Security Assessments

Product Details

SIEMENS

Plant-specific security roadmap
with Security Assessments

Operators of production facilities these days cannot afford to do without effective security measures. Industrial cybersecurity capacities are rarely available and there is time pressure due to new compliance requirements and laws such as the NIS 2 Directive or CRA.

Security Assessments provide a complete overview of the actual state of security of your automation systems.

Solution and Service

Security Assessments cover a holistic analysis of threats and vulnerabilities, the identification of risks & recommendations to close the identified gaps.

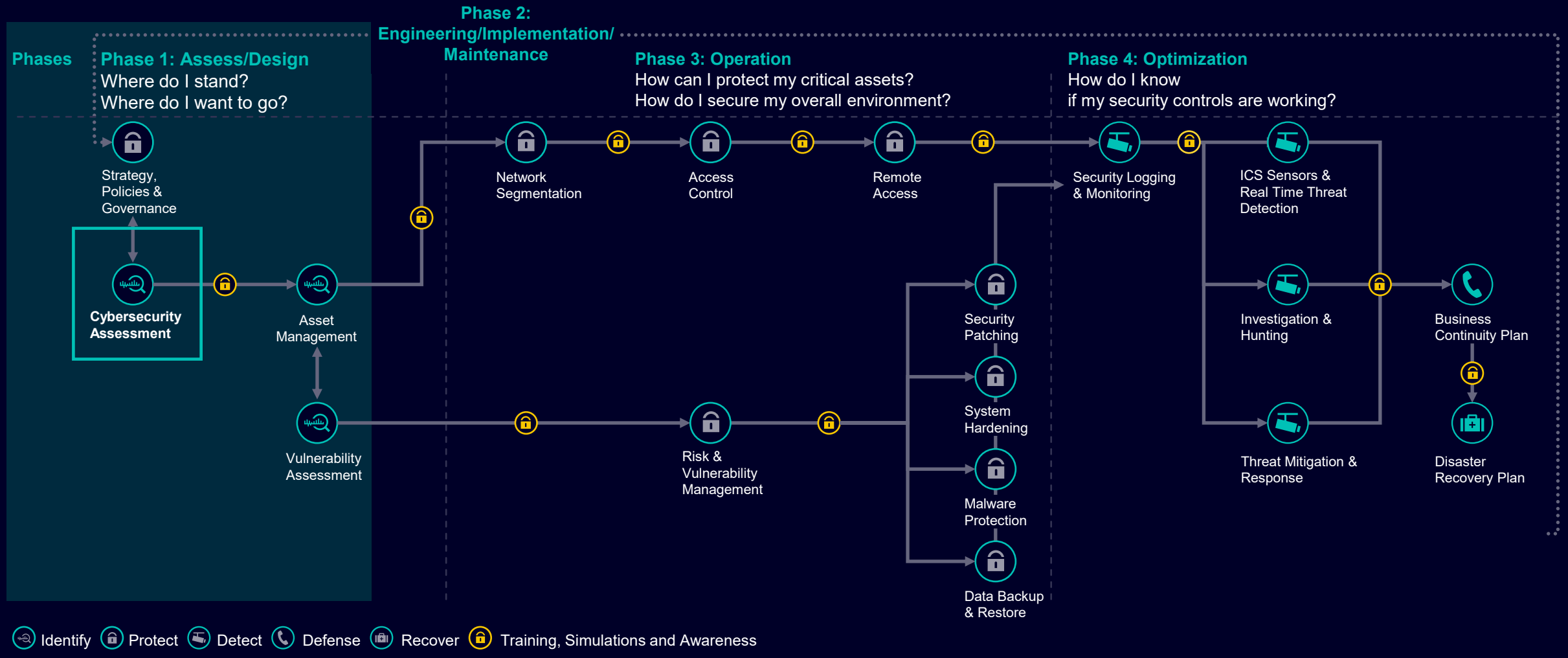
Would you like to have a deep **assessment** based on IEC62443 standard **for Industrial Control Systems?**	→ IEC 62443/NIS 2 Assessment
Do you prefer a **compact one-day on-site assessment?**	→ Industrial Security Workshop
How are you preparing for your machine's market access in light of the CRA?	→ CRA Readiness Assessment
Do you need to get an comprehensive picture tailored to your key risks & operational threats?	→ Industrial Risk Assessment

Your value

- Evaluation of the current security status
- Plant-specific and risk-based security roadmap
- Basis for transparent cost estimates

SIEMENS

Security Assessments as a first step



SIEMENS

Where to start with industrial security?

