



CyPRES is an IDS (Intrusion Detection System) coupled with dynamic monitoring of the operation of an OT system.

From listening to the industrial network, it provides IHM (control, presentation, investigation), alerts and recordings of security events.



FUNCTIONS

- ❑ Mapping of equipment and flows in real time
- ❑ Details of flows with metrics, metadata and context indicators
- ❑ A functional and temporal representation of system behavior
- ❑ An operating HMI consistent with SCADA
- ❑ Alerts relating to the inspection of protocols, the network, flows, process values, inconsistent behaviors
- ❑ Recordings replayable or usable by a SIEM
- ❑ A learning mode to evolve with the system over time



MAJOR ASSETS

- A behavioral analysis associated with a rules engine.
- An analysis of all the layers up to the operation of the process.
- Taking the context into account to reduce false alerts and enrich the information.
- The IHM with an Operation component to integrate.

The operator in the safety chain.





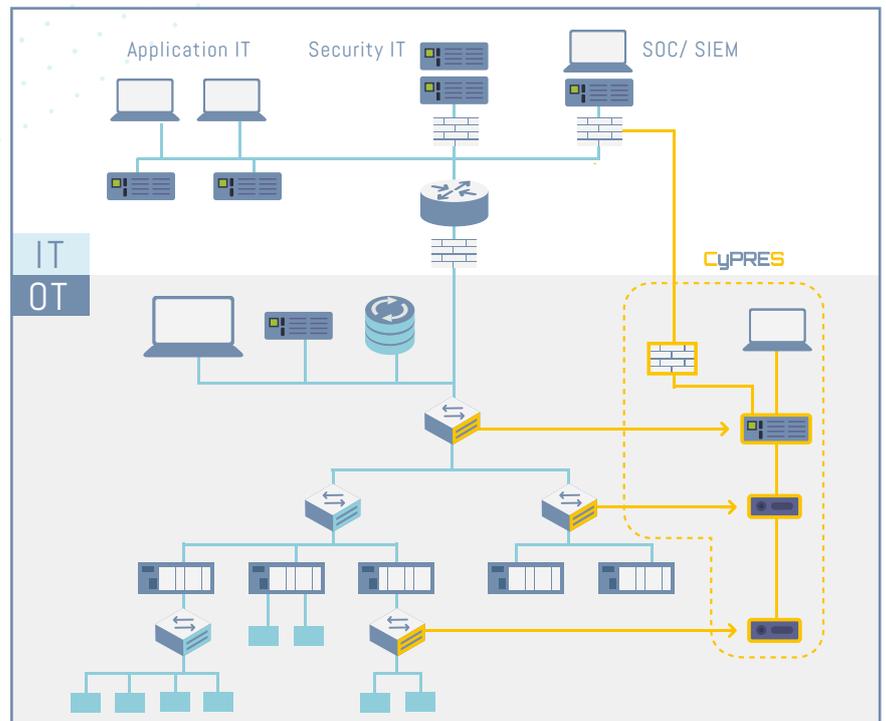
- Clean dissectors for most protocols.
- A behavioral analysis related to the dynamics of functions.
- Contextualization extracted from network frames and relating to resources and operating modes.
- A rules engine (AI) for alert generation.
- A sophisticated configuration system combining the parsing of PLC programs and the import of supervision tags, with the elements of the OT network.



IMPLEMENTATION

- CyPRES processes the network stream in real time from one or more capture points, either in port mirroring or using TAP.
- These captures are inherently passive and do not disrupt the OT network.
- The CyPRES HMIs are local or remote thin clients.
- The external connection to the SIEM according to infrastructure and SIEM.
- CyPRES is configured and developed on the customer's system, by CYBELIUS or the customer's integrator.

→ DEPLOYMENT EXAMPLE



PRESENTATION

CyPRES is a software product deployed on a standard server as well as remote collectors according to the architecture of the OT network.

CYPRES is marketed for rental or sale with an annual operating and maintenance license.