CyPRES

CyPRES est un IDS (Intrusion Detection System) doublé d'une surveillance dynamique du fonctionnement d'un système OT.

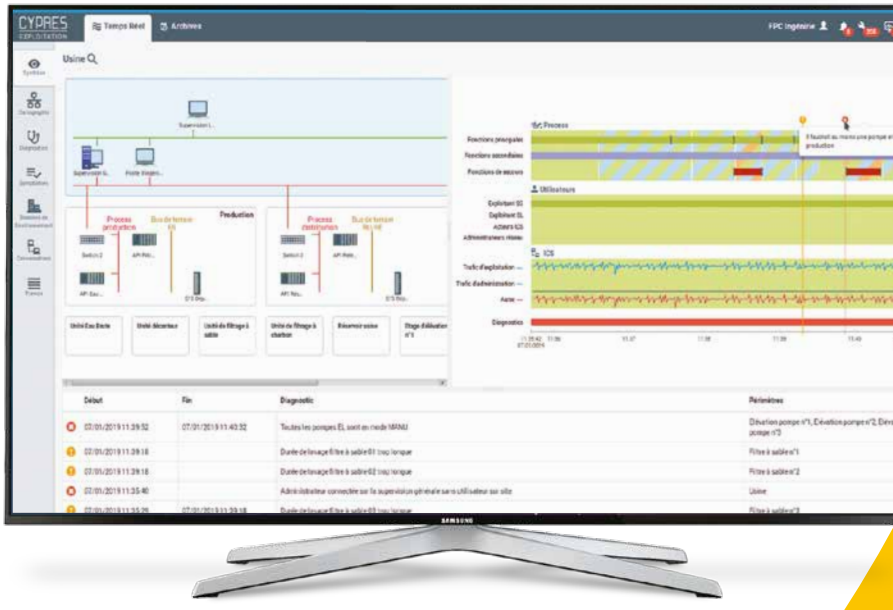
A partir de l'écoute du réseau industriel, il fournit des IHM (contrôle, présentation, investigation), des alertes et des enregistrements d'évènements de sécurité.

Fonctions

- ☐ Une cartographie des équipements et des flux en temps réel
- ☐ Le détail des flux avec des métriques, des métadonnées et des indicateurs de contexte
- ☐ Une représentation fonctionnelle et temporelle du comportement du système
- ☐ Une IHM d'exploitation cohérente avec le SCADA
- ☐ Des alertes portant sur l'inspection des protocoles, du réseau, des flux, des valeurs de process, des comportements incohérents
- ☐ Des enregistrements rejouables ou utilisables par un SIEM
- ☐ Un mode apprentissage pour évoluer avec le système dans le temps

Atouts majeurs

- Une analyse comportementale associée à un moteur de règles.
- Une analyse de toutes les couches jusqu'au fonctionnement du process.
- La prise en compte du contexte pour diminuer les fausses alertes et enrichir l'information.
- l'IHM avec un volet Exploitation pour intégrer l'opérateur dans la chaine de sécurité.



Cybelius
Industrial Cyber Solutions

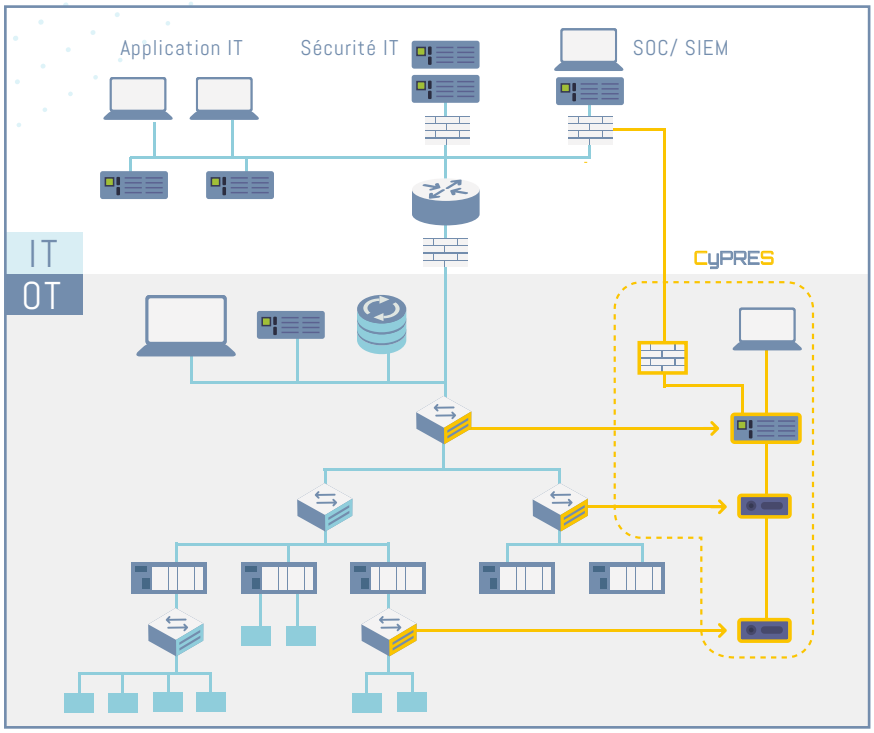
Technologies CyPRES

- Des dissecteurs propres pour la plupart des protocoles.
- Une analyse comportementale liée à la dynamique des fonctions.
- Une contextualisation extraite des trames réseau et portant sur les ressources et les modes de fonctionnement.
- Un moteur de règles (AI) pour la génération d'alerte.
- Un système de configuration perfectionné alliant le parsing des programmes des automates et l'import des tags de la supervision, avec les éléments du réseau OT.

Mise en œuvre

- CyPRES traite le flux du réseau en temps réel à partir d'un ou plusieurs points de capture, soit en port mirroring, soit à l'aide de TAP.
- Ces captures sont intrinsèquement passives et ne perturbent pas le réseau OT.
- Les IHM de CyPREs sont des clients légers locaux ou distants.
- La connexion externe vers le SIEM selon infrastructure et SIEM.
- CyPRES est configuré et mis au point sur le système du client, par CYBELIUS ou l'intégrateur du client.

→ EXEMPLE DE DÉPLOIEMENT



Présentation

CyPRES est un produit logiciel déployé sur un serveur standard ainsi que des collecteurs déportés selon l'architechture du réseau OT.

CYPRES est commercialisé en location ou vente avec licence annuelle d'exploitation et de maintenance.

Cybelius
8 place Camille Georges - 69002 Lyon
04 72 41 83 86
contact@cybelius.fr
www.cybelius.fr
@cybelius _
www. linkedin.com/company/cybelius