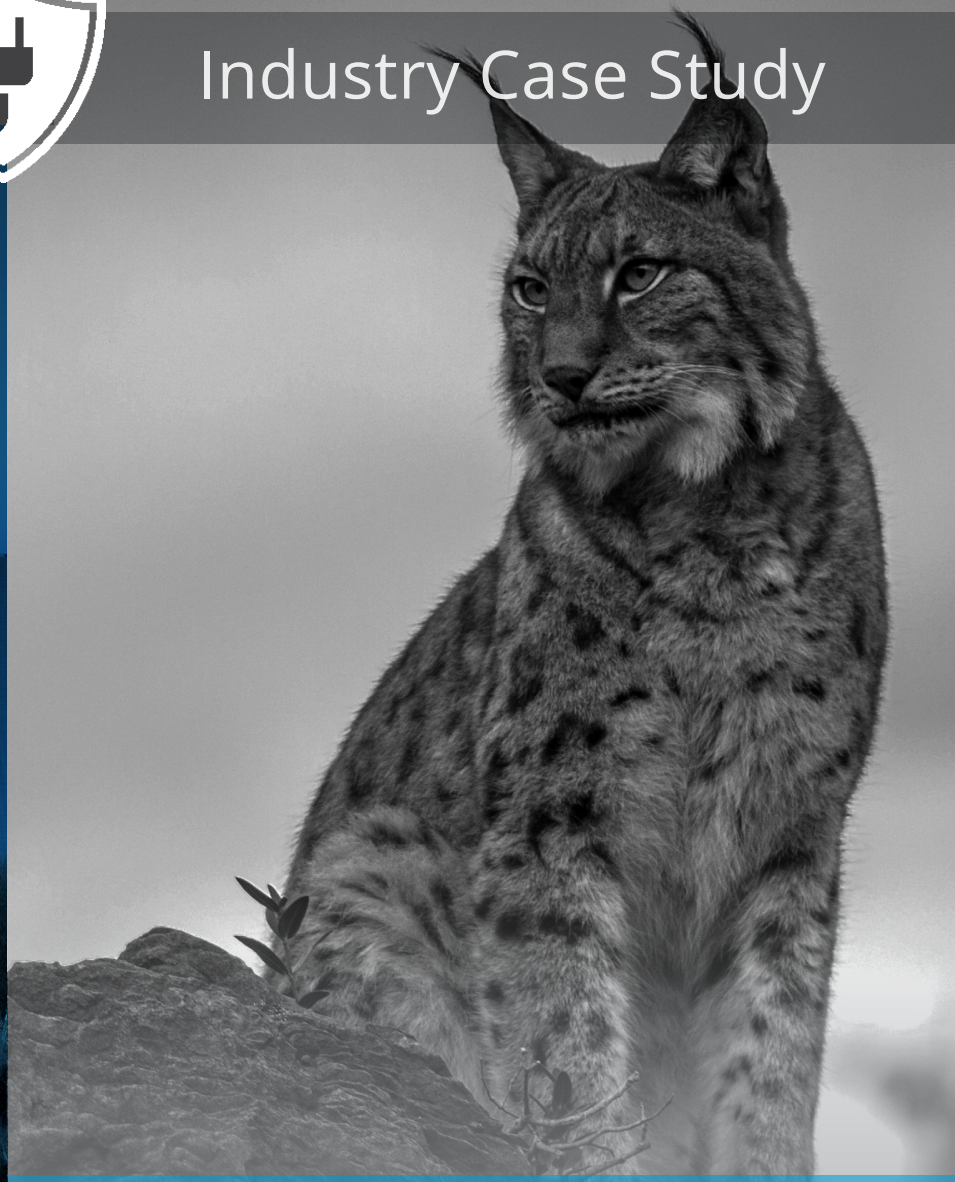
Industry Case Study



Energy Industry

CYBER SECURITY & RISK MANAGEMENT SOLUTIONS

LYNX TECHNOLOGY PARTNERS

ENERGY SOLUTIONS

The nuclear industry is struggling to meet compliance deadlines and find dedicated, knowledgeable resources who can be embedded into the existing workforce and function as a cohesive team. A typical nuclear plant contains thousands of Critical Digital Assets (CDAs) that need identified attributes collected and assessments conducted. With many plants identifying over 80 required attributes for each of thousands of devices, these projects can quickly become overwhelming.

enter... *Lynx Technology Partners*

A major nuclear energy company was struggling to find a partner that could ramp up quickly, learn their processes and procedures, and meet their very rigid timeline. They partnered with Lynx for assistance with the CDA identification, reference gathering, assessments, vulnerability analysis, policy and procedure review, and remediation efforts for two new nuclear facilities. ***"We joined with Lynx Technology Partners (Lynx) and could not have been happier. They provided the highest level of service and quality by providing personalized service and adapting to our needs."***

The security framework to be assessed included RG 5.71 and NEI 08-09. Lynx delivered extremely-qualified candidates with the required skills and experience. By developing a Center of Excellence, Lynx quickly trained and ramped up the Team during peak periods, allowing it to fully meet the timelines and expectations. The Team augmented their current staff, allowing them to seamlessly function together. The Lynx approach provided in-depth assessment of their current security posture, while clearly identifying the impediments to achieving security availability, integrity, and confidentially of all CDAs.

