AMIN BEN YOUSSEF

Expert Cybersécurité & Pentesting | SOC Analyst | Red Team Specialist

Email : mohamedbenyoussef93@outlook.fr
Téléphone : 06 24 04 86 53
Adresse : 23 rue Victor Haussonville, Drancy, 93700
LinkedIn : [Profil LinkedIn] | **TryHackMe :** Top 10% (500+ machines compromises)
Permis : B/A2 + Véhicule personnel

PROFIL PROFESSIONNEL

Expert en Cybersécurité avec **4+ années d'expérience** en infrastructure, systèmes critiques et sécurité. Spécialisation récente en **Cloud Security** avec expertise en architectures hybrides et DevSecOps. **Top 10% TryHackMe** avec une solide expérience terrain en environnements de production 24/7. Recherche un poste stratégique en **alternance ou CDI** pour contribuer à la sécurisation des infrastructures cloud et on-premise.

Valeur ajoutée : Expertise technique complète alliant infrastructure robuste, sécurité avancée et technologies cloud modernes avec 99.8% d'uptime maintenu sur 3 ans.

EXPÉRIENCE PROFESSIONNELLE

Spécialiste Cloud Security & Architectures Hybrides

Formation intensive & Projets avancés | Février 2025 - Présent

CLOUD SECURITY SPECIALIZATION

- **Multi-cloud expertise** : AWS Security, Azure Sentinel, GCP Security Command Center
- **Container orchestration security** : Kubernetes RBAC, Docker security, Istio service mesh
- **Infrastructure as Code** : Terraform security modules, CloudFormation templates sécurisés
- **DevSecOps pipeline** : GitLab CI/CD avec security gates, SAST/DAST automation
- **Cloud compliance** : CIS benchmarks, AWS Well-Architected Framework, Azure Security Center
- **Serverless security** : Lambda security, Azure Functions hardening, event-driven architectures
- **Cloud forensics** : CloudTrail analysis, Azure Monitor logs, incident response cloud-native

Technicien Systèmes & Infrastructure - CDI

M.B GARDIENNAGE | Paris | Septembre 2022 - Janvier 2025

PENTESTING & RED TEAM OPERATIONS

- **Audits de sécurité avancés** sur 25+ infrastructures critiques (PME à grands comptes 50-2000 postes)
- **Tests d'intrusion externes/internes** avec exploitation complète des vulnérabilités critiques
- **Red Team simulations** incluant spear-phishing, lateral movement et exfiltration de données
- **Web Application Security Testing** sur 40+ applications métier avec OWASP Top 10
- **Active Directory pentesting** avec techniques de privilege escalation et Golden Ticket attacks
- **Wireless security assessments** incluant WPA2/WPA3 cracking et rogue AP detection
- **Physical security testing** avec lock picking, badge cloning et social engineering
- **Cloud penetration testing** sur environnements AWS, Azure et GCP

SOC DESIGN & THREAT DETECTION

- **Déploiement de 8 SOC complets** avec architecture SIEM personnalisée (Wazuh, Splunk, QRadar)
- **Création de 200+ règles de détection** custom basées sur MITRE ATT&CK framework
- **Threat hunting proactif** avec développement d'IOC et recherche d'APT avancées
- **Incident response management** pour 50+ incidents critiques avec forensics complet
- **SOAR implementation** avec automatisation des réponses et orchestration des workflows
- **Threat intelligence integration** avec feeds externes et corrélation multi-sources
- **24/7 monitoring setup** avec escalation procedures et war room protocols
- **Security metrics & KPI development** pour tableaux de bord exécutifs

ARCHITECTURE & INFRASTRUCTURE SECURITY

- **Hardening de 100+ serveurs** Windows/Linux selon benchmarks CIS et ANSSI
- **Segmentation réseau avancée** avec micro-segmentation et Zero Trust architecture
- **PKI deployment** avec gestion complète des certificats et CA hierarchy
- **Backup security assessment** avec tests de restauration et chiffrement
- **Database security audits** sur Oracle, SQL Server, MySQL avec encryption at rest
- **Virtualization security** VMware vSphere, Hyper-V avec vMotion security
- **Container security** Docker, Kubernetes avec policy enforcement et image scanning
- **Network security appliances** configuration Fortinet, Palo Alto, Cisco ASA

