framatome

Cybersecurity solutions

Penetration testing

Reliable, sustainable and independent cybersecurity solutions to identify and mitigate cybersecurity weaknesses

Challenge

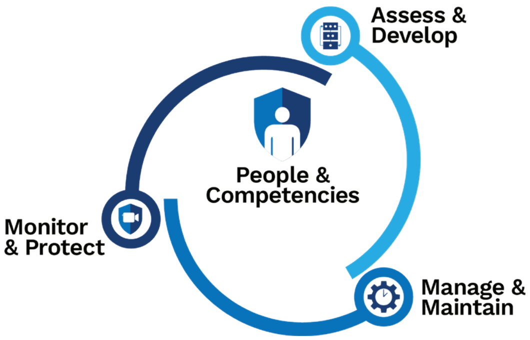
Businesses in almost every industry rely on critical digital infrastructure and systems to run operations. Cybersecurity threats have become more challenging, increasing in frequency with ever-changing origins. Evaluating the security level of digital systems and implementing mitigation strategies is critical to seamless operations and, in some scenarios, compliance with local regulatory requirements.

Solution

With worldwide expertise and a proven track record for reliability and performance for over 60 years, Framatome designs, services and installs components, fuel and instrumentation and control systems for all types of nuclear power plants. We understand the unique needs and challenges of control system security that critical asset owners face every day.

The Framatome approach to penetration testing is built on decades of experience developing and implementing cybersecurity solutions and expertise in industrial information systems.

Our understanding of the potential impacts to customer business during actual attacks, along with the breadth of our technology and expert knowledge of the latest cyber threats, allows our team to conduct tailored attacks on the environment, and develop mitigation plans to prevent such an attack.



Customer benefits

- Identification of weaknesses invisible through standard verification and validation of system function allowing operators to stay ahead of potential vulnerabilities
- Flexibility and knowledge to adapt to customer specific industrial context for a more vigilant, proactive workforce
- A custom and entirely tailored audit with no fully automated tool usage, custom attacks and tool/exploit development to enhance cybersecurity strategy and improve plant reliability

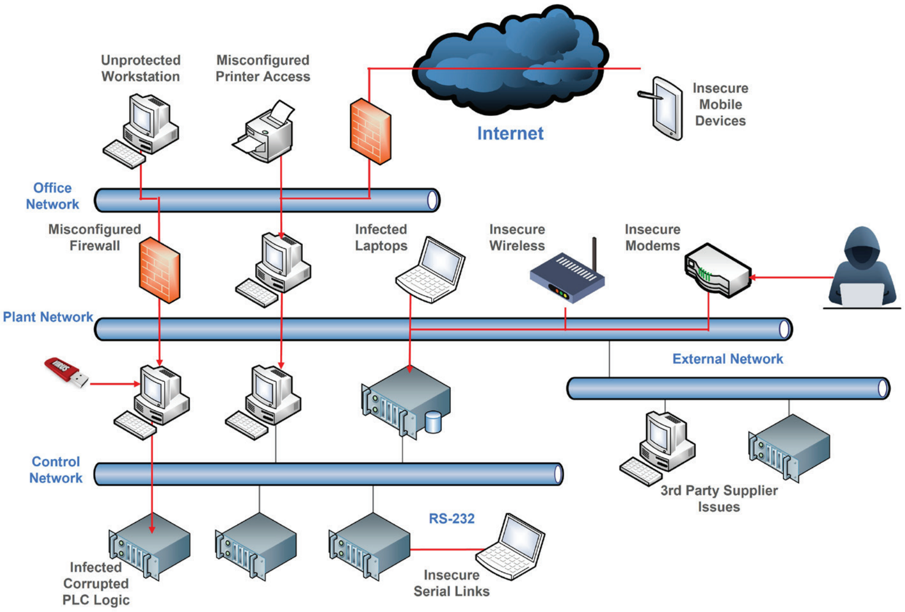
Your performance
is **our** everyday **commitment**

Technical information

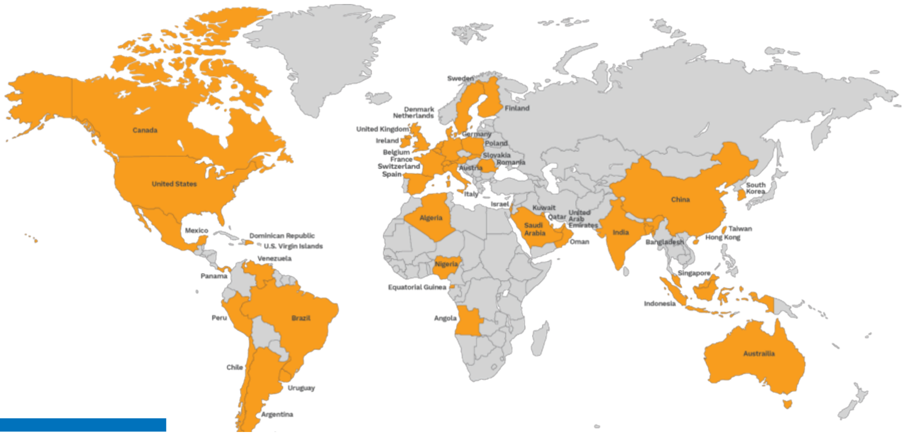
Penetration testing approach is based on standard steps from the Penetration Testing Execution Standard iterated in loops:

- Passive intelligence gathering (network listening, public OSINT activity) and active (port scan, service enumeration, architecture analysis) collections of information on the environment
- Threat modelling based on MITRE ATT&CK (regular and industrial control systems) tailored with our auditors' experience to define the intrusion strategy and to prioritize attack scenarios
- Vulnerability analysis of Common Vulnerabilities and Exposures (CVE) and misconfigurations
- Exploitation: execution of attacks in line with threat modelling and identified vulnerabilities
- Post-exploitation: use of the newly obtained access to gather more intelligence (credentials, interconnections, network traffic) helps pursue intrusions and assess defense-in-depth
- Reporting on each vulnerability and weakness with a criticality analysis and a synthesis of results

Typical industrial Operational Technology (OT) environment with multiple points of entry



Overall global references for critical industry cybersecurity solutions



Key figures

2,000 I&C professionals at **20** sites in **10** countries

More than **170** global cybersecurity experts on the team

Power on. For the future of clean energy.

Scan the QR code to see Framatome's Solutions Portfolio

Contact:
IC@framatome.com | **www.framatome.com**

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 for the use of or reliance on any information or data disclosed in this document. Property of Framatome or its affiliates.
PS_US_776_ENG_9-22

framatome