



Rhebo Industrial Security & Stability Assessment

Risk & Vulnerability Analysis for OT Networks



ASSET DISCOVERY
FOR OPERATIONAL
TECHNOLOGY



IN-DEPTH
VULNERABILITY AND
RISK DETECTION



DEFINITION
OF MITIGATION
MEASURES



»The audit has given us a clearer picture of all processes in our complex industrial control system. This enabled us to analyze all communication traffic extensively and check the ICS specifically for vulnerabilities.«

Rainer Fuhrmann | Head of I&C | EWR Netz GmbH

The Rhebo Industrial Security & Stability Assessment (RISSA) is an OT-focused cyber risk identification and vulnerability assessment. It enables cybersecurity managers in critical and industrial infrastructure to quickly gain a profound understanding of the OT, and to

target vulnerabilities, security gaps and error conditions. Thus, the Rhebo Industrial Security & Stability Assessment is the easy first step to implement effective OT cybersecurity and a network-based intrusion detection system (NIDS) for OT networks.

What you gain from a Rhebo Industrial Security & Stability Assessment



FULL VISIBILITY IN YOUR OPERATIONAL TECHNOLOGY

including devices, systems, and their connections, protocols, communication and firmware.



AN EFFICIENCY ASSESSMENT OF OF EXISTING SECURITY MEASURES

through identification of security-related communication anomalies.



A CLEAR VIEW ON SECURITY AND STABILITY RISKS FOR YOUR OT

with identification of vulnerabilities, misconfigurations, error states and malicious behavior.



IMMEDIATE ACTIONABILITY FOR ADVANCING OT SECURITY

with the localization of risks and recommendations for mitigation.



THE FOUNDATION FOR DETECTING ATTACKS

through detailed information for baselining the network-based intrusion detection system.



A SOUND BASIS FOR IMPLEMENTING

the requirements of ISO 27001, NIS2 and IEC 62443.

Let's Hunt Vulnerabilities In Your Operational Technology

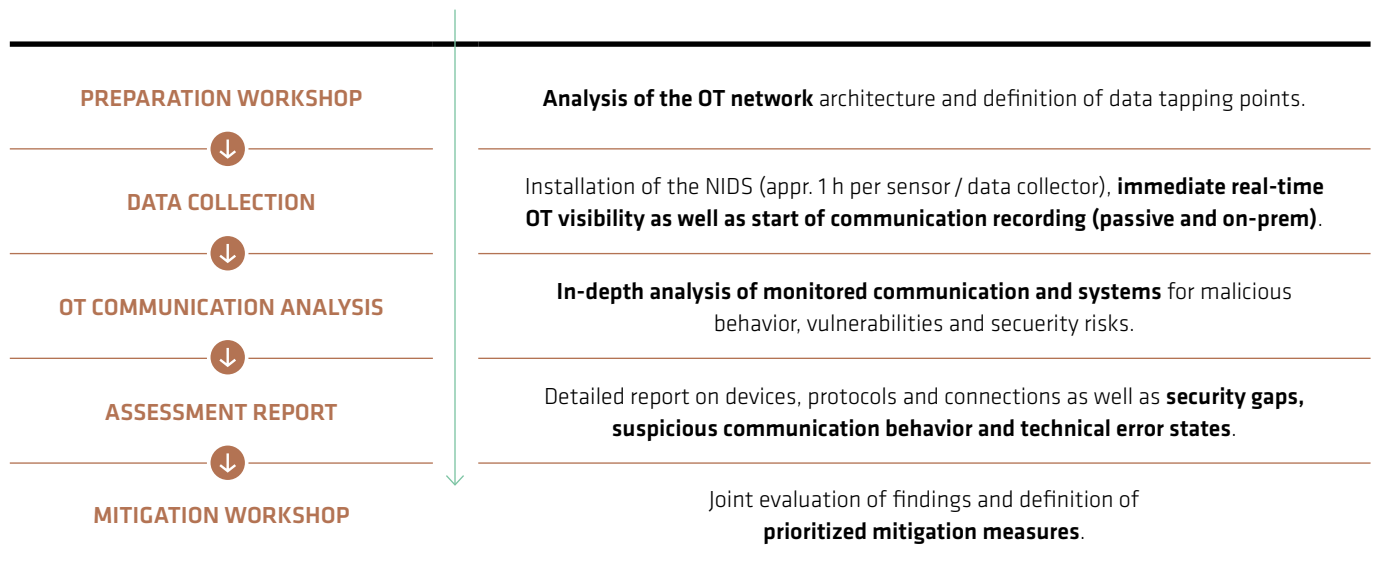
The Rhebo Industrial Security & Stability Assessment is an integral part of any detailed OT risk analysis providing a deep understanding of OT network assets and communication structure as well as its current risk exposure. Utilizing the passive OT monitoring capabilities of the network-based intrusion detection system (NIDS) Rhebo Industrial Protector, all communication within the OT is recorded over a defined period of time, and analyzed by Rhebo OT experts for:

- insecure devices and firmware with known vulnerabilities,
- suspicious, atypical communication behavior,
- insecure connections and communication,
- misconfigurations, technical error states, authentication risks and unwanted internet connection.

The results of the vulnerability and risk analysis include security events and technical error states that can lead to operational disruptions, e.g. in real-time processes and overall plant control. All anomalies are documented, evaluated, and recommendations for mitigation provided. In the concluding workshop, the findings and mitigation measures are discussed with your responsible experts.

The Rhebo Industrial Security & Stability Assessment provides the foundation and crucial information for detailed cyber security risk assessments (e.g. according to international standard IEC 62443-3-2 (ZCR 5)), as well as the baselining of the network-based intrusion detection system (NIDS).

The First Easy Step To OT Security



Bring Visibility To Your OT

www.rhebo.com | sales@rhebo.com | +49 341 3937900



Rhebo OT Security Made Simple

Rhebo provides simple and effective intrusion and anomaly detection Made in Europe for OT networks and IIoT edge devices for critical infrastructure, (multi-)utilities and manufacturing. We support companies with establishing OT security from the initial risk assessment to the operation of the network-based intrusion detection systems,

and forensic analysis of anomalies. As a trustworthy cybersecurity provider, Rhebo is ISO 27001 certified and was awarded the »Cybersecurity Made In Europe« label for its strict data protection and data security policies.

www.rhebo.com