Rhebo Profile

360° Cybersecurity for Operational Technology Networks

Rhebo provides dedicated solutions to detect any cyberattacks, manipulation and technical error states within operational technology (OT) networks. This enables Critical Infrastructure and multi-utility infrastructures to holistically secure their industrial automated and remotely controlled OT networks. Rhebo provides 360° cybersecurity solution including OT Risk & Maturity Assessments, Next Generation OT Intrusion Detection and Managed Protection services. Its next generation Intrusion Detection System (IDS) combines OT monitoring, intrusion and threat detection to identify and report known and unknown attack patterns otherwise overlooked by classic firewalls and IDS (see MITRE ATT&CK ICS matrix below). This includes, amongst others:

- **novel attack frameworks** (e.g., exploiting zero-day vulnerabilities);
- **malicious activities via authorized channels** (e.g., remote access points and administrator accounts);
- **changes within the OT and Industrial Control System (ICS)** (e.g., after spillover or successful network penetration. The latter includes network activities, adversaries use to evade detection, persist and escalate access as well as move laterally);
- **industry-specific attacks** (e.g., using industry protocols).

OT security engineers will be immediately informed of any changes in their OT – from the central ICS to edge networks and devices in substations (i.e. transformer substations, renewable energy resources). The Rhebo solution works in a passive and non-disruptive way. It does not actively intervene in the operations so as not to disrupt time-sensitive industrial processes. Those responsible receive all the necessary information on the location and characteristics of the suspicious incident in real time so they can immediately assess and implement appropriate countermeasures.

Rhebo OT Security In Three Steps

		
Step 1	**Step 2**	**Step 3**

OT System Risk & Maturity Assessment	Next Generation OT Intrusion Detection	Managed OT Protection
Objective	**Objective**	**Objective**
Understand the structure and risks of your operational technology and gain full OT visibility	Implement continuous Intrusion & Threat Detection in your OT	Get professional support to mitigate anomalies quickly and to prevent damage
• Identify and document assets and their communication structures within the OT in detail within a few days; • Identify and localize threats, vulnerabilities and error states in the OT network; • Assess risks and threats; • Coordinate mitigation measures.	• Detect, localize and analyze, evaluate and document anomalies in communication behavior in real time; • Define mitigation measures; • Check the effectiveness of security measures (e.g. firewall settings, authorization management or segmentation).	• Use technical, operational support from network experts; • Conduct forensic analysis of critical incidents and coordinate mitigation measures; • Profit from regular cyber event reviews.