Moussa Hassan Omar

📍 Gatineau, QC | ✉️ moussa-hassan12@hotmail.com | ☎️ 418-327-1522 | 🌐 GitHub : github.com/lorabijouti03

Profil professionnel

Je suis un analyste en cybersécurité orienté SOC, fort de plus de huit années d'expérience en technologies de l'information, dont plusieurs mandats au sein de la fonction publique québécoise. Mon expertise couvre la surveillance de la sécurité, la détection des menaces, la gestion des vulnérabilités et la réponse aux incidents.

Habitué à travailler dans des environnements complexes (Windows, Active Directory, Microsoft 365), j'utilise régulièrement des outils SIEM et EDR pour identifier, contenir et documenter les menaces. Méthodique, rigoureux et orienté amélioration continue, je vise à contribuer activement à la protection des actifs informationnels et à la détection proactive des cybermenaces.

Compétences clés

Surveillance et détection

- Surveillance continue via SIEM (Splunk, Microsoft Sentinel, QRadar)
- Corrélation d'événements et analyse de logs de sécurité
- Détection de comportements suspects : brute force, phishing, exfiltration
- Utilisation d'outils EDR : Defender for Endpoint, CrowdStrike Falcon, Carbon Black

Réponse aux incidents

- Investigation et confinement d'incidents (malwares, phishing, accès non autorisés)
- Vérification des IOC via VirusTotal, Any.Run et Hybrid Analysis
- Escalade et documentation technique pour les équipes CSIRT
- Rédaction de rapports et mise à jour des procédures internes

Sécurité des systèmes et réseaux

- Gestion des vulnérabilités (Nessus, OpenVAS, Qualys)
- Analyse du trafic réseau (Wireshark, Zeek, Suricata)
- Sécurisation d'environnements Active Directory, M365, Intune
- Application de correctifs et durcissement des systèmes

Outils et plateformes

- **SIEM :** Microsoft Sentinel, Splunk, QRadar
- **EDR :** Defender for Endpoint, CrowdStrike Falcon, Carbon Black
- **Analyse :** Wireshark, Autopsy, FTK Imager, OSINT Framework
- **Gestion de tickets :** EasyVista, Octopus, Jira, ServiceNow
- **Réseaux :** Cisco Packet Tracer, pfSense, Nmap
- **Autres :** Intune, SCCM, Entra ID, Azure AD, PowerShell

Projets pratiques en cybersécurité

- **Tests d'intrusion et post-exploitation (CR470)** : Réalisation d'un pentest complet (scan, énumération, exploitation, analyse LSASS) avec *CrackMapExec*, *Responder*, *John the Ripper* et *Hashcat*.
- **Infrastructure C2 et persistance** : Mise en place et interaction d'agents via *Sliver* et *Havoc* pour simuler des scénarios de commande et contrôle.
- **Projet Purple Teaming** : Collaboration offensive/défensive avec *Sysmon*, *Atomic Red Team* et *Kibana* pour la détection d'activités malveillantes.
- **Laboratoire SIEM (ELK Stack)** : Corrélation de journaux Windows et Sysmon, détection d'incidents et création de tableaux de bord.
- **Sécurisation WLAN et ACL Cisco** : Implémentation d'authentification WPA2-Enterprise et de politiques d'accès réseau.
- **Fusion d'arbres d'attaque (Python)** : Développement d'un outil de visualisation de scénarios d'attaque avec logiques AND/OR.
- **Sécurité Cloud AWS & Azure** : Configuration d'IAM, gestion des accès et renforcement de la sécurité des ressources virtuelles.
- **Projet Active Directory (Windows Server 2019)** : Gestion des GPO, des partages sécurisés et des protocoles d'authentification.
- **Automatisation (PowerShell/Python)** : Création de scripts de durcissement et de collecte automatisée de logs.
- **Développement web sécurisé (DjiCan Solutions)** : Conception d'un site multilingue (FR/EN/AR/SO) codé manuellement avec HTTPS et SEO optimisé.

Expérience professionnelle

Analyste SOC / Technicien en sécurité opérationnelle – MTMD (Ministère des Transports et de la Mobilité durable, via CGI)

Québec, QC | 2022 – Avril 2025

- Surveillance des systèmes via *Microsoft Sentinel* et *Defender for Endpoint*
- Corrélation d'événements de sécurité et détection de comportements anormaux
- Réponse aux alertes, containment et escalade vers les équipes CSIRT
- Rédaction de rapports d'incidents et documentation technique
- Support technique de niveau 2 lié aux incidents de sécurité

Technicien en sécurité et soutien informatique – MSSS (Ministère de la Santé et des Services sociaux)

Québec, QC | 2021 – 2022

- Gestion des identités et accès (Active Directory, Azure AD)
- Surveillance des antivirus, correctifs et mises à jour de sécurité

- Détection d’activités suspectes sur postes utilisateurs
- Contribution aux campagnes de sensibilisation à la cybersécurité

Technicien en sécurité des systèmes – CSPQ (Centre de services partagés du Québec)
Québec, QC | 2019 – 2021

- Application des politiques de sécurité gouvernementales
- Analyse et suivi des vulnérabilités détectées
- Participation au plan de continuité et de réponse aux incidents
- Gestion sécurisée du matériel et interventions sur site

Conseiller technique – Bell Canada
Québec, QC | 2018 – 2023

- Support technique réseau (connexion, DNS, routeurs)
- Détection d’incidents liés aux comptes clients
- Sensibilisation des usagers à la cybersécurité résidentielle

---

Formation académique

- Baccalauréat ès Sciences (B.Sc.) en cybersécurité – Polytechnique Montréal *(en cours – 2026)*
- DEC – Analyste en cybersécurité – Willis College, Ottawa (2025)
- Certificat en Analyse et cybersécurité opérationnelle – Polytechnique Montréal (2025)
- Microprogramme en réseaux et sécurité – Polytechnique Montréal (2023)
- DEP en soutien informatique – Québec (2016)

Langues

- Français : courant
- Anglais : professionnel

Loisirs et intérêts

- Veille technologique en cybersécurité, analyse de malwares, participation à des CTF
- Pratique régulière du soccer

Références

Disponibles sur demande