (analogique)	CY108 - Télécommunications I	CY109 - Mathématique	CY110 - Anglais I	CY111 - Réseaux I	CY112 - Systèmes d'exploitation I	CY113 - Logique et programmation orientée web	CY114 - Structures et données	CY115 - Introduction à la sécurité informatique		CY201 - Développement informatique II	CY203 - Réseaux II	CY204 - Réseaux III	CY2061-CY2062 - Systèmes d'exploitation II	CY2063-CY2064 - Administration système et réseaux	CY216 – Cryptographie Concepts et Usages	CY213 – Sécurisation des systèmes d'exploitation	CY207 - Electronique II (digitale)	CY214 – Sécurité des Systèmes Embarqués et IOT	CY208 - Télécommunications II	CY209 - Anglais II	CY210 - Approche éthique de l'entreprise	CY215 - Sécurité Applicative	CY2121 - Gestion des données I	T2122 - 3ème Internationale		CY301 - Administration et sécurisation des réseaux	CY308 – IA Détection de menace et automatisation	CY305-CY3051 - Déontologie et RSE	CY305-CY3052 - Droit lié à l'informatique	CY305-CY3053 -Communication	CY306 - Sécurité des Télécommunications	CY310 - Gestion et réponses aux incidents	CY311 - Red team vs Blue team	CY312 - Veille technologique
Formation générale (50)																																				
Fonctionnement des systèmes Architecture – systèmes d'exploitation - réseaux	4,5						4,5	5		2																										
Analyse et programmation informatique									6	6			5																							
Mathématiques et/ou statistiques appliquées	0,5				5		0,5		1																										
Communication et/ou langues étrangère						5																	5												
Liberté PO (36)			5	5																2		5		5		2	2			1,5	1,5	2	5			
Orientation Sécurité des systèmes (64)																																				
Principes de la sécurité											3			3	3	1,5	1,5	2	2						2	1			2						1	1	
Méthodologies de la sécurisation											1			1	1	1	1	1	1						1				2						1	2	
Outils pour la sécurité informatique											1			1	1				2						2				1	5					1	2	2
Sciences appliquées		5																			5															

Description et Contenus des Unités d'enseignement propres à l'orientation.

EPHEC Bachelier en Informatique – Orientation « sécurité des systèmes »

Les fiches des cours communs aux deux orientations « Technologies de l'informatique » et « Sécurité des Systèmes » sont disponibles sur notre site.

CY116 - Introduction à la Cybersécurité

Bloc : 1
Quadrimestre : Q2
Crédits ECTS : 5.0

UE prérequise(s) à cette UE : aucun
Cette UE est corequise avec les UE : aucun
Cette UE est prérequise pour les UE : aucun

Cette UE contribue à l'atteinte des compétences suivantes :
Compétences communes :
1.1 : Choisir et utiliser les moyens d'informations et de communication adaptés.
1.3 : Assurer la diffusion vers les différents niveaux de la hiérarchie (interface entre les collaborateurs, la hiérarchie et/ou les clients).

Acquis d'apprentissage spécifiques :
Au terme de l'activité d'apprentissage, l'étudiant sera sensibilisé aux enjeux de la sécurité informatique et de son impact sur l'organisation d'une entreprise.
L'apprenant pourra :

- Contextualiser les objectifs clés de la sécurité informatique (disponibilité, intégrité, confidentialité) ainsi que les objectifs secondaires (non-répudiation, autorisation, traçabilité…) ;
- Expliquer les notions permettant de mettre en place les objectifs précités (identification, chiffrement, disponibilité, stratégie de sécurité…) ;
- Définir la notion de risque informatique en fonction des notions de : vulnérabilité – menace – impact ;
- Identifier les menaces et vulnérabilités courantes ;
- Comprendre le rôle des principaux intervenants agissant dans la sécurité informatique ;
- Définir le rôle des principales instances du secteur qui influencent le domaine.
- Appréhender les mesures de protection de base.
- Laboratoires :
    - Études de cas sur des incidents de sécurité célèbres ;
    - Analyse de vulnérabilités simples et mise en place de correctifs.

