École d'ingénieurs Jules Verne (EIJV)

Ingénieur en Cybersécurité (2ème année)

Présentation

Objectifs

La spécialité Cybersécurité d'Amiens vise à former des spécialistes des problématiques liées à la sécurité informatique.

Depuis plusieurs années le nombre et la diversité des menaces informatiques augmentent de manière drastique, de par l'augmentation des équipements, des failles et des utilisateurs. Toutes les entreprises, quels que soient leurs domaines d'activités, sont touchées par ces menaces car les systèmes d'informations sont présents dans tous les secteurs d'activités.

Le titulaire du diplôme d'Ingénieur Cybersécurité exerce dans tous types d'entreprises, et sera capable d'aborder tous les aspects de la sécurité, au niveau du matériel, des méthodes, des systèmes et des logiciels.

L'ingénieur Cybersécurité est amené à réaliser des activités allant de la cartographie des risques, de l'organisation de la sécurité, de l'élaboration d'un cahier des charges à la mise en place de la sécurité, de la définition de la stratégie à élaborer dans la sécurisation des systèmes d'information.

Il participe au développement, à la maintenance et au test de logiciels sécurisés, à la gestion de la sécurité d'un système d'exploitation quels que soient le système et la plateforme, à la gestion de la sécurité du réseau et des accès.

Il apporte son expertise dans l'analyse des incidents, et sait mettre en place des solutions de prévention, et peut mener des audits de sécurité.

Enfin, l'ingénieur cybersécurité a les connaissances nécessaires pour appliquer les aspects juridiques à tous les éléments du système d'information et apporter du conseil en sécurité à tous les projets informatiques.

Compétences

Modalités de formation

EN ALTERNANCE

Informations pratiques

Lieux de la formation
École d'ingénieurs Jules Verne - Bâtiment Canopé, 45 Rue Saint-Leu, 80000 Amiens

Capacité d'accueil
30

Contacts Formation Initiale

SEC_EIJV

03 22 82 70 31

sec.eijv@u-picardie.fr

La certification implique la vérification des qualités suivantes :

ACQUISITION DES CONNAISSANCES SCIENTIFIQUES ET TECHNIQUES ET LA MAITRISE DE LEUR

MISE EN OEUVRE :

1. La connaissance et la compréhension d'un large champ de sciences fondamentales et la capacité d'analyse et de synthèse qui leur est associée.

2. L'aptitude à mobiliser les ressources d'un (ou de plusieurs) champ scientifique et technique spécifique.

3. La maitrise des méthodes et des outils de l'ingénieur : identification, modélisation et résolution de problèmes même non familiers et incomplètement définis, l'utilisation des approches numériques et des outils informatiques, l'analyse et la conception de systèmes, la pratique du travail collaboratif et à distance.

4. la capacité à concevoir, concrétiser, tester et valider des solutions, des méthodes, produits, systèmes et services innovants.

5. la capacité à effectuer des activités de recherche, fondamentale ou appliquée, à mettre en place des dispositifs expérimentaux.

6. la capacité à trouver l'information pertinente, à l'évaluer et à l'exploiter : « compétence informationnelle ».

ADAPTATION AUX EXIGENCES PROPRES DE L'ENTREPRISE ET DE LA SOCIÉTÉ

7. la capacité à prendre en compte les enjeux de l'entreprise : dimension économique, respect de la qualité, compétitivité et productivité, exigences commerciales, intelligence économique.

8. la capacité à identifier les responsabilités éthiques et professionnelles, à prendre en compte les enjeux des relations au travail, de sécurité et de santé au travail et de la diversité.

9 la capacité à prendre en compte les enjeux environnementaux, notamment par application des principes du développement durable.

10. la capacité à prendre en compte les enjeux et les besoins de la société.

PRISE EN COMPTE DE LA DIMENSION ORGANISATIONNELLE, PERSONNELLE ET CULTURELLE

11. la capacité à s'insérer dans la vie professionnelle, à s'intégrer dans une organisation, à l'animer et à la faire évoluer : exercice de la responsabilité, esprit d'équipe, engagement et leadership, management de projets, maitrise d'ouvrage, communication avec des spécialistes comme avec des non-spécialistes.

