



Function Profile: Cybersecurity Engineer – EN 18031 Projects

Role Title: Cybersecurity Engineer – EN 18031 Compliance Projects

Department: Security Engineering / Project Delivery

Location: Remote / On-site

Reports to: Cybersecurity Program Manager

Role Purpose:

The Cybersecurity Engineer will support clients in achieving compliance with **EN 18031-1/2/3:2024** through technical guidance, risk analysis, and structured documentation. This role requires a hands-on engineer with a deep understanding of **network security, threat modeling, and embedded or industrial systems** — capable of translating technical setups into standards-based evaluations.

Key Responsibilities:

- Guide clients through the **EN 18031 series** process from asset identification to risk analysis and mitigation planning.
 - Identify and classify **network assets, security assets, and entities** according to standard definitions.
 - Lead or support the creation of technical documentation such as:
 - Asset lists (e.g., NetAsset tables)
 - STRIDE threat models
 - Protocol/port mappings
 - Security configuration overviews
 - Analyze communication interfaces (e.g., FTP, NTP, DHCP) and assess their relevance to EN 18031.
 - Support clients in defining **security boundaries, access control rules, and attack surfaces**.
 - Collaborate with product teams, developers, and QA to gather required technical insights.
 - Stay up to date on evolving **cybersecurity standards**, regulatory requirements, and best practices.
 - Optionally: participate in external audits or reviews as a subject matter expert.
-

☎ +886 966 509 128

🌐 <https://www.iotapproval.com>

📍 Taipei Address:

F 10, 235, Section 4, Zhongxiao East Rd., Da An District, Taipei City, Taiwan



Required Qualifications & Skills:

- Bachelor's or Master's degree in Computer Science, Cybersecurity, Electronics, or related field.
- 3+ years of hands-on experience in **cybersecurity, embedded systems, or industrial device security**.
- Proven experience with **EN 18031, IEC 62443, ISO/IEC 27001**, or similar security standards.
- Solid understanding of **network protocols** (TCP/IP, FTP, DNS, DHCP, NTP, HTTPS).
- Familiarity with **threat modeling frameworks** such as STRIDE or attack trees.
- Ability to write clear, structured documentation for technical and non-technical audiences.
- Strong communication skills to interface with both clients and internal stakeholders.
- Fluent in English (spoken and written).

Preferred / Nice-to-Have:


- Experience in medical, automotive, or industrial domains (where EN 18031 is most relevant).
- Knowledge of secure software development (DevSecOps, SDLC).
- Experience with regulatory audits or notified bodies.

What We Offer:

- Work on high-impact cybersecurity projects with leading clients
- Opportunity to influence cybersecurity strategy and compliance at system level
- Flexible/hybrid work options
- Supportive and knowledgeable team
- Training budget for certifications and standards

If you're interested in this position, please reach out to us.

Michel Wouters v/d Oudenweijer

 +886 (0)966509128

 michel.wouters@iotapproval.com

 +886 966 509 128

 <https://www.iotapproval.com>

 Taipei Address:

F 10, 235, Section 4, Zhongxiao East Rd., Da An District, Taipei City, Taiwan