VIRTUAL GUARDIAN

PUBLIC HEALTH ORGANIZATION CASE STUDY

Pen Tests & Cybersecurity Audit Success Story

OVERVIEW

The client wanted to assess the robustness of its technological infrastructure and the maturity of its organizational security in light of the new framework established by the Ministry of Health and Social Services.

We assessed the organization's IT security posture, information security operations, and performed various penetration tests.

The overall objective of this mandate was to provide the necessary support and advice to ensure the client's visibility of its local networks based on cybersecurity best practices.

The mandate included the testing of computer networks through penetration tests, the drafting and updating of security policies, support for the implementation of patches and staff awareness to better prevent risks.

CHALLENGES

1. Critical nature of results and value of the report - executive, functional and technical report
2. Technological complexity and requirements of the methods used
3. Need to work with diverse teams at all levels of the organization, from decision makers to technical teams
4. Need to provide the most accurate picture possible for a large network of sites

Pen Tests & Cybersecurity Audit

Success Story

VIRTUAL GUARDIAN

RESULTS

- ESI produced a detailed technical report for security experts and a strategic version for senior management that was incorporated into the overall audit report.
- ESI's involvement in the project has resulted in an effective and intelligent roadmap to mitigate cybersecurity vulnerabilities.

Strategic Analysis

Intelligent Roadmap

OUR CONTRIBUTION

Our team used a two-step methodology conducted in parallel: workshop audit and penetration testing. First, as soon as the intervention protocol was approved by the client, we conducted a series of interviews with the teams responsible for the different departments. These workshops allowed us to collect the necessary data on cybersecurity by keeping a complete record of the evidence provided and classifying it. To complete this information phase, we conducted failure tests to detect vulnerabilities that could be attacked. One of the major challenges of this assignment was the importance of total data confidentiality.

We assessed the client's security posture according to three main areas of intervention. First, we met with the operational teams to analyze their daily activities. Second, meetings with the service managers to obtain a picture of the prevailing situation. Finally, following various incidents related to cybersecurity, a compilation of the results to provide the client with a portrait of the positive aspects and the elements to be corrected to improve the cybersecurity posture of the organization and its numerous regional networks.

The report produced included a remediation plan, measurable indicators and guidance for optimizing the operational structure. The results were presented behind closed doors to the relevant IT managers, including the responsible executive.

Due to the extent of the network and the importance of maintaining the confidentiality of the client's information, our specialists obtained safeguards in case of problems with the physical security managers of the various locations.

Intrusion tests were carried out in "black box" mode, including the installation of probes on unattended workstations or access to connection rooms. Once access to the network was obtained, the consultant proceeded with the scans as well as the evaluation of the security flaws.

Then, the severity of the detected vulnerabilities was evaluated according to the CVSS and OWASP benchmarks.

The exercise was repeated for all internal and external networks. Medical equipment, for obvious reasons of public protection, was excluded from the scope.