12. la capacité à entreprendre et innover, dans le cadre de projets personnels ou par l'initiative et l'implication au sein de l'entreprise dans des projets entrepreneuriaux.

Conditions d'accès

Niveau Bac+2 ou équivalent pour la première année, niveau Licence pour la deuxième année. La formation est ouverte aux élèves issus des Classes Préparatoires aux Grandes Ecoles (CPGE) de préférence dans la filières MP2I, des classes préparatoires aux Études Supérieures (CPES), et du cycle préparatoire intégré de l'Ecole d'Ingénieurs du Littoral Côte d'Opale (EILCO).

Les élèves de niveau Master 1, Licence 2, Licence 3 ainsi que les élèves titulaires d'un DUT ou d'un BTS peuvent également intégrer la spécialité.

Partenaire

Organisation

Organisation

Dispensé au cœur d'Amiens, le cycle ingénieur spécialiste en Cybersécurité par apprentissage se déroule sur 3 ans selon un dispositif FISEA (Formation d'Ingénieur sous Statut Étudiant en Apprentissage) :

- 1re année : sous statut étudiant à temps plein en école. La première année a lieu sous statut étudiant. Les droits de scolarité de formation d'ingénieur s'appliquent.
- 2e et 3e années : sous statut apprenti en alternance école/entreprise

Après validation de la première année, l'élève ingénieur rejoint le monde de l'entreprise avec un contrat d'apprentissage de 2 ans : il acquiert un statut salarié.

Les 3 années sont organisées selon le principe de semestrialisation et se décomposent donc en 6 semestres (S5 à S10).

Pendant les 2 premières années du cycle ingénieur, les élèves ingénieurs en cybersécurité suivent un tronc commun articulé autour des deux domaines :

- Sciences et Techniques de l'Ingénieur,
- Sciences Humaines & Sociales et Langues.

En dernière année, au semestre 9 les élèves ingénieurs approfondissent le tronc commun et, en fonction de leur projet professionnel, choisissent une des 2 options suivantes :

- Cryptographie : pour compléter les connaissances dans le domaine de la Cryptographie et de son pendant, la Cryptanalyse.
- Applications émergentes : pour former les ingénieurs sur le innovations technologiques les plus marquantes, comme la Blockchain, le Big data et plus largement l'I.A. et l'optimisation pour la cybersécurité.

Le dernier semestre (semestre 10) est intégralement réalisé en entreprise.

De plus, sur la durée du cycle ingénieur, l'élève ingénieur doit réaliser et valider une période d'au moins 9 semaines à l'étranger :

- En première année sous statut étudiant, cela peut prendre la forme d'une mobilité d'études ou de stage ERASMUS +.
- En deuxième et troisième année sous statut apprenti, la mobilité privilégiée sera une mobilité professionnelle. La structure d'accueil à l'étranger peut être une entreprise ou filiale du Groupe dans laquelle l'apprenti suit son alternance, une entreprise cliente, un partenaire, un fournisseur ou toute autre institution en lien avec la spécialité du diplôme préparé. Des dispositifs spécifiques existent au niveau du contrat d'apprentissage pour accompagner cette mobilité.

Contrôle des connaissances

L'approche par compétences permet d'évaluer :

- Les savoirs acquis via des évaluations diverses au cours des semestres
- La mise en œuvre de ces savoirs au travers de mises en situations professionnelles reconstituées et approches par projet.

Le référentiel des compétences de l'ingénieur en Cybersécurité comporte 9 compétences. La validation du diplôme d'ingénieur nécessite la validation de toutes ces compétences.

Chaque module du programme fait l'objet d'évaluations préalablement définies. Chacune de ces évaluations contribue à tout ou partie des compétences du référentiel.

