



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

From listening to the industrial network, it provides HMI (control, presentation, investigation), alerts and security event records.



FUNCTIONS

- Equipment mapping and real-time feeds
- The detail of flows with metrics, metadata and context indicators
- A functional and temporal representation of the behaviour of the system
- HMI operations consistent with SCADA
- Alerts concerning the inspection of protocols, the network, flows, process values, inconsistent behaviours
- Recordings, re-playable or usable by a SIEM
- A learning mode to evolve with the system over time



MAJORS FEATURES

- Behavioural analysis associated with a rules engine.
- Analysis of all the layers down to the operation of the process.
- Consideration of the context to reduce false alarms, and enrich the information.
- An HMI with an Operations component to integrate the operator into the security chain.





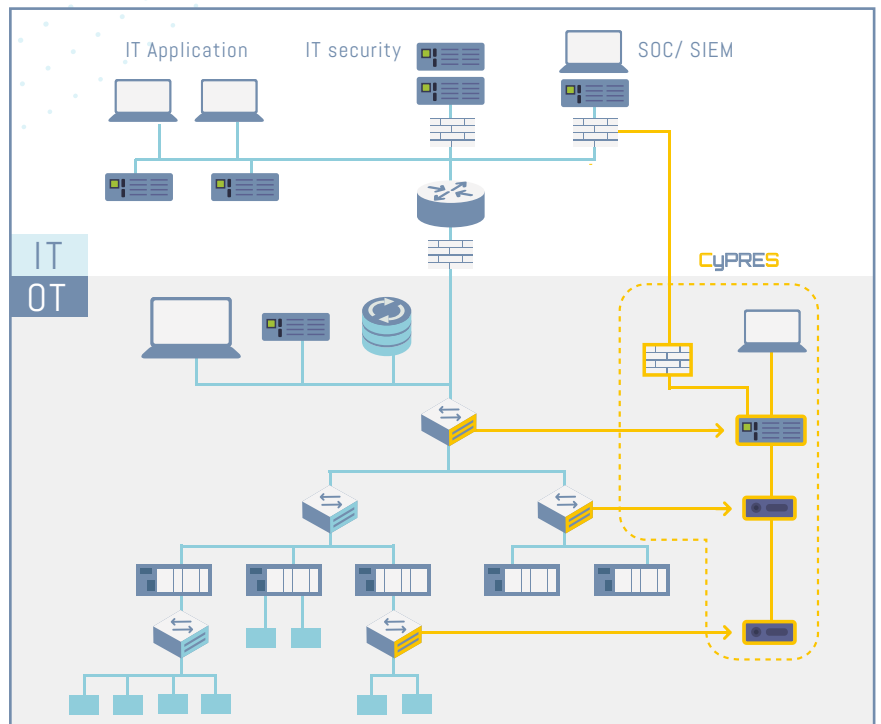
- Proprietary dissectors for most protocols.
- Behavioural analysis related to the dynamics of the functions.
- Contextualisation extracted from the network frames and related to the resources and operating modes.
- A rules engine (AI) for alert generation.
- An elaborate configuration system combining the parsing of PLC programs and the monitoring tags import, with the elements of the OT network.



IMPLEMENTATION

- CyPRES treats the network flow in real time from one or more capture points, either by port mirroring or with TAP help.
- These captures are intrinsically passive and do not impact the OT network.
- CyPRES HMI are local or remote thin clients.
- The external connection to the SIEM according to infrastructure and SIEM.
- CyPRES is configured and tuned on the customer's system, by CYBELIUS or the customer's integrator.

→ DEPLOYMENT EXAMPLE



PRÉSENTATION

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 license and maintenance.