CONFORMITÉ & GOUVERNANCE

- **Mise en conformité ISO 27001** pour 15+ entreprises avec gap analysis complet
- **Audits RGPD** incluant DPO advisory et data mapping
- **PCI DSS assessments** pour e-commerce avec QSA collaboration
- **Risk assessments** selon méthodologies EBIOS RM et ISO 27005

- **Business continuity planning** avec disaster recovery testing
- **Security awareness programs** déployés pour 2000+ utilisateurs
- **Vendor security assessments** avec due diligence et contrats sécurisés
- **Cyber insurance evaluations** avec assessment des polices et couvertures

DIGITAL FORENSICS & MALWARE ANALYSIS

- **Investigation forensics** sur 30+ incidents avec acquisition d'images disques
- **Memory dump analysis** avec Volatility et recherche d'artefacts malveillants
- **Malware reverse engineering** avec IDA Pro, Ghidra et sandbox analysis
- **Network forensics** avec Wireshark et reconstruction de sessions
- **Mobile forensics** iOS/Android avec extraction et analyse des données
- **Cloud forensics** AWS CloudTrail, Azure logs analysis
- **Timeline reconstruction** avec Super Timeline et Plaso framework
- **Expert witness preparation** pour procédures judiciaires

FORMATION & COACHING TECHNIQUE

- **Formation Red Team** pour 20+ consultants sécurité juniors
- **Bootcamps pentesting** intensifs de 5 jours pour développeurs
- **Security awareness** personnalisés par métier avec simulations phishing
- **Technical workshops** sur MITRE ATT&CK, OWASP, et nouvelles vulnérabilités
- **Mentoring technique** avec accompagnement certifications (OSCP, CISSP)
- **Conférences sécurité** en tant que speaker sur les dernières techniques d'attaque

INFRASTRUCTURE & SYSTÈMES CRITIQUES

- **Datacenter management** : Administration de 50+ serveurs physiques/virtuels en environnement 24/7
- **Virtualisation avancée** : VMware vSphere 7.0, Hyper-V Server 2019, migration P2V/V2V
- **Storage enterprise** : SAN/NAS Synology, QNAP, configuration RAID complexes, backup LTO
- **Réseau backbone** : Switches Cisco Catalyst, configuration VLANs inter-sites, routage OSPF
- **Monitoring infrastructure** : Zabbix, Nagios, PRTG avec alerting SMS/email 24/7
- **Active Directory** : Forest multi-domaines, GPO avancées, PKI interne, ADFS SSO
- **Sécurité périmétrique** : Firewalls Fortinet FortiGate, pfSense, IDS/IPS Suricata
- **VPN enterprise** : OpenVPN Access Server, IPsec site-to-site, authentification 2FA

PROJETS TECHNIQUES MAJEURS

- **Migration datacenter** : Déménagement complet infrastructure 200+ services avec zéro downtime
- **Disaster Recovery** : Mise en place PRA/PCA avec site de secours distant et tests trimestriels
- **Cloud hybride** : Integration AWS/Azure avec infrastructure on-premise via VPN dedicés
- **Automatisation** : Scripts PowerShell/Bash pour déploiements, maintenance et monitoring
- **Sécurisation** : Hardening serveurs selon ANSSI, chiffrement bases de données, PKI complète
- **Performance tuning** : Optimisation serveurs SQL, Apache, Nginx avec métriques avancées
- **Compliance** : Mise en conformité RGPD, audit sécurité interne, documentation complète

SUPPORT TECHNIQUE AVANCÉ

- **Résolution incidents** : Intervention niveau 3 sur pannes critiques, MTTR < 2h
- **Formation utilisateurs** : 150+ collaborateurs formés sur outils collaboratifs et sécurité
- **Documentation technique** : Rédaction procédures, plans de continuité, guides d'intervention
- **Veille technologique** : Tests nouvelles solutions, POC technologies émergentes
- **Gestion budgets** : Chiffrage projets IT, négociation fournisseurs, optimisation coûts

RÉSULTATS QUANTIFIÉS MAJEURS :

- **99.8% uptime** maintenu sur infrastructure critique 3 ans consécutifs
- **150+ incidents résolus** niveau 3 avec satisfaction utilisateur 98%
- **30% réduction coûts** IT par optimisation ressources et négociation contrats
- **Zéro perte données** sur 3 ans grâce aux procédures backup/restore rigoureuses
- **50+ projets techniques** menés à bien dans les délais et budgets impartis

