Abdel Kader Camara

Analyste SOC/CERT – Expert Cybersécurité

Contact

06 45 27 90 15
abdelkads2000@gmail.com
LinkedIn
kadercamara.com
Lyon, France

Compétences

- ✓ **SIEM :** Chronicle, Sentinel, ELK Stack
- ✓ **EDR/XDR :** SEKOIA.IO, HarfangLab
- ✓ **Cloud :** Azure, AWS, GCP
- ✓ **Infrastructure :** VMware, Proxmox, Docker
- ✓ **Réseaux :** Cisco, Fortinet, pfSense
- ✓ **Systèmes :** Linux, Windows Server
- ✓ **Dev :** Python, Bash, HTML/CSS, JS
- ✓ **Bases :** MySQL, MongoDB, Elasticsearch
- ✓ **Cybersécurité :** MITRE ATT&CK, threat hunting, forensic

Langues

- ✓ Français
- ✓ Anglais

Qualités

- ✓ Esprit d'équipe
- ✓ Autonomie & rigueur
- ✓ Veille technologique
- ✓ Adaptabilité

Loisirs

- ✓ Football
- ✓ Arts martiaux
- ✓ Mangas
- ✓ Gaming
- ✓ Musique

Profil

Ingénieur cybersécurité avec une expertise complète dans la supervision SOC, l'analyse d'incidents, la threat intelligence et la gestion de la vulnérabilité. J'interviens aussi bien en environnement on-premises que cloud, avec une approche proactive de la sécurité.

Expériences Professionnelles

- **Analyste SOC/CERT – Almond – 2023 à aujourd'hui**

✓ Analyse continue des alertes de sécurité via SIEM Chronicle et Microsoft Sentinel pour identifier les incidents critiques.
✓ Création, ajustement et optimisation des règles de détection MITRE ATT&CK afin de réduire les faux positifs et améliorer la pertinence.
✓ Gestion des vulnérabilités : identification, priorisation, recommandations et suivi de remédiation avec Hackuity.
✓ Veille sécuritaire proactive (CTI) pour suivre les menaces émergentes et mettre à jour les stratégies de détection en temps réel.
✓ Participation active aux réunions post-incident et rédaction de procédures standardisées pour renforcer l'efficacité de la réponse aux incidents.
✓ Collaboration interdisciplinaire avec les équipes réseau, système et développement pour une gestion globale des incidents.

- **Apprenti Ingénieur Cybersécurité – Dstny – 2020 à 2023**

✓ Déploiement de SIEM (ELK, OpenDistro) : collecte de logs (serveurs, pare-feu, endpoints), corrélation des événements et surveillance 24/7.
✓ Implémentation et tuning d'outils EDR/XDR (SEKOIA.IO, HarfangLab) pour la détection de comportements suspects et la traque proactive.
✓ Création de scénarios de détection réalistes en s'appuyant sur la matrice MITRE ATT&CK et les dernières cybermenaces identifiées.
✓ Analyse des journaux systèmes et réseaux pour la recherche d'IOCs et investigation approfondie en cas de compromission.
✓ Support technique de niveau 1 à 3 : résolution d'incidents réseau/système, accompagnement utilisateurs et documentation complète.
✓ Automatisation de tâches avec scripts Bash/Python pour améliorer la réactivité des équipes et fluidifier les opérations SOC.

Formation

Diplôme d'ingénieur – Informatique & Réseaux – CPE Lyon (2020–2023)

BUT Réseaux & Télécom – IUT de Roanne (2018–2020)

Certifications

- ✓ SEKOIA.IO C302 – Plateform Integrator
- ✓ Chronicle SIEM Fundamentals
- ✓ Splunk Fundamentals
- ✓ Microsoft Sentinel Fundamentals
- ✓ Fortinet NSE 3
- ✓ Wallix – Bastion PAM
- ✓ ANSSI – SecNumacadémie