WÄRTSILÄ

ENERGY

WÄRTSILÄ CYBER SERVICES

MANAGING CYBER SECURITY RISKS AT YOUR POWER PLANT

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 the 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 energy operations. It is now more important than ever that power generators have a reliable partner with the right know-how to ensure uninterrupted production and safety.

CYBER SECURITY IN THE ENERGY INDUSTRY

Cyber security is not a single solution to one problem, but a continuous process requiring multiple approaches and solutions. Today's industrial control systems (ICS) interconnect with multiple networks, systems and locations, and have greatly increased operational efficiencies. This development has also introduced cyber security concerns such as unauthorised access and malicious attacks. In addition, an increasing number of new local laws and regional regulations for power plants have come into force.

OUR SOLUTION

Wärtsilä Cyber services help to safeguard your power plants, placing the highest priority on functional safety while also helping you to comply with laws and regulations. Our approach relies on cutting-edge technology and industry best practices to safeguard our products and service operations throughout their lifecycle. We help you to develop the resilience required to defend against and recover from any form of cyber interference.

Wärtsilä Cyber services enable you to understand the current cyber security status of your operational environment and provide actions to mitigate identified cyber risks. Our services are designed to give a systematic 360-degree approach to cyber security risk mitigation, from assessing your current cyber posture to implementing cyber controls and lifecycle services.

All Wärtsilä Cyber services are designed according to best practices and are based on the international IEC 62443 cyber security standard. Our services are also adaptable to regional and local standards and regulations including:

- **NERC CIP**
- **NIST SP 800**
- **NIS DIRECTIVE**
- **AER**
- **HCIS SEC-12 CYBER SECURITY**

WÄRTSILÄ CYBER SERVICES

Maintaining cyber resilience is a continuous process that should never be thought of as completed. Wärtsilä Cyber services consist of four modules that should be continuously applied to increase your cyber defence.

CYBER ASSESSMENT

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

Wärtsilä ICS risk assessment
Identify your critical assets and understand your related cyber maturity level by revealing cyber risks, possible compliance gaps and technical vulnerabilities.

Wärtsilä ICS vulnerability assessment
Protect your industrial control systems (ICS) and operational technology (OT) environment by identifying and validating security vulnerabilities related to external connections and internal systems.

CYBER RECOVERY

Maintain resilience with active threat and security monitoring and effective incident response procedures. As an original equipment manufacturer (OEM) and service provider, we are the right partner for designing a cost effective and efficient orchestration of incident response through our PSIRT (product security incident response team) and global service networks.

Wärtsilä ICS security monitoring and response
Protect your ICS/OT environment by monitoring security events, detecting anomalies and enabling a proactive response to incidents.

CYBER FOUNDATION

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

Wärtsilä ICS security foundation
Establish or improve your ICS cyber security setup by finding the set of policies, standards, industry best practices and rules that best serve your overall risk management strategy.

CYBER PROTECTION

Implement procedural and technical controls and system upgrades to reduce cyber risks.

Wärtsilä ICS patching
Ensure that your installations are always equipped with the latest security updates to protect against cyber threats and to comply with regulations.

Wärtsilä ICS application whitelisting
Protect your systems from malware and other malicious programs with this easy-to-deploy solution that is a cost-effective way to improve your overall risk management.

WHY CHOOSE WÄRTSILÄ?

As an OEM and service provider we have a thorough understanding of the power plant systems and equipment that require securing. We can provide complete lifecycle support to mitigate cyber security risks along with a wide global service network of skilled service engineers, central cyber security experts and strategic partnerships.

Wärtsilä Cyber services are suitable for all Wärtsilä energy customers. Delivery is always tailored according to your specific needs and situation, but we recommend starting with a cyber assessment to define your current situation and identify what steps are needed to effectively mitigate your cyber risks. Our lifecycle services (Wärtsilä ICS patching service & Wärtsilä ICS security monitoring and response service) have been developed as a seamless and cost effective solution for Wärtsilä power plants.

YOUR BENEFITS

- **Identify your cyber risks and understand the actions needed to mitigate them**
- **Maintain an auditable and managed program to control your cyber security threats**
- **Ensure preventative protection of your installation against cyber risks and safeguard products and service operations throughout their lifecycle**
- **Recover quickly and maintain resilience to ensure maximum operational uptime and availability while increasing the reliability of your ICS assets**