CY213 - Sécurisation des systèmes d'exploitation

Bloc : 2
Quadrimestre : Q2
Crédits ECTS : 5.0

UE prérequise(s) à cette UE : aucun
Cette UE est corequise avec les UE : aucun
Cette UE est prérequise pour les UE : aucun

Cette UE contribue à l'atteinte des compétences suivantes :

Compétences communes :
4.2 : Respecter les normes, les procédures et les codes de bonne pratique.
Compétences liées à l'orientation :
6.3 : Configurer et déployer de manière efficace, les dispositifs de sécurité, et en assurer la maintenance.

Acquis d'apprentissage spécifiques :

Au terme de l'activité d'apprentissage, l'étudiant sera sensibilisé à la sécurisation des systèmes d'exploitation. Que ce soit pour des services internes, externes ou dans le Cloud.
Au terme de l'activité, l'apprenant pourra :

- Comprendre et mettre en place une politique d'authentification pour les utilisateurs sous Linux ou Windows en fonction d'un contexte donné ;
- Identifier et expliquer les vulnérabilités pouvant amener à une élévation de privilèges sur des machines Linux ou Windows ;
- Utiliser, expliquer et mettre en place différents types de contrôle d'accès (Active Directory, PAM…) ;
- Utiliser et élaborer des scripts (Powershell, Bash, Python…) dans un contexte de sécurité informatique ;
- Utiliser et d'exploiter des outils d'audit ou de renforcement de la sécurité (SELinux, PingCastle…) ;
- Reconnaître et évaluer les métriques pertinentes d'un système d'exploitation Linux ou Windows en vue de la mise en place d'un système de monitoring.
- Laboratoires :
    - Études de cas sur des incidents de sécurité célèbres ;
    - Sécurisation d'un serveur ou d'un client Linux / Windows ;
    - Analyse et prévention des attaques sur Linux / Windows ;
    - Utilisation et interprétation d'outils d'audit ou de renforcement de la sécurité.

CY214 - Sécurité des Systèmes Embarqués et IOT

Bloc : 2
Quadrimestre : Q2
Crédits ECTS : 5.0

UE prérequise(s) à cette UE : aucun
Cette UE est corequise avec les UE : aucun
Cette UE est prérequise pour les UE : aucun

Cette UE contribue à l'atteinte des compétences suivantes :

Compétences communes :
4.2 : Respecter les normes, les procédures et les codes de bonne pratique.
Compétences liées à l'orientation :
6.3 : Configurer et déployer de manière efficace, les dispositifs de sécurité, et en assurer la maintenance.

Acquis d'apprentissage spécifiques :

Utilisation de cartes de développement (comme Arduino ou Raspberry Pi) pour simuler des systèmes embarqués et expérimenter avec la sécurité des microcontrôleurs et des protocoles IoT.

- Au terme de l'activité, l'étudiant sera capable de :
- Définition et caractéristiques des systèmes embarqués ;
- Différencier les systèmes embarqués classiques et IoT ;
- Appréhender les applications courantes des IoT (domotique, santé, automobile, etc.) ;
- Comprendre les architectures matérielles et logicielles typiques des systèmes embarqués.
- Découvrir les vulnérabilités des systèmes embarqués ;
- Apprendre à sécuriser les communications entre les dispositifs IoT ;
- Comprendre les conséquences d'une compromission dans les environnements IoT.
- Mettre en œuvre des contre-mesures pour les attaques communes contre les systèmes embarqués.
- Laboratoires :
    - Configuration d'un environnement IoT sécurisé ;
    - Analyse des faiblesses d'un réseau IoT domestique ;
    - Mise en place d'une authentification mutuelle entre dispositifs IoT ;
    - Attaque par canal auxiliaire sur un microcontrôleur ;
    - Sécurisation d'une mise à jour OTA (Over The Air).