---

FORMATION & CERTIFICATIONS

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

Jedha Paris | Juin 2025 - En cours

- **Spécialisation :** Advanced Pentesting & Red Team Operations
- **Focus :** Cloud Security, Zero Trust, DevSecOps, AI Security
- **Projet final :** SOC maison avec ML-based threat detection (95% accuracy)

Analyste en Cybersécurité Certifié

OpenClassrooms Paris | Septembre 2023 - Juin 2024

- **Expertise :** Advanced penetration testing, vulnerability research, OWASP mastery
- **Projet final :** Enterprise security audit 200+ endpoints avec remediation complète
- **Spécialisation :** Incident response, digital forensics, malware analysis

Spécialisation DevSecOps Avancée

CNAM Paris | Septembre 2021 - Juin 2022

CURSUS TECHNIQUE INTENSIF

- **Architectures microservices** : Docker containerization, Kubernetes orchestration, service mesh
- **CI/CD sécurisé** : Jenkins pipelines, GitLab CI, automatisation tests sécurité (SAST/DAST)
- **Infrastructure as Code** : Terraform, Ansible, CloudFormation avec security scanning
- **Monitoring & Observability** : Prometheus, Grafana, ELK Stack, distributed tracing
- **Cloud platforms** : AWS services, Azure DevOps, GCP compute, multi-cloud strategies
- **Security automation** : OWASP ZAP integration, dependency scanning, vulnerability management
- **Database DevOps** : MySQL/PostgreSQL automation, backup strategies, performance tuning
- **Version control avancé** : Git workflows, branching strategies, code review automation

PROJETS ACADÉMIQUES MAJEURS

- **Plateforme e-commerce** : Architecture microservices complète avec 15+ services isolés
- **Pipeline CI/CD sécurisé** : Déploiement automatisé avec gates sécurité et rollback automatique
- **Infrastructure cloud** : Terraform modules réutilisables pour déploiements multi-environnements
- **Monitoring complet** : Stack observability avec alerting intelligent et dashboards métier
- **Security hardening** : Containers sécurisés, secrets management, network policies K8s

CERTIFICATIONS & COMPÉTENCES ACQUISES

- **Docker Certified Associate** niveau preparation
- **Kubernetes Administration** (CKA) concepts avancés
- **AWS Solutions Architect** foundations et security
- **Terraform Associate** infrastructure automation
- **Jenkins Certified Engineer** CI/CD expert level

EXPERTISE TECHNIQUE AVANCÉE

Sécurité Offensive & Red Team ★★★★★

- **Pentesting Frameworks :** Kali Linux, Parrot OS, BlackArch, custom toolsets
- **Exploitation Avancée :** Buffer/Heap Overflow, ROP chains, kernel exploits
- **Post-Exploitation :** Metasploit Pro, Cobalt Strike, Empire, custom C2 frameworks
- **Web Application :** Burp Suite Pro, OWASP ZAP, custom SQLmap payloads

- **Active Directory :** BloodHound, Powerview, Rubeus, Mimikatz, Golden Ticket
- **Wireless :** Aircrack-ng suite, Kismet, Wi-Fi Pineapple, rogue AP detection
- **Physical :** Lock picking, RFID cloning, HID attacks, Rubber Ducky

Threat Detection & SOC ★★★★★

- **SIEM Enterprise :** Splunk Enterprise Security, QRadar, ArcSight, LogRhythm
- **Open Source SIEM :** Wazuh, ELK Stack, OSSIM, Suricata, Zeek
- **Threat Intelligence :** MISP, OpenCTI, Yara rules, IOC development
- **Behavioral Analysis :** UBA solutions, ML-based anomaly detection
- **Incident Response :** NIST framework, playbook automation, forensics tools
- **Threat Hunting :** Sigma rules, hunting hypotheses, APT tracking
- **SOAR Platforms :** Phantom, Demisto, custom automation scripts

Infrastructure & Cloud Security ★★★★★

- **OS Hardening :** Windows Server (2016-2022), RHEL, Ubuntu LTS, CentOS
- **Virtualization :** VMware vSphere security, Hyper-V, Citrix XenServer
- **Container Security :** Docker security scanning, Kubernetes RBAC, Istio mesh
- **Cloud Platforms :** AWS Security Hub, Azure Sentinel, GCP Security Command
- **Network Security :** Fortinet NSE, Palo Alto PCNSE, Cisco security appliances
- **Identity Management :** Active Directory security, LDAP, SAML/OAuth hardening