Operative challenges

- Challenges for the plant IT administrator:
  Needs help to identify measures and get the gaps closed in a professional and efficient way.
- Challenges for the plant manager:
  - What is the potential impact of the current security posture?
  - What are the improvement potential areas?
  - How can a high security level be continuously kept up over the time?
  - There is a significant growth of compliance requirements on security in industrial environments as well as laws which aim to protect critical infrastructures (e.g. NIS 2 – see on the next slide). Are we affected? What factors should we be aware of?
- Industrial cybersecurity capacities are rarely available and there is time pressure due to new compliance requirements and laws such as the NIS 2 Directive.

Operators of production facilities these days cannot afford to do without effective security measures that prevent cyber attacks and misconduct. But where should the priorities lie?

Required solution/Possible consequences

Provide transparency about threat landscape and the plant-specific security status

Identify risks and recommend solutions to close the identified gaps in compliance with standards and requirements

Define priorities for the most effective security solution within the available budget

SIEMENS

Cybersecurity legislation from the EU – addressing the entire supply chain

	EU - NIS2 Directive (Network and Information Systems)	**EU - Machine Regulation** (Regulation 2023/1230)	**EU - Cyber Resilience Act** (CRA Law)
Primary target group 	Operating End Customer	OEMs, Machine builders	Manufacturer of “products with digital elements” e.g., OEMs
Main Focus 	Cybersecurity risk management and incident reporting	Safety, Cybersecurity and AI	Cybersecurity for the entire lifecycle of such products (CE marking)
In force by 	Oct 18, 2024	January 20, 2027	Reporting obligations: Q3/26 Full obligations: Q4/27

time

SIEMENS

Identify and evaluate risks – for a comprehensive security roadmap
with Security Assessments

Solution and Service

- Security Assessments cover a holistic analysis of threats and vulnerabilities, the identification of risks and the development of a security roadmap with recommendations to close the identified gaps by experts with know-how in automation, digitalization and cybersecurity.
- They maximize transparency and provide a complete overview of the actual state of security of your automation systems.
- This approach is ideal for identifying the necessary action to be taken in the area of industrial security and to implement the right measures for eliminating possible security vulnerabilities.

Deep OT **assessment** checking your current security level and giving a NIS2 check, all based on the IEC62243 norm	→ IEC 62443/NIS 2 Assessment
A focused and flexible **compact one-day, on-site,** IEC62243 based **security workshop**	→ Industrial Security Workshop
CRA readiness assessment to identify how to close security gaps of your machine regarding IEC62443 to ensure seamless market access	→ CRA Readiness Assessment
The risk assessment as a two-day onsite workshop to gain a comprehensive picture tailored to your key operational threats	→ Industrial Risk Assessment

SIEMENS

Security Assessments - Overview

	Risk Assessment (New)	CRA Readiness Assessment (New)	IEC 62443 Assessment /NIS2	Industrial Security Workshop (Updated)
Scope	• System operator • Machine builder	• Machine builder	• System operator • Machine builder	• System operator • Machine builder
Focus	• Threats, likelihood & impact • Risk calculation • SL-T definition	• CRA readiness gaps • Workshop on possible solutions	• Full gap analysis • SL-T vs. SL-A • Compliance mapping (NIS2)	• Basic gap analysis • Basic requirements
Reference	• IEC 62443 Risk Methodology	• Full IEC 62443-4-2 • Cyber Resilience Act	• Full IEC 62443-3-3 • Full ISO 27001 • NIS2 (optional)	• Baseline IEC 62443-3-3 • Baseline ISO 27001
Team	• 2 Assessors	• 2 Assessors	• 2 Assessors	• One Assessor • 2nd Assessor optional
Onsite	• 2 days	• 2 days	• 2 days	• One day
Report	• Risk register with heatmap	• Full report with roadmap	• Full report with roadmap	• Focused report with primary actions