CY215 - Sécurité Applicative

Bloc : 2
Quadrimestre : Q2
Crédits ECTS : 5.0

UE prérequise(s) à cette UE : aucun
Cette UE est corequise avec les UE : aucun
Cette UE est prérequise pour les UE : aucun

Cette UE contribue à l'atteinte des compétences suivantes :

Compétences communes :
2.6 : Documenter son travail afin d'en permettre la traçabilité et le cycle de vie.
4.2 : Respecter les normes, les procédures et les codes de bonne pratique.

Acquis d'apprentissage spécifiques :

Au terme de l'activité d'apprentissage, l'étudiant sera sensibilisé aux problèmes de sécurité lié aux applications et au différentes méthodes de sécurisation.
Au terme de l'activité, l'étudiant sera capable de :

- Identifier les failles de sécurité courantes dans les applications informatiques ;
- Comprendre et expliquer les principes et les mécanismes d'exploitation de failles de sécurité ;
- Comprendre les principes d'un développement sécurisé ;
- Connaître les vulnérabilités courantes dans les applications web (OWASP Top 10)
- Mettre en œuvre des tests et d'audit de sécurité afin de prévenir ou de réduire l'exploitation de failles ;
- Évaluer le danger des menaces en fonction d'une politique sécurité donnée.
- Laboratoires :
    - Études de cas sur des incidents de sécurité célèbres ;
    - Exploitation de vulnérabilités web (injections SQL, XSS) ;
    - Exploitation d'API, buffer over flow, Bypass EDR … ;
    - Utilisation d'outils de test de pénétration (Burp Suite, OWASP ZAP) ;
    - Analyse de malware ;
    - Mise en place d'outils de testing.

CY216 - Cryptographie : Concepts et usages

Bloc : 2
Quadrimestre : Q1
Crédits ECTS : 3.0

UE prérequise(s) à cette UE : aucun
Cette UE est corequise avec les UE : aucun
Cette UE est prérequise pour les UE : aucun

Cette UE contribue à l'atteinte des compétences suivantes :

Compétences communes :
1.4 : Utiliser le vocabulaire adéquat.
2.3 : Analyser une situation donnée sous ses aspects techniques et scientifiques.
2.4 : Rechercher et utiliser les ressources adéquates.
4.2 : Respecter les normes, les procédures et les codes de bonne pratique.

Acquis d'apprentissage spécifiques :

Au terme de l'activité d'apprentissage, l'étudiant disposera des concepts clés permettant la compréhension et la mise en place de solution simple utilisant la cryptographie.
L'apprenant pourra :

- Contextualiser et implémenter les concepts de base en cryptographie (chiffrement, signatures numériques…) ;
- Comprendre et utiliser les algorithmes de chiffrement symétrique et asymétrique ;
- Appréhender les limites des protocoles cryptographiques.
- Proposer et analyser des solutions utilisant de la cryptographie comme SSH, TLS ou différents types de VPN…
- Laboratoires :
    - Analyse de trafic réseau avec Wireshark ;
    - Études de cas sur des incidents de sécurité célèbres ;
    - Configuration d'SSH et analyse de trafic ;
    - Analyse de malware utilisant la cryptographie (ransomware...) ;
    - Mise en place d'un VPN (cas d'usage simple).

CY305 - Sécurité des réseaux

Bloc : 3
Quadrimestre : Q1
Crédits ECTS : 5.0

UE prérequise(s) à cette UE : aucun
Cette UE est corequise avec les UE : aucun
Cette UE est prérequise pour les UE : aucun

Cette UE contribue à l'atteinte des compétences suivantes :

Compétences communes :
2.5 : Proposer des solutions qui tiennent compte des contraintes.
Compétences liées à l'orientation :
5.3 : Identifier les faiblesses des dispositifs de sécurité implémentés, concernant l'infrastructure, les applicatifs et les systèmes.
5.5 : Proposer une solution technique répondant à une analyse en prenant en considération les aspects juridiques, organisationnels, éthiques et économiques.
6.1 : Respecter les normes, méthodologies, et standards de sécurité.

