

Kimy LAOU Alternante en Cybersécurité

kimy.laou14@gmail.com • 06 62 78 88 28 • Île-de-France • Rythme : 2 semaines entreprise / 1 semaine formation

linkedin.com/in/kimy-laou/ • <https://kimy-laou-portfolio.netlify.app/> • github.com/Kimiko4

À PROPOS DE MOI

Future alternante en 3e année à l'EFREI, je possède une double compétence en sécurisation des infrastructures et en audit technique. Mon expérience chez DigitalCube m'a permis de développer une vision concrète de la cybersécurité : identifier les failles pour proposer des solutions de protection efficaces. Polyvalente, je maîtrise aussi bien l'administration de réseaux sécurisés que la mise en place de mesures défensives sur les systèmes.

Rigoureuse et orientée solutions, je recherche une **alternance d'un an dès septembre 2026** pour accompagner la protection de vos systèmes d'information.

FORMATION

2024 – 2027 Villejuif	Bachelor Ingénierie et Cybersécurité - Grade de licence, Efrei - Ecole d'ingénieurs <ul style="list-style-type: none">Programme labellisé SecNumEdu par l'ANSSI (Cyber Hub EFREI)Élue Déléguée de promotion en 2ème année.
04/2026 – 06/2026 Kuala Lumpur, Malaisie	Mobilité internationale, Asia Pacific University (APU) Programme international : 6 semaines, 100 % en anglais
2021 – 2024 Caen	Baccalauréat Général : admise mention "très bien", Lycée Sainte Marie <ul style="list-style-type: none">Spécialités: Maths SVT1ère : Physique Chimie

EXPÉRIENCES

06/2026 – 07/2026 Bobigny	Stagiaire Développeuse Web Fullstack & Cybersécurité, AP-HP <ul style="list-style-type: none">Développement : Conception d'une application web sécurisée de gestion de plannings (PHP/Java, SQL, SVN).Automatisation : Algorithme de répartition équitable des gardes et calcul automatisé des heures (DRH).Sécurité & Réseau : Configuration de Firewalls Palo Alto (Panorama) et sécurisation du parc biomédical.IAM : Intégration de l'authentification SSO et connexion Active Directory.
04/2025 – 06/2025 Cergy	Stagiaire en Sécurité Applicative & Développement Backend, DigitalCube <ul style="list-style-type: none">Audit & Pentest : Tests d'intrusion (OWASP Top 10) et identification de failles critiques (SQLi, XSS).Reporting : Rédaction de rapports techniques et préconisations de remédiation pour les développeurs.Dév. Sécurisé : Sécurisation backend (Symfony) et gestion des droits pour garantir l'intégrité des données.

COMPÉTENCES

Sécurité Offensive (Pentest): Identification et exploitation de vulnérabilités critiques (Injections SQL, XSS, Brute-force) sur Kali Linux.

Administration Systèmes & Infra: Administration et sécurisation (Hardening) d'environnements Linux (Debian) et Windows Server avec gestion fine des droits.

Réseaux & Sécurité: Architecture TCP/IP, SSH, DNS, Firewalling, Segmentation réseau, Supervision/Monitoring.

Outils Cyber: BurpSuite, Nmap, SQLmap, OWASP ZAP, Wireshark, Metasploit, Cisco.

Développement & Scripting: Python (scripts d'automatisation d'attaques), PHP (Symfony), SQL (MySQL), JavaScript.

Gouvernance SSI: Application des bonnes pratiques ANSSI et conformité RGPD

SOFT SKILLS: Vulgarisation technique | Esprit d'équipe | Rigueur | Méthodologies Agiles | Adaptabilité

PROJETS

Infrastructures Datacenter & Virtualisation (MediCare) :

- Virtualisation** : Déploiement d'un cluster VMware/Proxmox avec stockage partagé (NFS/iSCSI) pour garantir la continuité de service.
- Administration** : Installation de serveurs Windows Server (Active Directory) et Linux pour la gestion des utilisateurs et des ressources.
- Réseau** : Segmentation de l'infrastructure en VLANs (Serveurs, DMZ, Gestion) pour isoler les flux critiques.

Architecture Réseau Cisco & Sécurité Wi-Fi (Packet Tracer) :

- Routing & Switching** : Configuration de routeurs et switchs Cisco (Inter-VLAN, routage statique/dynamique).
- Contrôle d'accès** : Implémentation de serveurs RADIUS et filtrage par ACLs pour l'isolation des réseaux.
- Diagnostic** : Tests de connectivité et analyse de trames pour valider l'étanchéité des segments réseaux.

Architecture 3-Tiers & Gestion des Flux (WordPress) :

- Flux Réseau** : Mise en place d'un Reverse Proxy (Nginx) pour la gestion des requêtes et terminaison HTTPS/TLS.
- Administration** : Configuration d'adresses IP statiques (Netplan) et isolation de la base de données.
- Sécurisation** : Durcissement (hardening) du système et réduction de la surface d'attaque.