NOZOMI NETWORKS | GENERALITAT VALENCIANA | nunsys GROUP

CASE STUDY

The Valencian Health Department Improves Security and Protection

About the Customer: The Valencian Health Department

The Department of Universal Health and Public Health is a department of the Council of the Generalitat Valenciana with powers in matters of health, public health, pharmacy, evaluation, research, quality and patient care, which also manages the network of hospitals and centers of public health care. It has 34 hospitals under its charge, 245 health centers, and multiple institutions dependent on it. Between Public Health, Primary Care, and Specialized Care, there are more than 50,000 employees.

The Challenge: How Can a Universal Healthcare Department Protect its 245 Health Centers and Over 50,000 Employees?

The Generalitat, with its need for consultations, remote primary care visits and the exchange of sensitive information, faced the challenge of increasing the security of its most critical systems, as well as being able to detect any security incident in its hospital environment at an early stage.

It was important that the solution allowed the Department to monitor the security of a Reference Hospital in real time, and to protect and expand two smaller remote hospitals, before extending the solution to the entire healthcare service. The proposed solution had to model, analyze, and correlate traffic to detect abnormal behavior and ensure compliance with current and future regulations (ENS, PIC Law or NIS2 directive). At the same time, it needed to improve the protection of IoMT (Internet of Medical Things) environments and allow a quick and efficient response in a healthcare language.

Company Profile

Industry: Healthcare
Employees: 50,000+
Location: Spain

Challenges

- **Monitoring, protecting** and expanding their hospitals
- **Ensuring compliance** with current and future regulations
- **Improving the protection** of IoMT environments