SIEMENS

Security Assessments - Comparison

		Industrial Security Workshop	IEC 62443 Assessment / NIS 2	CRA Readiness Assessment	Industrial Risk Assessment	Cybersecurity-Consulting	Information Security Management System (ISMS, CSMS)*
System Operators	Technical requirements (IEC 62443-3-3)	○	●●			●	
	Organizational requirements (IEC 62443-2-1, ISO 27001)	○	●●			●	●●
	NIS 2 (Network and Information Security Directive 2) (Mapped on basis of the ISO 27001)	○	●			●	
	Risk assessment and system design (IEC 62443-3-2)				●●	●	
	Security Management System					●	●●
Machine Builder	Technical requirements (IEC 62443-4-2)	○		●●		●	
	Organizational requirements (Secure Product Development Lifecycle Requirements IEC 62443-4-1)	○		○		●	
	CRA (Cyber Resilience Act) (Requirements on basis of IEC62443)	○		●●		●	
	Risk assessment and system design (IEC 62443-3-2)			○	●●	●	

●● Comprehensive ● Core ○ Foundational

* on project basis

SIEMENS

Why should you choose Security Assessments?

Evaluation

of the **current security status**
based on IEC 62443

Security roadmap

plant-specific and risk-based

Transparent cost estimates

based on this solution

SIEMENS

Siemens is your reliable partner to drive secure digitalization

We are the automation experts with specific industry know-how

We drive digitalization

We understand industrial security

We offer state-of-the-art technology and end-to-end services from a single source

Our processes and products are proven and certified

"We make sure that you can focus on your core business."

SIEMENS

Port of Antwerp, Belgium
Clear OT cyber security roadmap thanks to IEC 62443 Assessment

Port of Antwerp

The Port of Antwerp plays an important public role in Belgium by managing and maintaining the second largest port in Europe, causing more than 1,500 direct and more than 140,000 indirect jobs. The port is realizing 4.8 % of Belgian's Gross Domestic Product (GDP).

Customer objectives

- As part of good cybersecurity governance, having a clear overview of the maturity of your IT and OT environment is paramount.

Solution and Service

IEC 62443 Assessment

- Siemens mapped the OT systems of Port of Antwerp on the IEC 62443 standard to have a good understanding of the as-is situation.
- Afterwards, Siemens provided clear guidance on how to achieve a higher security level in the form of a very detailed and tangible roadmap.

Customer benefits

- Siemens provided Port of Antwerp a clear OT cybersecurity roadmap.
- A synergy was found between the knowledge/experience available within Port of Antwerp' internal IT/OT cybersecurity teams and Siemens' expertise in IEC 62443.

Siemens References ID: 23642

"As CISO, I'm responsible for both IT and OT cybersecurity. Having a clear understanding of the challenges specific for OT is very important. Siemens helped us by providing a clear analysis of the current situation, as well as defining a roadmap to mitigate the risks."

Yannick Herrebaut, CISO at Port of Antwerp

SIEMENS

Maysun Corporation – machinery manufacture Fuji City, Shizuoka Japan

Implentation OT security know how with Security Assessments solution to comply EU Cyber Resilience Act (CRA)

Maysun Corporation

Siemens conduct cybersecurity assessments to ensure compliance with the European Cyber Resilience Act (CRA) for machinery and equipment of Maysun Corporation in Fuji City, Shizuoka

Customer objectives

Customer has identified security gaps in current product design and consulted with Siemens to support with the solution :

- Prepare for CRA compliance to maintain EU market access
- Understand IEC62443 as a practical framework in absence of clear CRA guidance
- Identify cybersecurity gaps in current product design
- Get external input due to limited in-house OT security expertise
- Define next steps for product improvement and regulatory alignment

Solution and Service

Siemens offer Plant Security with Security Assessment services :

- Introduce IEC62443 and show its alignment with CRA technical requirements
- Hands-on assessment to identify current maturity and provide concrete improvement actions
- Combined expertise: Siemens offers both OT security know-how and relevant product solutions
- A single partner for both strategic guidance and technical implementation

Customer benefits

- Early orientation in a complex and evolving regulatory landscape
- Actionable roadmap based on the well-recognized industry standards IEC62443
- Internal awareness raised across engineering, quality and product teams
- Trusted support from a partner with both expertise and technology offering

Siemens References ID: 43862

“Thanks to the support of OT security professionals, we have made substantial progress in our CRA initiatives”

Haruo Yokoshizawa – Maysun Corporation

SIEMENS

You want to find out **more**?

Security Assessments

Siemens Contact Database

SIEMENS

Disclaimer

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 in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

SIEMENS

Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g., firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/cybersecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under https://www.siemens.com/cybersecurity.

SIEMENS