

Building a Managed Security Center



Telefónica the first Spanish Telecom Company needed a Security Management Solution for his more than one hundred Management Centers all over Spain.

Due to the security characteristics of these centers, the solution needed to have the capacity to monitor, detect and audit the network, been at the same time fully remote manageable.

“Now, we're able to know what's happening in our management networks, in terms of Security”

Javier Díaz-Palacios (Telefónica)

Technical needs

Telefónica Javier Diaz-Palacios, Security and Communications Responsible for the Management Centers had wide and ambitious requirements.

As a security responsible he needed the Solution to cover the complete life cycle of perimetral security:

- Firewall protection
- Intrusion Detection
- Anomaly Detection
- Monitoring and Inventory Systems
- Network and Host Audit

All this technology had to be integrated so it could be easy installed and configured.

A Security Console was also needed where all the events could be collected and at the same time offer high visibility with the following capacities:

- False positive cleaning
- Correlation
- Security Metrics

At last there were also some integration and customization needs:

- Integration with the already National Centre Alarm Console
- Collection of events from other external systems
- Customization to local languages and corporate look and feel
- Functionality and Cost

According to Telefónica the result of the project compared with other proposals received was:

- More than 10 times lower cost
- 35% more functionality

“We simply wouldn't have spent such amount on the license costs of a complete security solution with all this functionality on a network of this dimension”

Javier Díaz-Palacios Security Manager

Logistic needs

Because of the big number of the sensors and the wide geographic distribution the project had to solve important logistical problems:

- The minimum requirement was to implement one hundred sensors in one year
- So fast deployment with a small member team needed plug and play systems
- Automatic Updates, Distribution and Tuning to all sensors where needed
- Fast and practical recovery methods were also needed

Cost needs

As in any project the cost was a key driver. Previous solutions were not eligible due to high investments and maintenance costs.

The possibility to install the sensors in a low cost hardware not losing quality was a big value-added.