INGENIEUR INFORMATIQUE ET RESEAUX OPTION CYBERSECURITE

Informatique

01/07/2026

Résumé

Cette formation vise à former des ingénieurs spécialisés en cybersécurité, capables de protéger les systèmes informatiques et les réseaux contre les menaces et les attaques. Les ingénieurs formés seront aptes à :

Concevoir et mettre en œuvre des solutions de sécurité informatique.
Analyser les vulnérabilités et les risques des systèmes informatiques.
Développer des stratégies de défense et de réponse aux incidents

Public et prérequis

Prépa, BUT Mesure Physique/Réseaux et télépcomunication/Informatique, licence dans le domaine de l'informatique
Formation ouverte au personne en situation de handicap.

Pour une admission en 1ère année de cycle ingénieur, il faut valider son Bac + 2 si celui-ci est en cours.
Formation ouverte aux personnes en situation de handicap.
Prépa, BUT Mesure Physique/Réseaux et télépcomunication/Informatique, licence dans le domaine de l'informatique

Les objectifs pédagogiques et professionnels

Cette formation permet à l'ingénieur d'intervenir sur l'ensemble des étapes du cycle de développement et du déploiement d'un logiciel/d'un réseau en intégrant la sécurisation des données. L'ingénieur sera formé à évaluer les risques de sécurité au niveau logiciel/réseau afin de concevoir et déployer des
solutions adaptées permettant de limiter l'impact des cyberattaques en mettant en place une politique pertinente de sécurité ; application au contexte générale de la gestion des données ou plus spécifique des objets connectés.

Modalités d'accès

Pour candidater, il faut déposer un dossier par spécialité en apprentissage choisie (autant de candidatures que de spécialités visées) ;
Modalités : sur le site de POLYTECH DIJON, page « Admissions > Cycle Ingénieur sous statut apprenti ».

En cas d'admissibilité, le candidat doit passer un entretien de motivation. S'il est admis, il doit trouver et signer un contrat d'apprentissage pour que l'admission soit définitive (pour une admission en 1e année de cycle ingénieur, il faut valider son bac+2 si celui-ci est en cours)

Les méthodes pédagogiques et d'encadrement

- Formation dans un secteur très porteur
- Sécurité des Systèmes traitée à la fois au niveau logiciel et matériel
- Interventions régulières de spécialistes industriels

RÉFÉRENCE
INFCYB600025

RNCP
37881

DURÉE DE LA FORMATION
36 mois / 1614 heures

ACCUEIL PSH
Formation ouverte aux personnes en situation de handicap. Moyens de compensation à étudier avec le référent handicap du centre concerné.

PARTENAIRE

POLYTECH DIJON

Les + Formation 21-71

• 682 jeunes formés par an
• 291 contrats d'alternance à pourvoir
• 769 entreprises partenaires
• Accompagnement individualisé
• Diplômes reconnus par l'Etat

• Savoir être, management, sécurité
• Pédagogie innovante (par projets, en îlots, projet Voltaire, Olympiades des métiers)
• Equipement en machines modernes qui préparent aux métiers de demain

3 CENTRES en Bourgogne

- Apprentissage via l'expérimentation : évaluation par projet, travaux pratiques, mise en situation sur chaîne industrielle (partenariat avec l'UIMM)

Contenu de la formation

1ère année :

- Socle commun : Mathématiques, informatique, électronique analogique, algorithmique et programmation, introduction à la sécurité, réseaux informatiques, services réseaux, bases de données et développement web (487h/40 ECTS)
- Compétences transversales : Communication, philosophie, histoire des sciences, sécurité et analyse des risques, projet, anglais, management, qualité, sécurité, environnement (165h/10 ECTS)
- Entreprise (10 ECTS)

2ème année :

- spécialité : Cloud computing, virtualisation, sécurité des systèmes, Cisco Cyberops, projet cybersécurité, protocoles de sécurité, supervision des systèmes et réseaux, Pentesting (277h/24 ECTS)
- Compétences transversales : Management, droit de la propriété intellectuelle, projet éthique, innovation,anglais, entreprenariat, conférences (173h/10 ECTS)
- Socle commun : Cryptographie et chiffrement, développement applications mobiles, communication sans fils, apprentissage automatique et systèmes intelligents (173h/11 ECTS)
- Entreprise (15 ECTS)

3ème année :

- Spécialité : Big data, Data mining, audit de sécurité, normes internationales de sécurité, certification - CEH, analyse forensique, projet ethical haching, sécurisaton et réplication des données (256h/19 ECTS)
- Compétences transversales : Intelligence économique, droit du travail, enjeux sociétaux et environnementaux, management, anglais, e-commerce, marketing digital, gestion de projet (136h/6 ECTS)
- Entreprise (35 ECTS).

Equivalence

Niveau 7

Suite de parcours et passerelles possibles

Doctorat dans le domaine dela Cybersécurité

Métiers - Débouchés

- Expertise, bureau d'études, R&D dans un grand nombre de domaines liés au numérique : en informatique et cybersécurité, mais également défense, IoT, défense, santé, industrie 4.0
- Exemples de métiers : gestionnaire de crise de cybersécurité, architecte réseaux, responsable de la sécurité des systèmes d'informations (RSSI), ingénieur sécurité systèmes, responsable SOC (Security Operations Center), ingénieur logiciel, analyste et auditeur sécurité, ingénieur et manager des systèmes informatiques

Validation et certification

TOEIC: 785 minimum
UE validée si moyenne pondérée supérieure ou égale à 10 dans l'UE (entre les différents modules la constituant) et pas de note éliminatoire (<6) dans les parties théorique ou pratiques des modules.
Stage à l'international de 12 semaines

RNCP37881
Date d'échéance de l'enregistrement : 31-10-2026
Certificateur : UNIVERSITE BOURGOGNE EUROPE