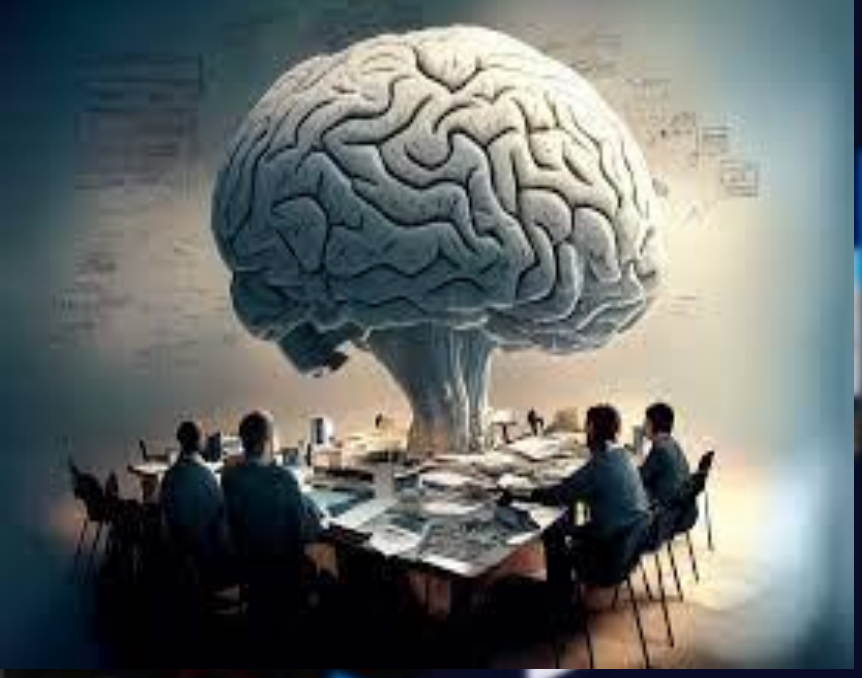


JFN

Innovation for a better world

FORMATIONS CERTIFIANTES

CATALOGUE 2023-2024

POURQUOI SE CERTIFIER ?

L’expérience est un atout indéniable, mais comment démontrer vos connaissances et compétences auprès d’employeurs ?

GRACE A LA CERTIFICATION !

De nos jours, il est primordial d’être capable de rallier à son diplôme un métier ; Ainsi, En obtenant une certification, vous démontrez votre expertise et prouvez votre capacité à vous différencier des autres sur le marché du travail de plus en plus concurrentiel d’aujourd’hui.

La certification apporte de la crédibilité à votre curriculum vitae, ce qui vous ouvre d’importantes possibilités d’évolution de carrière.
C’est un facteur clé de succès pour obtenir des opportunités d’emploi mieux rémunérées et une reconnaissance accrue.

Avantages :

- ❑ Amélioration de l’employabilité et de meilleures opportunités d’emploi.
- ❑ Emplois mieux rémunérés avec en prime augmentation de salaires
- ❑ Reconnaissance de carrière au sein de l’entreprise et auprès de ses pairs
- ❑ Accroissement de la crédibilité et de la notoriété
- ❑ Permet de booster des carrières et etre plus compétitif

CARTOGRAPHIE DE NOS FORMATIONS CERTIFIANTES

TABLE INDEX DES FORMATIONS CERTIFIANTES

REFERENCE	INTITULE DE LA FORMATION	ORGANISME DE CERTIFICATION	PARTENAIRE TECHNIQUE
SECURITE INFORMATIQUE & CYBERSECURITE			
Cybersécurité			
SI-CEH	Certified Ethical Hacker (CEH : identification des vulnérabilités des systèmes et réseaux informatiques.	**EC-COUNCIL**	**GROUP SOFT SARL**
SI-MEH	Méhari : méthode harmonisée d'analyse des risques.	**CLUSIF**	
SI-CPS	CompTIA Security+ (SY0-701)	**CompTIA**	

PROGRAMMES DÉTAILLÉS DES FORMATIONS CERTIFIANTES

SECURITE INFORMATIQUE ET CYBERSECURITE : Cybersécurité

Référence : **SI-CEH**	Intitulé de la formation certifiante**: Certified Ethical Hacker v 12(CEH : identification des vulnérabilités des systèmes et réseaux informatiques)**		
Durée : 192*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert en cybersécurité de JFN

Description et objectifs :

La certification CEH v12 (Certified Ethical Hacker) est un titre de compétence reconnu dans le domaine de la sécurité informatique et du hacking éthique. Elle est délivrée par EC-Council et vise à former des professionnels capables de comprendre et de contrer les techniques utilisées par les hackers malveillants afin d'assurer la sécurité des systèmes informatiques et des réseaux. De plus, dans le domaine du Hacking éthique, elle est la seule à offrir autant de ressources d'apprentissage, de labs, d'outils et de techniques. Elle certifie que le candidat possède les connaissances et les compétences nécessaires pour identifier les vulnérabilités, évaluer les risques de sécurité, mener des tests d'intrusion et mettre en place des contre-mesures appropriées.

