CYBERSECURITY 4 OT/IOT

Protecting your Industrial system or Products including strategy, implementation and monitoring by minimizing the impact on the production and always ensure not to degrade the safety, operations efficiency and the system performance.

How can I Detect, React and Recover from an Attack?

Our clients' challenges

Automation and digitization currently seem to be the holy grail for OT environments. Machines, systems and devices are more and more online connected to each other, communication with and between installations worldwide is becoming faster, more autonomous and more advanced but also much more vulnerable. A single wrong click can halt production for days or weeks!
It is key to detect any intrusion and react immediately to limit the impact.

Capgemini solution

We will **install and configure a dedicated OT probe and propose a L2/L3 team dedicated to OT to perform the investigations** (L1 is often done by the IT SOC).
We will handle **security alerts** (Known threat detection) and **integrity alerts** (baseline deviation / abnormal behavior)
We will also perform **preventive actions** (OT Vulnerability Scanning , leverage with other sites, support to on site engineers)

Key Assets

Baseline definition

CyberX Microsoft

key partner

Reuse of playbooks / procedures made for OT events

OT playbooks

Consultants with Security skills AND **Industrial background**

Dedicated Skills

GICSP

ISO

ISO/IEC 27001:2005

ISA/IEC 62443 CYBERSECURITY FUNDAMENTALS SPECIALIST

Certifications

OT alerts handling can be leverage with an existing SOC or in stand alone

Flexibility

Feedbacks on this service line

- ✓ Manage also sign of attacks (integrity alerts) on top of classical known threat detection
- ✓ Minimise attack risk by leveraging between site
- ✓ Periodic overview on the cybersecurity posture of the site (hygiene score)

Key experiences on this service line

Schneider Electric | DOLPHIN ENERGY دولفين للطاقة | orano | ENGIE | GE