Acquis d'apprentissage spécifiques :

Au terme de l'activité d'apprentissage, l'étudiant disposera d'une vue globale des problèmes de sécurité liés aux réseaux et des solutions possibles.
L'étudiant sera capable de :

- Identifier les failles de sécurité courantes dans les réseaux informatiques ;
- Mettre en place un RADIUS ;
- Sécuriser les services réseaux de bases (DNS, DHCP…) ;
- Comprendre et mettre en place des solutions de sécurisation avancées (tiering model, WAF, Reverse-Proxy…) ;
- Mettre en place des VPN avancés ;
- Mettre en place des solutions de Firewall avancés ;
- Comprendre les risques et menaces spécifiques au cloud ;
- Sécuriser des environnements cloud (IaaS, PaaS, SaaS) ;
- Comprendre et mettre en place la conformité et la gestion des identités dans le cloud ;
- Comprendre et appréhender les menaces et attaques sur les réseaux (DoS, sniffing, spoofing) ;
- Sécurité des réseaux sans fil (Wi-Fi).
- Laboratoires :
    - Configuration sécurisée d'une instance cloud (AWS, Azure) ;
    - A définir ;

CY305 - Droit lié à l'informatique – Communication - Déontologie et RSE

Bloc : 3
Quadrimestre : Q1
Crédits ECTS : 5.0

UE prérequise(s) à cette UE : aucun
Cette UE est corequise avec les UE : aucun
Cette UE est prérequise pour les UE : aucun

Cette UE contribue à l'atteinte des compétences suivantes :
Compétences communes :
Compétences liées à l'orientation :

Acquis d'apprentissage spécifiques :
Au terme de l'activité, l'étudiant sera capable de :

- Comprendre les enjeux éthiques en cybersécurité ;
- Comprendre les lois et régulations (RGPD, HIPAA, ANSSI, CERT...) ;
- Comprendre les normes et standards de sécurité (ISO 27001, NIST, CyFun).
- Utiliser des outils comme CISO-assistant ;
- Laboratoires :
    - Études de cas sur des incidents de sécurité célèbres ;
    - Études de conformité et mise en place de politiques de sécurité.

CY308 - IA Détection de menace et automatisation

Bloc : 2
Quadrimestre : Q1
Crédits ECTS : 5.0

UE prérequise(s) à cette UE : aucun
Cette UE est corequise avec les UE : aucun
Cette UE est prérequise pour les UE : aucun

Cette UE contribue à l'atteinte des compétences suivantes :

Compétences communes :
3.1 : Prendre en compte les aspects éthiques et déontologiques
3.3 : Développer une pensée critique
Compétences liées à l'orientation :

Acquis d'apprentissage spécifiques :

Au terme de l'activité, l'étudiant sera capable de :

- comprendre les concepts fondamentaux de l'IA et du machine learning (ML) ;
- comprendre les concepts fondamentaux des algorithmes supervisés et non supervisés ;
- Comprendre les méthodes d'analyse de données pour la détection d'intrusion (IDS) basées sur l'IA ;
- Explorer les attaques adversariales contre des modèles d'IA (comment tromper un modèle ML ou DL) ;
- Utiliser le machine learning pour détecter et classifier les malwares ;
- Étudier comment l'IA aide à l'analyse dynamique et statique des malwares;
- Étudier les principes de la cryptographie (chiffrement symétrique et asymétrique, hash, signatures) ;
- Explorer l'utilisation de l'IA pour briser ou renforcer les systèmes cryptographiques ;
- Étudier les méthodes de récupération et d'analyse de preuves numériques ;
- Utiliser des techniques d'IA pour automatiser l'analyse des logs et identifier des comportements anormaux.
- Explorer la sécurité des systèmes embarqués et IoT, et l'utilisation de l'IA pour protéger ces systèmes.
- Laboratoires :
    - Détection d'intrusions à l'aide du Machine Learning : Utilisation de l'algorithme K-means ou du réseau de neurones pour identifier des anomalies dans les logs réseaux (dataset comme KDD Cup 99 ou CICIDCY2017) ;
    - Attaques adversariales sur un modèle de reconnaissance d'image : Implémentation d'une attaque par perturbation de pixels sur un modèle de classification d'image, tel que ResNet, pour en tromper les prédictions ;
    - Classification des malwares à partir de leurs caractéristiques statiques ;
    - Attaques sur les algorithmes de chiffrement ;
    - Analyse forensique automatisée ;
    - Détection d'anomalies IoT avec l'IA.