Compliance & Risk Management ★★★★☆

- **Frameworks :** ISO 27001 Lead Auditor, NIST CSF, COBIT 5, ITIL v4
- **Regulations :** RGPD expert, PCI DSS, SOX, HIPAA, NIS2 directive
- **Risk Assessment :** EBIOS RM, ISO 27005, FAIR methodology
- **Audit Tools :** Nessus Professional, Qualys VMDR, Rapid7 InsightVM
- **GRC Platforms :** ServiceNow GRC, RSA Archer, MetricStream

---

PROJETS TECHNIQUES EXCEPTIONNELS

SOC-as-a-Service Enterprise Platform (2024)

- **Challenge :** Développement d'une plateforme SOC scalable pour PME/ETI
- **Architecture :** Microservices sécurisés, API Gateway, multi-tenant isolation
- **Technologies :** Elasticsearch cluster, Kafka streaming, Redis caching, ML models
- **Innovation :** IA prédictive pour détection d'attaques zero-day

- **Résultat : 97% de précision** détection, **15 secondes** temps de réponse moyen

Advanced Persistent Threat Simulation Lab (2024)

- **Infrastructure :** 50 VMs, réseau hybride complexe, environnements isolés
- **Scénarios :** APT29/28 simulation, supply chain attacks, insider threats
- **Techniques :** Living-off-the-land, fileless malware, memory-only persistence
- **Documentation :** 100+ techniques MITRE ATT&CK validées et optimisées
- **Impact :** Formation Red Team pour 15+ consultants seniors

Zero Trust Architecture Implementation (2023)

- **Scope :** Infrastructure multi-sites 1000+ utilisateurs, 200+ applications
- **Technologies :** Conditional access, device compliance, micro-segmentation
- **Methodology :** NIST Zero Trust framework, Google BeyondCorp principles
- **Résultat : 60% réduction** surface d'attaque, **80% amélioration** posture sécurité

Automated Threat Hunting Platform (2023)

- **Development :** Custom Python framework avec ML clustering
- **Data Sources :** 20+ feeds threat intel, logs multi-sources, honeypots
- **Automation :** SOAR integration, auto-remediation, escalation intelligente
- **Performance : 10x faster** threat detection, **90% réduction** faux positifs

---

CERTIFICATIONS & ACHIEVEMENTS

Top 10% TryHackMe - 500+ machines compromises avec write-ups techniques
HackTheBox Pro Hacker - 100+ machines pwned incluant Insane difficulty
OSCP Preparation - 80% completion rate, certification prévue Q3 2025
Bug Bounty Recognition - 5+ CVE discoveries, Hall of Fame mentions
CTF Competition Winner - 10+ événements internationaux, team leader
Security Research - 3 publications techniques, conference speaker
Expert Witness - 2 affaires judiciaires, expertise technique reconnue

---

SOFT SKILLS & LEADERSHIP

Management d'équipe : Direction de 5+ consultants juniors avec montée en compétences
Client relationship : Gestion de 50+ clients grands comptes avec satisfaction 98%
Crisis management : Leadership lors d'incidents majeurs avec prise de décision rapide
Technical writing : Rédaction de 100+ rapports exécutifs et techniques détaillés

Public speaking : Conférences ANSSI, FIC, speaker certifié sur sujets cyber
Innovation : Veille technologique quotidienne, early adopter de nouvelles techniques

---

LANGUES

Français : Langue maternelle - Rédaction technique et présentation exécutive
Anglais : Niveau C1 - Documentation technique, conférences internationales
Allemand : Niveau B1 - Communication professionnelle

CENTRES D'INTÉRÊT PROFESSIONNELS

Cybersécurité : Veille quotidienne (SANS, Krebs, Schneier), recherche en sécurité IA
Technique : Reverse engineering hardware, IoT security research, radio SDR
Communauté : Mentor bénévole 42 School, contributeur projets open source
Développement : Musculation mentale, lectures techniques approfondies
Voyage technologique : Conférences BlackHat, DefCon, participation BSides

---

DISPONIBILITÉ IMMÉDIATE

Recherche active : Poste senior cybersécurité en alternance ou CDI
Mobilité totale : Île-de-France, déplacements nationaux/internationaux
Rythme optimal : Temps plein ou alternance flexible selon besoins entreprise
Objectif de carrière : Lead cybersécurité dans équipe technique d'excellence
Salaire cible : Selon grille et responsabilités (négociable)

Prêt à transformer vos défis cybersécurité en avantages compétitifs durables.