

MAROUANE SASSI

ETUDIANT EN 5EME ANNÉE - CYCLE INGÉNIEUR (M2)
CYBERSÉCURITÉ INFRASTRUCTURES & LOGICIELS

DISPONIBLE IMMÉDIATEMENT — STAGE DE FIN D'ÉTUDES (6 MOIS)

CONTACT

+33 7 81 42 12 60
marouane.sassi@efrei.net
94170, Le Perreux-sur-Marne
Permis B

LIENS

Portfolio
RootMe
LinkedIn
HackTheBox

COMPÉTENCES

Sécurité offensive & vulnérabilités
Pentest web (SQLi, SSTI, SSRF, XXE, JWT), gestion de vulnérabilités (Rapid7 InsightVM), audits et durcissement. HackTheBox Pro Hacker, Root-Me 2500+ pts.

Blue Team & détection
SIEM Wazuh (déploiement, règles, agents), analyse d'alertes, mapping MITRE ATT&CK, CrowdSec, alerting automatisé.

Administration systèmes & réseau
Windows Server / Linux (Debian, Ubuntu), Active Directory & FreeIPA (IAM, MFA), pare-feu OPNsense, segmentation VLAN, nftables, AppArmor.

Cloud & virtualisation
Docker, Kubernetes, Hyper-V, ESXi — déploiement et sécurisation d'environnements virtualisés.

Développement & automatisation
Python (Flask, FastAPI), Bash, PowerShell, CI/CD (Gitea), intégration LLM (Mistral). Également : C, C++, C#, Java, JavaScript, PHP.

GRC & conformité
ISO 27001, EBIOS RM, NIS2, RGPD — analyse de risques et mise en conformité.

CERTIFICATIONS

Google Cybersecurity
Microsoft Cybersecurity Analyst
IBM Cybersecurity Analyst

LANGUES

- **Français** - Langue maternelle
- **Anglais** - C1 (TOEIC 885)
- **Espagnol** - B1
- **Arabe** - C2

CENTRES D'INTÉRÊT

Sport : Boxe Anglaise, Echecs, Voyages

EXPERIENCE

Stage ingénieur Cybersécurité - VINCI — 2024-2025

Rueil-Malmaison 92063 - 5 mois (novembre 2024 - mars 2025)

- Réduction du parc de serveurs vulnérables de **~300** à moins de **10** via un programme de **remédiation piloté avec Rapid7 InsightVM**
- Qualification et traitement des **alertes CERT**, priorisation des vulnérabilités selon criticité et exposition
- Conception d'un **dashboard BI (InsightVM)** pour le suivi des vulnérabilités auprès des équipes IT et du management
- **Durcissement** des serveurs Windows et **administration Active Directory (comptes, privilèges, GPO)**
- **Automatisation de tâches de sécurité** en **PowerShell** et **Bash** ; déploiement d'outils de **conformité et monitoring (WSUS, LogicMonitor)**
- Rédaction de **documentation technique** et support aux équipes IT sécurité

Stage Assistant commercial - AURAJOB — 2022

Nanterre 92050 - 1 mois

- Qualification des demandes et orientation des interlocuteurs
- Veille commerciale et suivi des contacts clients
- Mise à jour des informations clients et reporting simple

Stage Ouvrier d'exécution - SNTPP — 2021

Fontenay-sous-Bois 94033 - 1 mois

- Participation aux activités quotidiennes sur le terrain
- Travail en équipe et coordination avec les différents intervenants
- Respect des consignes de sécurité et des procédures

FORMATION

Diplôme d'ingénieur - EFREI, Villejuif — 2021-2026

Cybersécurité infrastructures & logiciels

- **Semestre international** - *Taltech* en Estonie (Tallinn) - **5 mois**
  Computer Network Security, Cyber Incident Handling, Cyber Defense Monitoring Solutions, Special Subjects of Cryptography, Management & Leadership
- **Séjour linguistique** - *Education First* aux États-Unis (New York) - **5 semaines**
- **Semestre international** - *Staffordshire University* au Royaume-Uni (Stoke-on-Trent) - **4 mois**
  Cryptographie, Projet de sécurisation web

Baccalauréat général - Lycée Paul Doumer, Le Perreux-sur-Marne 94170 — 2021

Spécialités **Mathématiques**, **Physique-Chimie** et **Mathématiques expertes**

PROJET

- **Homelab cybersécurité auto-hébergé :** Infrastructure virtualisée (Hyper-V) segmentée en VLANs avec pare-feu OPNsense, IAM centralisé FreeIPA (MFA TOTP), SIEM Wazuh, durcissement systèmes (nftables, CrowdSec, AppArmor), CI/CD Gitea, serveur public en production (reverse proxy Nginx, HTTPS, alerting Telegram). Auto-audit ISO 27001. Développement d'un SOC Assistant (Flask + LLM Mistral) pour l'analyse d'alertes Wazuh avec mapping MITRE ATT&CK.
- **SECUCLOUD – Cloud souverain sécurisé:** Architecture Cloud sécurisée sous Kubernetes avec services managés et console de déploiement.
- **Audit de sécurité Active Directory (ANSSI):** Audit AD selon les recommandations ANSSI avec scripts PowerShell automatisés.
- **CLOUDYF – Infrastructure virtualisée sur ESXi:** Déploiement d'une infrastructure Cloud virtualisée (Windows, Linux, sécurité).
- **Secure ChatBox (ChatSec):** Application de messagerie sécurisée avec gestion des accès et chiffrement.
- **Cyberlabs Blue/Red Team:** Labs pratiques en cybersécurité (HTB, TryHackMe, Rootme).