PAUL LEVRARD

Industrial (OT) Cybersecurity Consultant · IEC 62443

Founder of Axionis Cyber · Belgium and Luxembourg

PORTFOLIO

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

PROFILE

Cybersecurity engineer (ESAIP engineering degree in IT, specialisation in networking and security, 2022) with 4 years of experience, including 2 years in industrial environments: the production networks of an energy company, then critical public infrastructure.

I help operators secure their control systems in line with IEC 62443: OT asset inventory, zones-and-conduits risk analysis, OT/IT segmentation, industrial Active Directory, procedures and remediation roadmaps. Earlier consulting work covered IAM, data protection (DLP), NIST SP 800-53, ISO 27001 and security awareness.

Practical deliverables and independent recommendations.

SKILLS

OT SECURITY

- IEC 62443: zones, conduits, security levels
- OT risk analysis and treatment plans
- OT/IT DMZ and network segmentation
- Multi-site OT Active Directory
- OT asset inventory and mapping
- FAT / SAT with vendors and integrators
- NIS2 · CyberFundamentals (CyFun)

GOVERNANCE AND IT SECURITY

- ISO/IEC 27001 – 27005
- NIST CSF · NIST SP 800-53
- EBIOS RM · CIS
- IAM: AD / Entra ID, PAM, access lifecycle
- DLP strategy (Microsoft Purview)
- Phishing and awareness programmes
- Agile delivery (Scrum, Kanban)

TOOLS AND TECHNOLOGIES

- Cisco ISA3000 (FTD) · Check Point
- VLAN · DMZ · industrial firewalls
- 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)
Education	Engineering degree in IT, specialisation in networking and security – ESAIP (2017 – 2022) · Erasmus, Universidad de Castilla-La Mancha (2021 – 2022) · Cisco CCNA training
Languages	French: native · English: professional working proficiency
Sectors	Energy · Critical public infrastructure · Pharmaceuticals · Banking · Luxury · Construction

INDUSTRIAL (OT) CYBERSECURITY

Critical public infrastructure operator
Belgium

OT Cybersecurity Engineer — May 2026 – present

In the context of its NIS2 obligations, a public operator of critical infrastructure needed an OT cybersecurity expert to secure the operational technology behind its assets. I was brought in, through Axionis Cyber, to survey the sites, review the existing technical documentation and deliver recommendations.

Assignment summary

- Carry out on-site assessments across the infrastructure sites (field surveys, review of existing technical documentation)
- Build the OT asset inventory and map the industrial systems and networks
- Review the OT network architecture and segmentation (OT/IT boundaries, DMZ, network segregation)
- Draft and propose OT security procedures and operating guidelines
- Formulate security recommendations and contribute to the remediation roadmap

Achievements

- ✓ OT asset inventory and network mapping under way across several dozen sites
- ✓ Documentation of the OT application landscape (supervision, video, emergency communications)
- ✓ First security observations feeding the IEC 62443 analysis and the NIS2 / CyberFundamentals roadmap

Environment

Frameworks: IEC 62443 (zones and conduits, target security levels), NIS2, CyberFundamentals · Networking: VLANs, DMZ, OT/IT segmentation · Documentation: Microsoft Visio, draw.io

Luminus (energy)
Belgium

Cybersecurity Officer & Industrial Network Expert — 2 years

Within the Cybersecurity, Industrial Network & Data team, responsible for securing and operating the OT production networks of 6 hydro plants, around 130 wind sites and 6 thermal plants.

Assignment summary

- Define and review IEC 62443-aligned industrial network architectures (zones and conduits, access controls, DMZs)
- Perform IEC 62443 risk analyses based on zones and conduits (asset scoping, criticality, SL-T / SL-C, risk treatment planning)
- Draft and maintain OT access procedures and operating policies
- Design, deploy and administer an OT Active Directory and core system services across industrial sites
- Coordinate projects (BESS, NCCGT) from scoping and specifications to delivery
- Conduct FAT/SAT with vendors and integrators (2 FATs in Madrid, 2 SATs on site)
- Produce and maintain end-to-end network documentation
- Assess the cybersecurity maturity of the wind portfolio against the CyberFundamentals Essential level

Achievements

- ✓ Delivered an IEC 62443 risk register and treatment plan per zone and conduit, with target security levels and gaps against the current state
- ✓ Implemented DMZ patterns and network segmentation to harden OT/IT boundaries
- ✓ Authored and rolled out the OT access procedures and supporting policy set
- ✓ Completed FAT/SAT for the BESS and NCCGT programmes and validated designs against security requirements
- ✓ Conducted CyberFundamentals maturity assessments across ~130 wind sites and prioritised remediation actions
- ✓ Standardised network diagrams and documentation for consistent technical reviews

Environment

Frameworks: IEC 62443, CyberFundamentals (Essential), Agile · Identity and systems: Active Directory, VMware ESXi · Networking and security: Cisco ISA3000 (FTD), Check Point 1570R, VLANs, DMZ · Documentation: Microsoft Visio, draw.io

IDENTITY AND ACCESS MANAGEMENT

Luxury group
France

IAM Analyst — 9 months

Within the group's global IT team, deployment and evolutive maintenance of a single global identity management tool.

