PAUL LEVRARD

Consultant en cybersécurité industrielle (OT) · IEC 62443

Fondateur d'Axionis Cyber · Belgique et Luxembourg

PORTFOLIO

paul.levrard@axionis-cyber.com · +32 492 02 80 08 · linkedin.com/in/paul-levrard · axionis-cyber.com · Liège, Belgique

PROFIL

Ingénieur en cybersécurité (diplôme d'ingénieur ESAIP en informatique, spécialité réseaux et sécurité, 2022), 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 des actifs OT, analyse de risques par zones et conduits, segmentation OT/IT, Active Directory industriel, procédures et feuilles de route de remédiation. Mes missions de conseil précédentes portaient sur l'IAM, la protection des données (DLP), le NIST SP 800-53, l'ISO 27001 et la sensibilisation.

Des livrables concrets et des recommandations indépendantes.

COMPÉTENCES

SÉCURITÉ OT

- IEC 62443 : zones, conduits, niveaux de sécurité
- Analyse de risques OT et plans de traitement
- DMZ OT/IT et segmentation réseau
- Active Directory OT multi-sites
- Inventaire et cartographie des actifs OT
- FAT / SAT avec fournisseurs et intégrateurs
- NIS2 · CyberFundamentals (CyFun)

GOUVERNANCE ET SÉCURITÉ IT

- ISO/IEC 27001 – 27005
- NIST CSF · NIST SP 800-53
- EBIOS RM · CIS
- IAM : AD / Entra ID, PAM, cycle de vie des accès
- Stratégie DLP (Microsoft Purview)
- Phishing et programmes de sensibilisation
- Méthodes agiles (Scrum, Kanban)

OUTILS ET TECHNOLOGIES

- Cisco ISA3000 (FTD) · Check Point
- VLAN · DMZ · pare-feu industriels
- Windows Server · VMware ESXi
- Active Directory · Entra ID
- M365 · Purview · Sentinel · Defender for Cloud Apps
- ServiceNow · Power BI · PowerShell
- Visio · draw.io · Kali Linux · Wireshark

Certification	ISA/IEC 62443 Cybersecurity Fundamentals Specialist (ISA, 2026)
Formation	Diplôme d'ingénieur en informatique, spécialité réseaux et sécurité – ESAIP (2017 – 2022) · Erasmus, Universidad de Castilla-La Mancha (2021 – 2022) · Formation Cisco CCNA
Langues	Français : langue maternelle · Anglais : professionnel
Secteurs	Énergie · Infrastructures publiques critiques · Pharmaceutique · Banque · Luxe · Construction

CYBERSÉCURITÉ INDUSTRIELLE (OT)

Opérateur public d'infrastructures critiques
Belgique

Ingénieur cybersécurité OT — mai 2026 – aujourd'hui

Dans le cadre de ses obligations NIS2, un opérateur public d'infrastructures critiques avait besoin d'un expert en cybersécurité OT pour sécuriser les technologies opérationnelles de ses installations. J'interviens, via Axionis Cyber, pour visiter les sites, analyser la documentation technique existante et formuler des recommandations.

Missions

- Réaliser les évaluations sur site (relevés de terrain, revue de la documentation technique existante)
- Construire l'inventaire des actifs OT et cartographier les systèmes et réseaux industriels
- Analyser l'architecture et la segmentation du réseau OT (frontières OT/IT, DMZ, cloisonnement)
- Rédiger et proposer des procédures de sécurité OT et des consignes d'exploitation
- Formuler les recommandations de sécurité et contribuer à la feuille de route de remédiation

Réalisations

- ✓ Inventaire des actifs OT et cartographie réseau en cours sur plusieurs dizaines de sites
- ✓ Documentation du parc applicatif OT (supervision, vidéo, communications d'urgence)
- ✓ Premiers constats de sécurité alimentant l'analyse IEC 62443 et la feuille de route NIS2 / CyberFundamentals

Environnement

Référentiels : IEC 62443 (zones et conduits, niveaux de sécurité cibles), NIS2, CyberFundamentals · Réseau : VLAN, DMZ, segmentation OT/IT · Documentation : Microsoft Visio, draw.io

Luminus (énergie)
Belgique

Cybersecurity Officer & Industrial Network Expert — 2 ans

Au sein de l'équipe Cybersécurité, réseaux industriels et données, chargée de sécuriser et d'exploiter les réseaux OT de production de 6 centrales hydrauliques, d'environ 130 sites éoliens et de 6 centrales thermiques.

