TECHNICIEN SPÉCIALISÉ

CYBERSÉCURITÉ

Programme de formation • Conditions d'accès • Pièces à fournir

DIPLÔME	DURÉE	MODE
Technicien Spécialisé	**18 mois**	**Présentiel**

Présentation de la formation

La formation en Cybersécurité prépare les étudiants à prévenir, détecter et traiter les incidents qui menacent les systèmes d'information. Elle développe des compétences en administration des réseaux, sécurisation des infrastructures, analyse des vulnérabilités, protection des données et réponse aux cyberattaques. Grâce aux travaux pratiques, aux études de cas et aux stages en entreprise, les étudiants apprennent à appliquer les bonnes pratiques de sécurité dans des environnements professionnels.

Objectifs

- Comprendre, configurer et administrer les systèmes et les réseaux informatiques.
- Mettre en place les dispositifs essentiels de sécurisation des infrastructures.
- Automatiser certaines tâches de sécurité à l'aide de scripts et de Python.
- Identifier les vulnérabilités et participer aux audits de sécurité.
- Protéger les données, les identités et les accès aux ressources informatiques.
- Détecter les incidents, analyser les événements et participer à la réponse aux cyberattaques.

Une formation orientée vers la pratique : travaux pratiques, études de cas, projet de fin de formation et stage en entreprise.

Programme de la filière

Principaux axes d'enseignement

1. Systèmes & réseaux
Architecture des réseaux, protocoles TCP/IP, administration Linux et Windows et virtualisation.

2. Sécurité des réseaux
Pare-feu et filtrage, VPN et accès distants, segmentation réseau et supervision de sécurité.

3. Programmation & scripts
Algorithmique, Python, scripts PowerShell et Bash et automatisation des tâches.

4. Audit & vulnérabilités
Analyse de vulnérabilités, tests d'intrusion encadrés, durcissement des systèmes et rapports d'audit.

5. Protection des données
Cryptographie, gestion des identités, contrôle des accès, sauvegarde et reprise.

6. Incidents & supervision
Réponse aux incidents, analyse de journaux, qualification des alertes et suivi des événements suspects.

7. Administration sécurisée
Installation, configuration et maintenance d'environnements Linux et Windows sécurisés.

8. Gestion des accès
Authentification, autorisation, politiques de sécurité et contrôle des privilèges.

9. Sécurité opérationnelle
Application des bonnes pratiques de protection des infrastructures, services et informations sensibles.

10. Communication & documentation
Rédaction de comptes rendus, documentation des actions et collaboration avec les équipes techniques.

11. Projet de fin de formation
Mise en œuvre d'un projet permettant de mobiliser les compétences techniques acquises.

12. Stage en entreprise
Application des compétences dans un environnement professionnel et découverte des pratiques de terrain.

Admission et dossier d'inscription

CONDITION D'ACCÈS

Baccalauréat ou niveau supérieur

La formation est accessible aux candidats ayant le baccalauréat ou un niveau d'études supérieur.

Pièces à fournir

01	**4 enveloppes timbrées**
02	**4 copies légalisées du baccalauréat**
03	**4 photos d'identité**
04	**2 copies légalisées de la CIN**
05	**Formulaire d'inscription à remplir**

Informations pratiques

Diplôme préparé	Technicien Spécialisé
Durée	18 mois
Mode de formation	Formation présentielle
Expérience professionnelle	Stages en entreprise
Lieu	IET - El Jadida

IET - Institut d'Enseignement Technique • El Jadida

Formation • Innovation • Insertion professionnelle