Université numérique
CHEIKH HAMIDOU KANE

CAT
Centre des Académies et des Technologies

Pôle Sciences, Technologies et Numérique

Centre des Académies et des Technologies (CAT)

CERTIFICAT DE TECHNICIEN SUPPORT EN CYBERSÉCURITÉ (CISCO CERTIFIED SUPPORT TECHNICIAN CYBERSECURITY)

Foo nekk foofu la

cat@unchk.edu.sn

Lancez votre carrière en cybersécurité avec la certification CCST de Cisco

Les cyberattaques sont partout. Elles touchent les entreprises, les administrations, mais aussi les particuliers... et les besoins en protection n'ont jamais été aussi importants.

La bonne nouvelle ? Vous pouvez devenir un acteur clé de cette défense numérique, même sans expérience technique préalable en cybersécurité.

La cybersécurité est un enjeu majeur, et les entreprises recherchent des talents capables de protéger leurs systèmes. Avec la certification Cisco Certified Support Technician (CCST) Cybersecurity, vous apprendrez à détecter les menaces, sécuriser les réseaux et devenir un professionnel recherché.

Accessible même sans expérience technique préalable, votre motivation et votre curiosité suffisent pour commencer.

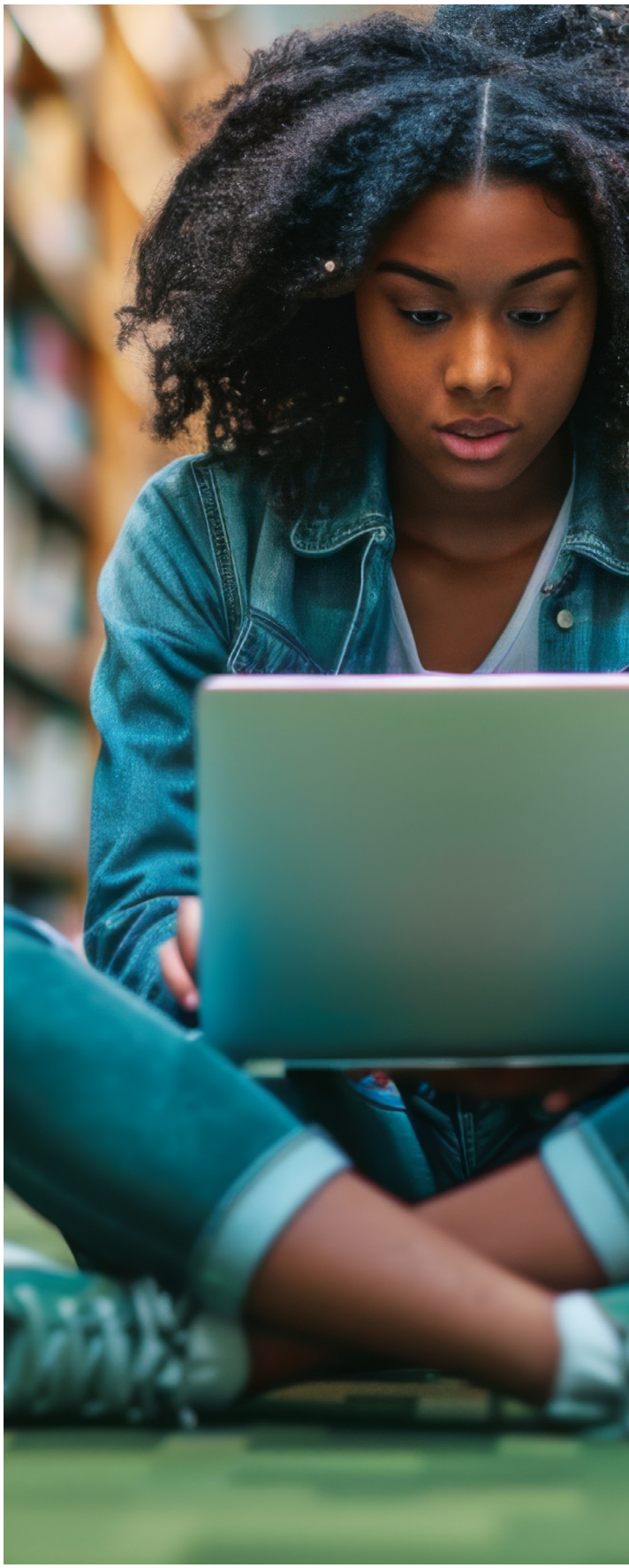
Ce certificat vous offre des compétences pratiques et reconnues par les employeurs du monde entier. Que vous soyez débutant ou en reconversion, c'est l'opportunité idéale pour vous lancer dans un secteur en pleine croissance.

