CUSTOMER

European Nuclear Power Plant Operator

Generating more than **half of the electricity consumed** in the country

With hundreds of **critical and air-gapped assets**

OBJECTIVES

Protect critical installations

Ensure availability of safety and operation process

Identify vulnerabilities, help operators carry out risk analysis and elaborate remediation plans

Comply with national and international cybersecurity requirements for nuclear installations

RESULTS

Implementation of a single on-premises solution to handle asset consolidation and vulnerability management

Minimization of attack surface, reduction of cyber risk exposure and general improvement of security posture

Compliance with National and European regulations requirements

Foxguard

https://foxguardsolutions.com/

requestinfo@foxguardsolutions.com

EUROPEAN NUCLEAR OPERATOR SUCCESSFULLY IMPLEMENTS ASSET & VULNERABILITY MANAGEMENT SOLUTION

In 2022, Nuclear Power Plants (NPPs) produced 21.8% of the EU's electricity. Ensuring their safety and security is crucial. Traditionally focused on physical threats, the industry now faces escalating cyber-attack risks, with notable incidents like Stuxnet in Iran and Wolseong in South Korea. Consequently, global regulations (e.g., IAEA, IEC 62645, NIS 2 Directive) emphasize protecting NPPs' digital assets, integrated into all operational aspects. A European NPP operator sought Foxfuard's help to implement an Asset and Vulnerability Management solution to enhance their security.

The customer challenges

Nuclear Power Plants (NPPs) face several challenges in securing industrial assets used for monitoring, operation, control, and protection:

Safety constraints
Safety systems require thorough requalification when modified, limiting asset updates to major overhauls (e.g., every 10 years in France).

Operational constraints
NPPs cannot be taken offline at will, so critical systems must always remain available.

Air-gapped environments
Isolated assets can't benefit from real-time threat intelligence or timely updates.

Operational constraints
NPPs cannot be taken offline at will, so critical systems must always remain available.

Regulations require nuclear operators to identify critical assets and monitor vulnerabilities, posing difficulties for those lacking expertise and resources.

IAEA Guidance recommends the following cyber requirements based on a risk-informed, graded approach addressing:

- Importance of Instrumentation and Control (I&C) system functions for both safety and security.
- The identified and assessed threats to the facility
- Attractiveness of the I&C system to potential adversaries
- Vulnerabilities of the I&C system
- Potential consequences that could either directly or indirectly result from a compromise of the system
- Operating environment

foxguard

The solution

Foxguard provided a European nuclear operator with an Asset & Vulnerability Management solution tailored for industrial assets in critical infrastructure.

Deployed on the customer's premises, it can monitor tens of thousands of assets. Vulnerability information is updated hourly from Foxguard's Knowledge Base via HTTPS or file transfer for air-gapped environments, ensuring up-to-date intelligence while preserving data privacy. This solution enables:

Asset consolidation
Hybrid approach with 0 impact on OT environment that include air-gapped discovery

Assessment & Prioritization
Simple and powerful automatic rules to classify assets and 3D prioritization technology that considers CVSS, exploitability and operational context to focus where it really matters

Vulnerabilities identification
Advanced mechanisms to detect vulnerabilities affecting systems involved in safety or critical processes

Remediation definition & implementation
Advanced risk exposure dashboard to select the adapted remediation, document decisions for traceability and auditability and trigger workflows in existing tools

The results

The European nuclear operator initially tested Foxguard's Asset & Vulnerability Management solution through a Proof-of-Concept (POC) involving around 300 air-gapped assets. The success of this POC led to a wider implementation on their premises. They were provided with a single tool for asset and vulnerability management, featuring a flexible and secure architecture that allowed them to:

- Integrate critical and air-gapped industrial assets into vulnerability management processes
- Implement a single-source, easy-to-maintain database for asset inventory
- Gain a clear understanding of risk exposure and reduce it by prioritizing vulnerabilities
- Track remediation measures and ensure compliance with regulations and internal policies

Thanks to Foxguard's Asset and Vulnerability Management solution, the European Nuclear Power Plant significantly enhanced the security of their critical assets and improved their overall cybersecurity posture allowing them to focus on their primary mission: safely and reliably generating power

> **Foxguard smoothly imported all software assets, enabling us to map CVEs and provide support to our OT administrators during patch management planning.**
> **– OT Cyber Security Team**

NUCLEAR SOLUTIONS PORTFOLIO

Building on the experience and expertise of its parent company Framatome, as a global leader in nuclear industry, Foxguard has developed an offer to safeguard critical nuclear assets, that additionally includes:

Risk assessment & compliance program review
We identify and prioritize major cybersecurity risks and develop a tailored risk treatment plan to mitigate these threats.

Asset management
Our specialists help you build an enterprise program for accurate asset collection, categorization, and management, ensuring you have full control over your critical assets.

Audit & inspections
We can conduct governance audits of your cybersecurity program using industry-leading methodologies.

System hardening
Enhance your infrastructure's security by reducing the attack surface of your critical assets and minimizing the opportunities of unauthorized access.

System architecture
Trust us to research, architect, design, build, validate, and implement tailored critical systems.

Incident Response capability drills
We can help you organize and conduct drills adapted to your specific environment.