le cnam
Nouvelle-Aquitaine

Fiche récapitulative

Diplôme d'ingénieur : CYC9106A | Diplôme d'ingénieur Cybersécurité

742
Total d'heures d'enseignement

180
Crédits ECTS

Accréditation
Valable jusqu'au 31/08/2024

Présentation

Le diplôme d'ingénieur Cybersécurité vous offre une formation spécialisée dans le domaine de la cybersécurité. Cette formation du Cnam vous permettra d'acquérir les compétences techniques et stratégiques nécessaires pour protéger les systèmes informatiques contre les cybermenaces, détecter les vulnérabilités, mettre en place des mesures de prévention et de réaction, et assurer la sécurité des données et des réseaux. Prêt à relever les défis complexes de la cybersécurité dans un monde numérique en constante évolution ?

Mentions officielles :

Intitulé officiel figurant sur le diplôme : Diplôme d'ingénieur Spécialité informatique parcours Cybersécurité

Code RNCP : 37357 open_in_new

Code(s) Formacode :

- sécurité informatique [31006]

Taux de réussite :

Les dernières informations concernant le taux de réussite des unités d'enseignement composant les diplômes

↓ Taux de réussite

Objectifs : aptitudes et compétences

Objectifs :

L'objectif pédagogique sera de délivrer un enseignement généraliste en cybersécurité afin de permettre aux élèves-ingénieurs de s'orienter vers l'un ou l'autre des métiers de l'ingénierie en cybersécurité :

ingénieur en sécurité opérationnelle : hautement qualifié pour mener des opérations de sécurité dans les centres de sécurité opérationnels (SOC), il est référent dans son domaine pour l'application et le maintien de mesures et contre-mesure de sécurité ; en situation défensive ou offensive, il assure tout type d'analyses de sécurité : vulnérabilités, investigation numérique légale, détection d'anomalie et d'intrusion, et décide de la remédiation adaptée ; enfin, il met en place les dispositifs de veille et de renseignement (CTI) et assure les activités de modélisation de la menace pour l'analyse de risques cyber.
ingénieur en conception et innovation de produits de sécurité : expert de haut niveau, il conçoit de nouveaux dispositifs ou de nouvelles technologies ou protocoles pour la cybersécurité, il est également force de proposition pour faire évoluer des produits ou protocoles existants dans un objectif de développement commercial ou d'innovation en milieu industriel. Il met en oeuvre des dispositifs IT Sec complexes, en assure la conception en réponse à des normes de certification, enfin, il gère et suit le programme de certification des produits qualifiés ou en cours de qualification.
ingénieur en développement d'applications cybersécurité : expert du génie logiciel, il accompagne le process de production des applications et du code, il développe de nouvelles applications de sécurité sous forme de logiciels, procédés ou services, en optimisant leurs coûts et leur sécurité à l'aide d'applications sécurisées "by design".

Compétences :

En tant que cadre supérieur, l'ingénieur cybersécurité sera en outre en mesure :

de déployer tout ou partie des architectures de sécurité des systèmes d'informations. Des datacenter aux IoT, réseaux de capteurs/actionneurs intelligents sécurisés, systèmes embarqués ou tout objet communicant sécurisé,

d'intégrer, mettre en oeuvre, configurer tous les dispositifs de sécurité visant la protection de ces composants de sécurité, leurs architectures et protocoles.
de mettre en oeuvre un service de veille et de renseignement et d'intelligence de la menace (CTI)
d'approfondir ses connaissances et d'acquérir par lui-même une expertise technique élevée,
d'auditer la sécurité d'un système d'information en constante évolution, de le corriger et l'optimiser par l'application de contre-mesures adaptées.
enfin, face aux situations d'incidents de sécurité, il sera en mesure de comprendre la menace, de manager des équipes opérationnelles, de les conduire sur les opérations techniques en situation de crise et de les conduire à capitaliser sur leurs expériences.

Prérequis

Pour le cycle préparatoire : Bac+2 (DPCT du Cnam, BTS, DUT, DEUG dans la spécialité ou une spécialité voisine, VES ou VAE).

Délais d'accès

Le délai d\'accès à la formation correspond à la durée entre votre inscription et la date du premier cours de votre formation.

- UE du 1er semestre et UE annuelle : inscription entre mai et octobre
- UE du 2e semestre : inscription de mai jusqu\'à mi-mars

Exemple : Je m\'inscris le 21 juin à FPG003 (Projet personnel et professionnel : auto-orientation pédagogique). Le premier cours a lieu le 21 octobre. Le délai d\'accès est donc de 4 mois.

