Orange Cyberdefense

ICS Mock-up

Raise awareness, test and secure by reproducing your industrial system

Despite the media coverage of cyber-attacks on industrial systems, awareness-raising is still needed (Executives, management, production teams, IT/OT experts...).

Therefore, it is essential to make them aware of the potential impacts of hacking through a personalized model, a faithful reproduction of the operating or production context.

Examples of Manufacturing industry and Process control mock-ups

Those mock-ups, total or partial representations of your system (existing or planned) have the objective of:

- Raising risk awareness
- Training on the different types of attacks
- Improving interaction between IT and OT Teams
- Setting the security measures to plan
- Testing and validating the security solutions selected
- Checking the robustness of the industrial environment
- Getting ready for crisis management

A funny experience, an asset for awareness-raising

- Practical tool
- Immersion in the skin of an hacker
- Truly and pragmatic simulations
- Visual consequences of a cyberattack
- Advanced and entertaining pedagogy
- Immediate awareness

Main steps to raise awareness, to test and to secure

1. Specify the industrial system reproduction

2. Design and produce the mock-up

3. Elaborate attack scenarios:
   - predefined via corrupted removable media, a corrupted email, the hijacking of the use of wireless technologies, and through the internet,
   - or customized the needs, through specific tools (remote access for maintenance,…)

4. Choose detection and/or protection solutions

5. Train, skills transfer and documentation

The options of the mock-ups

- Hardware and software maintenance
- Technological evolutions
- (IoT, Edge, Cloud, AI)
- Modular operating part
- Detection before protection solutions (firewall, probes, end-point)
- Customized training in the use of mock-ups

Our added value

- Mock-ups:
  - Standard (manufacturing production line, manufacturing industry or process control)
  - Customized according to your system
  - Carriable
  - Digital twins
- Visual consequences of cyberattacks: industrial sabotage, production slowdown, etc.
- Visual consequences of detection and protection solutions to counter attack scenarios