Lack of collective knowledge
There is a lack of collective knowledge in cybersecurity, and more particularly in the OT.\(^2\)

Lack of incentives
Trust and privacy are major hurdles for stakeholders to share data.\(^2\)

Insufficient resiliency
Centralized systems represent a Single Point of Failure and can induce a communication overhead.\(^3\)

Architectural isolation
The siloed architecture of detection systems is an obstacle to their effectiveness.\(^4\)

Four observations*:
*From 71 reviewed papers, including 15 surveys

(a) Lack of collective knowledge
(b) Lack of incentives
(c) Insufficient resiliency
(d) Architectural isolation

Research Question:
How to federate knowledge and defense between non-trusting parties?
- What to collect?
- What to share?
- How to share it?

Survey* on collaborative security for the IIoT
*From 71 reviewed papers, including 15 surveys

Collaborative security approaches

Fig. 1. Reference architecture
Fig. 2. Course of action
Fig. 3. Cencyble (IMT Atlantique) -- office used as a real-size model
Fig. 4. S2O spaces (TUM) -- scale models for smart building experimentations
Fig. 6. Industrial testbed (Chaire CyberCNI) -- attack scenarios on real production lines

Contact: leo.lavaur@imt-atlantique.fr