L'évaluation peut être un mix collectif/individuel, basé sur :

- Contrôle continu intégral,
- Examen sur table (études de cas et/ou projets)
- Présentations orales
- Élaboration de dossiers écrits
- Mises en situations professionnelles reconstituées
- Mémoires et soutenances liés aux missions en entreprise

De plus, un niveau d'anglais certifié, attesté par un test reconnu et externe (le test TOEIC), est exigé pour valider le diplôme. Le niveau souhaitable pour un ingénieur est le niveau C1 du "cadre européen de référence pour les langues" du conseil de l'Europe. En aucun cas, le diplôme d'ingénieur EIL parcours Cybersécurité ne sera délivré à un élève ingénieur n'atteignant pas le niveau B2 certifié (soit 785 points pour le TOEIC).

Consulter le règlement des études (pdf)Consulter le règlement des études (pdf)

Responsable(s) pédagogique(s)

Cyril Drocourt

cyril.drocourt@u-picardie.fr

Programme

Programmes

SEMESTRE 7 CYBERSECURITE	Volume horaire	CM	TD	TP	ECTS
UE SCIENCES ET TECHNIQUES DE L'INGENIEUR					11
Analyse des risques	30	10	12	8	3
Cryptographie	30	12	12	6	3
Introduction à la recherche	30	8	12	10	3
Projet					2
UE SCIENCES DE SPECIALITE					9
Développement Logiciel Sécurisé	30	10	11	9	3
Sécurité des Systèmes d'exploitation	30	10	12	8	3
Stockage et Sécurité	30	10	10	10	3
UE SCIENCES HUMAINES, ECONOMIQUES, JURIDIQUES ET SOCIALES					3
Droit du numérique	30	18	12		3
UE OUVERTURE INTERNATIONALE					2
Langue vivante 1 Anglais	30		30		2
Langue vivante 2 (Allemand, Espagnol, Anglais renforcé)	20		20		0
UE ALTERNANCE / CONFERENCES					5
Bonus (Activités Sportives, Culturelles et Artistiques)					0
Alternance : Travail, rapport, soutenance					5
Conférence : évaluation et auto-évaluation	10	10			0

SEMESTRE 8 CYBERSECURITE	Volume horaire	CM	TD	TP	ECTS
UE SCIENCES ET TECHNIQUES DE L'INGENIEUR					12
Données privées et anonymisation	26	10	8	8	3
Gestion de l'identité et de l'authentification	26	10	2	14	3
Recherche opérationelle et optimisation	30	12	14	4	3
Théorie de l'information	30	12	14	4	3
UE SCIENCES DE SPECIALITE					11
Analyse Forensique et Post-Mortem	30	8	10	12	3
Audit, test d'intrusion et Ingenierie Sociale	30	10	10	10	3

Audit, test d'intrusion et ingénierie sociale	30	10	10	10	3
Gouvernances, normes et certifications	20	6	6	8	2
Sécurité des réseaux et protocoles	28	6	2	20	3
UE OUVERTURE INTERNATIONALE					2
Langue vivante 1 Anglais	30		30		2
Langue vivante 2 (Allemand, Espagnol, Anglais renforcé)	20		20		0
Soutien Anglais	20		20		0
UE ALTERNANCE/ CONFERENCES					5
Bonus (Activités Sportives, Culturelles et Artistiques, Enga					0
Alternance: Travail, rapport, soutenance					5
Conférences "Insertion professionnelle"	10	10			0

Formation continue

A savoir

Niveau d'entrée : Niveau II (Licence ou maîtrise universitaire)
Niveau de sortie : Niveau I (supérieur à la maîtrise)

Références et certifications

Codes ROME : M1801 - Administration de systèmes d'information M1802 - Expertise et support en systèmes d'information M1803 - Direction des systèmes d'informa

M1806 - Conseil et maîtrise d'ouvrage en systèmes d'information M1810 - Production et exploitation de systèmes d'information

Codes FORMACODE : 14297 - Criminologie 31095 - Schéma directeur informatique 31006 - Sécurité informatique 24273 - Architecture réseau 32062 - Recherche d

Codes NSF : 326 - Informatique, traitement de l'information, réseaux de transmission des données

Contacts Formation Continue

--

Le 08/10/2024