The Lynx-tailored Cyber Security Assessment (CSA) allowed the client to achieve a detailed understanding of its CDA current compliance with security control requirements and comprehend the current security posture, alternative controls, and necessary remediation methods. The Lynx Cyber Security Vulnerability Analysis Approach provided a comprehensive search methodology that identified all known CDA vulnerabilities which provided a clear roadmap for mitigation.

The assessment included an evaluation of the security configuration of the network and infrastructure, along with a review of the policies, procedures, and practices at both plants to ensure compliance

Results at a Glance

We're here to help.

- 6,612 Total Assessments, involving 76 systems, in just over 11 months.
- Reference material including vendor manuals, network diagrams, and design documents were identified for all CDAs.
- The LRM SW solution was installed and implemented to track progress, run reports, and distribute surveys.
- 26 Policy and Procedure documents were reviewed, which correlates to 481 Control Surveys (RG 5.71) for each plant.
- 4,354 Vulnerabilities were found: 1,488 Critical; 1,138 High; 1,544 Medium; and 184 Low.

what we do *differently*

Lynx Technology Partners is the trusted Information Security and Risk Management Advisor that customers in highly regulated industries worldwide depend on to improve security posture, facilitate compliance, reduce risk, and refine operational efficiency.

With world-class skills and knowledge capital built over 30 years, Lynx security experts help customers recognize and control IT-related risks and maintain compliance with major industry and government standards.

with Regulatory Guide (RG) 5.71 and NEI 08-09 industry-recognized compliance frameworks. Lynx's ability to produce quality work within a very aggressive timeline, complete the large number of assessments, and assist in the identification of vulnerabilities in less than one year was described as "Incredible" by the client.

Lynx Risk Manager (LRM), a leading-edge risk assessment tool, was used to perform the assessments of over 6,600 CDAs. LRM is a leading and robust IT risk and compliance solution that allowed the client to immediately improve its audit workflow and assess the IT risk posture against internal and external regulations. Each identified CDA was passed through a questionnaire within LRM to further assist with the understanding of scoping and classification requirements by identifying the associated risk profile attributes. This minimized the survey questionnaire to which the assessor was to respond. For similar devices, additional controls were grouped into commonalities. A "Generic Device" was assessed, and all common controls relevant to those device types were scored. These device-level common controls were then sent to the actual CDA assessments via ScoreSync. This LRM feature cut thousands of hours and reduced costs by hundreds of thousands of dollars by combining similar device types and makes/models into common asset groups.

High *Level Results*

- **6,612 Total Assessments, involving 76 systems (including SCADA Systems), in just over 11 months.**
- **Reference material including vendor manuals, network diagrams, and design documents were identified for all CDAs.**
- **The LRM SW solution was installed and implemented to track progress, run reports, and distribute surveys.**
- **26 Policy and Procedure documents were reviewed, which correlates to 481 Control Surveys (RG 5.71) for each plant.**
- **4,354 Vulnerabilities were found: 1,488 Critical; 1,138 High; 1,544 Medium; and 184 Low.**

IT-Related Regulations

Energy organizations are facing an increasingly complicated regulatory environment.

Typical Challenges We Help With:

- Preparing for NERC CIP Audits
- Complying with NRC Standards
- Asset Identification
- Information Protection
- Systems Security Management
- Change Control and Configuration Management
- SCADA System Assessments

Compliance Standards

- NERC CIP
- NRC Milestone 8
- NEI 08-09
- NEI 13-10
- ISO 27000 Series
- RG 5.71
- NIST 800-82
- State Mandates

Lynx *Risk Manager*

Streamlined Workflow for Assessing Physical and Procedural Controls:

Automated NEI 08-09 assessment workflow that provides structure around the process of collecting scores and providing evidence for physical and procedural controls. Additional workflows native to the solution manage compensating controls, exceptions, and escalation procedures.

Automated Importing and Dynamic Grouping of IT Assets:

Automatically import CDA's into the solution from outside sources like Database, Excel, XML, CSV, etc. and group CDA's around process, workflow, plant systems, or anything that is required by the assessment or reporting requirements

Automated Self-Assessment Surveys:

Send multiple-choice surveys to system owners to request up-to-date control implementation status for their areas of responsibility. Once approved, survey responses automatically update compliance scores.

Attachments for Evidence Collection:

Provides a convenient way to manage the myriad of evidence artifacts required to demonstrate the validity of self-assessment scores.

LYNX TECHNOLOGY PARTNERS

Global Headquarters
244 5th Ave Suite 1220
New York, NY 10001

New York | Pittsburgh | Washington, D.C.

800.314.0455
www.LynxTechnologyPartners.com
InsideSales@LynxTP.com