MAJOR ENERGY EQUIPMENT VENDOR CASE STUDY

FOXGUARD SOLUTIONS®

BACKGROUND

FoxGuard Solutions has been working with a major energy equipment vendor since 2004 to design and deliver cyber security and compliance program solutions to their electric utility customers. In 2004, this client contacted FoxGuard Solutions to assist with a cyber security incident experienced by one of their large international electric utility customers.

The utility customer learned that their Human Machine Interface (HMI) computers within their Industrial Control System (ICS) environment had been infected by malware. They found that a contractor had connected an infected engineering laptop to a free port on their network switch located in the control room. The customer requested a vendor approved method of remediating the specific malware infection they had experienced and patching their HMIs to address known vulnerabilities.

THE SOLUTION

FoxGuard worked with the energy equipment vendor to develop a comprehensive offering which:

- Mitigated risk of the proposed solution by fully testing and validating malware remediation and patch deployment in a representative lab environment prior to site deployment.
- Remediated the utility's reported malware infection.
- Delivered a fully automated patch deployment application to upgrade systems to current patch level.
- Provided a recurring monthly subscription of applicable system patches.
- Provided documentation and training on anti-malware software and automated patch deployment tools.
- Validated and deployed an operating system upgrade path from legacy versions to a supported version.

After the initial successful site deployment, FoxGuard travelled to all remaining utility customer sites throughout their geographic region to implement the solution which prevented further incident. While onsite, FoxGuard also refurbished legacy HMI hardware to improve reliability of the system.

During this project, FoxGuard and the energy equipment vendor identified a market need that could be taken to the vendor's vast customer base to improve the cyber security and compliance posture of their electric utility customers. A comprehensive program was developed which addressed multiple key areas:

- Full lab validation of software patches and updates applicable to utility customer's control system.
- A recurring subscription offering fully validated patches, software updates, anti-malware definitions and Intrusion Detection System (IDS) signature definitions deployed via local and networked methods.
- A software suite offering centralized log aggregation, intrusion detection, and full system backup and restore capabilities.
- Onsite and remote deployment, program training and technical support.
- Full program documentation to ensure adherence to relevant NERC CIP and NEI 08-09 compliance standards.

This program was formally launched in 2009. Since then the program has been delivered to over 250 utilities globally improving the cyber security and compliance posture of their business operations. FoxGuard has continued to collaborate with the energy equipment vendor to support the growing demands of their utility customers.

For more information, contact FoxGuard:

FoxGuard Solutions 2285 Prospect Dr. NE, Christiansburg, VA 24073 877-446-4732 foxguardsolutions.com