Assignment summary

- Draft specifications as user stories for improvements, evolutions and fixes of the identity management tools
- Model the access management processes (onboarding, offboarding, mobility, change requests)
- Manage releases: testing and communication through release notes
- Monitor the data quality of identities and permissions for user, privileged and technical accounts
- Level 3 support

Achievements

- ✓ Delivered around 150 user stories (evolutions, fixes, design)
- ✓ Created the access management workflows in ServiceNow
- ✓ Documented all IAM processes (onboarding, offboarding, mobility, change requests)
- ✓ Ran workshops to define and formalise the access management lifecycle
- ✓ Used PowerShell and Power BI to monitor the quality of identities and access for over 150,000 accounts

Environment

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

DATA PROTECTION

Pharmaceutical group
Belgium

DLP Analyst — 5 months

Definition of a global data loss prevention (DLP) strategy and roadmap, with the Information Security Manager.

Assignment summary

- Perform a data leak risk assessment and gap analysis
- Define the DLP strategy
- Build the DLP project roadmap

Achievements

- ✓ Ran 8 business workshops to identify sensitive data and risk scenarios
- ✓ Ran 5 IT workshops to evaluate the existing data loss prevention measures
- ✓ Used the EBIOS RM methodology for risk analysis and evaluation
- ✓ Drafted a risk assessment report with 21 risk scenarios and related vulnerabilities
- ✓ Defined the processes, tools and skills needed to mitigate those risks
- ✓ Built the roadmap to implement the DLP processes and deploy Microsoft Purview, Sentinel and Defender for Cloud Apps

Environment

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

GOVERNANCE, RISK AND COMPLIANCE

Bank
Luxembourg

NIST Analyst — 3 months

Research and analysis of evidence for the NIST SP 800-53 framework, with the CISO.

Assignment summary

- List and prioritise the controls and evidence needed for NIST SP 800-53
- Prepare and lead workshops with stakeholders
- Collect, analyse and archive the evidence
- Draft the remediation plan

Achievements

- ✓ Prioritised 360 controls across 5 scopes
- ✓ Facilitated 5 workshops (one per scope)
- ✓ Assessed the 360 controls and defined their remediation

Environment

NIST SP 800-53

Printing services company
Luxembourg

Cybersecurity Expert — 4 months

Cybersecurity expert role to set up an ISMS, reduce the risks raised by a penetration test and raise staff awareness.

Assignment summary

- Implement an ISMS based on ISO 27001:2022
- Identify and remediate the risks raised by a penetration test report
- Support the business impact analysis (BIA) and business continuity plan (BCP)
- Create cybersecurity awareness sessions

Achievements

- ✓ Resolved 50 of 93 control points for the ISMS implementation
- ✓ Identified 50 risks from the pentest report and remediated 30 of them
- ✓ Created 8 awareness sessions on cyber risks and good practices
- ✓ Supported the BIA and BCP with the business units

Environment

ISO 27001:2022 · Brainframe

SECURITY AWARENESS

Public sector and construction
France and Belgium

Phishing campaigns and awareness — 4 months

For two clients, the IT department of the town halls of Maine-et-Loire and a building construction company: phishing simulations, prevention campaigns and reporting for mayors and IT teams.

Assignment summary

- Install, configure and operate the Gophish platform
- Create simulated phishing emails and configure an SMTP server
- Design and present a prevention campaign for town hall staff
- Collect campaign data and write the campaign report

Achievements

- ✓ Ran phishing campaigns for 4 municipalities (520 users)
- ✓ Ran phishing campaigns for the construction company (350 users)
- ✓ Delivered 10 awareness sessions for town hall staff
- ✓ Analysed and reported the campaign results; documented the tool for future campaigns

Environment

Gophish, Linux · HTML / CSS

Energy company
Belgium

Awareness – escape game — 2 months

Awareness campaign in an escape-game format, at the client's request. I was in charge of the technical preparation of the sessions.

Assignment summary

- Install and configure the virtual machines for the escape game
- Set up and document a simulated landing-page tool
- Design workshops where participants put themselves in an attacker's shoes
- Create a cybersecurity awareness quiz

Achievements

- ✓ Delivered 40 sessions for 200 employees

Environment

Kali Linux · Pyphisher, John the Ripper · Slido