Les objectifs étant de :

- S'imprégner du concept de hacking éthique
- Appréhender les concepts de "test d'intrusion"
- Appréhender et comprendre les tests d'intrusion
- Connaitre et savoir identifier les vulnérabilités d'une infrastructure
- Connaitre et maitriser les principales attaques système et réseau
- Connaitre et maitriser les principales attaques applicatives
- Connaitre et maitriser les principales attaques sociales
- Découvrir et apprendre utiliser de nombreux outils d'intrusion
- Envisager la sécurité informatique du point de vue de l'attaquant
- Comprendre les attaques sur les environnements IOT et OT
- Comprendre les attaques sur les environnements Cloud

Programme :

Module 1 : **INTRODUCTION AU PIRATAGE ETHIQUE**
Module 2 : **Identification des empreintes et reconnaissance**
Module 3 : **Analyse des réseaux**
Module 4 : **Enumération**
Module 5 : **Analyse des vulnérabilités**
Module 6 : **Piratage de système**
Module 7 : **Menaces de logiciels malveillants**
Module 8 : **Attaques par sniffing**
Module 9 : **Ingénierie sociale**
Module 10 : **Attaques par déni de service**
Module 11 : **Détournement de session**
Module 12 : **Contournement des systèmes de détection des intrusions, pare-feu, leurres informatiques**
Module 13 : **Piratage des serveurs web**
Module 14 : **Piratage des applications web**
Module 15 : **Injections SQL**
Module 16 : **Piratage des réseaux sans fils**
Module 17 : **Piratage des plateformes mobiles**
Module 18 : **Piratage de l'internet des objets et de la technologie opérationnelle**
Module 19 : **L'informatique en nuage**
Module 20 : **La cryptographie**

SECURITE INFORMATIQUE ET CYBERSECURITE : Cybersécurité

Référence : **SI-CEH**	Intitulé de la formation certifiante **: : CEHv12 : identification des vulnérabilités des systèmes et réseaux informatiques.**		
Durée : 192 *H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert en cybersécurité de JFN

Cible :

- Responsable informatique / Responsables de la sécurité des SI;
- Administrateurs IT
- Professionnels de la sécurité
- Administrateur systèmeIngénieur système
- Analyste cybersécurité
- Technicien Support/HelpDesk
- Auditeur interne/externe
- Décisionnaires et professionnels concernés par l'intégrité de l'infrastructure réseau
- professionnels titulaires d'une certification MCSA, MCSE, CCNP ou encore CCNA et voulant se perfectionner dans le domaine du Hacking éthique
- Professionnels souhaitant apprendre et comprendre les solutions et outils qui existent aujourd'hui en matière de sécurité informatique
- Responsables sécurité

Prerequis :

Connaissances professionnelles de TCP/IP, Linux et Windows Server..
Connaissances en réseaux et systèmes (Linux et Windows).
Maitrise de l'anglais technique (supports de cours et certification en anglais)

Débouchés :

CEH permet d'accéder à un large éventail de métiers. La certification offre divers débouchés pour les professionnels de la sécurité informatique ainsi que de nombreuses perspectives de carrière associées notamment:

- les rôles d'analyste en cybersécurité,
- testeurs d'intrusion
- pentesters
- chercheurs en sécurité offensive
- Red teamer
- Bug hunters
- consultant indépendant / gestion de la sécurité / d'administration de site
- auditeur IT,
- analyste en vulnérabilités
- administrateur système ou encore ingénieur réseau

SECURITE INFORMATIQUE ET CYBERSECURITE : Cybersécurité

Référence **SI-MEH**	Intitulé de la formation certifiante **: : Méhari : méthode harmonisée d'analyse des risques**		
Durée : 192*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert MEHARI de JFN

Description et objectifs :
MEHARI (Méthode harmonisée d'analyse des risques) a été développée par le CLUSIF, une organisation de sécurité de l'information à but non lucratif. L'objectif de cet outil d'appréciation des risques est d'appuyer la gestion des risques liés à la sécurité de l'information qui est basée sur l'ISO / CEI 27005 et d'analyser les scénarios de risques à court et à long terme.
La formation permet d'acquérir l'expertise et les connaissances nécessaires pour analyser les risques liés à la sécurité de l'information inclus dans de différentes étapes du cycle de vie de la sécurité dans un organisme.