Prêt à faire la différence ? Obtenez votre certification CCST et soyez au cœur de la protection numérique.

Rejoignez le mouvement et devenez acteur de la sécurité numérique de demain !

Inscrivez- vous
https://forms.gle/r9eXRzhZ69fNgZAw7

Formez-vous. Certifiez-vous. Protégez



objectifs pédagogiques

- Obtenir la certification Cisco Certified Support Technician (CCST) Cybersecurity
- Acquérir des compétences techniques fondamentales et pratiques en cybersécurité : principes de sécurité, réseau, endpoint security, gestion des vulnérabilités, réponse aux incidents, intelligence des menaces, forensique, cryptographie, etc.
- Occuper des postes de niveau débutant : technicien cybersécurité, analyste cybersécurité junior, support Help Desk, Tier 1
- Comprendre comment fonctionnent les attaques informatiques
- Apprendre à protéger les réseaux et les appareils
- Réagir efficacement face aux incidents de sécurité
- Découvrir les outils et les méthodes utilisés par les professionnels du métier.

pourquoi choisir ce certificat ?

- **Accessible** : Pas besoin d'être informaticien pour commencer
- **Reconnu mondialement** : Cisco est leader dans les réseaux et la cybersécurité
- **Utile pour l'emploi** : Veille sur les menaces, Sécurité réseau, Gestion des risques
- **Une voie d'avenir pour vous**

Ce certificat prépare aux métiers de niveau débutant dans le domaine, notamment :

- Technicien en cybersécurité
- Analyste junior en cybersécurité
- Support technique niveau 1

public cible

- Débutants : sans expérience préalable en informatique ou cybersécurité
- Étudiants, stagiaires ou professionnels IT souhaitant se lancer dans la cybersécurité
- Techniciens IT cherchant à évoluer vers un rôle plus axé sur la sécurité

durée et modalités

- **Durée** : 120 jours
- **Format** : Flexible, 100% en ligne
- **Supports** : Cours interactifs + vidéos, Labs virtuels, accompagnement instructeurs
- **Evaluation** : Evaluation progressive durant chaque module + examen de certification à la fin
- **Badge numérique** délivré par CISCO à la fin de chaque module
- **Attestation de maîtrise d**élivrée par le CAT à la fin de chaque module
- **Cisco Certified Support Technician Cybersecurity** délivré par CISCO après passage de la certification chez CISCO
- **Coût** : Des coûts de formation et de délivrance de l'attestation pourraient être demandés par le CAT

contenu du certificat

Module 1 – Introduction à la cybersécurité
Durée : 6 jours
Objectifs pédagogiques :

- Expliquer les bases de la sécurité en ligne, y compris ce qu'est la cybersécurité et son impact potentiel.
- Expliquer les menaces, attaques et vulnérabilités informatiques les plus courantes.
- Expliquer comment se protéger en ligne.
- Expliquer comment les organisations peuvent protéger leurs activités contre ces attaques.
- Accéder à diverses informations et ressources pour explorer les différentes carrières possibles en cybersécurité.

Contenus abordés :

- Les bases de la cybersécurité et son rôle fondamental dans le monde numérique.
- Les types de menaces : logiciels malveillants, d'ingénierie sociale, attaques réseau.
- Comment se protéger : outils, bonnes pratiques, sensibilisation
- Les carrières en cybersécurité : panorama des métiers et débouchés dans le domaine

Module 2 – Notions de base sur les réseaux
Durée : 22 jours
Objectifs pédagogiques :

- Comprendre les bases de la cybersécurité et son importance dans la protection en ligne.
- Identifier les menaces, attaques et vulnérabilités les plus courantes sur Internet.
- Apprendre à se protéger efficacement lors de l'utilisation d'Internet.
- Découvrir comment les organisations défendent leurs systèmes contre les cyberattaques.
- Explorer les différentes opportunités de carrière dans le domaine de la cybersécurité

Contenus abordés :

- **Ce qu'est un réseau informatique :** types de réseaux (LAN, WAN), composants (routeur, switch, modem).
- **Comment les données circulent :** câbles, Wi-Fi, protocoles, commutation de paquets.
- **Concepts essentiels :** adresse IP, DNS, bande passante, débit, latence.
- **Applications concrètes :** comment se connecter à un réseau, résoudre des problèmes simples, configurer un petit réseau.

