The Context

The increasing number of attacks on industrial networks means that the level of security of the IS must be raised by integrating the industrial tool.

However, industrial systems are opaque to the CIO due to a very low level of security instrumentation and the absence of continuous monitoring. Their integration into an ISMS is problematic.

CyFENCE
Keenaï

Gfi – Cybelius solution

The cybersecurity division at Gfi designs, markets and integrates management and supervision solutions for IS security of the SIEM type.

The partnership with Cybelius enables these solutions to be extended to the industrial world (OT).
The CyFENCE & SEM Service offer brings IT security technologies for OT systems, without impacting their operation. It also includes a continuous monitoring of the cyber risks of the industrial tool, at the CIO, with an integrated IT SIEM - OT.

For this, we install the CyFENCE product. It is positioned to cut off the incoming and outgoing links of the system to be protected, thus creating a fence and ensuring defence in depth.

A team of Cyber Analysts connects to CyFENCE using a secure connection to carry out an analysis and report as the attached example for IT teams.

The criteria taken into account are the quality of protection, trust, simplicity of implementation, relevance to the OT world.
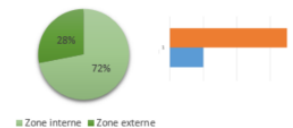
Summary of activity in January 2020

System

A windows update has been performed on all computers in the system.
Backups have been made on a regular basis.
The next audit is scheduled: date unknown.

System access

The number of connections to the system is increasing slowly.
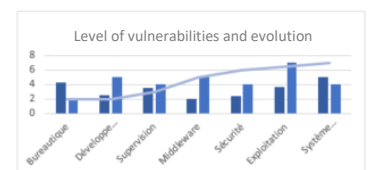Unsuccessful connection attempts are drastically increased.

■ Zone interne ■ Zone externe

Transferred files

The number of transferred files is stable

● Entrant ● Sortant

Vulnerabilities

New vulnerabilities were detected over the same period.
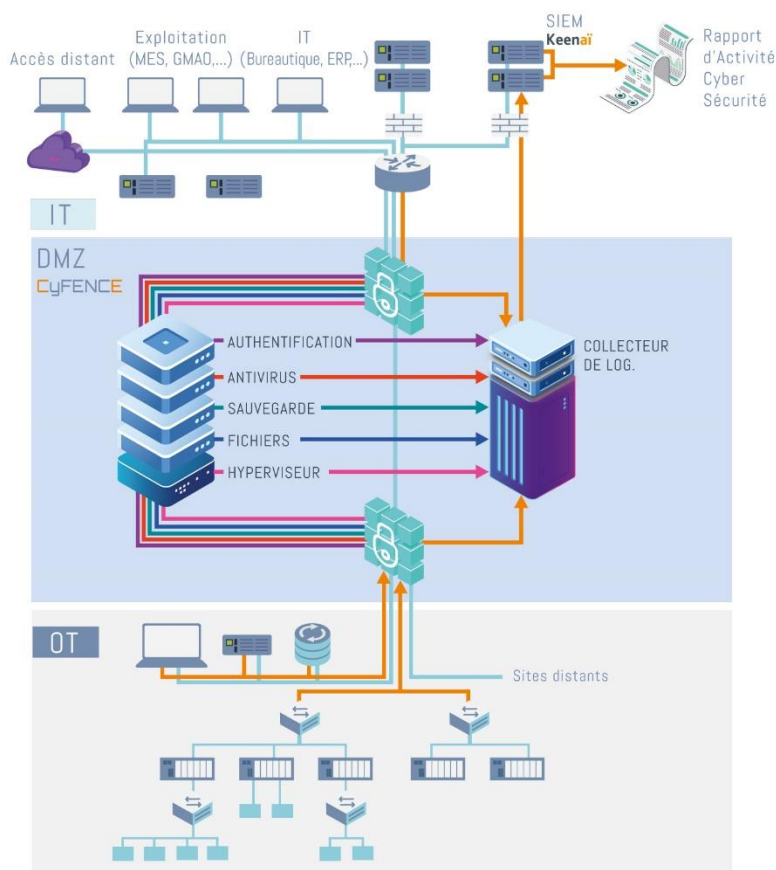
The overall level of vulnerability is changing.

Level of vulnerabilities and evolution

Alerts

The major alerts for the period are the same as those for the previous month

■ Mai ■ Juin
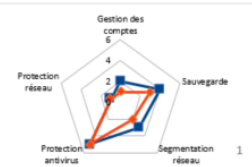
Cyber security Activity Report

- ✓ Synthesis - KPI
- ✓ Access
- ✓ Alerts
- ✓ Status of vulnerabilities

The various safety functions supported by CyFENCE

- ✓ Authentication management
- ✓ Control of access paths to areas and equipment
- ✓ Management of all types of remote access
- ✓ Management of automatic or manual updates
- ✓ Creating security records and collecting system logs
- ✓ Backup and restore
- ✓ Protocol breaks on critical exchanges

Major assets of this solution

- ✓ Providing visibility to the CIO on the safety of industrial systems
- ✓ Monitoring of compliance with the main reference systems in the ANSSI domain
- ✓ Secure management of IT - OT exchanges and reduction of the attack area
- ✓ Operation report by a cyber analyst to improve the cybersecurity posture
- ✓ Installed to cut off incoming and outgoing communications, and secure an existing system by minimizing impacts
- ✓ Modularity of functions and communications to adapt to existing or new systems
- ✓ Redundant version available for availability needs
- ✓ Thanks to its positioning between IT and OT, "CyFENCE & SIEM Service" allows to extend IT security services to OT (Anti-virus, authentication, logging...).

Cybelius

At the crossroads between IT and OT, Cybelius is made up of experts in industrial computing and cybersecurity. It is the first company in France to ensure the security of your industrial installations and infrastructures. From the evaluation, to the securing as well as the real-time monitoring of industrial systems, Cybelius solutions cover the whole process of cybersecurity.