Hydropower

OTORIO helps Hydropower Company Comply With NIS2 Security Directive

Customer Case Study

Operational cyber security in Hydropower operations

The company is a power utility organization that runs large hydropower stations and small thermal power plants involved in the electricity value chain being generation, transmission, distribution, and supply. The company operates across a wide geographic area with various distant power plants and has faced challenges with partial asset visibility of its assets throughout its operational environment. As Operators of Essential Services (OES), they have a responsibility to secure their complex operational environments and comply with the NIS2 security directive. To ensure readiness and compliance, companies must proactively prepare for the directive's effective implementation by October 17, 2024.

To achieve operational resilience in line with NIS2 guidelines, the company contacted OTORIO to conduct the following tasks:

- Discover and inventory the organization's operational technology (OT) assets across all stations and plants.
- Identify vulnerabilities and assess cyber security risks across the hydropower operational environment.
- Ensure compliance with NIS2 regulations to prevent major power outages and mitigate the financial impact of non-compliance.

NIS2 implication for the Hydropower company

The hydropower company supplies electricity and energy solutions for a wide region. A disruption to the hydropower industry would significantly impact the economy, society, and would have potential environmental implications. Therefore, the industry now falls under the regulatory obligations set forth by the NIS2 directive.

According to NIS2 directive, hydropower companies are required to:

Assess their cyber risks on a regular basis, taking into account the specific risks associated with their operations. For example, hydropower companies are at risk of cyberattacks that could disrupt the generation or transmission of electricity. Stations, and plants operators need to address:

- Asset and network visibility
- Operational Risk management

What is the NIS2 Directive?

The NIS2 Directive is a legislative framework established by the EU to enhance the cybersecurity and resilience of critical infrastructure sectors. It is becoming the baseline for cybersecurity regulations in the EU and applies to both EU and non-EU organizations that provide services within Member States. The NIS2 Directive addresses the following objectives:

- Strengthen the security requirements
- Secure the supply chains
- Streamline reporting obligations
- More stringent supervisory measures
- Stricter enforcement requirements
- Harmonized sanctions across the EU

OTORIO

Hydropower

Implement appropriate security measures to mitigate the identified risks. These measures could be installing firewalls, implementing intrusion detection systems, and training employees on cybersecurity best practices addressing:

- Supply chain security and access management
- Protection against cyber-attack

Report cybersecurity incidents to the authorities without undue delay. Including incidents that have a significant impact on the operation of the company's essential services. To ensure operational resilience hydropower stations, and plants operators should address:

- Incident and Crisis management
- Response and recovery planning

OTORIO Safe Active Query

Discovers and identifies assets and security misconfigurations that can increase digital risk to the asset and the operational process to which it belongs.

Customer challenges

The company lacked asset visibility over its geographically spread hydropower stations and thermal power plants, leaving gaps in the coverage of remotely located systems. As a result, the company was unable to have a complete digital footprint of its operational environment, which is a crucial step in securing the supply chain as per NIS2 guidelines. It also experienced challenges with:

- Unclear and partial asset visibility, with limited details and poor context.
- Based on manual effort and managing the inventory with Excel spreadsheets.
- Multi-generation assets (OS from Win7 to Win10, ICS component lifetime of 10-15 years).
- Multiple vendors, including for security controls (different AV/EDR in each division - transmission, generation, distribution)
- An inability to prioritize risk effectively and efficiently
- Limited coverage and maintenance of remotely located systems
- Struggling to detect and respond to threats and lack of proactive OT security risks mitigation.

OTORIO’s solution

To strengthen the Hydropower company OT security protection in their efforts for NIS2 Directive compliance, OTORIO’s cybersecurity experts deployed OTORIO's Titan solution for continuous OT cyber risk assessment and management. The OTORIO Titan solution successfully established a comprehensive OT asset inventory and network visibility by integrating with the company's multi-vendor, multi-generation industrial and security systems across generation, transmission, and distribution plants and substations.

OTORIO Titan improved asset information and accurately identified network configurations and installed software using passive and safe active querying, integration with DCS, firewalls, EDRs, and log events analysis. This enabled precise mapping of OT-specific vulnerabilities, providing insights prioritized by the level of operational risk in alignment with business priorities. Security practitioners were then provided with clear mitigation guidance tailored to the needs of Hydropower operational environments.

Results

OTORIO's expertise in deploying safe integrations (with DCS, SCADA, Historian, PLC, RTU, CCTV, HMI, industrial and electric-specific protocols) and extracting meaningful data from existing security controls to identify process paths and associated risk levels, resulted in a unified view for OT cybersecurity risk management, detection and response.

OTORIO Titan's seamless integration with the company's industrial systems and existing security controls provided central visibility, complete asset coverage and a single source of truth for all divisions: generation, transmission and distribution. This simplifies the management of OT cybersecurity detection and crisis management.

In compliance with the NIS2 security directive, OTORIO Titan delivers a comprehensive asset inventory and enhances asset attribution by considering the operational context of OT processes and paths. It conducts thorough security posture controls and compliance assessments, identifies known vulnerabilities and the impact level of each operational asset.

Additionally, OTORIO Titan conducted security configuration audits to guarantee NIS2 guidelines compliance. This process revealed critical vulnerabilities such as SMBv1 protocol enabled on multiple assets, a large number of End Of Life (EOL) assets, and unauthenticated remote desktop configurations within the operational environment, posing high-risk exposure to ransomware groups.

OTORIO empowers security practitioners to ensure operational continuity and safety through proactive risk monitoring of the company’s security posture. With clear and actionable risk-mitigation guidance tailored for the hydropower-specific operational environment, practitioners gain access to best practices for enhancing security configurations and network interfaces.

> "We chose to implement OTORIO's Titan solution into our hydropower stations and plants to enhance our cybersecurity and operational resilience, while ensuring compliance with the NIS2 Directive. OTORIO Titan has proven to be a user-friendly platform, enabling every operator to easily engage with it. By offering comprehensive visibility into our OT assets and networks, OTORIO Titan effectively identifies critical security misconfigurations and delivers prioritized mitigations, providing clear guidance on necessary actions for any plant operator (one of the biggest benefits we found). Ultimately, OTORIO Titan equips us with the necessary tools to strengthen the company's resilience against cyber threats."

Benefits for the Hydropower company

OTORIO improved the company preparedness for the NIS2 Directive safely, efficiently, and effectively with:

- A comprehensive OT assets visibility with a unified view of risk for converged IT-OT-IIoT network security systems and industrial systems in the OT environment
- The company's security teams have operational context and impact analysis of an asset or process-level for OT risk-based management.
- Exposures identifications based on correlation between security posture and asset inventory.
- OTORIO's Titan provides the company with insights that improved their MTTD and MTTR, while reducing noise and highlighting which risks and vulnerabilities to prioritize.
- The company receives safe operational security posture assessments that don't disturb its ongoing operations.
- The company improved ROI, leveraging existing security controls and solutions by integrating them with OTORIO's OTORIO Titan platform.
- Security practitioners teams now have quick risk mitigation playbooks with clear instructions to harden site-specific OT network risks and vulnerabilities.

About OTORIO

OTORIO is a leader in OT security solutions, dedicated to safeguarding enterprise IoT and OT environments for enhanced safety, productivity, compliance and resilience. Its flagship platform, OTORIO Titan, provides an all-encompassing suite of applications that brokers IIoT, OT, and CPS security controls into IT workflows, ensuring proactive protection and efficient risk management.

Visit OTORIO.com