DIGITAL

ESC École Supérieure de Commerce DES 3 FRONTIÈRES BAC À BAC+5

Inscris toi !

BACHELOR EUROPÉEN CYBERSECURITE ET GESTION DES RESEAUX - NIVEAU 6 CEC

Niveau
6 CEC *(Cadre européen des certifications)*

Durée
1 an

Crédits
60 ECTS

Public visé
Étudiants - demandeurs d'emploi - salariés et professionnels du secteur

Prérequis
Candidats titulaires d'un diplôme de niveau 5 du CEC ou d'un diplôme équivalent à l'obtention de 120 ECTS

Rythme
Initial ou en alternance

Méthodes pédagogiques
Cours théoriques, TD et TP
Études de cas et mises en situations professionnelles
Projets individuels et en groupes

Évaluations professionnelles :
- Contrôle continu
- Epreuve écrite + étude de cas (3h)
- Epreuve écrite + étude de cas (3h)
- Rapport d'activité et soutenance orale (30 min)

LV1 :
- Compréhension écrite (1h)
- Présentation orale (45 min)

CCE :
- QCM(s) (1h20)

La FEDE, en tant que certificateur, est en charge des processus d'évaluation
- Organisation et planification des sessions d'examens
- Elaboration des sujets et des corrigés types
- Contrôle du respect du règlement des examens, de la conformité de leur supervision (respect de l'anonymat, intégrité, confidentialité)
- Evaluation et correction des copies
- Communication des résultats, délivrance des diplômes, suppléments aux diplômes et parchemins

www.fede.education/charte-qualite/

Face à l'explosion des cybermenaces et à la hausse des pertes économiques mondiales, la cybersécurité est devenue un enjeu stratégique pour tous les secteurs.
Le Bachelor européen en cybersécurité et gestion des réseaux forme des professionnels capables de concevoir, sécuriser et piloter des infrastructures numériques fiables et résilientes. Il répond à une forte demande du marché, dans un contexte marqué par la montée en puissance de l'IoT, le rôle croissant de l'IA dans la détection des menaces et l'importance des normes de conformité comme le RGPD ou ISO 27001.

OBJECTIFS DE LA FORMATION

- Évaluer les risques et recommander des correctifs en mobilisant des méthodologies d'audit reconnues (OWASP, CVSS, ISO 27005)
- Configurer, déployer et administrer des solutions de sécurité (pare-feux, VPN, IAM) selon les standards (ISO 27001, NIST)
- Mettre en œuvre une architecture réseau et des environnements Cloud sécurisés
- Piloter une stratégie de réponse aux incidents et exploiter un système SIEM pour détecter, analyser et traiter les cybermenaces
- Réaliser des tests d'intrusion et des audits techniques à l'aide d'outils spécialisés (Metasploit, Nmap, Burp Suite)
- Concevoir des politiques de cybersécurité conformes aux normes en vigueur (RGPD, NIS2, ISO 27001)
- Assurer une veille proactive pour anticiper les menaces et adapter les dispositifs de défense
- Sensibiliser les collaborateurs aux enjeux de cybersécurité pour ancrer une culture de sécurité dans l'organisation

PROGRAMME

EXPERTISE PROFESSIONNELLE (485 À 620 H)

Programmation en Python - Les bases de données SQL - Mathématiques appliquées et optimisation algorithmique - Initiation à la conduite de projets informatiques - Introduction à l'administration des systèmes et réseaux - Durcissement et sécurité des systèmes d'exploitation - Sécurité des réseaux : segmentation, pare-feu et surveillance - Sécurité des identités et des accès (IAM) - Cryptographie et protection des données - Sécurité des applications et services numériques - Réponse aux incidents et gestion des crises cyber - Sécurisation des environnements cloud et Big Data - Normes, conformité et gestion des risques en cybersécurité - Veille et prospective en cybersécurité

Mission professionnelle (≥12 semaines)
Stage en entreprise - Alternance - Emploi salarié

LANGUE VIVANTE (60 À 80H)
LV1 - Niveau B1 du CECRL
Allemand, Anglais, Espagnol, Français, Italien, Portugais
LV2 et LV3 (facultatives)
Allemand, Anglais, Arabe, Chinois, Espagnol, Français, Italien, Portugais

PERSPECTIVES D'EMPLOI

Liste des métiers accessibles en début de carrière (0 à 2 ans d'expérience) :
- Analyste SOC
- Technicien sécurité réseau ou systèmes
- Chargé de veille en cybersécurité
- Consultant cybersécurité junior
- Spécialiste IAM (Identité et accès) junior
- Spécialiste sécurité Cloud ou IoT

Évolutions possibles après 2 à 5 ans d'expérience :
- Auditeur en sécurité informatique
- Ingénieur DevSecOps
- Consultant cybersécurité senior
- Chef de projet cybersécurité
- Spécialiste en réponse aux incidents et forensic numérique
- Responsable cybersécurité
- Expert en cybersécurité industrielle (SCADA, systèmes OT)

L'ATOUT FEDE - DIPLÔME EUROPÉEN

CULTURE ET CITOYENNETÉ EUROPÉENNES (40H)

Le projet européen : culture et démocratie pour une citoyenneté en action
- Importance de l'histoire (OHTE)
- L'Europe Actuelle
- L'Europe et le monde
- Cultures et diversité en Europe
- La citoyenneté européenne
- Le fonctionnement de l'Union européenne
- Enjeux, défis et avenir de la construction européenne
- Focus sur la corruption (GRECO)

Le management interculturel et les ressources humaines
- Culture et diversité culturelle
- La communication interculturelle dans une organisation
- Gérer l'interculturel et résoudre des conflits culturels
- Travailler en Europe
- Les systèmes de protection sociale en Europe
- La responsabilité sociétale des entreprises