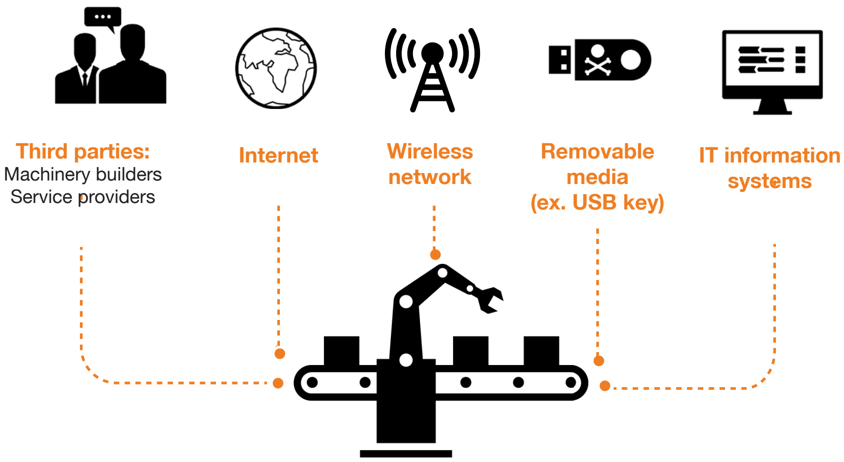
Orange
Cyberdefense

ICS Ethical Hacking

Testing the resistance of industrial systems to cyber attacks

The growing openness of industrial systems (OT) significantly increases their exposure to the risks of cyber attacks.

Main interconnections to industrial systems



OT Environment

Through realistic attack scenarios, Orange Cyberdefense allows you to:

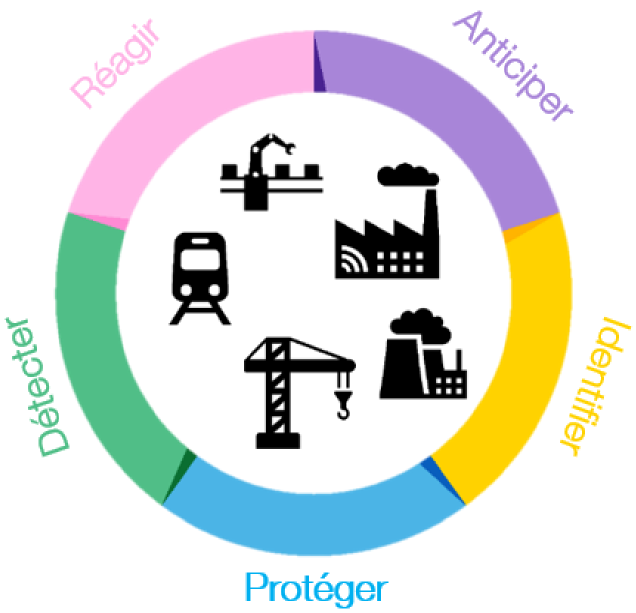
- Determine the level of security in your industry (weaknesses but also strengths),
- Know the consequences of a potential intrusion,
- Verify the effectiveness of the measures put in place for the protection of critical systems,
- Prioritize actions to be taken to reduce the threat level,
- Raise awareness of cyber risks among uninformed teams through strong demonstration.

The factory is a target

- Targeted attacks via infected emails
- Outside parties intentionally or unintentionally committing malicious actions
- Infected removable devices
- Industrial systems directly connected to the internet
- Hijacking the use of wireless technologies (RFID, Wi-Fi, Bluetooth...)

How do you evaluate the security level of industrial systems?

Goal: verify the usability of threat scenarios on different industrial perimeters*



- **Global industrial audit**

  Make a global inventory of the situation including potential impacts over the entire IT and OT systems

- **Global industrial audit without a production line**

  Make a global inventory of the situation including potential impacts over the full range of IT system (information and operation technology))

- **Penetration test targeting the IT/OT segmentation**

  Check the permeability between both environments

- **OT environment audit**

  Make a global inventory of the situation including potential impacts over the entire OT system

- **Penetration test targeting a production line without industrial information systems**

*All these tests are conducted while maintaining process security, availability and productivity. When this is not possible, these tests are carried out during production shutdown or a representative

Our added value

- Experts specialized in offensive security of industrial systems
- Scenarios adapted to the industrial environment
- Reproduction of real attacks
- Feedback from our incident response and monitoring teams

For more information check www.orangecyberdefense.com