siemens-energy.com/i&c-service

SIEMENS energy

Wien Energie Austria

Supported by cybersecurity experts

The Company

Wien Energie is Austria's largest regional energy provider. The company reliably supplies around two million people and 230,000 commercial and industrial facilities with energy. Electricity and heat production comes from cogeneration, waste recycling and renewable energy such as solar, wind and hydropower as well as biomass. Wien Energie is massively expanding its share of renewable energy sources and making an active contribution to Austria's goal of climate neutrality by 2040.

The Task

As the risk of cyberattacks on critical infrastructure increases, so do the requirements to which energy companies are subject. Specific know-how on increasingly complex plant technologies and cybersecurity is required for the state-of-the-art operation of all Wien Energie assets. In most cases, operators do not have local access to the necessary level of expertise.

Your Benefits

- **Up-to-date and comprehensive cybersecurity status based on control system data**
- **Rapid 24/7/365 remote support for analysis, identification, classification, and resolution of events**
- **Support for regulatory reporting requirements and in the event of a cybersecurity incident**
- **Coverage of the standard requirement ISO/IEC27001 and IT-SiG 2.0**

Our Solution

Siemens Energy's Remote Expert Center (REC) Cybersecurity team supports Wien Energie with a combination of preventive and corrective services. The goal of offering an integrated service that addresses all known potential threats to availability makes cybersecurity a consistent extension and core component of the current REC service. The support provided by SE cybersecurity experts ranges from the detection of security events and the classification of cybersecurity events and incidents, to forensic analyses and appropriate countermeasures:

Cyber Inspection: Detect security events

- Online view and report on the on-site cyber situation (daily updates)
- In case of a classified event/alarm, a ticket is immediately opened and processed by the REC Cybersecurity Hotline

Cyber Hotline: Process events and classify incidents

- Fast remote support, e.g., in case of suspicious log entries/processes/access behavior, incidents caused by users, and also in case of Omnivise T3000 cybersecurity malfunctions

Incident Response: Analyze cyber incidents and initiate countermeasures

- In-depth analysis and remediation of a classified cyber incident
- Assistance with further mitigation and elimination of the cyber incident (via common Remote Service Platform or on-site)

©Foto: Wien Energie/ Ludwig Schedl

“The REC Cybersecurity team fully convinced us that their offering optimally complements Wien Energie‘s existing processes.”

Philipp Lellek,
OT Cybersecurity Expert,
Wien Energie GmbH

Published by and copyright © 2022
Siemens Energy Global GmbH & Co. KG
Otto-Hahn-Ring 6
81739 Munich, Germany

For more information, please visit our website:
www.siemens-energy.com/i&c-service