



SIEMENS CYBERSECURITY SERVICES

Cybersecurity Assessments

Identify hidden vulnerabilities, strengthen defense, and align security with business goals.

Our Cybersecurity Assessment in compliance with ISA/IEC 62443 uncovers risks before they escalate, enabling proactive protection, compliance and resilient operations.

Request
now

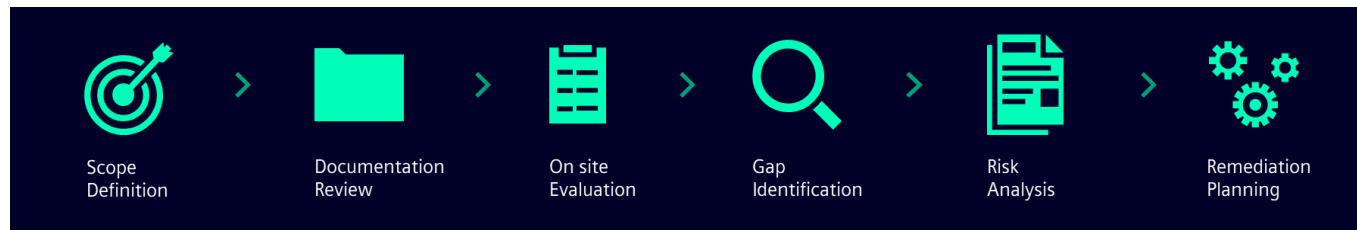


SIEMENS

SMART INFRASTRUCTURE – CYBERSECURITY ASSESSMENTS

Identify your gaps, strengthen your cyber defense posture

Protecting critical assets begins with understanding your cybersecurity posture and identifying vulnerabilities. Our Cybersecurity Assessment Service uncovers vulnerabilities, evaluates risks, and aligns security practices with standards such as ISA/IEC 62443. Fully customizable from high-level executive overview to detailed technical analysis, it delivers actionable recommendations, prioritizes improvements, and provides a strategic roadmap to enhance resilience, strengthen defense, and ensure compliance across your organization.



Our service scope

1. IEC 62443 Maturity Assessment

- Evaluate the maturity of your organization's OT cybersecurity in terms of governance, procedures and organizational & technical controls.
- Measures current practices against IEC 62443-2-1 and IEC 62443-3-3, perform gap analysis and produce mitigation recommendation.

Optional Add-On: Mapping local standards

2. Vulnerability Assessment & Penetration Testing

Evaluate your OT infrastructure to uncover vulnerabilities and test defenses through real-world penetration scenarios.

3. Threat and Risk Assessment (TRA)

Assess your exposure to potential threats, determine risk levels, prioritize vulnerabilities and map actionable mitigation measures to strengthen overall resilience.

Your benefits

- **Enhanced Security Posture:** Identify and mitigate system gaps and vulnerabilities for a robust defense.
- **Regulatory Compliance:** Align seamlessly with industry standards and security frameworks.
- **Proactive Risk Mitigation:** Evaluate threats and prioritize remediation with focus on critical assets.
- **Operational Efficiency:** Optimize resources and reduce costs through targeted, risk-based actions.
- **Informed Decision-Making:** Gain actionable insights for strategic cybersecurity planning.
- **Peace of Mind:** Enhance trust among key stakeholders and resilience with transparent, proactive security measures.

Published by Siemens AG

Smart Infrastructure
Electrification & Automation
Mozartstraße 31C
91052 Erlangen, Germany

For the U.S. published by Siemens Industry Inc.

3617 Parkway Lane
Peachtree Corners, GA 30092
United States

For more information, please contact Customer Support: [siemens.com/energy-automation-support-contact](https://www.siemens.com/energy-automation-support-contact)

© Siemens AG 2026.

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification during further development of the products and services. The requested services are binding only when they are expressly agreed upon in the concluded contract.

Unrestricted | © Siemens 2026