Le cours est conçu de manière à doter l'apprenant des compétences nécessaires pour examiner les services de sécurité, détecter les risques critiques et analyser les scénarios de risque en conformité avec la méthode d'analyse des risques MEHARI.B ; basée sur des exercices pratiques et des études de cas, elle octroie les compétences nécessaires pour réaliser une analyse et une classification des enjeux, évaluer les services de sécurité, mener une analyse du risque et définir les plans de sécurité.
À l'issue de cette formation MEHARI Risk Manager, vous aurez acquis les connaissances et les compétences nécessaires pour :

- Comprendre les concepts et les principes généraux associés à la méthode d'analyse des risques MEHARI
- Maitriser les quatre étapes de l'approche MEHARI
- identifier les dysfonctionnements, analyser les scénarios de chacun, identifier l'échelle de la valeur et préparer une classification formelle des actifs du système d'information
- évaluer la qualité des services de sécurité dans un organisme à l'aide de la méthode MEHARI
- Comprendre le modèle de risque MEHARI
- définir les risques, analyser les situations de risque et réaliser une analyse quantitative d'une situation de risque
- élaborer des plans de sécurité basés sur l'approche MEHARI

Cible:
MEHARI Risk Manager s'adresse principalement aux :

- Personnes souhaitant acquérir des connaissances approfondies sur la méthode d'analyse et le modèle de risque de MEHARI
- Gestionnaires désirant développer les compétences nécessaires pour soutenir les organismes en matière d'analyse du risque lié à la sécurité de l'information
- Auditeurs souhaitant acquérir une connaissance approfondie de la méthode MEHARI Membres d'une équipe de sécurité de l'information souhaitant améliorer leurs compétences et maîtriser l'évaluation de la qualité des services de sécurité

Prérequis :
Une connaissance en management des risques est recommandée pour suivre cette formation

Débouchés :
Les professionnels certifiés MEHARI peuvent trouver des opportunités dans les domaines suivants :
Gestion de la sécurité
Analyse des risques et conformité
Consultation

SECURITE INFORMATIQUE ET CYBERSECURITE : Cybersécurité

Référence **SI-MEH**	Intitulé de la formation certifiante **: Méhari : méthode harmonisée d'analyse des risques**		
Durée : 192*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert MEHARI de JFN

Leçon 1 - Introduction aux concepts et aux étapes de la méthode d'analyse de risque MEHARI
Leçon 2 - Conduire une analyse de risque en utilisant la méthode MEHARI
Leçon 3 - Planification de la sécurité selon la méthode MEHARI et examen de certification

L'examen couvre les domaines de compétence suivants :

Domaine 1 : **Principes et concepts fondamentaux de la méthode MEHARI relative à l'analyse des risques**
Domaine 2 : **Analyse des enjeux et classification**
Domaine 3 : **Évaluation des services de sécurité**
Domaine 4 **: Analyse du risque**
Domaine 5 : **Définition de plans de sécurité basés sur la méthode MEHARI**

SECURITE INFORMATIQUE ET CYBERSECURITE : Cybersécurité

Référence **SI-CPS**	Intitulé de la formation certifiante : **CompTIA Security+ (SY0-701)**		
Durée : 192*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert en Cybersécurité JFN

Description et objectifs :

cette formation enseigne les compétences et les informations essentielles requises pour l'examen de certification CompTIA (SY0-701). A la fin de la formation, les apprenants seront en mesure de :

