



✉ cheicknasanogo223@gmail.com

🏠 Marrakech, Maroc

🔗 www.portfolio.com

🇲🇱 Malien

☎ +212 774 36 64 31

## Langues

### Bambara

Langue maternelle

### Français

Deuxième langue

### Anglais

Niveau B2

## Réseaux sociaux

in @Cheickna Sanogo

🐦 @ChK101011

## Atouts

Adaptabilité

Créativité

Communication

Esprit analytique

Travail d'équipe

## Centres d'intérêt

Sport

Mangas

Lecture

Échecs

CTF

Cheickna SANOGO

## Élève Ingénieur Cyber Défense | SOC Analyst - Threat Hunting & Forensics

Je poursuis un cycle d'ingénieur en Génie Cyber Défense, avec un intérêt marqué pour l'analyse forensique et le threat hunting, et je complète ma formation par des exercices pratiques. Prêt à intégrer une équipe SOC, j'apporterai une forte curiosité technique, un sens du détail et une capacité à collaborer pour détecter et contenir les incidents.

## Diplômes et Formations

### ● Cycle d'Ingénieur : Génie Cyber Défense et Systèmes de Télécommunication Embarqués

Depuis 2023 ENSA Marrakech Maroc

### ● Cycle Préparatoire : Sciences et Techniques pour Ingénieurs

De 2021 à 2023 ENSA Safi Maroc

### ● Baccalauréat Sciences Exactes – Mention Bien

De 2020 à 2021 Lycée Privé Mamba Bamako, Mali

## Expériences professionnelles

### ● Co-fondateur & Porteur de Projet

Depuis octobre 2025 Cité de l'Innovation de Marrakech (CIM) Marrakech, Morocco  
Projet HayTech - Dispositif médical portable d'analyse de l'haleine pour détection précoce de maladies chroniques (diabète, maladies rénales, pulmonaires).

#### Réalisations :

- Sélectionné parmi 400+ projets candidats pour intégrer le programme de pré-incubation (Top 20)
- 3 prix obtenus : Innovation Sans Frontières, Admission à la Pré-incubation, Meilleur Projet Innovant
- Développement du prototype intégrant capteurs multi-gaz, IA embarquée et application mobile (Flutter)
- Dossier de brevet en préparation pour technologie brevetable unique

**Stack technique :** Électronique médicale, ESP32/Raspberry Pi, IA embarquée, Flutter, Bluetooth

### ● Stagiaire Ingénieure Cyber Sécurité

De juillet 2025 à septembre 2025 OpenLluna Remote

**Mission :** Conception et développement d'un Security Dashboard pour automatiser les analyses SAST/DAST.

#### Réalisations :

- Développement d'une plateforme web (Node.js/Express.js) intégrant 9 outils de sécurité
- Création d'un module d'analyse de sécurité des API avec scoring automatique
- Interface interactive avec visualisations temps réel (Chart.js)
- Normalisation des résultats multi-outils en format JSON unifié

**Impact :** Réduction de 70% du temps d'analyse avec centralisation des rapports dans une interface unique.

**Stack :** Node.js, Express.js, Docker, Chart.js, OWASP ZAP, CodeQL, Semgrep

Compétences

**Audit et assurance sécurité (ISO 27001, NIST)**

**Sécurité des données & chiffrement**

**Sécurité réseau avancée (IDS/IPS, VPN, segmentation)**

**Développement Frameworks :**  
TensorFlow, PyTorch, scikit-learn  
**NLP :** Transformers, RoBERTa, LLMs (LLaMA, Mistral)  
**Processing :** Pandas, NumPy, TF-IDF, SVM

**DevSecOps & AppSec SAST/DAST :** CodeQL, Semgrep, OWASP ZAP, Nikto, Nuclei, ESLint  
**Security Automation :** CI/CD Security, Docker Security, TruffleHog, Trivy  
**Vulnerability Management :** npm audit, dependency scanning

**Offensive Security Pentesting :** Metasploit, Nmap, Burp Suite, OSINT  
**Exploitation :** Privilege Escalation, Lateral Movement

**Sécurité Opérationnelle & SOC SIEM & Monitoring :**  
Splunk, Elastic Stack (ELK), Wazuh, Kibana, Grafana  
**IDS/IPS :** Snort, Suricata, Zeek  
**Analyse Réseau :** Wireshark, Tshark, Brim, tcpdump  
**Threat Intelligence :** MITRE ATT&CK, MISP, OpenCTI, TheHive

**Forensics & Incident Response Disk/Memory Analysis :**  
Autopsy, Volatility, Redline, KAPE, Velociraptor, FTK Imager  
**Detection :** Anomaly Detection, Behavioral Analysis, EDR

Autres Projets

**LLM Jailbreak Defense System Avril- Juin 2025**  
Architecture hybride de détection et prévention des attaques jailbreak dans les LLMs avec système de double validation (détecteur + juge).  
- Développement d'un détecteur ML (SVM + TF-IDF) et d'un modèle juge (RoBERTa-base) pour classification binaire  
- Intégration multi-modèles (LLaMA 3.2, Mistral 7B, Phi-2) via Ollama pour évaluation comparative de robustesse  
- Pipeline backend Django avec API REST et dashboard interactif pour visualisation temps réel  
- **Résultats :** 67% de détection des jailbreaks (vs 17% avec détecteur seul), réduction de 50% des faux négatifs  
**Technologies :** Python, Django, TensorFlow/PyTorch, RoBERTa, Ollama, SVM, TF-IDF, REST API

**Smart LoanCheck Avril- Juin 2025**  
Développement d'une application web full-stack pour l'évaluation automatisée de crédits  
**Backend :** API REST Spring Boot (sécurisée par JWT) + base PostgreSQL  
**IA :** Modèle XGBoost entraîné sur données financières  
**Frontend :** Dashboard admin/utilisateur avec Thymeleaf et Bootstrap

**Infrastructure Réseau Haute Disponibilité Novembre-Décembre2024** Conception d'une architecture réseau redondante (Active-Passive) avec basculement automatique via HSRP et STP. Sécurisation des VLANs IT/RH avec politiques de filtrage sur FortiGate (synchronisation HA).  
**Outils :** GNS3, VMware, Wireshark | Protocoles : HSRP, STP, HTTP/SSH

*Pour voir les autres projets veuillez consultez mon portfolio sur lien suivant :*

Certifications

**CompTIA Cybersecurity Analyst (CySA+) CS0-003 Specialization — Pearson/Coursera**  
Octobre 2025 | Certificat ID ZXNSWO65M5UF

**Blue Team Junior Analyst Pathway Bundle — Elearnig Security Blue Team**  
Septembre 2025 | Certificat ID 424010410

**DevSecOps — TryHackMe**  
Juillet 2025 (26h 45min) | Certificat ID THM-1RWBPRITN8

**Digital Forensics and Incident Response — LetsDefend**  
Juillet 2025 | Certificat ID

**SOC Analyst Learning Path — LetsDefend**  
Juin 2025 | Certificat ID

**SOC Level 1 — TryHackMe**  
Juin 2025 (87h 50min) | Certificat ID THM-6BSKAWNWO5

*Pour voir les autres certifications, veuillez consulter mon portfolio*