CY309 - Sécurité des Télécommunications

Bloc : 3
Quadrimestre : Q1
Crédits ECTS : 5.0

UE prérequise(s) à cette UE : aucun
Cette UE est corequise avec les UE : aucun
Cette UE est prérequise pour les UE : aucun

Cette UE contribue à l'atteinte des compétences suivantes :

Compétences liées à l'orientation :
5.3 : Identifier les faiblesses des dispositifs de sécurité implémentés, concernant l'infrastructure, les applicatifs et les systèmes.
6.1 : Respecter les normes, méthodologies, et standards de sécurité.
6.2 : Évaluer la sécurité des systèmes, en identifiant les faiblesses, et adapter les solutions implémentées.

Acquis d'apprentissage spécifiques :

Au terme de l'activité, l'étudiant sera capable de :

- Identifier les failles de sécurité courantes dans les applications informatiques ;
- Comprendre le fonctionnement des satellites (orbites, types de satellites, etc.) ;
- Comprendre les concepts de base des télécommunications par satellite (modulation, codage, etc.) ;
- Appréhender les réseaux satellitaires (GEO, MEO, LEO) ;
- Comprendre les protocoles de communication par satellite (TCP/IP adapté aux satellites, DVB-S2, etc.) ;
- **Appréhender la sécurité des Réseaux Satellitaires**
- **se familiariser avec les normes et Régulations de la Sécurité Satellite ;**
- **Analyser et Répondre aux Incidents dans les Réseaux Satellitaires ;**
- Comprendre les menaces spécifiques aux télécommunications satellitaires
- Comprendre les attaques sur les liaisons montantes et descendantes
- Utiliser le chiffrement afin de protéger des données dans les communications par satellite ;
- Mettre en place des politiques de sécurité pour les réseaux satellitaires.
- Laboratoires :
    - Laboratoire de Simulation de Réseaux Satellitaires ;
    - Laboratoire d'Attaque et de Défense des Liens Satellitaires ;
    - Laboratoire de Cryptographie Appliquée aux Télécommunications Satellitaires.

CY310 - Gestion et réponses aux Incidents

Bloc : 3
Quadrimestre : Q1
Crédits ECTS : 3.0

UE prérequise(s) à cette UE : aucun
Cette UE est corequise avec les UE : aucun
Cette UE est prérequise pour les UE : aucun

Cette UE contribue à l'atteinte des compétences suivantes :

Compétences communes :
1.3 : Assurer la diffusion vers les différents niveaux de la hiérarchie (interface entre les collaborateurs, la hiérarchie et/ou les clients).
2.6 : Documenter son travail afin d'en permettre la traçabilité et le cycle de vie.
4.2 : Respecter les normes, les procédures et les codes de bonne pratique.

Acquis d'apprentissage spécifiques :

Au terme de l'activité d'apprentissage, l'étudiant sera sensibilisé aux problèmes liés à la réponse aux incidents.
L'étudiant sera capable de :

- Comprendre l'importance de la gestion des évènements de sécurité dans les réseaux modernes ;
- Collecter et de corréler les données d'une multitude de sources en vue d'une analyse post-incident ;
- Comprendre les techniques d'analyse post-incident les plus courantes ;
- Identifiant les faiblesses des dispositifs implémentés ;
- Proposer et mettre en des solutions permettant de répondre à la politique de sécurité de l'information de l'entreprise en fonction du risque.
- Utiliser les outils comme :
    - CVE details ;
    - Exploit Database ;
    - CVE -MITRE.
- Laboratoires :
    - Études de cas sur des incidents de sécurité célèbres ;
    - Analyse des politiques de sécurité et de conformité cloud.
    - Mise en place d'un Monitoring.
    - Mise en place d'un SIEM – HIDS – IDS/IPS ;
    - Analyse Forensique d'un Disque Dur.