·

- Comparer et opposer les différents types de contrôles de sécurité.
- Résumer les concepts de sécurité fondamentaux.
- Expliquer l'importance des processus de gestion du changement et leur impact sur la sécurité.
- Expliquer l'importance de l'utilisation de solutions cryptographiques appropriées.
- Comparer et opposer les acteurs et les motivations des menaces les plus courantes.
- Expliquer les vecteurs de menace courants et les surfaces d'attaque.
- Expliquer les différents types de vulnérabilités.
- Analyser les indicateurs d'activité malveillante.
- Expliquer l'objectif des techniques d'atténuation utilisées pour sécuriser l'entreprise
- Comparer et opposer les implications de différents modèles d'architecture en matière de sécurité.
- Appliquer les principes de sécurité pour sécuriser l'infrastructure de l'entreprise
- Comparer et opposer les concepts et les stratégies de protection des données.
- Expliquer l'importance de la résilience et de la récupération dans l'architecture de sécurité.
- Appliquer les techniques de sécurité courantes aux ressources informatiques.
- Expliquer les implications en matière de sécurité d'une bonne gestion du matériel, des logiciels et des données.
- Expliquer les différentes activités associées à la gestion des vulnérabilités.
- Expliquer les concepts et les outils d'alerte et de surveillance de la sécurité.
- Modifier les capacités de l'entreprise pour améliorer la sécurité.
- Mettre en œuvre et maintenir la gestion des identités et des accès.
- Expliquer l'importance de l'automatisation et de l'orchestration dans le cadre d'opérations sécurisées.
- Expliquer les activités appropriées de réponse aux incidents.
- Utiliser les sources de données pour soutenir une enquête.
- Résumer les éléments d'une gouvernance efficace de la sécurité.
- Expliquer les éléments du processus de gestion des risques.
- Expliquer les processus associés à l'évaluation et à la gestion des risques par des tiers.
- Résumer les éléments d'une conformité efficace en matière de sécurité.
- Expliquer les types et les objectifs des audits et des évaluations.
- Mettre en œuvre des pratiques de sensibilisation à la sécurité

Prerequis :

Pour tirer le meilleur parti de cette formation et être en mesure de préparer l'examen, il est recommandé de réussir l'examen de certification CompTIA Network+ et avoir acquis 24 mois d'expérience dans le support réseau et l'administration informatique

Les compétences et connaissances suivantes sont necessaires :

- Utiliser un clavier et une souris.
- Connaître la fonction et les caractéristiques de base des c[illegible] d'un PC.

·

SECURITE INFORMATIQUE ET CYBERSECURITE : Cybersécurité

Référence **SI-CPS**	Intitulé de la formation certifiante : : **CompTIA Security+ (SY0-701)**		
Durée : 192 *H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert en Cybersécurité JFN

- Être capable d'utiliser Windows pour créer et gérer des fichiers et utiliser les fonctions administratives de base (Explorateur, Panneau de configuration et Consoles de gestion).
- Connaître la terminologie et les fonctions de base des réseaux (tels que le modèle OSI, la topologie, Ethernet, TCP/IP, les commutateurs et les routeurs).
- Comprendre l'adressage TCP/IP, les protocoles de base et les outils de dépannage.

Cible :

Ce cours est spécialement conçu pour :

- les professionnels de l'informatique qui possèdent des compétences en matière de mise en réseau et d'administration des réseaux TCP/IP (Transmission Control Protocol/Internet Protocol) basés sur Windows.
- Il convient également aux personnes familiarisées avec d'autres systèmes d'exploitation tels que MacOS, Unix ou Linux.
- ceux qui souhaitent améliorer leur carrière dans les technologies de l'information en acquérant des connaissances de base en matière de sécurité, en se préparant à l'examen de certification CompTIA Security+ ou en utilisant Security+ comme tremplin pour obtenir des certifications de sécurité plus poussées ou pour saisir des opportunités de carrière.
-
- Ceux qui désirent acquérir des connaissances essentielles sur les concepts de sécurité qui leur permettront d'évoluer professionnellement dans le domaine des technologies de l'information.
- Que vous cherchiez à élargir vos connaissances, à obtenir la certification CompTIA Security+ ou à obtenir des certifications ou des rôles avancés en matière de sécurité, cette formation constitue une base idéale pour atteindre ces objectifs.