Module 3 – Périphériques réseau et configuration initiale
Durée : 22 jours
Objectifs pédagogiques :

- Comprendre l'architecture des réseaux : Identifier les composants d'un réseau hiérarchique, expliquer le rôle des routeurs, des commutateurs, de l'ARP, du DNS et du DHCP.
- Maîtriser les concepts de virtualisation et des services cloud : Expliquer les caractéristiques de la virtualisation et des services en nuage.
- Savoir manipuler les systèmes de numération : Convertir des valeurs entre les systèmes décimal, binaire et hexadécimal, et calculer un plan de sous-réseaux IPv4.
- Analyser le fonctionnement des communications réseau : Expliquer le rôle des protocoles de couche réseau et de transport pour assurer la connectivité de bout en bout.
- Mettre en œuvre et tester un réseau simple : utiliser Cisco IOS, construire un petit réseau avec des équipements Cisco, et utiliser des outils pour tester la connectivité réseau.

Contenus abordés :

- ***Identifier les équipements réseau de base :*** routeur, commutateur (switch), point d'accès, modem.
- ***Effectuer une configuration de base :*** connexion à l'interface d'un périphérique, affectation d'adresses IP, activation du Wi-Fi.
- ***Manipuler les outils essentiels :*** câbles, interfaces réseau, ports.
- ***Comprendre le rôle de chaque périphérique*** dans l'acheminement des données et le bon fonctionnement d'un réseau local.

Module 4 – Sécurité des points de terminaison
Durée : 27 jours
Objectifs pédagogiques :

- Comprendre les attaques informatiques : Expliquer comment les cybercriminels exécutent les attaques les plus courantes et exploitent les vulnérabilités du protocole TCP/IP.
- Maîtriser les principes de la sécurité réseau : Expliquer les notions clés de la sécurité des réseaux et les dispositifs/services utilisés pour la renforcer.
- Appliquer des mesures de protection : Recommander des solutions pour atténuer les menaces et mettre en œuvre les bonnes pratiques en cybersécurité afin de garantir la confidentialité, l'intégrité et la disponibilité.
- Gérer la sécurité des systèmes : Utiliser les outils d'administration Windows, implémenter la sécurité de base sous Linux, et évaluer les protections des postes de travail face aux malwares.
- Diagnostiquer et sécuriser les connexions réseau : Dépanner un réseau sans fil et vérifier la sécurité des terminaux et des connexions.

Contenus abordés :

- Qu'est-ce qu'un point de terminaison et pourquoi il est une cible fréquente des cyberattaques.
- Comment protéger un appareil avec des outils comme les antivirus, les pare feux, et les correctifs logiciels.
- Mettre en place une stratégie de sécurité efficace : politiques de mot de passe, mises à jour automatiques, surveillance.
- Détection et réponse aux incidents : que faire en cas de compromission ou d'alerte.

Module 5 – Défense du réseau
Durée : 27 jours
Objectifs pédagogiques :

- Élaborer des politiques de sécurité conformes aux exigences de gouvernance et de conformité en cybersécurité.
- Utiliser des outils d'analyse et de test pour évaluer la sécurité des réseaux.
- Exploiter des sources de renseignements sur les menaces afin d'anticiper les cyberattaques.
- Évaluer et gérer les vulnérabilités des postes de travail et autres terminaux.
- Appliquer des mesures de sécurité et des modèles de réponse aux incidents, basés sur les résultats d'analyse des risques et les techniques de forensic.

Contenus abordés :

