ARMEXA

Case Study:

OT Cybersecurity Design Reviews and Site Acceptance Testing for a State-of-the-Art Semiconductor Materials Manufacturing Facilityy

Armexa conducted validated OT system cybersecurity design reviews, as well as developed and supported Cyber Site Acceptance Testing (Cyber SAT) for a client's newly constructed facility in Taiwan. This greenfield site represents a $500 million investment and is designed to manufacture high-value components that support semiconductor production and its ecosystem, including advanced liquid filters, high-purity chemical drums, deposition materials, and CMP pads and slurries.

Prior to this engagement, our team supported the client by conducting cyber risk assessments, developing their corporate OT cybersecurity governance), and participated in the cybersecurity design of their Operational Technology (OT) reference architecture.

Industry: Manufacturing / Chemicals / Semiconductor

Location: East Asia

Armexa Services:
Cyber Security Acceptance Testing (CSAT)

Validated System Design Review (VSDR)

Challenges

The complexity and scale of this Green Hydrogen project presented several challenges:

- **Multi-Vendor Environment:** A diverse equipment footprint from multiple vendors complicated integration and testing.
- **Integration with Existing IT Infrastructure:** The client aimed to leverage corporate IT tools and protocols, creating alignment challenges with OT systems and vendor-specific equipment.
- **Language and Time Zone Barriers:** Coordination between global teams and local Taiwanese staff introduced logistical and communication hurdles.
- **Evolving Security Culture:** Operational teams were still developing familiarity with recently developed corporate OT cybersecurity governance and OT reference architecture.
- **No Legacy Benchmark:** As a newly designed facility with a new OT reference architecture, there was no existing system to benchmark against.
- **Skill Gaps:** A mix of highly experienced professionals and newer staff required tailored training and support.

Our Solution

We developed a comprehensive, collaborative approach involving IT, OT, and project teams to ensure successful validated cybersecurity design reviews and Cyber SAT implementation. Key elements included:

- **Integrated Workplan:** Coordinated execution across IT, OT, and project management functions.
- **Validated System Design Review (VSDR):** A structured cybersecurity assessment that analyzes technical data from operational control systems and networks.
- **Cyber SAT Test Plan:** Developed custom test procedures aligned with the client's framework.
- **Remote Execution:** Armexa supported testing activities remotely to accommodate geographical and logistical constraints.
- • **Detailed Reviews & Reports:**
    - **Documented results of architecture and test plan execution**
    - **Provided findings, recommendations, and risk insights based on actual test data**
    - **Performed attack path analysis using test findings**
    - **Proposed potential penetration test scenarios for future validation**

Outcomes & Impact

This project marked the first successful deployment of the client's OT reference architecture and security framework in a production facility, allowing cyber risks to be identified and mitigated before turning the plant over to operations. The process strengthened collaboration between IT and OT teams and delivered a scalable, repeatable Cyber SAT methodology for future global projects. As a result, the facility entered production with increased operational readiness and as a significantly enhanced security posture.

ARMEXA