AMIN BEN YOUSSEF

Spécialiste Cybersécurité & Pentesting | SOC Analyst

Email : mohamedbenyoussef93@outlook.fr
Téléphone : 06 24 04 86 53
Adresse : 23 rue Victor Haussonville, Drancy, 93700
LinkedIn : [Profil LinkedIn] | **TryHackMe :** Top 10%
Permis : B/A2 + Véhicule personnel

OBJECTIF PROFESSIONNEL

Spécialiste en Cybersécurité avec expertise en pentesting et analyse SOC, recherche un poste en **alternance ou CDI** pour contribuer à la sécurisation des infrastructures IT. Passionné par la sécurité offensive/défensive avec une expérience pratique en tests d'intrusion, détection d'incidents et sensibilisation cyber.

EXPÉRIENCE PROFESSIONNELLE

Technicien Support & Cybersécurité

M.B GARDIENNAGE | Paris | *Septembre 2023 - Juin 2024*

- **Sécurisation réseau PME** : Déploiement et configuration firewall, VPN, segmentation VLAN pour 50+ postes
- **Monitoring SOC** : Surveillance 24/7 des logs de sécurité via Wazuh et ELK Stack
- **Détection d'incidents** : Identification et remédiation de 15+ incidents de sécurité par mois
- **Support technique** : Résolution de vulnérabilités critiques et mise à jour des politiques de sécurité
- **Formation utilisateurs** : Sensibilisation cybersécurité pour 100+ collaborateurs

---

FORMATION & CERTIFICATIONS

Bac+4 - Spécialiste en Cybersécurité et Réseaux *(RNCP Niveau 6)*

Jedha Paris | *Juin 2025 - En cours*

- Spécialisation : Pentesting & Sécurité Offensive
- Sécurisation architectures Cloud & On-Premise
- Gestion des incidents et réponse d'urgence

Formation - Analyste en Cybersécurité

OpenClassrooms Paris | *Septembre 2023 - Juin 2024*

- Tests d'intrusion et analyse de vulnérabilités
- Détection d'attaques et réponse aux incidents
- Projet final : Audit sécurité complet d'une infrastructure

Spécialisation DevOps

CNAM Paris | *2021 - 2022*

- Sécurisation des pipelines CI/CD
- Automatisation des déploiements sécurisés

COMPÉTENCES TECHNIQUES

Sécurité Offensive ★★★★★

- **Pentesting** : Kali Linux, Metasploit, Burp Suite Professional, Nmap
- **Exploitation** : Buffer Overflow, Injection SQL, XSS, CSRF
- **CTF** : TryHackMe (Top 10%), HackTheBox, Root-Me

Audit & Vulnérabilités ★★★★★

- **Scanners** : Nessus Professional, OpenVAS, Qualys, Acunetix
- **Méthodologies** : OWASP Top 10, NIST, OSSTMM
- **Reporting** : Rédaction de rapports d'audit détaillés

SOC & SIEM ★★★★★

- **Plateformes** : Splunk Enterprise, Wazuh, ELK Stack (Elasticsearch, Logstash, Kibana)
- **Détection** : Création de règles de corrélation, analyse comportementale
- **Incident Response** : Playbooks, forensics, containment

Infrastructure & Réseau ★★★★☆

- **Systèmes** : Windows Server, Linux (Ubuntu, CentOS), Active Directory
- **Réseau** : VLAN, Firewall (pfSense, Fortinet), VPN, DMZ
- **Cloud** : AWS Security, Azure Security Center

Conformité & Gouvernance ★★★★☆

- **Réglementations** : ISO 27001, RGPD, NIS2, SOX
- **Risk Management** : Analyse de risques, matrices de criticité

PROJETS TECHNIQUES MARQUANTS

Création d'un SOC Maison *(2024)*

- **Objectif** : Déploiement d'un SOC complet avec détection automatisée
- **Technologies** : Wazuh, ELK Stack, Suricata, pfSense
- **Résultat** : Détection de 95% des attaques simulées en temps réel

Laboratoire Red Team/Blue Team *(2024)*

- **Infrastructure** : 15 VMs (Windows/Linux), Active Directory, DMZ
- **Scénarios** : Simulation d'attaques APT, lateral movement, exfiltration
- **Métriques** : Documentation de 50+ techniques d'attaque MITRE ATT&CK

Audit Sécurité Complet *(2023)*

- **Périmètre** : Infrastructure de 200+ postes, 15 serveurs
- **Découvertes** : 25 vulnérabilités critiques identifiées et corrigées
- **Impact** : Amélioration du niveau de sécurité de 40%

Campagne de Phishing Avancée *(2023)*

- **Outils** : Gophish, SET, domaines typosquatting
- **Cible** : 500+ collaborateurs
- **Résultat** : Réduction de 70% du taux de clic après formation

---

RÉALISATIONS QUANTIFIÉES

- **Classement Top 10%** sur TryHackMe avec 500+ machines compromises
- **15+ audits de sécurité** réalisés sur infrastructures critiques
- **95% de détection** des incidents de sécurité via solutions SIEM
- **50+ CTF** complétés avec focus sur Windows/Linux privilege escalation
- **100+ personnes** formées aux bonnes pratiques cybersécurité

LANGUES

- **Français** : Langue maternelle
- **Anglais** : Niveau B2 (lecture documentation technique, communication internationale)
- **Allemand** : Niveau scolaire

CENTRES D'INTÉRÊT

Cybersécurité : Veille technologique, Red Team, Cloud Security
Technique : Mécanique moto, électronique
Gaming : Challenges CTF, communauté hacking éthique
Sport : Musculation, développement personnel
Voyages : Irlande, Norvège, Tunisie

DISPONIBILITÉ

Disponible immédiatement pour alternance ou CDI
Mobilité : Île-de-France et région parisienne
Rythme : Temps plein ou alternance (3j/2j ou 1 sem/1 sem)

"La cybersécurité n'est pas une destination, c'est un voyage permanent vers l'excellence."