Parcours conseillé

Année 1

- S1 UTC503 - UTC504 - UTC505
- S2 UTC501 -UTC502 - ANG100

Année 2

- S1 UAAD91 - NFP121 - 6 ects
- S2 RCP104 - NSY115 - NFE108

Année 3

- S1 NFE107 - 6 ects au choix
- S2 SEC101 - SEC105 - SMB111

Année 4

- S1 6 ects au choix - 6 ects au choix
- S2 SEC201 - UA2B30

Année 5

- S1 NSY205 - ENG221
- S2 UAMM91

Programme

Légende:

Cours en présentiel

Cours 100% à distance

Mixte: cours en présentiel et à distance

Tronc commun de démarrage

Unités Obligatoires	Année 2023/2024	Année 2024/2025	Année 2025/2026
UTC501 | Outils mathématiques pour Informatique 3 ECTS 26 heures	Semestre 2	Semestre 2	Semestre 2
UTC502 | Principes fondamentaux des Systèmes d'exploitation 3 ECTS 26 heures	Semestre 2	Semestre 2	Semestre 2
UTC503 | Paradigmes de programmation	Semestre 1	Semestre 1	Semestre 1

3 ECTS 26 heures			
UTC504 | Systèmes d'Information et Bases de Données 3 ECTS 26 heures	Semestre 1	Semestre 1	Semestre 1
UTC505 | Introduction à la cyberstructure de l'internet : réseaux et sécurité 3 ECTS 26 heures	Semestre 1	Semestre 1	Semestre 1
UAEP01 | Expérience professionnelle 9 ECTS			
UAAD91 | Examen d'admission à l'école d'ingénieur 0 ECTS 3 heures	Semestre 2	Semestres 1 et 2	Semestres 1 et 2

Une UE à choisir parmi :	Année 2023/2024	Année 2024/2025	Année 2025/2026
ANG100 | Anglais général pour débutants 6 ECTS 51 heures	Semestre 2	Semestre 2	Semestres 1 et 2
ANG330 | Anglais professionnel 6 ECTS 51 heures	Semestre 2	Semestres 1 et 2	Semestres 1 et 2

Unité(s) de base métier

Unités Obligatoires	Année 2023/2024	Année 2024/2025	Année 2025/2026
RCP104 | Optimisation en informatique 6 ECTS 51 heures		Semestre 2	
NFP121 | Programmation avancée 6 ECTS 51 heures	Semestre 2	Semestre 1	Semestre 1
NSY115 | Conduite d'un projet informatique 6 ECTS 51 heures	Semestre 2	Semestre 2	Semestre 2
NFE108 | Méthodologies des systèmes d'information 6 ECTS 51 heures	Semestre 2	Semestre 2	Semestre 2
SEC101 | Cybersécurité : référentiel, objectifs et déploiement 6 ECTS 51 heures	Semestre 2	Semestre 2	Semestre 2
SEC105 | Architectures et bonnes pratiques de la sécurité des réseaux, des systèmes, des données et des applications 6 ECTS 51 heures	Semestre 2	Semestre 2	Semestre 2
SMB111 | Systèmes et applications répartis pour le cloud 6 ECTS 51 heures	Semestre 2	Semestre 2	Semestre 2
NFE107 | Architecture d'Entreprise et Urbanisation des Systèmes d'Information 6 ECTS 51 heures	Semestre 1	Semestre 1	Semestre 1
UAEP02 | Expérience professionnelle 9 ECTS 3 heures	Semestre 2	Semestres 1 et 2	Semestres 1 et 2

Unité(s) plug-in

18 crédits à choisir parmi 45 :	Année 2023/2024	Année 2024/2025	Année 2025/2026
ESC101 | Mercatique I : Les Etudes de marché et les nouveaux enjeux de la Data 6 ECTS 51 heures	Semestre 1	Semestre 1	Semestre 1
MSE147 | Principes généraux et outils du management d'entreprise			

9 ECTS 78 heures	Semestre 2	Semestre 1	Semestre 1
DSY101 | L'organisation & ses modèles : Panorama (1) 6 ECTS 51 heures	Semestre 2	Semestre 2	Semestre 2
ESD104 | Politiques et stratégies économiques dans la mondialisation 6 ECTS 51 heures			Semestre 1
FPG114 | Outils RH 6 ECTS 51 heures	Semestre 2	Semestres 1 et 2	Semestres 1 et 2
DRS101 | Droit du travail : relations individuelles 6 ECTS 51 heures	Semestre 2	Semestres 1 et 2	Semestres 1 et 2
DRS102 | Droit du travail : relations collectives 6 ECTS 51 heures	Semestre 2	Semestres 1 et 2	Semestres 1 et 2

Unité(s) d'approfondissement et d'application

Unités Obligatoires	Année 2023/2024	Année 2024/2025	Année 2025/2026
SEC201 | IAML : IA et du ML pour la cybersécurité 6 ECTS 51 heures	Semestre 2	Semestre 2	Semestre 2
NSY205 | Architectures et technologies pour l'intégration des systèmes 6 ECTS 51 heures	Semestre 1	Semestre 1	Semestre 1

