CONTACT

Téléphone
06 45 27 90 15

Email
abdel-kader.camara@proton.me

LinkedIn
linkedin.com/in/abdel-kader-camara-network-cybersecurity/

Site web
kadercamara.com

Localisation
Lyon, France

COMPÉTENCES

- SIEM : Chronicle, Sentinel, ELK Stack
- EDR/XDR : SEKOIA.IO, HarfangLab, SentinelOne, Microsoft Defender
- Cloud : Azure, AWS, GCP
- Infrastructure : VMware, Proxmox, Docker
- Réseaux : Cisco, Fortinet, pfSense
- Systèmes : Linux, Windows Server
- Développement : Python, Bash, HTML/CSS, JS
- Bases de données : MySQL, PostgreSQL, Elasticsearch
- Cybersécurité : MITRE ATT&CK, threat hunting, forensic, OSINT
- IA & assistants : Qevlar AI, Dust
- SOAR : Chronicle SOAR, Torq

CONTACT

- Français
- Anglais

QUALITÉS

- Esprit d'équipe
- Autonomie & rigueur
- Veille technologique
- Adaptabilité
- Gestion du stress et du temps

LOISIRS

- Arts martiaux
- Mangas
- Gaming
- Musique

ABDEL KADER CAMARA

ANALYSTE SOC – EXPERT CYBERSÉCURITÉ

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

- Analyse continue des alertes de sécurité via un SOAR 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.
- Participation au déploiement de l'outil Qevlar AI (assistant d'analyste N1) pour accélérer l'analyse des alertes et le triage des incidents.
- Création et maintenance de workflows d'automatisation sur les plateformes SOAR (Chronicle SOAR, Torq) afin d'industrialiser la réponse aux incidents.
- Déploiement et configuration de la solution SEKOIA.IO pour plusieurs clients (collecte de logs, règles de détection, playbooks, intégration SIEM/EDR).
- Participation à des présentations commerciales de SEKOIA.IO et des offres SOC auprès de prospects et de clients.
- Onboarding de nouveaux analystes SOC : présentation des procédures, des outils (SIEM, EDR, SOAR) et des bonnes pratiques de détection et d'investigation.

Apprenti Ingénieur Cybersécurité
Dstny

- 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.

FORMATIONS

- Diplôme d'ingénieur – Informatique & Réseaux – CPE Lyon (2020–2023)
- BUT Réseaux & Télécom – IUT de Roanne (2018–2020)

CERTIFICATIONS

SEKOIA.IO 302 - Integrator | **Chronicle Fundamentals** | **Splunk Fundamentals** | **Microsoft Sentinel Fundamentals** | **Fortinet NSE 3** | **Wallix PAM** | **ANSSI – SecNumacadémie**