ARMEXA

Case Study:

US Energy Company enriches security posture with OT security program development

A major oil and gas company with complex operations across 75 facilities in the United States had experienced frequent network issues causing operational disruptions and outages that impacted its business productivity and reliability. Its executive leadership team needed a formal security program to better align their people, processes, and technology. The company called our team to evaluate, develop, and implement an enterprise-wide security framework to protect business assets and mature their security posture to drive real-world risk mitigation practices at scale.

Challenge: Identifying cybersecurity risks and opportunities

The company's existing operational technology (OT) and industrial control system (ICS) security practices had numerous opportunities for improvement, including:

- Lack of formal OT cybersecurity program or training protocols in place.
- IT and OT professionals viewed "security" differently, and due to organizational silos and cultural barriers, the teams lacked strategic executive alignment. Key obstacles included tension over blurring responsibilities, IT's misunderstanding of OT's process control environment, and confusion around the different employed technologies and their discrete functions.
- Operational processes were prone to reliability issues that led to business disruption and network outages.

Industry:
Energy & Chemical

Location:
United States

Current OT Enviroment:

- 75 facilities
- 500 active users
- 400+ human-machine interfaces (HMIs), SCADA servers, and engineering workstations

Services:

- Network segmentation
- Remote sccess
- OT/IT team alignment
- Architecture design & review

Solution: Collaborating on a comprehensive security program

Armexa developed a unified security strategy and deployed a range of security tools into the OT environment to prevent operational disruptions. Our program solution helped build their cyber program from the ground up to improve security, productivity, efficiency, uptime, and safety.

Deployed security tools included:

- **Network segmentation**, including process VLANs, switch port lockdown, strong firewall policies, and site-to-site VPNs. This increased security of the networks and device communications, decreased unnecessary traffic on OT networks, and added visibility through telemetry for all network devices
- **Centrally managed demilitarized zone**, including Microsoft Active Directory to control all OT access and applications
- **Remote access** via Citrix and Pulse Secure, Microsoft Azure multi-factor authentication, self-service password reset, RADIUS/LDAP integration, NetApp, and Acronis backups for secure log-in and appropriate access permissions
- **High-enforcement application allow listing** utilizing VMware Carbon Black App Control for automated, real-time monitoring and control of program use
- **Integration with greenfield engineering** to secure facilities during the design
- **Centralized logging** using Splunk software for streamlined insight into security events
- **Security and infrastructure portals** for IT and security teams with site-specific dashboards for personnel to track infrastructure issues and user access.

Impact: Enterprise management with a single solution

After implementing this security suite, the oil and gas client made significant improvements in its OT/ICS security. The single comprehensive security program enabled the operator to manage more than 75 facilities with high uptime and exceptional security.

ARMEXA

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

armexa.com

REV0-31.MAY.2022