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 en cybersécurité pour tous

Foo nekk foofu la

cat@unchk.edu.sn

Université numérique
CHEIKH HAMIDOU KANE

CAT
Centre des Académies et des Technologies

cybersécurité pour tous – un atout pour tous, quel que soit votre métier !

Dans un monde de plus en plus connecté, la cybersécurité est l'affaire de tous, pas seulement celle des experts informatiques. Que vous travailliez dans l'administration, les ressources humaines, le marketing ou tout autre secteur, comprendre les bases de la sécurité numérique est devenu essentiel.

Nous vous proposons de participer au certificat Cybersécurité pour tous proposé gratuitement par le Centre des Académies et des Technologies (CAT) du Pôle des Sciences, Technologies et Numérique.

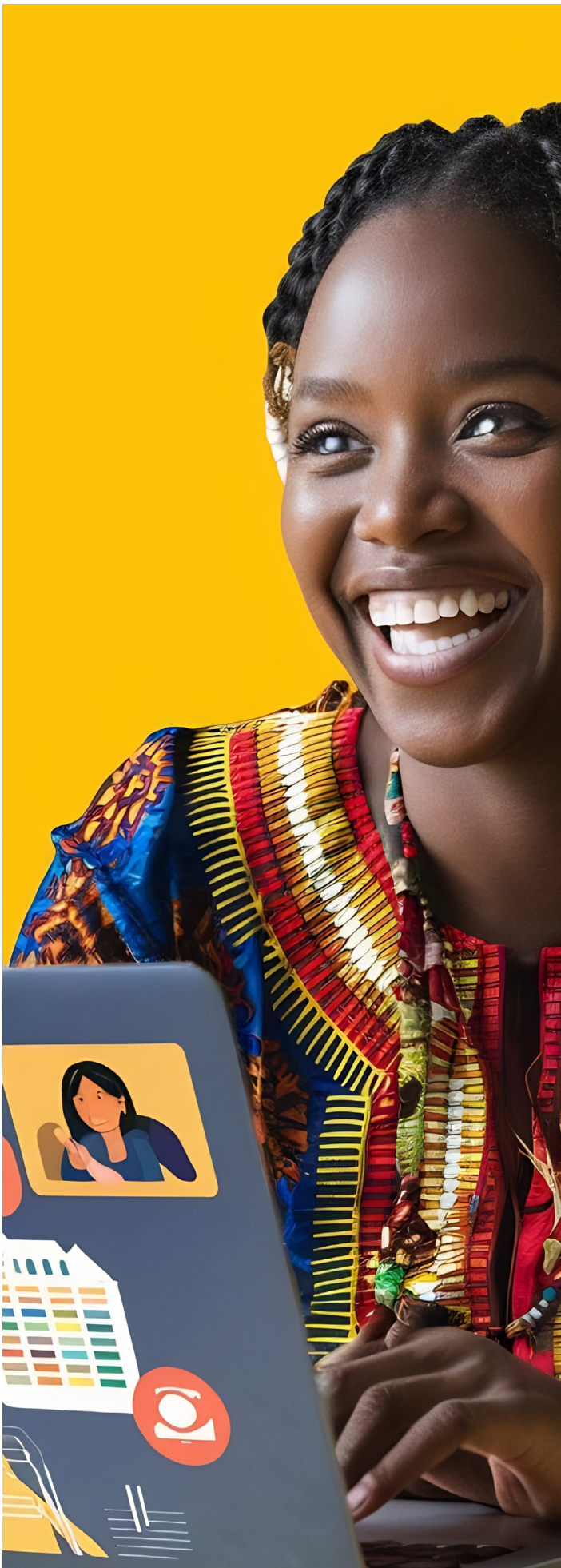
Pourquoi suivre cette formation ?

- Accessible à tous : Pas besoin de connaissances techniques – idéale pour les débutants.
- Utile au quotidien : Apprenez à reconnaître les e-mails frauduleux, sécuriser vos mots de passe, éviter les fuites de données, etc.
- Valorisant sur le CV : Montrez que vous êtes conscient des enjeux numériques actuels.
- Pertinent pour tous les métiers : Tous les secteurs sont concernés par la sécurité de l'information.

