Your Operational Technology. Protected.

Monitoring and responding to threats on your industrial network.

www.tuv.com/informationsecurity

TÜVRheinland®
Precisely Right.

INDUSTRIAL CYBERSECURITY THREAT MONITORING

The trend to digitization and system inter-connectivity means that operational technology engineering and systems personnel may not realize the full extent of cybersecurity vulnerabilities they face. In addition they are often not equipped with suitable tools to detect cyberattack attempts on their industrial security systems. This is compounded by the number of cybersecurity related incidents in operational technology (OT) and industrial control networks that have risen in recent years. So how can OT and industrial networks be monitored in a non-invasive but still effective way to provide targeted and actionable alerts?

EMBRACING THE MONITORING CHALLENGE

Organizations operating industrial facilities have a responsibility to monitor, detect and mitigate cybersecurity attacks in order to maintain the safety, integrity and availability of their plant which, if compromised, may have a severe and detrimental impact on society. Leading cybersecurity standards for industrial control systems emphasize that systems operators should have cybersecurity monitoring solutions in place. TÜV Rheinland has decades of experience in testing and certifying industrial systems and has worked across some of the most challenging industries. Its solutions and services can provide end-to-end visibility, threat detection and continuous vulnerability assessment for OT and industrial cybersecurity risks.

HOW ARE INDUSTRIAL SYSTEMS MONITORED?

TÜV Rheinland has partnered with a leading industrial detection and threat intelligence company to provide an OT threat monitoring capability. The solution can be retro-fitted in any industrial plant, across all sectors and across legacy or modern equipment and protocols. The solution provides non-invasive and passive OT network monitoring so the industrial process remains unaffected. The plant architecture is mapped and then network data tapped and fed to the solution. Our experts will work with you during the installation and setup of the solution to ensure that the correct tooling is in place and the monitored network is suitably architected. Once the solution has been implemented we will offer ongoing management, support and assistance as required.

RESPONDING TO INDUSTRIAL CYBERSECURITY INCIDENTS

TÜV Rheinland has a comprehensive incident response and recovery planning service where the team will develop suitable playbooks using industry best practices, previous experience and frameworks adapted to your business needs. By planning a response, you can demonstrate to regulators, customers and suppliers that you have considered cybersecurity risk to your business and have a realistic plan in place when an incident occurs. In addition a well thought out plan will save money, time and significantly reduce the turmoil associated with unplanned responses.

WORKING WITH TÜV RHEINLAND

The TÜV Rheinland 145+ year heritage gives us a deep understanding of the markets we serve, with unmatched depth of experience solving complex safety, security, data privacy, and infrastructure challenges.

INDUSTRIAL SECURITY RISK ASSESSMENTS Do you understand your operational technology and industrial security risk?	**OT ARCHITECTURE REVIEW** Is your industrial technology design and architecture secure and compliant with cybersecurity standards and regulations?	**OT SYSTEMS PENETRATION TESTING** Do you need to undertake operational technology vulnerability assessments and penetration tests?	**OT SERVICES FOR THE NUCLEAR INDUSTRY** Do you understand your nuclear facility operational technology and industrial security risk?
OT POLICY, PROCESS AND PROCEDURE REVIEW Are your policies, processes and procedures keeping up with the unique cybersecurity and regulatory requirements of industrial and operational technology systems?	**OT SYSTEMS INCIDENT RESPONSE AND RECOVERY** Do you have existing operational technology incident response and recovery plans in place?	**OT SYSTEMS SECURITY MONITORING** Do you know what is happening on your OT network and systems?	**OT SERVICES FOR THE RAIL AND TRANSIT INDUSTRY** Do you understand your overall rail and transit systems operational technology and industrial security risk?

Overview industrial security service portfolio

TÜV Rheinland
Digital Transformation & Cybersecurity
otsecurity@tuv.com

www.tuv.com/en/industrial-sec

TÜVRheinland®
Precisely Right.