UPJV

Ingénieur en Cybersécurité

Objectifs
Organisation
Programme
Controle de connaissance
Débouchés
Contacts
CANDIDATURE

La spécialité **Cybersécurité**du campus 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.

Activités visées :

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.

Dispensé sur le campus 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 12 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.

> télécharger le fichier (pdf)

Programme spécialité cybersécurité (pdf)

L'approche par compétences permet d'évaluer :
Les savoirs acquis via des évaluations diverses au cours des semestres
La mise en oeuvre de ces savoirs au travers de mises en situations professionnelles reconstituées et approches par projet.
Le référentiel des compétences de l'ingénieur en Logistique innovante 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,
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 réglement des études (pdf)

Les ingénieurs diplômés en spécialité Cybersécurité exercent leur activité dans le cadre d'entreprises issues des secteurs suivants :

Sociétés de service Informatique, sociétés de conseil, Industries, e-Commerce.

Type d'emplois accessibles :

En pilotage, organisation et gestion des risques
- Responsable de la sécurité des systèmes d'information (RSSI)
- Correspondant sécurité
- Spécialiste en gestion de crise Cyber
- Responsable du plan de continuité d'activité (RPCA)

En management de projets et cycle de vie
- Chef de projet sécurité
- Développeur de sécurité
- Architecte de sécurité
- Intégrateur de sécurité

En opération et maintien en condition opérationnelle
- Administrateur sécurité

En support et gestion des incidents
- Analyste SOC
- Expert réponse à incident (CERT)

En conseil, audit, expertise
- Consultant sécurité « organisationnel »
- Consultant sécurité « technique »
- Cryptologue
- Juriste spécialisé en cybersécurité
- Évaluateur sécurité
- Analyste de la menace
- Délégué à la Protection des Données (DPD)

Responsable du cycle Ingénieur spécialité Cybersécurité

Cyril Drocourt
Enseignant Chercheur (Campus d'Amiens)
ingenieurs-cybersecurite@u-picardie.fr

Date limite de candidature : 12 juin 2023

Les candidats auront une réponse le 5 juillet 2023 au plus tard indiquant : ADMIS / ADMISSIBLE/ REFUSE.

Les candidats admissibles seront auditionnés en visioconférence les 6, 7,10 ou 11 juillet et seront déclarés admis ou sur liste d'attente, à l'issue des auditions, et au plus tard le 13 juillet.

Les candidats devront confirmer au plus tard le 20 juillet.

Candidater sur e-Candidat

télécharger la plaquette (pdf)