Utility Cybersecurity: Recommended Practices by OMICRON and DNV

1 hour | English | # rWcyb09en

With power grids gradually becoming software intensive and digitally connected, their exposure to cyber threats has increased, putting key assets and the operations of an organization at risk. At the same time, the sophistication of cyber-attacks is rising.

In this joint webinar recording, speakers from DNV and OMICRON present their insights about recommended practices for ensuring the cybersecurity of OT-networks in utilities and for ensuring efficient detection and response processes. The key for securing the power grid is that IT security officers and power engineers work together to implement security measures while still allowing efficient maintenance and operation of the grid.

Objectives

> Understanding best practices to secure the networks in control centers, power plants and substations
> Selecting the right countermeasures and preventive actions to take
> Learn why it is important that power engineers and IT security officers work together to secure the grid
> Identifying why intrusion detection in power utility automation networks is key for minimizing the consequences of cyber-attacks

Content

Bas Kruimer, Business Director Digital Grid Operations, DNV

> Utility Cybersecurity – People – Processes – Technology
> The journey to implement cybersecurity in the utility OT environment
> Recommended practices and examples

Andreas Klien, Power Grid Cybersecurity Expert, OMICRON

> Why do I need to monitor for cyber intrusions in power grid OT-networks?
> Common issues when applying IDS in control centers, power plants and substations
> Recommendations on how power engineers and IT officers can efficiently work together in OT security processes

Solutions

StationGuard: intrusion detection tailor-made for the power grid

Audience

OT and IT security officers in utilities

Prerequisites

Basic knowledge about OT security

Join our training courses and get registered on www.omicron.academy

OMICRON Academy