

Sunnoogo Caleb TAPSoba

Stage de fin d'études en Cybersécurité & Cloud – Mars 2026

✉ sunnoogo-caleb.tapsoba@efrei.net

☎ +33 0744888912

🔗 Portfolio

🐙 Github

🌐 LinkedIn

📍 Cachan, France

Élève-ingénieur à l'EFREI Paris, spécialisé en Cybersécurité et Cloud Security. Compétences développées en sécurité réseau, environnements cloud, IAM/AD/Entra et pratiques DevSecOps. Curieux, rigoureux et orienté défense, je me passionne pour la Blue Team, la protection des systèmes et la conception d'architectures sécurisées, résilientes et automatisées.

🎓 FORMATION

Diplôme d'Ingénieur – Cybersécurité & Cloud

EFREI Paris – Grande École d'Ingénieurs

08/2024 – 08/2026 | Villejuif, France

Modules principaux : SOC & Threat Hunting, Architecture sécurisée et analyse de vulnérabilités, Endpoint Detection & Response (EDR), Sécurité Azure Cloud, DevSecOps, Analyse de malwares, PKI & IAM, RGPD & Gestion des risques, Tests d'intrusion, Réponse aux incidents.

Bachelor of Engineering Science – Semestre d'échange

Staffordshire University

01/2024 – 05/2024 | Stoke-On-Trent, Royaume-Uni

Classes préparatoires (MPSI → MP*) – Mathématiques & Physique

Institut National Polytechnique Félix HOUPOUËT-BOIGNY

09/2021 – 05/2023 | Yamoussoukro, Côte d'Ivoire

🏢 PROJETS ACADÉMIQUES & PERSONNELS

SecureFlow Platform — Cloud & DevSecOps sécurisé

Projet d'ingénierie : Conception et déploiement d'une plateforme Cloud sécurisée intégrant une chaîne CI/CD complète et des contrôles DevSecOps.

11/2025 – aujourd'hui

- Mise en place d'une pipeline CI/CD GitLab/GitHub Actions avec validation, scans SAST/Trivy/Checkov et déploiement automatisé.
- Infrastructure Azure déployée en IaC (Terraform) : réseau segmenté, VM applicative, reverse proxy, NSG Zero Trust.
- Intégration des tests de sécurité bloquants (SAST, IaC scanning) dans les pipelines.
- Mise en œuvre d'un pattern DevSecOps : revue de configuration, durcissement, monitoring sécurité.

Impulse – Plateforme Cloud et DevSecOps sécurisée

Conception et déploiement d'une application cloud-native sécurisée, appuyée sur une architecture Azure, des pipelines CI/CD et des pratiques DevSecOps.

11/2025 – aujourd'hui

- Mise en place d'une **chaîne CI/CD complète** avec GitHub Actions (build, tests, sécurité, déploiement automatisé)
- **Déploiement cloud sécurisé via Terraform** (Infrastructure as Code)
- **Gestion applicative via Azure Web App et Azure Container Registry (ACR)**
- Implémentation d'un **modèle applicatif structuré** : gestion des utilisateurs, contenus, interactions et recommandations (sans préciser la nature du produit)
- Intégration d'**Entra ID** pour l'authentification, le SSO et la gestion centralisée des identités
- Mise en œuvre d'**Azure RBAC, Azure Politiques** et durcissement **Zero Trust**
- Supervision avancée & posture sécurité :
 - **Microsoft Sentinel** (détection, corrélations, dashboards SOC)
 - **Microsoft Defender for Cloud** (CSPM + protection des workloads)
 - Analyse via **Log Analytics & Azure Monitor**
- Sécurisation des secrets, configurations et accès via **Azure Key Vault**
- Contribution active à la stratégie **Blue Team / SOC** : détection d'anomalies, analyse de logs, durcissement de l'environnement cloud

📜 CERTIFICATIONS

- Cybersecurity Essentials & Introduction to CyberSecurity (CISCO)
- Microsoft – AZ-900 ; AZ-800 ; SC-900 ; AZ-104 ; AZ-500 (En Préparation)

</> COMPÉTENCES TECHNIQUES

Cybersécurité & Ingénierie Cloud

- **Cloud & DevSecOps (Azure)** : Azure App Service, AKS (Kubernetes), Azure DevOps Pipelines, GitHub Actions, Infrastructure as Code (Bicep), Azure Monitor, Defender for Cloud, Key Vault, Entra ID / IAM.
- **Architecture & Analyse de sécurité** : évaluation de vulnérabilités, conception d'architectures réseau sécurisées, analyse de risques ISO 27001 / 27005, conformité RGPD.
- **SOC & Réponse aux incidents** : SIEM (Wazuh, Microsoft Sentinel), EDR (Defender for Endpoint), threat hunting, forensic, gestion et containment d'incidents.
- **Identité & PKI** : configuration Active Directory multi-forêts, déploiement PKI (hiérarchie CA, gestion des certificats), intégration IAM (GLPI, Keycloak).
- **Réseaux & Supervision** : DNS, DHCP, VPN, pare-feux, Syslog, analyse du trafic réseau.

🏢 EXPÉRIENCE PROFESSIONNELLE

Stagiaire en Cybersécurité – Blue Team & Sécurité Cloud

Ecobank Ghana PLC - eProcess

12/2024 – 03/2025 | Accra, Ghana

Sage d'observation au sein du pôle Cybersécurité de la division technologique du groupe Ecobank (*eProcess International*). Rotation au sein de cinq équipes : IT Security, SOC, Business Security & Architecture, Engineering et SIRT (Security Incident Response Team). Découverte des opérations de sécurité en environnement bancaire et apprentissage du fonctionnement des outils, politiques et processus de protection des systèmes d'information.

- Sensibilisation à la protection des postes et des identités via **Microsoft Intune, Defender** et **Cisco ISE**.
- Observation des activités du **SOC** et des outils **Microsoft Sentinel** et **Group-IB** (threat intelligence).
- Découverte des principes d'architecture réseau et applicative sécurisée avec l'équipe **Engineering**.
- Présence à des réunions de **revue de conformité** et de **sécurité réglementaire** (ISO 27001, PCI-DSS).

Outils et technologies observés : Microsoft 365 Security (Defender, Intune, Sentinel), **Azure AD / Entra ID**, **Cisco ISE**, **Radware Cloud**.

🤝 SOFT SKILLS

Travail en équipe | Adaptabilité | Résolution de problèmes | Leadership technique

🌐 LANGUES

Anglais : courant – TOEIC : 935/990 – C1

🎵 ACTIVITÉS EXTRA-SCOLAIRES

Music – Piano :

Pratique régulière, discipline et créativité.