Fin de parcours

Unités Obligatoires	Année 2023/2024	Année 2024/2025	Année 2025/2026
UA2B30 | Test d'anglais 0 ECTS 2 heures	Semestre 2	Semestres 1 et 2	Semestres 1 et 2
ENG221 | Information et communication pour l'ingénieur - Oral probatoire 6 ECTS 51 heures	Semestre 1		
UAEP03 | Expérience professionnelle 15 ECTS 0 heures	Semestre 2	Semestres 1 et 2	Semestres 1 et 2
UAMM91 | Mémoire ingénieur 42 ECTS 3 heures	Semestre 2	Semestres 1 et 2	Semestres 1 et 2

Modalités

Modalités pédagogiques

Les modalités pédagogiques sont détaillées dans chaque unité qui compose le parcours.

Modalités de validation

Le diplôme d'ingénieur CYBERSECURITE en HTT est délivré après validation de chacune des UE et UA le constituant :

- Tronc Commun scientifique : 5UE/15 ECTS, chaque UE a 3 ECTS : UTC501, UTC502, UTC503, UTC504, UTC505,

- Anglais : 1UE /6 ECTS et un test d'anglais niveau B2 (non crédité), Bulats ou équivalent.

- UAAD91 : 1 UE/0 ECTS, examen d'admission à l'Ei-Cnam (0 ECTS).

- UAEP01, 1 UE/9 ECTS, bloc d'expérience.

- Bloc dit « de base » : 6 UE/36 ECTS pour acquérir les savoirs et compétences scientifiques et techniques de base et orientés "coeur de métier" de la spécialité.Le choix du parcours cybersécurité impose le choix d'au moins 2 UE SEC parmi SEC101, SEC102, SEC105, ce qui lève uniquement la règle d'exclusion pour le parcours Cybersécurité.

- Bloc dit « de spécialisation » : 2 UE/12 ECTS, pour se spécialiser en cybersécurité en choisissant 2 UE dans le bloc cybersécurité, avec au moins I UE SEC et de préférence 2 UE SEC.

- Un bloc d'UE, dites « plug-in » : 18 ECTS à 21 ECTS selon les spécialités permettant d'acquérir des savoirs et compétences complémentaires aux UE "coeur de métiers".

- Bloc dit « d'approfondissement» : 2 UE/12 ECTS, permet de se spécialiser en cybersécurité en choisissant 2 UE dans le bloc cybersécurité, avec au moins I UE SEC et de préférence 2 UE SEC.

- Examen probatoire : 1UE/6 ECTS, codifiée ENG221, elle est le préalable indispensable à la réalisation du mémoire (voir infra)

- Test d'anglais :1 UE/0 ECTS, codifiée UA2B30 pour valider le niveau B2

- Mémoire Ingénieur : 1 UE/42 ECTS, codifiée UAMM91

Tarif

Avec mon CPF	10.040 €
Mon employeur finance	20.365 €
Pôle Emploi finance	10.040 €
Je finance avec le co-financement Région	Salarié : 3.518 €
Je finance avec le co-financement Région	Demandeur d'emploi : 2.827 €

Plusieurs dispositifs de financement sont possibles en fonction de votre statut et peuvent financer jusqu'à 100% de votre formation.

Salarié : Faites financer votre formation par votre employeur

Demandeur d'emploi : Faites financer votre formation par Pôle emploi

Votre formation est éligible au CPF ? Financez-la avec votre CPF

Si aucun dispositif de financement ne peut être mobilisé, nous proposons à l'élève une prise en charge partielle de la Région Nouvelle-Aquitaine avec un reste à charge. Ce reste à charge correspond au tarif réduit et est à destination des salariés ou demandeurs d'emploi.

Pour plus de renseignements, consultez la page Financer mon projet formationopen_in_new ou contactez nos conseillers pour vous accompagner pas à pas dans vos démarches.

Blocs de compétences

Pas de possibilité de valider un ou des blocs de compétences sur ce diplôme.

Suites de parcours : poursuites d'études possibles

Pas de suites de parcours possibles.

Passerelles : lien entre certifications

Passerelles possibles sur 3 parcours :

- Architecture et ingénierie des systèmes et des logiciels (AISL) (CYC9101A)
- Informatique, réseaux, systèmes et multimédia (IRSM) (CYC9104A)
- Informatique systèmes d'information (ISI) (CYC9105A)

Débouchés - Métiers visés

Débouchés :

Types d'emplois accessibles :

- Ingénieur architectures de sécurité des systèmes d'informations
- Ingénieur cybersécurité