ARMEXA

Case Study:

50+ Site Deployment of Network Monitoring Tools in Midstream Oil and Gas Company

Our client faced several significant challenges, primarily centered around integrating security tools and the lack of experience in managing and monitoring operational assets. One of the main issues was that most of the client team had little to no experience with Operational Technology (OT), and their teams' backgrounds were primarily in Information Technology (IT). This created a substantial gap in knowledge when it came to monitoring and securing OT environments.

Moreover, the team had limited experience deploying security monitoring tools, and their prior exposure was focused solely on IT environments, not on OT systems. The client's operational security was significantly at risk due to the absence of OT-specific expertise and tools—particularly critical given that OT systems, with their real-time functions and impact on safety-critical operations, can demand a fundamentally different approach.

Our Solution

Drawing from our deep expertise in OT environments and security, we designed a comprehensive solution to support the client in addressing these challenges. Our solution focused on accelerating the deployment of the right tools and ensuring the effective operationalization of security measures, all while enhancing cross-functional teamwork.

Industry:
Midstream Oil and Gas / Pipeline Assets / Critical Infrastructure

Location:
North America

Armexa Services Provided::

- Cybersecurity Governance
- Run & Maintain Services
- Technical Support Services
- Risk Management
- Security Technology Configuration, Deployment, and Optimization

Solution

1. **Rapid Design and Implementation of Security Monitoring Tools:** We helped the client rapidly deploy robust security monitoring tools (Armis) chosen for their ability to offer real-time visibility into critical processes, enabling the detection of vulnerabilities and potential threats. This solution empowered the client to take immediate action to address security gaps and better protect their OT infrastructure.
2. **Baselining and Operationalization Post-Deployment:** After deploying the security tools, we assisted in establishing baselines for the OT systems. This process involved capturing the normal operating behaviors of the systems, which is crucial for identifying abnormal activities that could indicate a security breach. Once baselining was complete, we helped operationalize the monitoring tools, integrating them into the client's workflows to ensure they were used effectively for ongoing monitoring and incident management.
3. **IT/OT Asset Personnel Cultural and Communication Barriers:** A key part of our approach was to improve communication and collaboration within the OT teams. Cultural differences between IT and OT philosophies, as well as different approaches to problem-solving and communication, created friction. OT professionals often work in environments with high safety standards and low tolerance for risk, while IT staff are often accustomed to working in less formal, reboot if needed environments. These differences needed to be addressed to ensure smooth cooperation.

A key part of our approach was to improve communication and collaboration within the teams so that they could share insights and work together seamlessly to manage OT security.

Outcome & Impact

The solution had several positive outcomes:

- **Improved Visibility and Security:** With the new monitoring tools in place, the client gained full visibility into their OT systems, including critical process control networks and safety systems. This allowed the team to quickly identify security gaps and take proactive measures to close them, significantly enhancing their security posture.
- **Increased Collaboration and Efficiency:** By strengthening relationships among IT/OT personnel, the client saw improved collaboration, leading to more efficient workflows, faster incident response, and better overall security management. This enhanced collaboration also ensured that teams were more effective in addressing both security and operational concerns in tandem.

Conclusion

The solution we provided helped the client address their lack of OT-specific security experience and knowledge by implementing effective monitoring tools, establishing a baseline for security, and fostering stronger collaboration among OT personnel. This comprehensive approach allowed the client to gain better visibility into their systems, improve security, ensure their critical infrastructure remained protected from cyber threats, and achieve regulatory compliance.

ARMEXA

Ready to talk all things cybersecurity?
Contact us at info@armexa.com