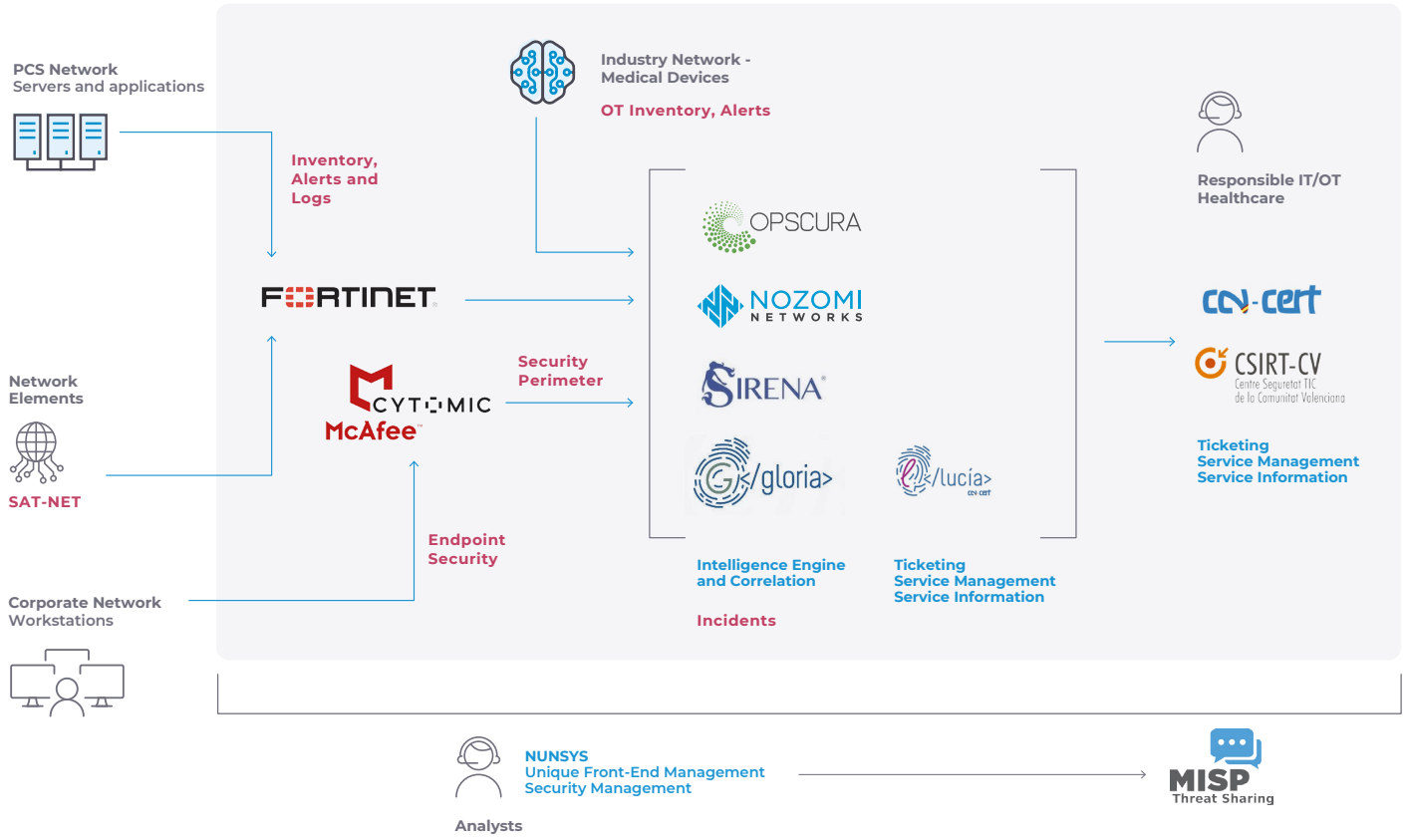
Results

- **Real-time asset** inventory
- **Accurate risk** analysis
- **Enhanced visibility** into devices, traffic and communications

Enhanced Security with Nozomi Networks, Nunsys Group, and Opscura

The Valencian Health Department implemented solutions from Nozomi Networks, Nunsys Group, and Opscura. The Opscura Lunaria probes allow for the securing, capturing and sending of remote traffic with segmentation, patching, hiding, firewall, etc. The Nozomi Networks Guardian allows for the inventory, monitoring and detection of vulnerabilities and threats in assets, which provides both a network map and an inventory and security posture of each IT, OT device (CCTV, sensors, or air conditioning) and IoMT (with all types of devices and appliances). Finally, the asset information has been connected in real time with the risk analysis for compliance with the ENS, adding context to each asset through Nunsys Group Sirena, and the alerts are “translated into health language” and attended to by the Nunsys CyberSOC.

Security Architecture



The Valencian Health Department implemented three capture sensors and remote sending of traffic from two smaller hospitals through Opscura technology. This complements the reactive infrastructure made up of firewalls, endpoints, and other barriers that prevent the execution of attacks on the infrastructure.

The Nozomi Network platform allows, in addition to analysis and modelling, the detection of anomalies and vulnerabilities. Therefore, an additional layer of software, Sirena technology, will be added to the infrastructure to complement the functionalities of Nozomi Networks, “translating” and adding context to assets with a natural health language.

The integration is carried out in OSI's centralized SIEM platform, in this case Gloria, for the centralized management of any alert. This allows said integration to also investigate incidents coming from Gloria through the specialized Nozomi Networks cybersecurity system, allowing for the study and resolution of the incidents, with all the extra context that Sirena provides.

Finally, the OSI operation teams provide control of all the infrastructure necessary for protection, and Nunsys acts as an integrator to provide support in the administration of their own platforms in the project, as well as high-level support and monthly service.

Full Visibility into Devices, Communications, and Threats

One of the first things the Valencian Health Department achieved was a complete real-time inventory of all components using Nozomi Networks and Sirena. They were able to self-label and characterize 95% of the assets detected, giving a first version of risks and anomalies very useful for carrying out an accurate risk analysis. Both the inventory of assets, as well as the threats predicted by the ENS and the real ones, have been configured in Sirena. Nozomi Networks analyzes protocols (including that of medical equipment such as Dicom) and has made it possible to detect non-isolated equipment, improper and poor-quality communications, use of devices, schedules, and anomalies in operation or suspicious traffic through multiple pre-existing rules. The Valencian Health Department has managed to considerably expand the capabilities of its existing technology, increasing security for the exchange of information. The implementation of probes and the vertical CyberSOC has provided the previous system with industrial automation and thus has a detection and high-level early warning. If you do not analyze IT/OT/IoMT traffic you will never know what is happening in your systems.

About Nunsys Group

Nunsys Group participates in the consortium awarded the Incibe challenge to create a CyberSOC for Healthcare valued at €1.8MM, which allows it to develop cutting-edge national technology. In addition, it has extensive experience in this type of technologies, having anticipated the needs of the sector and creating a unique bundle of solutions that work together: OPSCURA + NOZOMI NETWORKS + SIRENA + ERIS-CERT.

Learn more at **nunsys.com**

About Nozomi Networks

Nozomi Networks protects the world's critical infrastructure from cyber threats. Our platform uniquely combines network and endpoint visibility, threat detection, and AI powered analysis for faster, more effective incident response. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

nozominetworks.com