devoteam
Cyber Trust

Case Study

Alert Readiness Framework

Client

A **European energy provider** that operates critical infrastructure and manages sensitive customer data, supported by us for more than eight years.

The Challenge

Given the complexity of the ICT infrastructures supporting the global energy business, the client sought a **proactive approach** to security management and business continuity. As an operator of critical infrastructure, the client needed to take a step forward in consolidating its state of readiness in the face of emerging threats. The challenges identified were:

- **Global Complexity:** Management of critical and geographically dispersed ICT infrastructures within the energy sector.
- **Operational Gaps:** Difficulty in mapping threats to alert levels and activating controls in an agile manner.
- **Communication Silos:** Inefficiencies in coordination between technical teams (SOC) and business management during crisis situations.
- **Reactive Posture:** The need to evolve towards proactive readiness, given its role as a critical infrastructure operator.

Solution

The adoption of the ARF was identified as the **primary vehicle** to structure and align threat response processes. Unlike traditional GRC solutions, which tend to have a more static and preventive perspective, the ARF adds a proactive layer that structures the organisation's state of readiness to respond to different alert levels in real time.

- **Alert Readiness Framework:** Implementation of a dynamic model focused on readiness levels.
- **360° View:** A "People, Process, Technology & Business" approach to engage the entire organisational hierarchy.
- **IntegrityGRC:** Automation of alerts and response plans through a centralised platform.

Expected Outcome

With the full implementation of the framework, the client expects to achieve a new level of maturity and resilience:

- **Active Resilience:** Consolidated, immediate contextual responses to real threats.
- **Accelerated Response:** Streamlined controls through workflows to support rapid decision-making and the involvement of all teams.
- **Business Enabler:** Cybersecurity embedded into daily strategy and decision-making.

For more information, please visit
www.integrity.pt