Inscrivez- vous
https://formsgle/2yvWTHniDQ7cTm9RA

objectifs pédagogiques

- Comprendre les concepts fondamentaux de la cybersécurité
- Identifier les principales menaces et types de cyberattaques
- Protéger les données personnelles et la vie privée en ligne
- Comprendre comment les organisations sécurisent leurs systèmes
- Découvrir les métiers et perspectives de carrière en cybersécurité



Pourquoi choisir ce certificat ?

- Accessible : aucun prérequis technique
- Sensibilisation essentielle à la sécurité numérique
- Reconnu internationalement par Cisco Networking Academy
- Idéal pour débuter un parcours en cybersécurité
- Badge numérique Cisco délivré à la fin du cours

Public cible

- Débutants en informatique et numérique
- Étudiants de toutes disciplines
- Enseignants et formateurs
- Professionnels souhaitant renforcer leur culture numérique
- Personnes intéressées par les métiers de la cybersécurité

Durée et modalités

- **Durée** : 6 jours
- **Format** : Autoformation guidée 100% en ligne
- **Supports** : Cours interactifs, exercices pratiques, tests d'évaluation
- **Evaluation** : Evaluation progressive durant chaque module + examen à la fin
- **Badge numérique** délivré par CISCO à la fin de chaque module
- **Attestation de maîtrise** délivrée par le CAT à la fin de la formation
- **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

Objectifs pédagogiques :

- Définir la cybersécurité et son importance dans le monde connecté d'aujourd'hui.
- Comprendre pourquoi les données personnelles et organisationnelles doivent être protégées.
- Expliquer les conséquences potentielles des cyberattaques sur les individus et les organisations.

Contenus abordés :

- Qu'est-ce que la cybersécurité et pourquoi est-elle essentielle.
- Les notions de données personnelles et données organisationnelles sensibles.
- Présentation du rôle des cybercriminels et des motivations des attaques.
- Aperçu du paysage des menaces actuelles en cybersécurité.

Module 2 – Attaques, concepts et techniques)
Objectifs pédagogiques :
- Reconnaître les types courants de menaces, attaques et vulnérabilités.
- Comprendre les méthodes et techniques utilisées par les attaquants pour infiltrer les systèmes.

Contenus abordés :
- Catégories d'attaques (par exemple : phishing, malwares, ransomwares).
- Vulnérabilités typiques dans les systèmes et réseaux.
- Analyse des techniques utilisées dans une attaque.
- Principales caractéristiques d'un cyber-incident.

Module 3 – Protection de vos données et de votre vie privée
Objectifs pédagogiques :
- Appliquer de bonnes pratiques pour sécuriser les appareils et les données personnelles.
- Comprendre les risques associés aux comportements en ligne imprudents.

Contenus abordés :
- Sécurisation des appareils personnels (mots de passe forts, mises à jour).
- Technologies et techniques pour protéger la vie privée en ligne.
- Bonnes pratiques de sécurité des comptes et des réseaux personnels.
- Stratégies de prévention contre l'exploitation des vulnérabilités

Module 4 – Protection de l'organisation
Objectifs pédagogiques :
- Découvrir comment les organisations se défendent contre les attaques.
- Comprendre les approches et outils employés par les équipes de sécurité professionnelles.

Contenus abordés :
- Défense réseau et sécurité organisationnelle.
- Processus de sécurité comme la détection des intrusions, les pare-feux et les contrôles d'accès.
- Concepts tels que la cybersécurité comportementale et les stratégies de défense.
- Introduction aux rôles et responsabilités des équipes de sécurité informatique.

Module 5 – Votre avenir dans la cybersécurité
Objectifs pédagogiques :

- Explorer les opportunités de carrières dans la cybersécurité.
- Comprendre les aspects juridiques, éthiques et réglementaires liés à la cybersécurité.
- Encourager à poursuivre des formations et certifications dans le domaine

Contenus abordés :

- Présentation des voies de carrière en cybersécurité.
- Rôles professionnels dans la sécurité informatique.
- Bases des questions éthiques et règles juridiques relatives à la cybersécurité.
- Ressources et conseils pour la progression professionnelle.

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 fooju la