Ayoub Goubraim

+33 7 53 44 54 36 · ayoub.goubraim@ecole.ensicaen.fr · ayoubgoubraim · AyGoub · aygoub.github.io

Étudiant ingénieur en cybersécurité, orienté sécurité applicative et pentest. Recherche un stage PFE de 6 mois à partir de septembre 2026.

Certifications & CTFs

- **TryHackMe — Top 2% mondial** (+16 000 points) **INE eJPT** : Certification en préparation
- **Root-Me** : +900 points

Expériences Professionnelles

FORVIA (Faurecia) — Interior Systems **Avr. 2025 – Juil. 2025**
Stagiaire Ingénieur IT — Sécurité & Infrastructure *Méru, France*

- Conception d'une plateforme sémantique sécurisée (VocBench 3, GraphDB, AWS Neptune) avec analyse des risques selon le cadre **EBIOS RM** et automatisation de l'infrastructure On-Prem.
- Évaluation de la conformité **RGPD / ISO 27001** et gestion des permissions **IAM** (principe du moindre privilège) pour l'intégration sécurisée d'assistants IA — approche *Security by Design*.

Formation

UNICAEN — Université de Caen Normandie : Double Diplôme, Spécialisation Cybersécurité **2025 – En cours**
Biométrie, Cryptographie post-quantique, Forensique, Pentesting avancé, Audit SSI, Cryptanalyse *Caen, France*

ENSICAEN — École Nationale Supérieure d'Ingénieurs de Caen : Cycle Ingénieur Informatique **Sept. 2023 – En cours**
Majeure e-Paiement & Cybersécurité : Sécurité réseaux, Cryptographie, Dev web sécurisé, Systèmes *Caen, France*

Projets

StudentSecScore : Plateforme SaaS de Scan DevSecOps **Fév. 2026**

- Développement d'une application web d'analyse automatisée de la sécurité de dépôts GitHub (OAuth), couvrant l'ensemble du cycle de détection : SCA (Trivy), SAST (SonarQube / Semgrep) et DAST (OWASP ZAP).
- Détection et classification des vulnérabilités applicatives et des secrets exposés selon le référentiel OWASP Top 10, avec scoring dynamique de la surface de risque avant mise en production.
- Génération de rapports exploitables (recommandations de remédiation, suivi de la correction).

Pentest applicatif & offensif *(TryHackMe, Root-Me, HTB)* **2025 – En cours**

- Exploitation de vulnérabilités web (injections SQL, XSS, SSRF, IDOR, contournement d'authentification) sur environnements de laboratoire, selon la méthodologie **OWASP**.
- Reconnaissance et exploitation réseau (**Nmap, Burp Suite, Metasploit**), élévation de privilèges Linux/Windows et post-exploitation.
- Rédaction de comptes-rendus d'exploitation (preuve de concept, impact, recommandations de remédiation).

SIEM Open Source : Supervision Blue Team & Centralisation de logs **Nov. 2025**

- Déploiement d'un SIEM OSSIM/AlienVault avec intégration de 5+ sources de logs (syslog, Apache, SSH) et installation d'agents HIDS pour la supervision continue de l'état des systèmes.
- Configuration de 15+ règles de corrélation personnalisées pour détecter brute-force, scans réseau et élévations de privilèges — **détection d'intrusions et réponse aux alertes en temps réel**.

Compétences

Sécurité Pentesting (Nmap, Burp Suite, Metasploit, Hashcat), SIEM (AlienVault), IDS/IPS, OWASP TOP 10

DevSecOps Git, Docker, Kubernetes (K8s), Helm, GitLab CI, ArgoCD, CI/CD, Scan de vulnérabilités (Trivy, SonarQube, OWASP ZAP), Secrets Management (Vault)

Observabilité Prometheus, Grafana, Loki (Stack PLG), Elasticsearch (ELK), Monitoring de performance, Alerting, Centralisation de logs

Cloud & Sys AWS (IAM, Neptune, S3), **Azure (notions : AKS, IAM, RBAC)**, Linux (Ubuntu, Kali), Windows Server, TCP/IP, SSL/TLS, VPN, Nginx

Développement Python, Node.js, React, Bash, C/C++, Java, JavaScript, PostgreSQL, MySQL, MongoDB

Conformité PCI-DSS, ISO 27001, HDS, RGPD, Audit SSI, Gestion des risques

Soft skills Rigueur, Analyse critique, Travail d'équipe, Autonomie, Veille technologique, Documentation, Vulgarisation

Langues & Intérêts

- Français (courant) • Anglais (TOEIC 850) • Arabe (langue maternelle) • Football, Voyage, Musique, Veille IT (CTF, blogs sécurité, CVE, Menaces)