framatome cybersecurity



Framatome Cybersecurity

In an increasingly complex geopolitical and technological environment, operators of critical infrastructure are seeking ways to strengthen their cybersecurity posture and improve the resilience of their operations.

With its unique positioning as an expert in both industrial systems and cybersecurity, Framatome Cybersecurity is **protecting what powers the world** by helping organizations implement effective, tailored cybersecurity programs and measures that prioritize operational and safety constraints while ensuring regulatory compliance.

© 2026 Framatome. All rights reserved.

Critical infrastructures are facing cybersecurity challenges:

An Evolving Threat Landscape

Cyber attackers are increasingly targeting critical infrastructure, legacy industrial systems, and supply chains, creating new risks to operational continuity and safety.

An Expanding Attack Surface

As IT and OT systems become more connected, digital tools and remote operations expand, critical environments face a growing number of potential entry points for cyber threats.

AI-Driven Risks

Artificial Intelligence is accelerating the discovery of vulnerabilities and the development of malicious code, increasing the speed and scale of cyber threats.

Rising Regulatory Pressure

Regulations such as NIS2 and the Cyber Resilience Act (CRA) are introducing stricter cybersecurity requirements, greater oversight, and stronger penalties for non-compliance.

A Strategic Imperative

Cybersecurity is now fundamental to the certification, resilience, operation, and long-term sustainability of nuclear and other critical infrastructure systems.



Focus on NIS2:

NIS2 is written primarily in the language of IT security. When applied to industrial environments, however, some requirements cannot be implemented directly. For example, endpoint agents cannot be installed on certified safety controllers, and patching schedules are often constrained by production and requalification requirements. The challenge therefore lies not in mapping requirements, but in demonstrating equivalence: identifying where a measure is not applicable, defining compensating controls, and documenting the rationale to withstand regulatory scrutiny. This is where NIS2 aligns with IEC 62443, helping translate cybersecurity requirements into operational technology environments. Likewise, the 24-hour incident notification obligation is as much an organizational challenge as a technical one, requiring clear processes and governance for timely reporting.

© 2026 Framatome. All rights reserved.

framatome cybersecurity

About Us

Framatome Cybersecurity: Protecting what powers the world

A robust defense-in-depth approach at overall and system level during the complete lifecycle of a nuclear facility:

- Dedicated team of 270+ engineers specialized in industrial cybersecurity for nuclear facilities and safety critical I&C systems.
- Supporting 1000+ customers operating critical infrastructures worldwide
- Experts on nuclear regulation and certification:
  ISO, IEC, NIST, UK NISR, French LPM, US NRC, NIS2, NERC CIP, RCC-E

Implementing cybersecurity programs compliant with best practices and requirements for operation

- Cybersecurity program definition and implementation
- Support to regulatory and licensing submissions
- Identification of cybersecurity governance frameworks and compliance mapping
- System cartography, risk assessment and risk treatment
- Compliance audits to standards (IEC, ISO)
- Maturity assessments of stakeholders and supply chain
- Technical audits: architecture, configuration and penetration testing

Designing cybersecure systems and architectures across every phase of the V-cycle

- Network segregation and communication filtering based on security devices (diodes, firewalls)
- Advanced detection and diagnosis capabilities based on the processing of multiple sensors (network probes, host agents, system logs) and interface with local SIEM/SOC
- Standardized, modular hardening solutions for kernel security, access control, networking, and monitoring, aligned with CIS benchmarks, NIST guidance, vendor recommendations, and international standards (IEC 63096, IEC 62443)
- Customized hardening in a risk-based approach for most critical systems

Ensuring long-term cybersecurity and resilience

- Vulnerability management services: identification, assessment, prioritization and risk-based remediation consistent with system-specific operational constraints and security needs including patching, hardening or reinforced monitoring
- Monitoring technologies that detect anomalies and cyber threats, providing advanced insight and context to support investigation and informed operations

© 2026 Framatome. All rights reserved.



Why choose Framatome as a strategic partner for nuclear cybersecurity?

A unique combination of nuclear and cybersecurity expertise:

- Expertise on nuclear regulation and certification for streamlined compliance
- Comprehensive, cross-functional approach to cybersecurity for a complete view of risks and protections across the entire project
- Experience on reducing licensing and integration risks
- A partner with over 60 years of proven stability with the long-term commitment to stand by you for the next 60

Our customers say it best:

"Today, Framatome brings its expertise and cybersecurity capabilities, demonstrating its ability to understand the operation and architecture of nuclear industrial systems."

— Head of Information Systems Security, French Nuclear Research Reactor

"We were particularly impressed by the project management and the proactive, solution - oriented approach demonstrated by the Framatome Cybersecurity teams. It is a true partnership that enables us to make informed decisions."

— Cybersecurity Manager, European Gas and Transportation provider

"I was impressed by the level of detail and the quality of the network diagrams, which gave us valuable visibility into our outsourced network. The assessment helped us better understand an environment for which we previously had limited insight and enabled us to take back ownership of our local IT operations "

— Site CISO and Business IT Manager, European nuclear component manufacturer

Contact: cyber-services@framatome.com
Website: Cybersecurity Solutions Portfolio

The data and information contained herein are provided solely for illustration and informational purposes and create no legal obligations by Framatome. None of the information or data is intended by Framatome to be a representation or a warranty of any kind, expressed or implied, and Framatome assumes no liability or the use of or reliance on any information or data disclosed in this document.

All rights reserved. © 2026 Framatome. All rights reserved.