CYBERFERO

Continuous vulnerability assessment OT

- Complete visibility of ot assets
- Vulnerability detection prioritized by risk
- Real-time monitoring and alerts

www.cyberfero.com

WHAT IS IT?

Protect your plant from OT threats without stopping production. A continuous managed service that identifies assets, vulnerabilities, and anomalous behavior in the OT world: sensors (temperature, pressure, level, vibration, flow), PLCs, HMI/SCADA, industrial networks, actuators, valves, and field components.

In OT environments, the issue isn't just whether a vulnerability exists, but how much it can impact the process: line downtime, quality degradation, safety risks, inefficiencies, and system downtime. Furthermore, the heterogeneity (new and legacy machines, different suppliers, industrial protocols, remote access) makes it impossible to rely on spot checks.

Continuous monitoring is required, designed for industrial operations.

Continuous vulnerability assessment OT is the equivalent of continuous vulnerability assessment IT, applied to the operational world:

01 Scan and observe the OT ecosystem continuously

02 Identify vulnerabilities and configuration issues

03 Detect unauthorized changes and network/process anomalies

04 Produces priorities and recommended actions, geared towards business continuity

WHAT DO WE MONITOR?

asset OT and IoT

- PLC, HMI, SCADA, gateway, switch and industrial network segments
- Sensors: temperature, pressure, level, vibration, flow
- Actuators and field components: valves, hydraulic locks, auxiliary systems
- IT/OT interconnections and remote access
- Connected IP devices, even unmanaged ones

HOW DOES IT WORK?

1) Visibility

System inventory and mapping: what is connected, where it is located, what role it plays, and what changes over time.

3) Answer

Risk-based prioritization and action support: what to fix first, what to plan for during shutdowns, what to mitigate now.

2) Detection

Continuous monitoring to intercept:

- ✓ Known vulnerabilities and new exposures
- ✓ Abnormal behaviors
- ✓ Variations from authorized configurations

TECHNICAL APPROACH

To ensure effectiveness in an industrial environment, the service combines:

- On-site probes positioned at strategic points of the plant network
- Centralized management and event correlation
- Hybrid monitoring: passive (observes traffic without interfering) and active (targeted queries when necessary)

Objective: Increase security and resilience without introducing unnecessary complexity.

BENEFITS:

- Dashboard with asset inventory, criticality and security status
- Periodic report (monthly or as needed) with:
  - Vulnerabilities detected and prioritized
  - Evidence, impact and technical recommendations
  - Action plan for mitigation and correction
- Alerts on anomalies, new connections, and unauthorized changes
- Possibility of supporting the internal team and suppliers for remediation (on request)

WHO IS IT RECOMMENDED FOR?

Ideal for companies that:

01 They manage plants with critical operational continuity

02 They have mixed legacy/modern environments and different vendors

03 They must reduce downtime and operational risk

04 They want to build a solid foundation for audit, group policy and compliance

CYBERFERO

For over 10 years a leader in the Cybersecurity and Security sector

Cyberfero is a Managed Security Service Provider (MSSP) specializing in providing comprehensive security solutions for businesses of all sizes. As a trusted partner, we offer a broad range of security services designed to protect your organization from cyber threats, data breaches and other security risks.

Website

Contacts

+39 0522 1685330

https://www.cyberfero.com

info@cyberfero.com

Via Statuto 3, 42123 - Reggio nell'Emilia (RE)