1 INTRODUCTION À LA CYBERSÉCURITÉ

- Concept de sécurité
- Planification de La défense

2 MENACES, ATTAQUES, ET VULNÉRABILITÉ

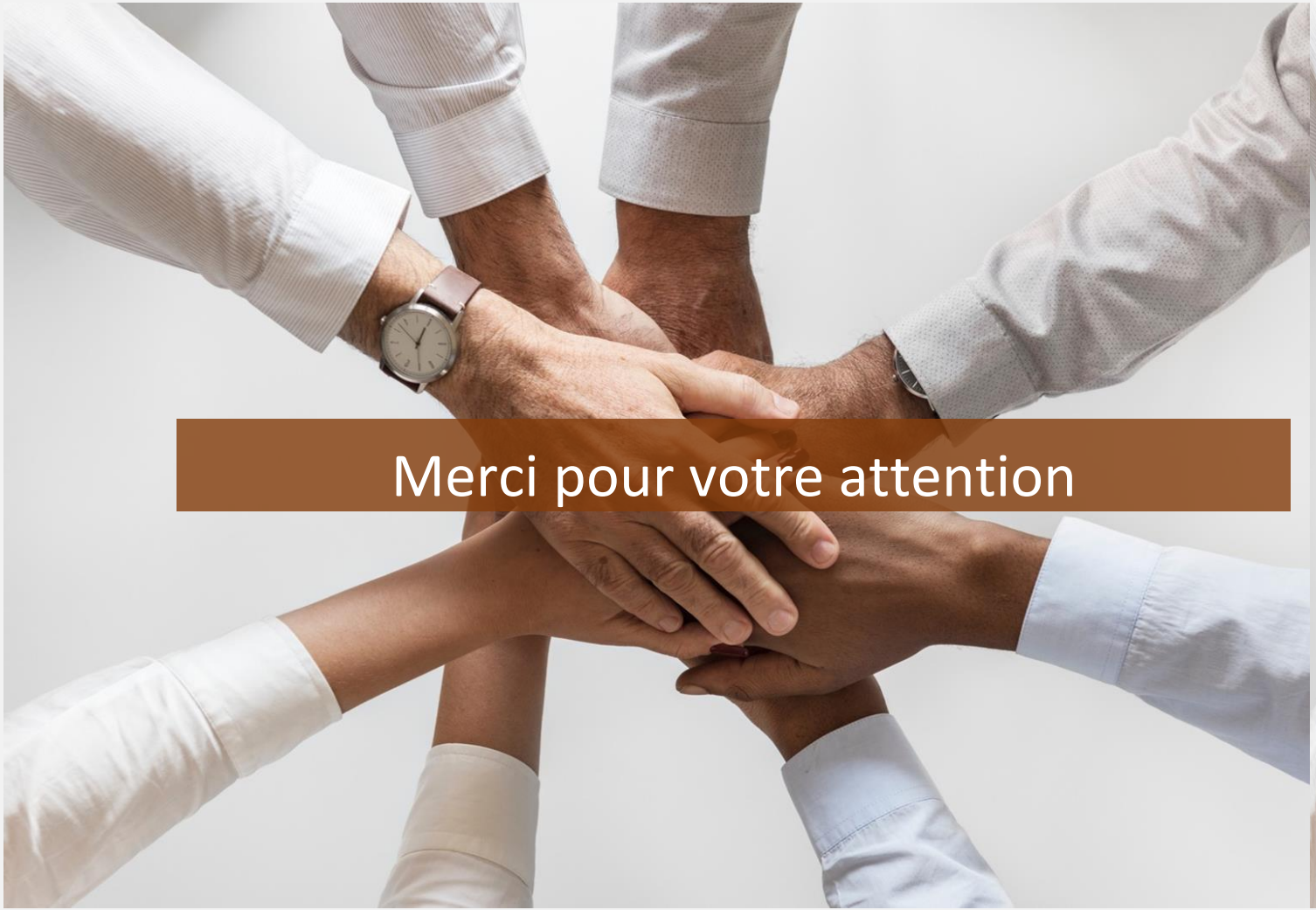
- Introduction aux attaques
- Exemples de malwares
- Ingénierie sociale

3 CONTRÔLE DE LA SÉCURITÉ PHYSIQUE

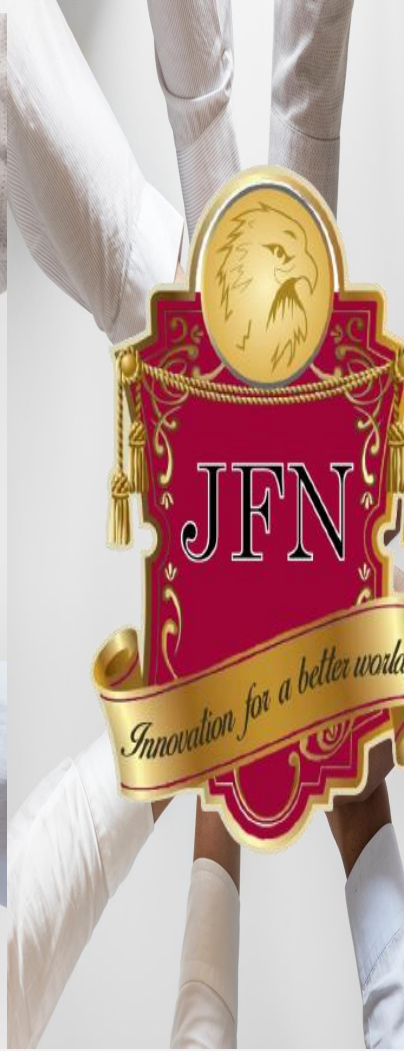
- Menaces physiques
- Protection des dispositifs et des réseaux
- Contrôles environnementaux

