Maël Dorville

Analyste SOC junior - Cybersécurité

Schœlcher | Martinique | 0696 00 00 00 | mael.dorville@example.com | https://mael-dorville.dev

Diplômé d'un BUT Informatique réalisé en partie en alternance, je souhaite rejoindre une équipe SOC ou sécurité opérationnelle. Je sais qualifier une alerte, documenter une investigation, automatiser les contrôles simples et maintenir un laboratoire reproductible.

PREUVES CLÉS

- 35 investigations documentées
- 9 runbooks opérationnels
- 14 règles de détection testées
- 6 machines virtuelles reproductibles
- 2 exercices de phishing accompagnés

EXPÉRIENCES

Alternant analyste sécurité - Antilles SecOps - Fort-de-France

2025-09 | 2026-08 | 12 mois

Appui à une petite équipe sécurité assurant supervision, qualification et accompagnement de clients locaux.

ENVIRONNEMENT

Wazuh | Microsoft 365 | Linux | Python | GLPI | MITRE ATT&CK

Qualification et documentation d'alertes

12 mois | Triage, investigation, escalade, reporting

Analyse de premier niveau sous supervision et amélioration progressive de la base documentaire.

DÉMARCHE

- Reproduction des alertes en laboratoire
- Création d'une grille de qualification
- Cartographie MITRE des cas fréquents

RÉSULTATS ET PREUVES

- 35 investigations documentées
- 9 runbooks relus par l'équipe
- Script Python de normalisation des exports
- Support à deux exercices de phishing

Concepteur du laboratoire - Mini-SOC - homelab personnel

2025-01 | 2025-09 | 9 mois

Laboratoire isolé destiné à comprendre la chaîne complète de collecte, détection et investigation.

ENVIRONNEMENT

Proxmox | Wazuh | Suricata | Zeek | Ubuntu | Windows 11 | Docker

Chaîne de détection reproductible

9 mois | SIEM, IDS, logs, règles

Collecte de journaux Windows et Linux puis création de scénarios de détection contrôlés.

DÉMARCHE

- Architecture réseau isolée
- Jeux de logs et scénarios
- Critères de validation des alertes

RÉSULTATS ET PREUVES

- 6 machines virtuelles documentées
- 14 règles de détection testées
- Tableau de bord d'investigation
- Guide de reconstruction du lab

COMPÉTENCES

- Python, Bash, PowerShell, SQL
- MITRE ATT&CK, analyse de risque, gestion d'incident, veille, rédaction de runbooks
- Elasticsearch, SQLite
- Linux, Windows Server, Active Directory, Wazuh, Suricata, Zeek, Docker, GitHub Actions

DOMAINES D'INTERVENTION

- Qualification d'alertes
- Analyse de journaux
- Durcissement Linux
- Vulnérabilités
- Documentation et sensibilisation

FORMATION

BUT Informatique - Réalisation d'applications : conception, développement, validation | IUT de la Martinique - Université des Antilles, campus de Schœlcher | 2023-2026

LANGUES

Français: Maternel | Créole martiniquais: Courant | Anglais: Technique B2