ZEROLYNX | OSANE CONSULTING
A ZEROLYNX COMPANY
CYBERSECURITY & INTELLIGENCE

Cybersecurity in the **Industrial** Sector

OVERVIEW

The chemical industries, metallurgies, waste and water management, and materials production and transformation plants are some of the industries that make up the sector. Industry is the backbone of the European economy and, consequently, are also one of the most targeted sectors, receiving one in every three cyberattacks. The slow digitization of the sector and IoT are expanding the attack surface. The low patching level, unsupported systems, and the deployment of few security measures are allowing cybercriminals to exploit multiple vulnerabilities to steal personal data, disrupt services, and cause irreparable damage.

CHALLENGES

Industrial equipment is beginning to become obsolete. High amortization periods force organizations to extend their lifespan, maintaining industrial control systems (ICS), SCADA, HMIs, PLCs, sensors, and other OT assets that are unsupported and vulnerable to threats already addressed, such as Wannacry. The increasing interconnection of these devices, the expansion of IIoT technologies, and the overall digitization of the sector are exposing industries to new security breaches.

SOLUTIONS

NIS2, GDPR, National Security Frameworks, or Acts on the Protection of Critical Infrastructure are some of the regulations affecting the sector. Zerolynx designs, implements, maintains, and operates comprehensive cybersecurity plans based on the six areas of NIST (Govern, Identify, Protect, Detect, Respond, and Recover).

BENEFITS

Identification and Detection

Through our cyber intelligence and ethical hacking services, we offer a comprehensive solution, monitoring, detecting, and reporting various risks, such as exposed confidential data or severe vulnerabilities, ensuring the security of infrastructure and sensitive data.

Protection and Response

Our cybersecurity and DFIR (Digital Forensics and Incident Response) services safeguard your institution's attack surface, mitigate and respond to any threat, minimizing the impact on public services.

KEY FIGURES

- **Ransomware** remains prevalent in industrial companies. **32% experienced a data encryption intrusion in the last year**.
- **80% of cyber incidents** in the industrial sector **were concentrated in Europe and the US**.
- **Cybersecurity incidents** in the sector **have grown by 11%** in the last year.

"As an international company, BOJ Global interacts and collaborates with suppliers worldwide, which has compelled us to have cybersecurity measures in line with multiple regulations. Zerolynx has helped us raise our cybersecurity levels in this complex scenario and define and implement response plans to address any incidents"

Kristina Apiñaniz
CEO of BOJ GLOBAL

TOP REFERENCES

MAHOU SANMIGUEL · CAF Signalling · BØJ SINCE 1905

ABOUT ZEROLYNX

European Cybersecurity and Intelligence Provider.
Global Top 100 Providers ranked 2023.

info@zerolynx.com
info@osaneconsulting.com

CYBERSECURITY MADE IN EUROPE