



FORMATION

2025 - 2028	EPITECH Bachelor en Cybersécurité Pentest, sécurité applicative, threat modeling, réponse à incident.	Paris, France
-------------	---	---------------

EXPÉRIENCE PROFESSIONNELLE

Avr. 2026 - Act.	PoC Innovation Association Responsable Événements Cybersécurité · Développeur R&D - Conception et animation d'événements nationaux de cybersécurité : ateliers pratiques d'attaque et de défense, démonstrations live et accompagnement des participants. - Coordination des partenaires académiques et industriels (MIT, UCL, CISP, Kiln). - R&D : ChainBreak, plateforme d'entraînement offensif de l'association (28 challenges, sessions terminal isolées, validation des flags côté serveur) ; moteur de recherche inversée d'images d'I.R.I.S, système embarqué de reconnaissance et d'OSINT (Python, Playwright, YOLO).	Paris
Juil. - Août 2026	Bank of Africa Banking & Finance Application Security Intern - Audits de sécurité applicative sur applications internes et exposées : tests d'intrusion web et API, reproduction des failles et rédaction des rapports de remédiation, plusieurs vulnérabilités critiques remontées. - Formation éditeur à une solution EDR : détection sur les postes, tri et investigation des alertes.	France
Jan. - Juin 2026	Startup SaaS B2B/B2G Lead Security Engineer - Pilotage de la posture sécurité de la plateforme en production (Next.js, Fastify, PostgreSQL, Docker Compose) : gouvernance IAM, chiffrement au repos et en transit, gestion des vulnérabilités et remédiation continue. - Durcissement de l'infrastructure : RBAC, sécurisation des pipelines CI/CD et du reverse proxy, fail2ban, sécurisation d'un pipeline RAG, correction de CVEs sur les dépendances NPM.	Paris, France
Jan. - Avr. 2026	Alignerr Technology AI Model Trainer / Evaluator Deux missions d'évaluation commanditées par Anthropic et Airbnb : rounds d'évaluation agentic coding sur Claude Code, rédaction de tâches sur dépôts open source (EigenLayer), comparaison A/B et notation des solutions.	Télétravail

LANGUES ET COMPÉTENCES INFORMATIQUES

Français: Langue maternelle | **Anglais:** Courant
Offensif: pentest web/API (OWASP Top 10), gestion de vulnérabilités, ingénierie sociale | **Défensif:** durcissement système, IAM, EDR, sécurité CI/CD
Langages: Python, Bash, TypeScript, C | **Outils:** Burp Suite, OpenVAS/GVM, GoPhish, Docker, GitHub Actions, Linux/BlackArch | **Agentic coding:** Claude Code

PROJETS ET INTÉRÊTS PERSONNELS

Keter — 1^{er} prix, Hackathon Dauphine x Delubac
Plateforme de conformité MiCA / RGPD pour tokens ERC-1400 : circuits Noir / UltraPlonk, vérification on-chain (Sepolia), preuves générées côté client (NoirJS).
REDTEXT — outil open source de Red Team (Python)
Génération de scénarios d'ingénierie sociale (phishing, vishing, smishing, quishing) pour engagements autorisés ; déploiement des campagnes via l'API GoPhish. github.com/keuchnotkush/REDTEXT
Autres projets open source — gvm-blackarch : installation reproductible du scanner de vulnérabilités Greenbone / OpenVAS sur Arch et BlackArch (Docker, shell). **OWASP Juice Shop** : 18 writeups d'exploitation web (CTF EPITECH). **SAMPO** : agrégateur d'offres full-stack (React, Node/Express, FastAPI, PostgreSQL, JWT + RBAC, Docker).
Passionné d'art néo-expressionniste (Jean-Michel Basquiat ; Georg Baselitz)