Nassim Zerhouni

Analyste Cybersécurité Junior

Grenoble, France | nassim.zerhouni@gmail.com | +33 6 51 84 37 29 | linkedin.com/in/nassimzerhouni

Diplômé d'un Master Cybersécurité de l'ENSIMAG avec **6 mois de stage** au SOC d'Orange Cyberdefense. Analyse de **2 000+ alertes de sécurité** et identification de **35 incidents confirmés**. Maîtrise de Splunk, QRadar et Cortex XSOAR. Certifié CompTIA Security+ et formé au référentiel ANSSI. Classé top 10 national en compétitions CTF.

EXPÉRIENCE

Stagiaire Analyste SOC, Orange Cyberdefense, Lyon *Janv. 2025 – Juin 2025*

Stage de 6 mois au Security Operations Center (SOC) niveau 1 et 2 (surveillance 24/7 pour 45 clients).

- Analyse de **2 000+ alertes de sécurité** sur Splunk et QRadar, identification de **35 incidents confirmés**
- Rédaction de **35 rapports d'incident** détaillés avec analyse de la kill chain et recommandations de remédiation
- Automatisation de **8 playbooks** de réponse aux incidents sur Cortex XSOAR, réduisant le temps de traitement de **30 %**
- Veille quotidienne sur les menaces : rédaction de **12 bulletins de sécurité** diffusés aux clients

Assistant Sécurité IT (Projet universitaire rémunéré), ENSIMAG, Grenoble *Mars 2024 – Août 2024*

Mission d'audit de sécurité sur l'infrastructure IT du campus.

- Scan de vulnérabilités sur **120 serveurs** avec Nessus, identification de **28 vulnérabilités critiques**
- Test d'intrusion (pentest) sur **3 applications web** internes, rapport de **45 pages** avec correctifs
- Déploiement d'un SIEM Elastic sur le réseau du laboratoire (**50 postes** supervisés)

FORMATION

Diplôme et spécialité, ENSIMAG (Grenoble INP), Grenoble *Sept. 2022 – Juil. 2025*

Diplômé avec mention Bien (**15,3/20**). Formation labellisée SecNumEdu par l'ANSSI.

- Modules principaux : Sécurité des systèmes d'information, Cryptographie, Analyse de malware, Forensique numérique
- Projet de fin d'études : développement d'un outil de détection d'anomalies réseau par machine learning, noté **17/20**

COMPÉTENCES

SIEM (Splunk, QRadar, Elastic) • SOAR (Cortex XSOAR) • Analyse d'incidents de sécurité • Scan de vulnérabilités (Nessus, Qualys) • Wireshark et analyse de paquets • MITRE ATT&CK Framework • Linux (administration sécurisée) • Python (scripts d'automatisation) • Normes ISO 27001 et ANSSI • Rédaction de rapports d'incident

CERTIFICATIONS

CompTIA Security+, CompTIA *Mars 2025 – Mars 2025*

Certification SecNumEdu (label ANSSI), ANSSI *Juil. 2025 – Juil. 2025*

LANGUES

Français (langue maternelle) • Anglais (C1) • Arabe (courant)

PROJETS

Compétitions CTF — Team GreHack *Sept. 2023 – Juin 2025*

Participation active aux compétitions Capture The Flag avec l'équipe étudiante GreHack.

- Participation à **6 compétitions CTF** nationales et européennes (GreHack, MUSIC, ECSC qualifications)
- Classement **top 10 national** au CTF MUSIC 2024 (catégorie étudiants, 120 équipes)
- Spécialités : forensique numérique, analyse de malware et exploitation web

RÉFÉRENCES

Karim Bensaid, Team Lead SOC L2, Orange Cyberdefense, k.bensaid@orange.com, +33 4 72 56 83 19

ACTIVITÉ EXTRA-SCOLAIRE

Vice-président — Club Cybersécurité ENSIMAG *Janv. 2024 – Juin 2025*

Animation du club de cybersécurité de l'école avec **45 membres actifs**.

- Organisation de **8 workshops** pratiques (pentest, forensique, reverse engineering)
- Coordination de la participation de l'école à **4 compétitions CTF**