framatome cybersecurity

SIMULATION & VALIDATION PLATFORM

Ability to replicate a production environment and validate the impact of cybersecurity solutions

Maintenance of industrial equipment in secure conditions is an essential monitoring activity.

Challenge

In a complex and sensitive industrial environment, maintaining industrial control systems (ICS) in secure conditions without impacting this environment is critical.

Another major challenge is to test and validate cybersecurity remediation plans before they are implemented on site. Not disrupting industrial operations is the key point and it must be realized effectively enabling to mitigate the risks of cyberattacks.

Solution

Framatome's cybersecurity platform is based on an advanced virtualization solution enabling modeling complex OT architectures. In order to meet the constraints of a complex industrial environment, this is an opened platform, interfacing with external equipment such as a physical industrial control system (PLC, Switches, Firewall, Data Diode, Gateway, etc.).
The platform allows to:

- Identify equipment and all components that require protection.
- Identify and assess the vulnerabilities of these systems.
- Develop a remediation plan.
- Perform intrusion tests in a controlled environment.
- Test and validate the remediation plan in a secure environment:
    - Hardening.
    - Patch deployment.
    - Non-regression tests.
- Prepare and validate the implementation process to be carried out on site.

Customer benefits

- Carry out risky operations in a controlled and isolated environment.
- Time and costs savings on configuration, integration and validation, so that you can focus on operational objectives.
- Better coordination between maintenance and operations teams.

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

@ Framatome Platform

Technical information

- **Virtualize** complex environments composed of tens or hundreds of virtual machines or containers.
- **Hardware in the loop:** Integrate physical equipment or systems.
- **Network frames:** Generate traffic to simulate an intrusion.
- **Attack scenario:** Use operational engine to check defense-in-depth solutions.

Key figures

60% of cyber-attacks have proven business consequences.

24% with production disruptions.

25% of companies say they have suffered at least one ransomware attack.
2023 CESIN Barometer (Club of Information and Digital Security Experts)

Contact: cyber-services@framatome.com
www.framatomecybersecurity.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. © 2023 Framatome. All rights reserved.