Mandengue NJIME

Ingénieur en transformation digitale industrielle et cybersécurité

mnjime_vie@proton.me
+33 6 15 16 67 03
Mobilité internationale
linkedin.com/in/mandengue
Paris, Île-de-France
belatedi.com

Profil

Ingénieur en transformation digitale industrielle et cybersécurité, avec 4 ans d'expérience dans les environnements industriels et informatiques. Compétences en architectures IT/OT, plateformes de données industrielles, systèmes event-driven, infrastructures cloud AWS et cybersécurité. Intérêt particulier pour l'IA industrielle, l'interopérabilité des systèmes et la convergence IT/OT.

Expérience professionnelle

Ingénieur industry 4.0 & cybersécurité – We Network 09/2023 – 06/2026 · Angers, France

- Conçu des architectures IT/OT évolutives et déployé un Unified Namespace (UNS) basé sur MQTT, intégrant MES, ERP, équipements IoT, AMR et cobots.
- Développé des pipelines de données industrielles et des plateformes historisées avec Telegraf et InfluxDB pour la supervision temps réel, la gouvernance des données et l'analyse des anomalies.
- Appliqué les principes de défense en profondeur aux infrastructures IT/OT, renforcé les environnements conteneurisés et contribué aux audits, analyses de risques et réponses aux incidents, en référence à ISO 27001, NIS2 et IEC 62443.

Développeur full-stack et analyste en sécurité applicative – ITGStore SAS 06/2024 – 09/2024 · Douala, Cameroun

- Intégré un scanner biométrique à une interface web pour la captation, le traitement et la transmission sécurisée des données.
- Conçu un système centralisé d'enrôlement avec deux interfaces dédiées aux opérateurs des agences gouvernementales et aux administrateurs du ministère.
- Réalisé des évaluations de sécurité applicative selon l'OWASP Top 10, identifié des vulnérabilités et formulé des recommandations correctives.

Technicien infrastructures IT et sécurité – Speedy France 09/2022 – 09/2023 · Paris, France

- Analysé les problématiques techniques et organisationnelles, identifié les causes racines et formulé des recommandations d'amélioration priorisées.
- Contribué aux audits de sécurité et aux projets d'infrastructure : serveurs, VPN, sécurisation des systèmes et automatisation des procédures opérationnelles.
- Administré et configuré les postes de travail, serveurs et services d'infrastructure pour assurer leur disponibilité et leur maintien en condition opérationnelle.

Projets marquants

Écosystème IIoT et connectivité industrielle – LowPlant 2026

- Conçu une architecture de connectivité industrielle intégrant automates PLC, Kepware (OPC UA), brokers MQTT, Unified Namespace et ThingWorx pour la collecte de données machines, la supervision temps réel et le suivi des indicateurs TRS/OEE.

Unified Namespace industriel – We Network 2023 – 2026

- Structuré un modèle de données industriel avec une architecture MQTT et un référentiel UNS gouverné par YAML dans Git, facilitant l'organisation des flux IoT et leur exploitation par les applications métier.

Formation

Diplôme d'ingénieur CTI – Cybersécurité & IoE · ESAIP · 2023 – 2026
Niveau Master · Alternance · Dernier semestre : 17,45/20
BTS SIO (Services Informatiques aux Organisations) – option SISR · Efrei Paris · 2021 – 2023
Systèmes, Réseaux & Infrastructures · 18,5/20

Certifications

ISA/IEC 62443 Cybersecurity Fundamentals Specialist · ISA · En cours
ISA-95 / IEC 62264 Enterprise-Control System Integration · ISA · En cours
CEH – Certified Ethical Hacker · EC-Council · 2026 · Obtenue

Compétences techniques essentielles

Systèmes industriels et OT/IoT : Unified Namespace, MQTT, OPC UA, ISA-95, Kepware, ThingWorx, Ignition, MES/ERP.
Données industrielles et IA : Telegraf, InfluxDB, Node-RED, Grafana, RAG, vLLM, LangGraph.
Infrastructure, DevOps et Cloud : Linux, Docker, Kubernetes, Terraform, Ansible, GitLab CI, AWS, Azure.
Cybersécurité et gestion des risques : Sécurité IT/OT, IEC 62443, ISO 27001, NIS2, OWASP.
Développement logiciel : Python, C++, TypeScript, React, Next.js, Node.js, SQL.

Langues

Français Langue maternelle · **Anglais** C1 · TOEIC 945