Missions

- Définir et revoir des architectures de réseaux industriels alignées sur l'IEC 62443 (zones et conduits, contrôle d'accès, DMZ)
- Réaliser des analyses de risques IEC 62443 par zones et conduits (périmètre des actifs, criticité, SL-T / SL-C, plan de traitement)
- Rédiger et maintenir les procédures d'accès OT et les politiques d'exploitation
- Concevoir, déployer et administrer un Active Directory OT et les services système associés sur les sites industriels
- Coordonner des projets (BESS, NCCGT) du cadrage et des spécifications jusqu'à la livraison
- Produire et maintenir la documentation réseau de bout en bout
- Mener les FAT/SAT avec les fournisseurs et intégrateurs (2 FAT à Madrid, 2 SAT sur site)
- Évaluer la maturité cybersécurité du parc éolien par rapport au niveau Essentiel de CyberFundamentals

Réalisations

- ✓ Livraison d'un registre des risques IEC 62443 et d'un plan de traitement par zone et conduit, avec niveaux de sécurité cibles et écarts par rapport à l'existant
- ✓ Mise en place de modèles de DMZ et d'une segmentation réseau pour durcir les frontières OT/IT
- ✓ Rédaction et déploiement des procédures d'accès OT et des politiques associées
- ✓ FAT/SAT des programmes BESS et NCCGT réalisés, conceptions validées au regard des exigences de sécurité
- ✓ Évaluations de maturité CyberFundamentals sur environ 130 sites éoliens et priorisation des actions de remédiation
- ✓ Standardisation des schémas et de la documentation réseau pour des revues techniques homogènes

Environnement

Référentiels : IEC 62443, CyberFundamentals (Essentiel), méthodes agiles · Identité et systèmes : Active Directory, VMware ESXi · Réseau et sécurité : Cisco ISA3000 (FTD), Check Point 1570R, VLAN, DMZ · Documentation : Microsoft Visio, draw.io

GESTION DES IDENTITÉS ET DES ACCÈS

Groupe du luxe
France

Analyste IAM — 9 mois

Au sein de l'équipe IT globale du groupe, déploiement et maintenance évolutive d'un outil unique de gestion des identités.

Missions

- Rédiger les spécifications sous forme de user stories pour les évolutions et corrections des outils de gestion des identités
- Modéliser les processus de gestion des accès (arrivées, départs, mobilités, demandes de modification)
- Gérer les mises en production : tests et communication par notes de version
- Surveiller la qualité des données d'identités et de droits pour les comptes utilisateurs, à privilèges et techniques
- Support de niveau 3

Réalisations

- ✓ Environ 150 user stories livrées (évolutions, corrections, conception)
- ✓ Workflows de gestion des accès créés dans ServiceNow
- ✓ Documentation de tous les processus IAM (arrivées, départs, mobilités, demandes de modification)
- ✓ Ateliers pour définir et formaliser le cycle de vie des accès
- ✓ Suivi de la qualité des identités et des accès de plus de 150 000 comptes avec PowerShell et Power BI

Environnement

Entra ID (Azure AD), Active Directory · ServiceNow · PowerShell, Power BI · Méthodes agiles

PROTECTION DES DONNÉES

Groupe pharmaceutique
Belgique

Analyste DLP — 5 mois

Définition d'une stratégie et d'une feuille de route globales de prévention des fuites de données (DLP), avec le responsable de la sécurité de l'information.