CY311 – Red team vs blue team

Bloc : 3
Quadrimestre : Q1
Crédits ECTS : 5.0

UE prérequise(s) à cette UE : aucun
Cette UE est corequise avec les UE : aucun
Cette UE est prérequise pour les UE : aucun

Cette UE contribue à l'atteinte des compétences suivantes :

Compétences communes :
2.6 : Documenter son travail afin d'en permettre la traçabilité et le cycle de vie.
3.4 : Travailler tant en autonomie qu'en équipe dans le respect de la structure de l'environnement professionnel.
Compétences liées à l'orientation :
6.3 : Configurer et déployer de manière efficace, les dispositifs de sécurité, et en assurer la maintenance.

Acquis d'apprentissage spécifiques :

Au terme de cette activité d'apprentissage, l'étudiant sera capable de :

- collaborer avec une équipe ;
- Réaliser un Pentest dans les règles d'une infrastructure réseau, ses serveurs et des services (Red Team) ;
- Détecter et de répondre aux incidents (Blue Team) ;
- Collaborer et d'optimiser une infrastructure donnée (Purple Team) ;
- Répondre à un cahier des charges ;
- Rédiger des rapports techniques ;
- Présenter et défendre leur projet
- Laboratoires :
    - Scanning de vulnérabilités ;
    - Exploitation de failles connues ;
    - Simulation d'un phishing ;
    - Configuration et utilisation d'un SIEM ;
    - Analyse de logs pour identifier et réagir à une attaque simulée ;
    - Investigation d'une intrusion sur un serveur compromis ;
    - Exercice de Purple Teaming avec analyse des points forts et faibles ;
    - Atelier de réévaluation des défenses après un exercice de Red Team.

CY312 - Veille technologique

Bloc : 3
Quadrimestre : Q1
Crédits ECTS : 2.0

UE prérequise(s) à cette UE : aucun
Cette UE est corequise avec les UE : aucun
Cette UE est prérequise pour les UE : aucun

Cette UE contribue à l'atteinte des compétences suivantes :

Compétences communes :
4.3 : Respecter les prescrits légaux relatifs au contexte dans lequel s'exerce l'activité (exemple code du bien-être au travail, RGPD, le droit à l'image, licences logiciels …).
Compétences liées à l'orientation :
5.4 : Prendre en considération les défaillances matérielles, humaines, prévisibles ou non.

Acquis d'apprentissage spécifiques :

Au terme de l'activité, l'étudiant sera capable de :

- comprendre l'importance de la veille dans le domaine de la cybersécurité ;
- d'utiliser des outils et méthodologies pour effectuer une veille efficace ;
- effectuer de la v**eille technologique** : Nouveaux outils de sécurité, solutions matérielles et logicielles.
- **effectuer de la veille réglementaire** : Nouvelles lois et régulations (RGPD, NIS2, etc.) ;
- **effectuer de la veille concurrentielle** : Suivi des tendances et innovations chez les acteurs du marché ;
- **effectuer de la veille sur les menaces** : Analyse des nouvelles cybermenaces, malwares, ransomwares, attaques ciblées ;
- **effectuer de la veille sur les vulnérabilités** : Identification des vulnérabilités logicielles et matérielles.
- Laboratoires :
    - Laboratoire avec des outils automatisés : Agrégateurs de flux RSS, alertes Google, plateformes d'information ;
    - Laboratoire avec des outils spécialisés : Blogs, forums, portails de sécurité (ex : CERT, Mitre ATT&CK, etc.).
    - **Laboratoire avec des Réseaux sociaux** : Twitter, LinkedIn (pour suivre des experts ou entreprises spécialisées).
    - **Utilisation des publications scientifiques et conférences** : Articles de recherche, rapports, événements comme Black Hat, DEFCON.
    - Analyse et validation de l'information ;
    - Exemples réels de mise en place de veilles technologiques dans des entreprises ;
    - Étude d'incidents de sécurité récents (ex : SolarWinds, Colonial Pipeline) et analyse des failles.