المدرسة العليا للتكنولوجيا
ECOLE SUPÉRIEURE DE TECHNOLOGIE

جامعة سيدي محمد بن عبد الله بفاس
UNIVERSITÉ SIDI MOHAMED BEN ABDELLAH DE FES

Diplôme de Bachelor en Technologie
Cybersécurité des Systèmes Intelligents Connectés (CSIC)
Département Génie Electrique et Systèmes Intelligents

PRÉSENTATION

Le Bachelor CSIC de l'EST de Fès est une formation universitaire professionnalisante d'une durée d'un an (deux semestres), ouverte aux titulaires d'un diplôme Bac+2 en réseaux, informatique ou disciplines connexes.

Cette formation vise à doter les étudiants des compétences nécessaires pour concevoir, sécuriser et administrer des infrastructures réseau modernes, tout en intégrant la protection des systèmes intelligents et des objets connectés. Elle combine une approche théorique approfondie et des mises en pratique intensives autour de la cybersécurité offensive, défensive et des solutions de protection des données.

Le programme accorde une place importante aux outils professionnels (tests d'intrusion, supervision, réponse aux incidents, cryptographie, automatisation par scripts et IA) et prépare les étudiants à répondre aux exigences du marché de l'emploi en cybersécurité.

À l'issue de la formation, les diplômés sont prêts à intégrer des entreprises, administrations ou organismes spécialisés en réseaux et cybersécurité, à occuper des postes tels qu'analyste SOC, administrateur systèmes et réseaux, consultant en cybersécurité, expert en sécurité IoT, ou encore à poursuivre en master pour approfondir leurs compétences.

OBJECTIFS DE LA FORMATION

- **Concevoir, déployer et administrer** des infrastructures réseau sécurisées intégrant les services essentiels (DNS, DHCP, Active Directory, VPN, pare-feu).
- **Détecter, analyser et traiter les vulnérabilités** grâce à des outils professionnels, en maîtrisant les approches de cybersécurité offensive (tests d'intrusion éthiques) et défensive (contre-mesures adaptées).
- **Sécuriser les systèmes intelligents et les objets connectés**, en tenant compte de leurs contraintes spécifiques, et appliquer la cryptographie pour protéger les données et les communications.
- **Exploiter et sécuriser les données** (traitement, modélisation, protection) et automatiser des tâches de cybersécurité à l'aide de scripts et d'outils d'intelligence artificielle.
- **Développer des compétences professionnelles transversales** : rédaction de rapports techniques, respect des normes et réglementations, travail en équipe pluridisciplinaire, veille technologique et amélioration continue.

COMPÉTENCES À ACQUÉRIR

- **Administration des réseaux sécurisés** : conception, déploiement et gestion d'infrastructures intégrant les services critiques.
- **Cybersécurité offensive et défensive** : détection, analyse, exploitation éthique et mitigation des vulnérabilités.
- **Sécurisation des systèmes émergents** : protection des objets connectés et systèmes intelligents, avec usage de la cryptographie.
- **Gestion et automatisation des données** : traitement, modélisation, sécurisation et automatisation par scripts et IA.
- **Compétences professionnelles transversales** : communication technique, respect des normes, travail collaboratif, veille et amélioration continue.

SECTEURS D'ACTIVITÉS

- **Infrastructures réseaux et télécommunications** : conception, administration et sécurisation des systèmes d'information.
- **Cybersécurité et audit informatique** : tests d'intrusion, gestion des vulnérabilités, SOC (Security Operations Center).
- **Systèmes intelligents et IoT** : sécurisation des objets connectés, environnements embarqués et industriels.
- **Gestion et protection des données** : sécurité des bases de données, gouvernance, confidentialité et intégrité des informations.
- **Conseil, conformité et support technique** : accompagnement des entreprises en sécurité, respect des normes et réglementation, assistance technique.

DÉBOUCHÉS PROFESSIONNELS

- **Administration et ingénierie des réseaux** : administrateur systèmes et réseaux, ingénieur en infrastructures sécurisées, responsable réseau.
- **Cybersécurité opérationnelle** : analyste SOC, pentester (testeur d'intrusion éthique), analyste en réponse aux incidents, consultant en cybersécurité.
- **Sécurisation des systèmes intelligents et IoT** : ingénieur sécurité IoT, expert en systèmes embarqués sécurisés, responsable cybersécurité industrielle.
- **Gestion et protection des données** : data security officer, administrateur bases de données sécurisées, consultant en gouvernance et conformité des données.
- **Conseil, audit et accompagnement réglementaire** : consultant en conformité (RGPD, ISO 27001…), auditeur sécurité SI, formateur en cybersécurité.

CONTENU DE LA FORMATION

	Module 1	Module 2	Module 3	Module 4	Module 5	Module 6	Module 7
Semestre 1	Outils mathématiques et informatiques pour la cybersécurité et l'IA	Architectures et sécurisation de base des réseaux IP	Technologies réseau sans fil	IoT : Architectures, protocoles et applications	Déploiement et sécurisation d'un réseau d'entreprise	Bases de la cybersécurité et de la cryptographie appliquée	Cybersécurité Offensive : Techniques d'Attaque et d'Intrusion
Semestre 2	Cybersécurité Défensive : Méthodes et Outils	AI Driven Cybersecurity for Embedded and IoT Systems	Ingénierie de données : traitement et sécurité	Entrepreneuriat et innovation technologique	Stage technique en entreprise		

CONDITIONS D'ACCÈS

Les candidats au Bachelor CSIC doivent justifier d'un diplôme de niveau bac+2 reconnu par l'état : DUT (Réseaux & Télécoms, Réseaux, Sécurité des réseaux, Systèmes Embarqués, Informatique ou disciplines connexes), BTS (Réseaux & Télécoms, Réseaux, Sécurité des réseaux, Systèmes Embarqués, Informatique ou disciplines connexes) ou diplôme jugé équivalent.

PROCEDURE DE SELECTION

1. Présélection sur dossier
2. Tests écrits présentiels

Ecole Supérieure de Technologie de Fès - BP 2427 Route d'Imouzzer 30000 Fès
TEL:(+212) 6 66 21 46 30 - support.est@usmba.ac.ma