CASE STUDY

DIGITAL INNOVATION AND CYBERSECURITY AT OSPEDALE ISRAELITICO: MEDIGATE BY CLAROTY INTRODUCED IN ICT INFRASTRUCTURE PROTECTION SYSTEMS.

The solution is the first step towards a global project "health global security", for the security of the entire hospital network.

The rising number of attacks against critical infrastructures, particularly in the healthcare sector, is increasingly alarming. According to the Clusit 2023 Report, hospitals have become prime targets for cybercriminals. Due to the complexity of their operating systems and the essential services they provide to citizens, hospitals are among the most vulnerable critical infrastructures in need of protection.

Understanding the Challenge

The Israelitic Hospital, one of Rome's oldest healthcare facilities with over 400 years of history, has recognized the importance of technological innovation in addressing these security challenges. The hospital has integrated its IT infrastructure with advanced solutions to enhance security. Dr. Riccardo Fragomeni, the Head of Information Systems at the Israelitic Hospital, emphasizes the need for a comprehensive approach to security – **"We have gained in the field, day after day, the awareness that it is necessary to have a broader approach to security, which is not limited to perimeter data**

"It is necessary to develop solutions that are able to detect vulnerabilities and promptly suggest actions to 'secure' and protect the information that determines the health profile of our patients and especially the data that manage their therapies - solutions that contribute primarily to safeguarding the continuity and access to non-deferrable, increasingly digital, remote and computerized services that we offer to citizens."

Dr. Riccardo Fragomeni

protection, IT equipment and individual managed processes. It is essential to adopt solutions that guarantee monitoring and 360° cyber coverage of everything that contributes to the provision of the Diagnosis and Patient Care Service."

Finding a Partner

During the market analysis phase, Medigate by Claroty stood out by offering a unified solution that provides comprehensive monitoring and cybersecurity protection for both infrastructure and processes. The proposal seamlessly integrates with the existing solutions and applications at the hospital, such as CUP, ADT, Operating Register, and OE. In April of this year, Israelitic Hospital implemented Medigate with the support of a certified System Integrator, who effectively configured the solution to complement the other system components.

Results

The Medigate platform by Claroty provides the Israelitic Hospital with complete visibility of information flows and the ability to monitor the proper functioning of workstations, medical devices, and wearable devices used by patients. It also provides processes allowing for the identification of anomalies and swift action in response by SOC (Security Operations Center) and SIEM (Security Information and Event Management) services staffed by specialized operators familiar with healthcare. Medigate's interoperability with ERP systems and other cybersecurity solutions further enhances the hospital's defense against cyber threats.

The Medigate solution also enables the Jewish hospital an ability to centrally manage the activities and production volumes of medical devices connected to the network. This has revolutionized the way operators interact with the machines and simplified system and end-point operations. Through a user-friendly dashboard, operators monitor systems and processes in real-time, detect instrument anomalies, track productivity levels, and estimate upgrade requirements. This proactive approach enables prompt intervention to prevent or mitigate problems.

Looking to the Future

Within one month of implementation, the Israelitic Hospital has already witnessed positive results. This success has prompted consideration of expanding the security solution to protect all five offices of the hospital group through the "Health Global Solution" (HGS) project. By integrating the Medigate platform into the HGS framework, the hospital can integrate new algorithms and appliances to monitor information flows in waiting rooms, access gates, server

"We needed a solution that would allow us to improve our ability to react in the event of an attack. A framework which is always ready to collect the changing information in the field that manifests possible vulnerabilities. We know that correct cyber protection is based on three management skills, one must be: predictive, preventive and proactive. Medigate has allowed us not only to include these three elements in a single solution, but to further broaden the vision of safety, working on the concept of cyclicality."

Dr. Riccardo Fragomeni

processors, and devices worn by patients. This comprehensive approach embraces a global concept of security and enables real-time monitoring of criticality, overcrowding, or agitation in waiting rooms, as well as the interception of threatening keywords in dialogues between call center operators and users. **“It is essential to analyze what happened, decode the events, carry out an analysis of the situation and vulnerability found and always measure the effectiveness of the action taken. HGS has this goal. Only in this way is it possible to improve defense, decrease reaction times and increase the resilience capacity of one’s IT infrastructure in order to guarantee the continuity of IT services in response to adverse events”**, says Dr Fragomeni. The ultimate goal is to build a centralized framework supported by machine learning algorithms and artificial intelligence to analyze data accurately and activate automated and semi-automated remediation actions to support technical interventions.

Conclusion

The Israelitic Hospital’s commitment to comprehensive security measures showcases their dedication to safeguarding critical healthcare services and protecting patient information in the face of evolving cyber threats. By effectively combating evolving cyber threats, Medigate enables the hospital to ensure the uninterrupted delivery of essential care while maintaining the highest standards of data security.

About Claroty

Claroty empowers industrial, healthcare, commercial, and public sector organizations to secure all cyber-physical systems in their environments: the Extended Internet of Things (XIoT). The company’s unified platform integrates with customers’ existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, network protection, threat detection, and secure remote access.

Backed by the world’s largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.

For more information, visit claroty.com or email contact@claroty.com.