Radiflow

Use Case

Cybersecurity for Renewable Energy Production Plants

With the migration to renewable energy sources on the rise, their role in the overall national power supply has become critical. As such, their automation (SCADA, IIoT) systems have become a primary target for hackers, including well-funded state-sponsored hacker groups.

Renewable power plants are usually located in remote, isolated areas, and they tend to have a complex composition of stakeholders, including the plant owner who usually manages several sites, the system integrator in charge of ongoing operation and maintenance, and the power utility that purchases the electricity.

Adding to the complexity is the interconnectedness of DER (distributed energy resources) grids, which introduce network risk to renewable energy plants from across the entire distribution system.

In addition, renewable energy operators are subject to a host of security and environmental regulations. It's not surprising, then, that despite the technological advances and innovation, renewable energy operators have yet implemented adequate OT network protection and risk mitigation measures.

The Challenges of Securing Renewable Energy Plants

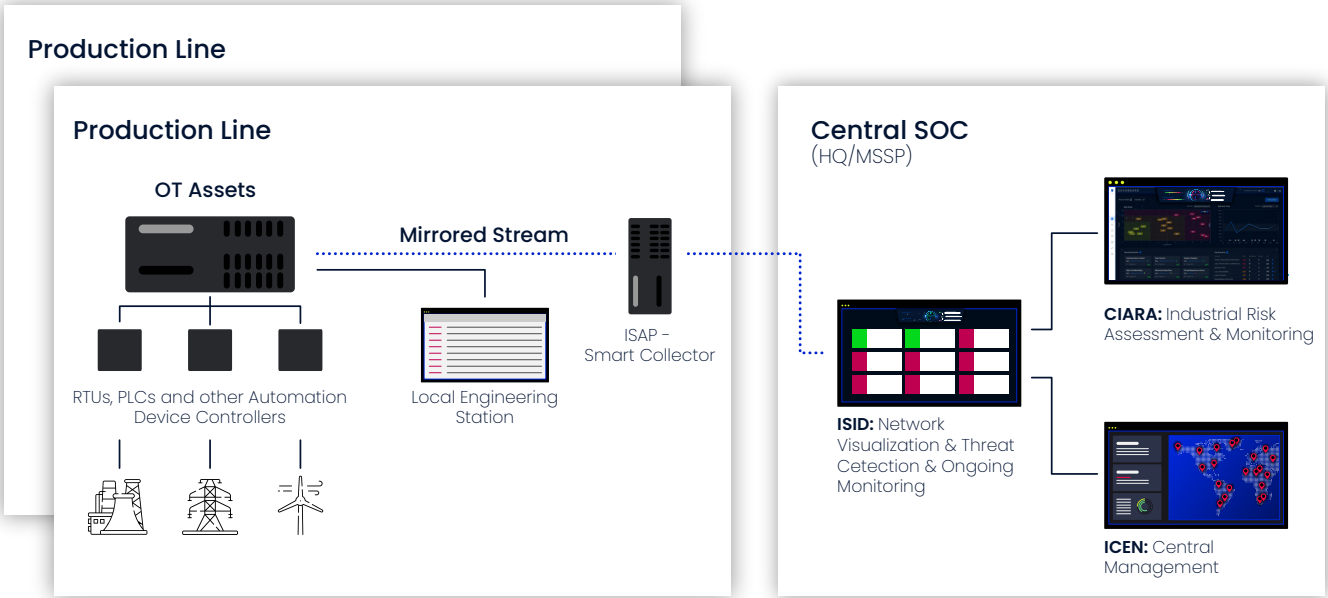
Renewable power facilities face operational scenarios that are not only complex but also the cause of multiple vulnerabilities, due to the sheer number of components. These complexities are multiplied by the addition of IT/OT connectivity, which exists to streamline processes, but also complicates the cybersecurity element.

Also, the dispersed nature of renewable energy networks makes “inside job” easier and requires sending large volumes of network data from remote locations to a central SOC for analysis. Another challenge is the danger of politically-motivated malicious attacks. As with conventional energy facilities, renewable energy facilities may be targeted as part of global cyberwarfare, on top of profit-motivated hackers

Creating a Comprehensive Cyber Security Solution for Distributed Renewable Power Plants

Securing any energy facility must be a high priority, and the constant increase in demand for renewable energy sources means that it is essential for the ICS to take into account the specific challenges and needs of renewable energy facilities.

1. Network modeling and visibility: this stage involves creating a model of the renewable energy facility's complete network, including topology, device properties, state, vulnerabilities, and potential inter-zone attack vectors; protocols and ports, etc. The result is a virtual model which can be used for OT-BAS (breach and attack simulations), as well as providing complete network visibility.
2. Risk assessment: this stage includes simulating relevant breach attempts using the virtual model to provide an accurate risk-assessment of the entire network.
3. Implementation: The simulation data enables generating an ROI-optimized OT security plan matching the user's security preferences and budget constraints, and provides the user with key indicators and reports for the network's risk state. The user is presented with a prioritized list of mitigation measures toward strengthening and optimizing OT security, in accordance with IEC62443.
4. Long-term security management: The facility's OT network is not static, and the security system takes this into consideration, allowing for the addition of new components and updated software. The key to long-term system security is ICS network monitoring, which provides constant identification and mitigation of breaches as well as changes in the risk posture due to newly evolved threats. which provides constant identification and mitigation of intrusions as well as changes in the risk posture due to new threats.



Radiflow Solutions for Renewable Energy and Power Plants

Radiflow offers a range of cybersecurity solutions which have been designed especially for OT systems. Even the complexities of securing a remote renewable energy plant can be undertaken with Radiflow's innovative threat detection and risk-assessment systems:

- **MAP (VISUALIZE)** - Radiflow's iSID, industrial threat detection and monitoring system, generates a visual model of the entire facility network including assets, connections, protocols, and vulnerabilities.
- **KNOW** - Radiflow's CIARA industrial risk assessment and management platform uses the iSID data along with MITRE ATT&CK and other resources to thoroughly understand which threat actors and attack tactics are most relevant for testing. By using non-intrusive threat intelligence-based breach and attack simulations it is possible to assess the effectiveness of corresponding mitigation measures (IEC62443-compatible).
- **ACT** - Prepare and implement a security roadmap based on the organization's long-and short-term security preferences (e.g. strengthening a single business unit vs. reducing overall risk) as well as budgetary constraints.
- **MONITOR** - Detect abnormal behavior indicating breach attempts and changes to various components and continuously monitor the network at the corporate SOC or offsite. Designed especially for OT, Radiflow's solutions support all relevant OT protocols (e.g. BACnet, Profibus) for accurate modeling and anomaly detection (new devices, topology changes, abnormal memory access, and firmware changes) as well as ethernet and serial interfaces for modern and legacy devices.

About

Radiflow develops unique OT cybersecurity tools to protect and ensure organizations' digital

resilience. The company closely collaborates with Managed Security Service Providers to oversee the discovery and management of all relevant data security points. Founded in 2009, Radiflow has offices and partners in Europe, USA and APAC. Its field-proven solutions are installed at over 6000 sites around the globe.

Radiflow | For more info: **radiflow.com**