Missions

- Évaluer les risques de fuite de données et réaliser l'analyse d'écarts
- Définir la stratégie DLP
- Construire la feuille de route du projet DLP

Réalisations

- ✓ 8 ateliers métiers pour identifier les données sensibles et les scénarios de risque
- ✓ 5 ateliers IT pour évaluer les mesures existantes de prévention des fuites
- ✓ Analyse et évaluation des risques selon la méthode EBIOS RM
- ✓ Rapport d'analyse de risques avec 21 scénarios et les vulnérabilités associées
- ✓ Définition des processus, outils et compétences nécessaires pour réduire ces risques
- ✓ Feuille de route pour mettre en œuvre les processus DLP et déployer Microsoft Purview, Sentinel et Defender for Cloud Apps

Environnement

M365, Microsoft Purview, Sentinel, Defender for Cloud Apps · EBIOS RM, NIST

GOUVERNANCE, RISQUES ET CONFORMITÉ

Banque
Luxembourg

Analyste NIST — 3 mois

Recherche et analyse des preuves de conformité au référentiel NIST SP 800-53, avec le RSSI.

Missions

- Lister et prioriser les contrôles et les preuves nécessaires pour le NIST SP 800-53
- Préparer et animer des ateliers avec les parties prenantes
- Collecter, analyser et archiver les preuves
- Rédiger le plan de remédiation

Réalisations

- ✓ Priorisation de 360 contrôles sur 5 périmètres
- ✓ Animation de 5 ateliers (un par périmètre)
- ✓ Évaluation des 360 contrôles et définition de leur remédiation

Environnement

NIST SP 800-53

Entreprise de services d'impression
Luxembourg

Expert cybersécurité — 4 mois

Rôle d'expert cybersécurité pour mettre en place un SMSI, réduire les risques relevés par un test d'intrusion et sensibiliser le personnel.

Missions

- Mettre en œuvre un SMSI selon l'ISO 27001:2022
- Identifier et traiter les risques relevés par un rapport de test d'intrusion
- Accompagner l'analyse d'impact sur l'activité (BIA) et le plan de continuité d'activité (PCA)
- Créer des sessions de sensibilisation à la cybersécurité

Réalisations

- ✓ 50 points de contrôle sur 93 résolus pour la mise en place du SMSI
- ✓ 50 risques identifiés dans le rapport de pentest, dont 30 traités
- ✓ 8 sessions de sensibilisation créées sur les risques cyber et les bonnes pratiques
- ✓ Accompagnement du BIA et du PCA avec les différents métiers

Environnement

ISO 27001:2022 · Brainframe

SENSIBILISATION

Secteur public et construction
France et Belgique

Campagnes de phishing et sensibilisation — 4 mois

Pour deux clients, le service informatique des mairies du Maine-et-Loire et une entreprise de construction : simulations de phishing, campagnes de prévention et rapports pour les maires et les équipes IT.

Missions

- Installer, configurer et exploiter la plateforme Gophish
- Créer des e-mails de phishing simulés et configurer un serveur SMTP
- Concevoir et présenter une campagne de prévention pour les agents des mairies
- Collecter les données des campagnes et rédiger le rapport

Réalisations

- ✓ Campagnes de phishing pour 4 communes (520 utilisateurs)
- ✓ Campagnes de phishing pour l'entreprise de construction (350 utilisateurs)
- ✓ 10 sessions de sensibilisation pour les agents des mairies
- ✓ Analyse et restitution des résultats ; documentation de l'outil pour les campagnes suivantes

Environnement

Gophish, Linux · HTML / CSS

Entreprise du secteur de l'énergie
Belgique

Sensibilisation – escape game — 2 mois

Campagne de sensibilisation sous forme d'escape game, à la demande du client. J'étais chargé de la préparation technique des sessions.

Missions

- Installer et configurer les machines virtuelles de l'escape game
- Mettre en place et documenter un outil de fausse page de connexion
- Concevoir des ateliers où les participants se mettent dans la peau d'un attaquant
- Créer un quiz de sensibilisation à la cybersécurité

Réalisations

- ✓ 40 sessions animées pour 200 collaborateurs

Environnement

Kali Linux · Pyphisher, John the Ripper · Slido