ZEROLYNX | OSANE CONSULTING
A ZEROLYNX COMPANY
CYBERSECURITY & INTELLIGENCE

Cybersecurity Services for **CSOs**

OVERVIEW

On a daily basis, Chief Security Officers (CSOs) face numerous challenges, many of them multifaceted as they combine responsibilities for physical security and cybersecurity, depending on corporate strategy. Dependency on external vendors, thefts, regulatory changes, and budgetary limitations are some of the challenges CSOs encounter, along with other cybersecurity-related issues like diffuse security perimeters, data breaches, and increasingly sophisticated cyber attacks. The rapid technological evolution and complexity of modern architectures, coupled with a lack of security awareness and pressures for innovation, increase the attack surface. Internal incidents, the evolving cyber threat, and resource limitations make their management more challenging. To address all these issues, CSOs must adopt comprehensive strategies, collaborate with other areas, and stay updated on the latest trends.

SOLUTIONS

We deeply understand the needs of CSOs and strive to address them comprehensively by designing, implementing, maintaining, and operating comprehensive security plans based on the six areas of NIST (Govern, Identify, Protect, Detect, Respond, and Recover). Among these areas, and considering the competencies encompassed by the CSO role, we focus on three prominent functions:

- **Govern:** We align the IT activities of your organization with its business objectives, manage risks, and comply with laws, regulations, and standards such as DORA, National Security Schemes, Data Protection Acts/GDPR, Private Security Law 5/2014, NIS2, ISO 27001, ISO 22301, or CIS Controls.
- **Identify:** We detect leakages, exposed data, malicious actors, breaches, and other threats to prevent potential new actions that could lead to a cyber incident. Our reports are signed as private investigators in compliance with Spanish Private Security Law 5/2014, of April 4, and Royal Decree 2364/1994.
- **Respond:** Using forensic techniques, we assist you in containing potential incidents such as ransomware or fake invoice scams and investigate their origin to prevent new breaches. Our work is endorsed by qualified engineers, complying with the Spanish Civil Procedure Law (1/2000) Article 340, allowing it to be brought to court.

KEY FIGURES

- **72% of CSOs** claim that **their employees have more access levels than necessary** to perform their tasks.
- **87% of organizations use cloud services**, and among them, **82% of CSOs** believe that **their employees do not properly follow security policies.**
- **25% of companies** that **suffered an incident** did not have their **ISMS** (Information Security Management System) **certified**.

"Zerolynx helped us improve our response capabilities to Ransomware. Their expertise in evidence preservation, chain of custody, investigation, response, and recovery were crucial to strengthen our contingency protocols and backup strategy. Zerolynx is certainly a highly recommended provider."

CSO of a major company in the Telecommunications sector

TOP REFERENCES

MINISTERIO DEL INTERIOR · renfe · euskaltel · Athletic Club

ABOUT ZEROLYNX

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

info@zerolynx.com
info@osaneconsulting.com

CYBERSECURITY MADE IN EUROPE