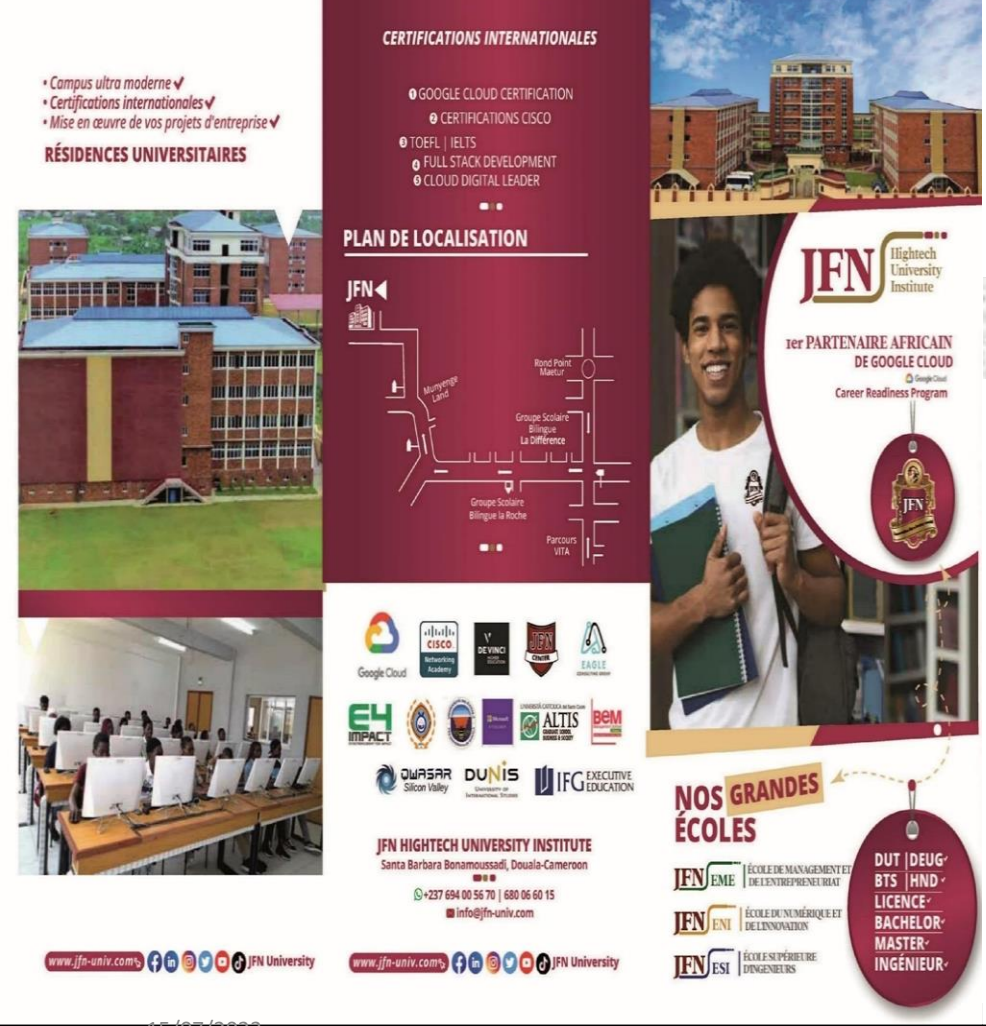
4 CONCEPTION ET DIAGNOSTIC DES RÉSEAUX ET DES HÔTES

- Plan de réseau gérable
- Durcissement du système Windows
- Sécurité des serveurs de fichiers
- Sécurité des hôtes Linux
- Aperçu sans fil
- Attaques sans fil
- Défenses sans fil



Merci pour votre attention





- ☑ Innovation,
- ☑ Entrepreneuriat,
- ☑ Formation Professionnelle et Continue