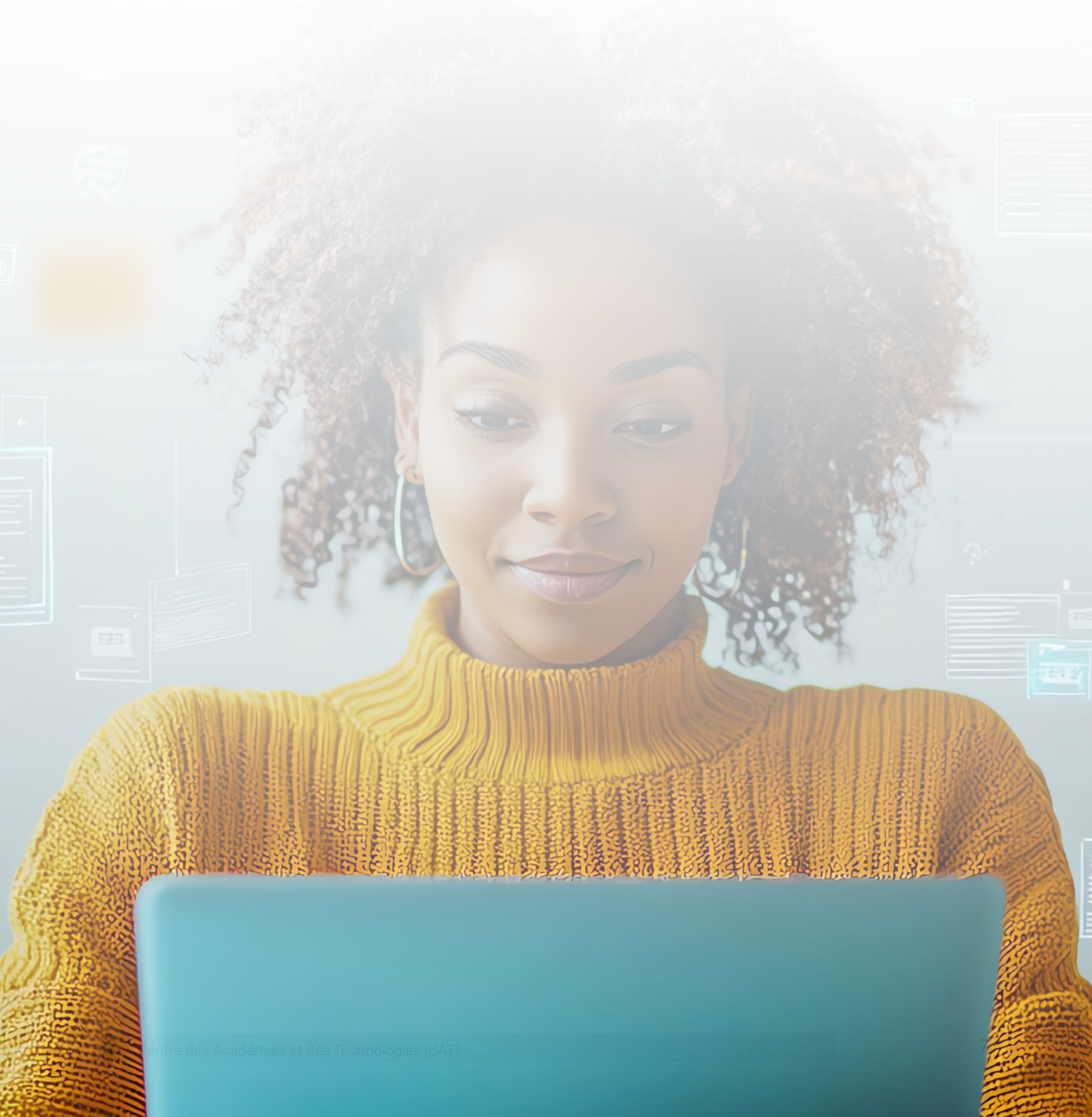
- **Les bases de la défense réseau** : segmentation, pare-feu, filtrage du trafic.
- **Stratégies de sécurité préventive** : surveillance des activités réseau, gestion des accès, prévention des intrusions.
- **Compréhension des menaces avancées** : attaques DDoS, exploitations de failles, ingénierie 983
- **Outils de sécurité** : solutions logicielles, protocoles de sécurité, et bonnes pratiques pour sécuriser un réseau d'entreprise.

Module 6 – Gestion des cybermenaces
Durée :16 jours
Objectifs pédagogiques :

- Comprendre les attaques informatiques : Expliquer comment les cybercriminels exécutent les attaques les plus courantes et exploitent les vulnérabilités du protocole TCP/IP.
- Maîtriser les principes de la sécurité réseau : Expliquer les notions clés de la sécurité des réseaux et les dispositifs/services utilisés pour la renforcer.
- Appliquer des mesures de protection : Recommander des solutions pour atténuer les menaces et mettre en œuvre les bonnes pratiques en cybersécurité afin de garantir la confidentialité, l'intégrité et la disponibilité.
- Gérer la sécurité des systèmes : Utiliser les outils d'administration Windows, implémenter la sécurité de base sous Linux, et évaluer les protections des postes de travail face aux malwares.
- Diagnostiquer et sécuriser les connexions réseau : Dépanner un réseau sans fil et vérifier la sécurité des terminaux et des connexions.

Contenus abordés :

- Identifier les cybermenaces : malwares, ransomwares, menaces persistantes avancées (APT), attaques internes.
- Analyser les impacts des attaques sur la sécurité des entreprises et des données personnelles.
- Mettre en œuvre une gestion efficace des menaces : détection, analyse, réponse et prévention.
- Travailler avec les outils et processus de gestion des risques liés à la cybersécurité.



CAT
Centre des Académies et des Technologies

Cité du savoir - Diamniadio
Avenue Bourguiba, rue n°13, Immeuble Adja Rokhaya
+221 30 108 41 53
BP 15126 Dakar - Fann
www.unchk.sn

Foo nekk foofu la