## Cyber assessment

Wärtsilä ICS vulnerability assessment

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 marine and energy industries, cyber security is becoming critical not only for data protection, but also for reliable and safe operations. The Wärtsilä ICS vulnerability assessment service helps you to protect your industrial control systems/operational technology (ICS/OT) environment by identifying and validating security vulnerabilities related to external connections and internal systems including applications, operating systems, devices and servers.

Key benefits

- Be the first to discover vulnerabilities in your ICS/OT environment

- Ensure operational availability by obtaining concrete recommendations on how to secure your systems and networks

- Reduce risks related to loss of production, health, safety and environment (HSE), and intellectual property
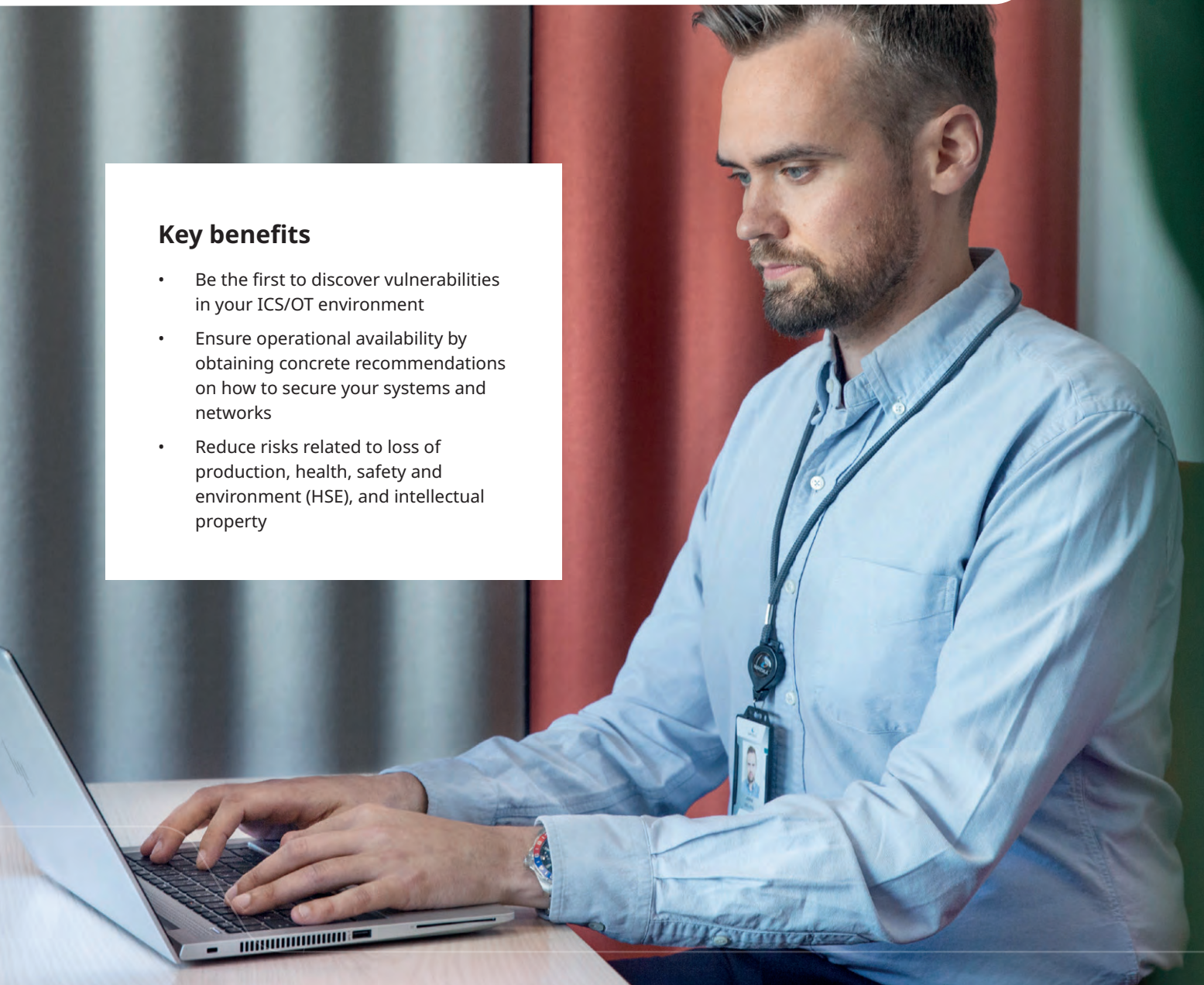
A tailored service based on yor needs

The Wärtsilä ICS vulnerability assessment service is tailor-made to your needs and can be performed by using different methods:

- Configuration review
- External vulnerability examination
- Internal network traffic analysis
- Internal vulnerability examination

All identified vulnerabilities are verified to weed out false positives. Proof of concept code is given and a common vulnerability scoring system (CVSS) is calculated where applicable. The impact of any discovered vulnerabilities is analysed against availability, integrity and confidentiality (the AIC triad).

The vulnerability assessment report describes the conclusions of the findings and their impact on your security posture, as well as listing recommended mitigation measures. After the initial vulnerability assessment, we recommend scheduling a follow-up vulnerability review to ensure that the desired level of cyber security is reached and maintained. After this, annual reviews are suggested to maintain a strong ICS cyber security posture.

Scope of supply

Delivery is always tailored according your needs and environment. Upon agreement, Wärtsilä assigns a security consultant and an ethical hacker who performs the assessment based on selected parts from available industry best practices and ethical hacking methods.

The ICS vulnerability assessment service does not implement the needed changes – these mitigation actions can be provided through other Wärtsilä Cyber services.

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.

Cyber assessment
Assess your current situation and understand where you are in terms of cyber risks, compliance gaps or technical vulnerabilities

Cyber recovery
Maintain resilience with active threat and security monitoring and effective incident response

Cyber resilience

Cyber foundation
Establish the foundation for your cyber risk management by setting up a cyber security management system, governance and policies

Cyber protection
Implement procedural and technical controls and system upgrades to reduce cyber risks