voith.com

VOITH

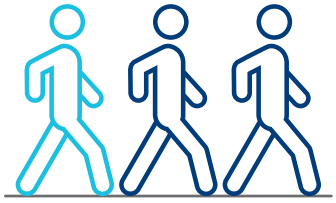
Embark on a journey to secure your operations

Voith cyber security assessments

The cyber security journey – a structured approach to protection

- Stage 1: understand the current situation
- Stage 2: secure operations
- Stage 3: continuous improvement

At Voith, we invite our customers to join us on a comprehensive cyber security journey designed to secure their operations and protect valuable assets from cyber threats. This journey is structured into three critical stages: Understanding the Current Situation, Securing Operations, and Continuous Improvement. Each stage is tailored to our customers' unique needs, providing clear deliverables that guide the path forward.



Stage 1
Understand the current situation

The journey begins with a thorough understanding of your current cyber security landscape. This initial stage focuses on conducting a comprehensive cyber security risk assessment in compliance with IEC 62443-3-2 standards. Key activities include:

- Risk assessment: Conducting a detailed evaluation of potential cyber security threats and vulnerabilities.
- Systems and network architecture analysis: Reviewing the design and layout of your systems and networks to identify potential weaknesses.
- Systems configuration analysis: Examining the configuration of your systems to ensure they meet security best practices.

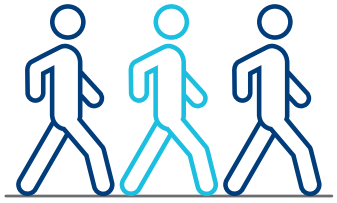
Deliverables for stage 1

- Risk assessment report: A detailed document outlining identified risks and vulnerabilities.
- Architecture analysis summary: Insights into the strengths and weaknesses of your current architecture.
- Configuration analysis findings: Recommendations for configuration improvements.

These deliverables are crucial for transitioning to the next stage, ensuring a structured and effective approach to enhancing cyber security.

Join the cyber security journey with Voith

By joining Voith on this structured cyber security journey, you ensure a comprehensive approach to protecting your digital assets. Each stage of the process builds upon the previous one, ensuring that your operations remain secure and resilient against cyber threats.



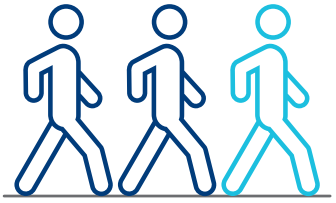
Stage 2 Secure operations

Building on the insights gained in the first stage, we move to securing your operations. This stage involves implementing tailored security solutions designed to address identified vulnerabilities and protect your systems from threats.

- Implementation of security measures: Deploying solutions that enhance the security of your operations.
- Integration with existing processes: Ensuring new security measures work seamlessly with your current operations.

Deliverables for stage 2

- Security implementation plan: A customized roadmap for deploying security solutions.
- Operational integration strategy: Guidelines for integrating security measures with existing processes.



Stage 3 Continuous improvement

Cyber security is an ongoing process. The final stage focuses on continuous improvement, ensuring your systems adapt to evolving threats and maintain a high level of security.

- Regular monitoring and updates: Keeping your systems secure with ongoing assessments and improvements.
- Adaptive security strategies: Modifying security measures to counteract new threats.

Deliverables for stage 3

- Continuous improvement plan: A framework for regular security evaluations and updates.
- Adaptive strategy recommendations: Suggestions for evolving your security posture.

Voith Group
St. Poeltener Str. 43
89522 Heidenheim
Germany

www.voith.com/paper

Contact:
Phone +49 7321 37-0
cybersecurity.paper@voith.com