Westfalen Weser Netz GmbH

OT monitoring with MDR and OT-SOC

The client

Westfalen Weser Netz GmbH is a leading network operator in the Westphalia and Weserbergland region in Germany. With its extensive network, it ensures a reliable electricity and gas supply for private and business customers. The company is actively committed to a sustainable energy future and relies on innovative technologies and solutions. Through its expertise and commitment, Westfalen Weser Netz GmbH makes a significant contribution to the development of a secure and efficient energy infrastructure.

The challenge

- Mandatory implementation of attack detection systems in accordance with the German IT Security Act 2.0 by 01.05.2023.
- Challenges in implementing the requirements of the IT Security Act 2.0 and achieving the required maturity level through a verification assessment.
- Identification of a suitable OT-IDS solution for the underlying infrastructure.
- Establishment of a 24x7 OT-SOC for continuous monitoring of the infrastructure.

Westfalen Weser Netz GmbH

OT monitoring with MDR and OT-SOC

The solution

To address the challenges, a holistic approach was chosen with the following activities:

- Conducting an OT security assessment to evaluate the general threat situation
- Realization of a proof of concept (PoC) for network evaluation
- Performing a comprehensive network analysis
- Supporting the implementation, operation and monitoring of the deployed OT-IDS sensors, OT-SOC and a Managed Detection and Response (MDR) platform
- Assistance with a successful subsequent audit (regulations § 11 para. 1d, 1e EnWG in conjunction with BSI-orientation guide)

The impact

The project leads to a comprehensive threat reduction for WWN by using synergies of existing IT projects. A holistic approach was pursued to monitor both the IT infrastructure and the OT infrastructure and to respond optimally to alarms with specially trained SOCs.

The implementation contributes to the fulfilment of compliance requirements according to the German IT Security Act 2.0 and the required attack detection systems. It increases the security level in the control and command technology by enabling threats to be detected at an early stage.

An assessment of the current infrastructure parameters served as the basis for the optimal implementation. This positively influenced the project planning and execution.

Why Eviden?

Due to the close cooperation during the Proof of Concepts (PoCs) and the OT-Security Assessment at the beginning of the project, as well as the resulting recommendations for action, Eviden was able to successfully implement a holistic project approach within the given timeframe.

Eviden was able to provide targeted support due to its experience and synergies with other projects in the field of technology consulting and integration. As a result, the required attack detection systems were successfully implemented and operational by 01.05.2023.

The implementation was successfully confirmed by an external audit.