ROVISYS®
Automation & Information Solutions

CASE STUDY

IMPROVING CYBERSECURITY RESILIENCE AND OPERATIONAL VISIBILITY

The adoption of Industry 4.0 involves the transformation of the manufacturing shop floor and the integration of digital technology. While this evolution increases operational efficiency, it also introduces vulnerabilities and the risk of cyberattacks. Leadership at this pharmaceutical giant turned to RoviSys to better safeguard the future.

ROVISYS

RoviSys has provided extensive support to this client, delivering various automation solutions, including system migrations, upgrades, expansions, and resource augmentation since 2017. The capabilities and competencies RoviSys delivers align well with the client's needs.

When our automation team became aware of the security initiative, RoviSys IT-OT immediately engaged. Engineers and consultants facilitated multiple rounds of discussions, exploration of potential approaches, technology review, and interviews with key stakeholders.

One of the world's leading biopharmaceutical innovation companies in Tuas, Singapore recently initiated a global exercise to fortify their security profile, by evaluating key industry standards and planning a wave of next-generation solutions. This initiative enables the company to address and stay ahead of the ever-growing security threats facing the pharmaceutical and biotech industry.

Traditionally, such initiatives would be handled by IT teams. However, with the emergence of digital automation, smart devices, and mobile apps, the client required a solution partner who possesses knowledge of pharmaceutical regulations as well as deep operational technology (OT) expertise to bridge the IT-OT gaps.

THE PROBLEM

To begin, the RoviSys team undertook a thorough exploration, assessing status, examining existing frameworks, and gaining a high-level understanding of the approach and established schedules. This discovery phase lasted for a duration of three months. The subsequent step involved coordinating the implementation of these initiatives within the client's production schedules. Since certain aspects necessitated deployment during non-peak production times, meticulous planning was crucial to guarantee a seamless integration process.

The client specifically approached RoviSys due to our recognized expertise in network infrastructure, particularly in the field of operational technology (OT).

THE SOLUTION

The implementation plan was divided into two phases to minimize operational impact and accommodate the client's production schedules.

Phase 1 of the implementation plan prioritized network fortification by adopting the layered networking principles of the IEC 62443 standard. This involved segregating the network to enhance overall security, with core control devices now protected by firewalls and a significant reduction in cross-platform traffic. Technologies used include Claroty xDome for Asset Discovery and Management, Vulnerability and Risk Management, Network Protection and Threat Detection, and Digital Immunity DI PROTECT, Cyber-threat Prevention for Operational Technology Environments. Both provided real-time visibility of network traffic and connections, enabling proactive identification and addressing of potential threats.

Phase 2 of the implementation focuses on providing comprehensive protection against cyber threats and improving operational resiliency. We deployed Windows Server Update Services and implemented Industrial Control Systems cybersecurity measures, which include automated asset discovery and passive monitoring of OT traffic to identify potential malware threats. Additionally, an endpoint security software suite was deployed to safeguard the network from emerging threats.

THE RESULT

Both phases of the implementation were successfully completed, meeting the client's global timelines while minimizing operational downtime. The client expressed satisfaction with the outcome, as they now have an integrated IT-OT cybersecurity solution that complies with the IEC 62443 standard and aligns with cybersecurity best practices. This solution ensures operational availability, enhances visibility for the site automation team and OT security engineers, and provides robust security measures.

> “*Both phases of the implementation were* ***successfully completed,*** *meeting the client's global timelines while minimizing operational downtime.*”