



# WÄRTSILÄ ICS SECURITY MONITORING AND RESPONSE

The threat of a cyber attack is one of the most prominent business risks to enterprise information and operation systems. With the rapid digitalisation of the energy industry and increased use of integrated systems and software in power plants, cyber security is becoming critical – not only for data protection, but also for reliable and safe operations. The Wärtsilä ICS security monitoring and response service helps protect your industrial control systems/operational technology (ICS/OT) environment by monitoring security events, detecting anomalies and enabling a proactive response to incidents.



## KEY BENEFITS

- Increase the reliability of your ICS/OT assets to maintain uptime and ensure availability
- Minimise losses from a potential cyber security incident by detecting and responding to anomalies in a proactive manner
- Ensure active monitoring and log collecting
- Enable a solid service level agreement (SLA) for incident response

## ENSURE A PROACTIVE APPROACH TO SECURITY THREATS

All intelligent devices are potential targets for viruses, hacking and other malware attacks. At Wärtsilä, our security approach uses the latest technology and industry best practices aimed at safeguarding all of our products and service operations throughout their lifecycle.

The Wärtsilä ICS security monitoring and response service is integrated with the Wärtsilä monitoring backend. This includes security incident and event management (SIEM) as well as security operations centre (SOC) capabilities for support and response by our skilled cyber security and product experts.

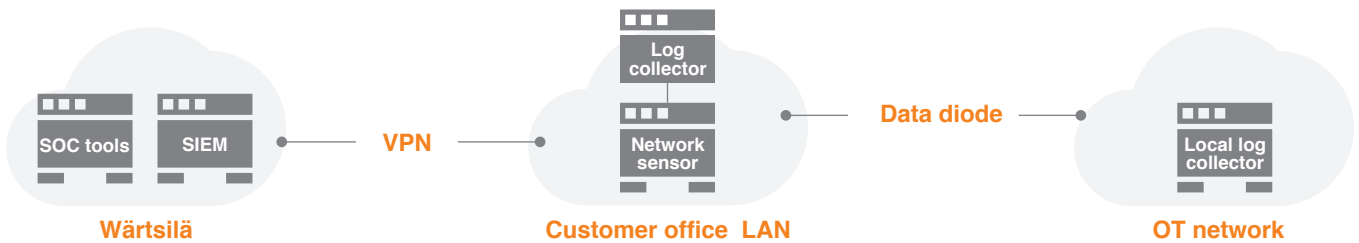
The Wärtsilä ICS security monitoring and response service consists of a log collector, data diode(s) and network

sensor, as well as the SOC for active monitoring and incident response capabilities.

Logs are collected from the OT network to the log collector via secure one-way connections using a data diode whenever applicable. With the network sensor it is possible to implement intrusion detection system/intrusion prevention system (IDS/IPS) and network traffic analysis, for example. The SOC performs active 24/7 monitoring and reacts to any detected anomalies.

## SCOPE OF SUPPLY

The Wärtsilä ICS security monitoring and response service is customised and tailored to fit your installation. The service is currently designed for stationary applications including both Wärtsilä and non-Wärtsilä energy installations.



## WÄRTSILÄ CYBER SERVICES

Wärtsilä Cyber services help you to understand the cyber security status of your operational environment and mitigate identified risks. We use a systematic approach, from assessing your current cyber posture to implementing appropriate cyber controls and lifecycle services.

