CONTACT

paul.levrard@axionis-cyber.com

+32 492 02 80 08

linkedin.com/in/paul-levrard

axionis-cyber.com

Liège, Belgique

CERTIFICATION

ISA/IEC 62443 Cybersecurity Fundamentals Specialist
ISA · 2026

COMPÉTENCES OT

- IEC 62443 : zones et conduits, niveaux de sécurité (SL-T / SL-C)
- Analyse de risques OT, EBIOS RM, ISO 27005
- Segmentation réseau et DMZ OT/IT
- Active Directory OT multi-sites
- Inventaire et cartographie des actifs OT
- NIS2 · CyberFundamentals (CyFun)
- FAT / SAT avec fournisseurs et intégrateurs
- ISO 27001 · NIST SP 800-53

ENVIRONNEMENTS

Cisco ISA3000 (FTD) · Check Point
VLAN · DMZ · pare-feu industriels
Windows Server · VMware ESXi
SCADA · automates · réseaux industriels
Visio · draw.io

FORMATION

Ingénieur informatique et réseaux, spécialité cybersécurité
ESAIP · 2017 – 2022

Erasmus
Universidad de Castilla-La Mancha · 2021 – 2022

Formation Cisco CCNA
Formation suivie

LANGUES

Français — langue maternelle
Anglais — professionnel

AXIONIS CYBER

PAUL LEVRARD

Consultant en cybersécurité industrielle (OT) · IEC 62443

Fondateur d'Axionis Cyber · Belgique et Luxembourg · Disponible en freelance

PROFIL

Ingénieur en cybersécurité, 4 ans d'expérience dont 2 ans en environnement industriel : réseaux de production d'un énergéticien, puis infrastructures publiques critiques. J'aide les exploitants à sécuriser leurs systèmes de contrôle-commande selon l'IEC 62443 : inventaire, analyse de risques, segmentation, procédures et feuille de route. Des livrables concrets et des recommandations indépendantes.

EXPÉRIENCE

Fondateur, consultant cybersécurité OT

avr. 2026 – aujourd'hui

Axionis Cyber · Liège

Mission en cours (depuis mai 2026) : opérateur public d'infrastructures critiques en Wallonie.

- Inventaire des actifs OT et cartographie des réseaux industriels sur **plusieurs dizaines de sites**
- Revue des architectures et de la segmentation OT/IT, documentation du parc applicatif OT
- Analyse **IEC 62443** (zones et conduits, niveaux de sécurité cibles) et recommandations de sécurisation
- Cadrage de la mise en conformité **NIS2 / CyberFundamentals** et feuille de route de remédiation

Cybersecurity Officer & Industrial Network Expert

oct. 2024 – oct. 2026

Luminus · Liège

Équipe Cybersécurité, réseaux industriels et données : 6 centrales hydrauliques, ~130 sites éoliens, 6 centrales thermiques.

- Analyses de risques **IEC 62443** par zone et conduit : registre des risques, SL cibles, plan de traitement
- Conception, déploiement et administration d'un **Active Directory OT** multi-sites
- Architectures **DMZ OT/IT** et segmentation réseau (Cisco ISA3000, Check Point)
- Évaluations de maturité **CyberFundamentals** (niveau Essentiel) sur le parc éolien (~130 sites)
- Projets BESS et NCCGT : spécifications sécurité, **2 FAT** (Madrid) et **2 SAT** sur site
- Procédures d'accès OT et politiques d'exploitation, documentation réseau de bout en bout

Consultant en cybersécurité

2022 – 2024

HeadMind Partners · Bruxelles, Luxembourg, Paris

- **IAM** pour un groupe du luxe : processus et workflows ServiceNow, ~150 user stories, **150 000 comptes**
- Stratégie **DLP** et analyse de risques **EBIOS RM** pour un groupe pharmaceutique (21 scénarios)
- Évaluation **NIST SP 800-53** pour une banque : **360 contrôles** sur 5 périmètres, plan de remédiation
- Mise en place d'un **SMSI ISO 27001:2022** et traitement d'un rapport de pentest (Luxembourg)
- Sensibilisation : campagnes de phishing (**870 utilisateurs**), 40 sessions d'escape game (200 personnes)

SECTEURS

Énergie (hydraulique, éolien, thermique, stockage par batteries) · Infrastructures publiques critiques · Pharmaceutique · Banque · Luxe

Auparavant : stage en cybersécurité chez SIRI49 (2021), campagnes de phishing et sensibilisation pour des mairies.