CUSTOMER

North American utility industry's **bulk electric system** (BES)

Cooperatives, Investor-Owned Utilities (IOU's) & Municipalities

Providing electric energy to **millions of end-customers**

Spread across **multiple states**

OBJECTIVES

Comply with NERC CIP 007 patching requirements

Save time to focus on operations

RESULTS

Compliance with NERC CIP requirements through monthly secure patch intelligence reporting and secure delivery of associated patch binaries

Improvement of OT (Operational Technology) security posture

Foxguard

https://foxguardsolutions.com/

requestinfo@foxguardsolutions.com

US UTILITIES COMPLY WITH NERC CIP (CRITICAL INFRASTRUCTURE PROTECTION) PATCHING REQUIREMENTS.

The NERC CIP Reliability Standard CIP-007-61 that became effective on April 1, 2016, focuses on entities monitoring their networks for vulnerabilities and streamlining plans to tackle vulnerabilities via a documented patch management process.

The objective is to "manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES (bulk electric system) Cyber Systems against compromise."

Requirement 2.1 requires entities to "have a patch management program that covers tracking, evaluating, and installing cyber security patches." This includes documentation and collection of evidence that the correct patches have been retrieved.

Requirement 2.2 requires documentation and adhering to a security patch evaluation timeline for applicability purposes. The BPS (bulk power system) operator must determine the applicability of each patch in their infrastructure every 35-calendar days to ensure that patches are up-to-date and there are no redundancies in the network.

The customer challenges

Under the NERC CIP regulation, utilities are required to implement a monthly patch management cycle. With over 50,000 assets spread across multiple facilities from various vendors, including legacy systems or air-gapped environments, utilities often face challenges due to limited time and expertise in implementing an end-to-end patching program.

Some utilities did not have a patch management process in place, while others manually performed research for patch availability.

foxguard

> We did it internally, each of the security engineers would manually perform the checks and then one person would oversee everything. It was so hard, it's very nice to have one source. We had about 50 different sources we checked each month. It was a very significant amount of time.
>
> — Utility Representative

The solution

To answer utilities' specific needs, Foxguard developed the Patchintel Solution:

Patchintel Report:

Detailed patch intelligence information relevant to assets within your environment, delivered at least once every 35-days as human and machine-readable reports.

Patchintel Binaries:

Patch binary files within the patch availability report, delivered via secure digital download or secure media.

Patchintel equips utilities with a single source of truth, a unified patch calendar, and a secure supply chain - ensuring compliance with NERC CIP requirements while safeguarding customer privacy. No customer data is stored in the cloud, and asset lists remain fully protected.

The results

Utilities have implemented a Patch Management Program that meets NERC CIP standards and ensures a secure supply chain for acquiring the necessary patches. Thanks to Patchintel, customers can update critical assets more efficiently, saving time and alleviating the burden on their personnel, allowing them to focus on operations.

> "Foxguard has provided a reliable, secure solution for our patch management needs and the detailed report expedites our patching process every month"
>
> — Utility Representative

CYBER SECURITY SOLUTIONS PORTFOLIO

Program Development Services

Our Governance Program Development services provide a comprehensive approach to establishing a cybersecurity program aligned with your business objectives, identifying essential people, processes, and technologies.

Audit/Inspection Support Services

Our Governance Audit/Inspection Support services help organizations prepare for regulatory compliance by conducting thorough audit readiness drills, assessing governance frameworks, and identifying compliance gaps.

Tabletop Exercise Services

Our Tabletop Exercise services provide guided simulations, workshops, and activities with key stakeholders to assess your organization's readiness and ability to respond to business-impacting events.

Assessment Services

Our Assessment services offer comprehensive evaluations of assets, systems, and policies tailored to the customer's industry, regulatory environment, and security maturity level.

Asset Visibility Services

Our asset visibility services utilize automated tools and on-site resources to identify all network and non-network connected devices, delivering a comprehensive asset inventory report that includes asset inventory creation, network topology, and cyber hygiene assessments.

Hardening Services

Our Hardening services focus on securing operating configurations by assessing device-specific settings, implementing best practices, and configuring controls to reduce vulnerabilities across your environment. We also provide high-level programmatic guidance to ensure regulatory compliance.

Patch & Vulnerability Management Services

Our Patch & Vulnerability Management services use patch and vulnerability intelligence to develop targeted tactical mitigations or comprehensive strategies for identified vulnerabilities, creating mitigation plans and recommending technologies to close security gaps and strengthen your organization's cyber posture.