SIEMENS
Ingenuity for life

Transparency for the best possible security

Identify and evaluate risks – for a comprehensive security road map with Assess Security

siemens.com/plant-security-services

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 in order to implement the most effective security solution within the available budget?

Assess Security from Siemens takes a close look at all aspects of IT security in production facilities. It can focus on compliance with the relevant standards, such as IEC 62443 and ISO 27001, or examine the best possible use of certain Siemens products.

The assessments 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.

"Assess Security suggests very precise optimization measures. It assists us in assessing and prioritizing the costs and benefits of each individual activity. The assessment has been entirely worthwhile."

Alojz Ivicic, responsible for the maintenance and upkeep of automation systems at Kreiswerke Grevenbroich

Benefits

- **Identifies and assesses risks in the categories of technology, system and network architecture as well as employees**
- **Recommends and prioritizes suitable security measures**
- **Basis for transparent cost estimates**

Assess Security at a glance

All security assessments cover aspects such as network architecture, data flows, production systems and processes as well as employees. An assessment of this type has a conceivably simple and clearly structured workflow. For this purpose, the Siemens specialists have developed both data acquisition programs and various questionnaires, which they process together with managers from relevant departments such as Production, Maintenance, Planning and Security.

The results make the areas immediately apparent where there is more or less urgent need for action.

The final report that Siemens subsequently prepares contains specific proposals and concepts, tailored to the specific divisions under review for the purpose of gradually improving industrial security.

Identifying security vulnerabilities according to IEC 62443

IEC 62443 is the leading series of standards for security in the automation environment. Generally valid, universal solutions for protecting production facilities and automation systems are described in IEC 62443.

- Question-based evaluation of the security status according to the requirements of IEC 62443
- For automation systems from Siemens based on Totally Integrated Automation and systems from third-party suppliers
- Report with recommendations for eliminating the identified security vulnerabilities

Identifying security vulnerabilities according to ISO 27001

ISO 27001 is a leading stand that covers the requirements of information security management systems.

- Question-based evaluation of the security status according to the requirements of ISO 27001
- For automation systems from Siemens based on Totally Integrated Automation and systems from third-party suppliers
- Report with recommendations for eliminating the identified security vulnerabilities

Checking the security configuration according to the security concept for SIMATIC PCS 7 and WinCC

The SIMATIC PCS 7 & WinCC security concept contains recommendations for security activities based on the state of the art, leading standards and the characteristics of the products used

- Question-based evaluation of the security status according to the SIMATIC PCS 7 & WinCC security concept
- Specifically for SIMATIC PCS 7 & WinCC environments
- Report with recommendations for eliminating the identified security vulnerabilities

Comprehensive identification and evaluation of threats and vulnerabilities

The relevant threats are first selected in this assessment. This is followed by a search for possible vulnerabilities in order to identify, classify and evaluate risks on this basis.

- Tool-supported acquisition or collection of security-related data from automation systems
- Risk classification and evaluation according to the Common Vulnerability Scoring System (CVSS)
- Basis for a risk-based, plant-specific security road map

About Siemens Plant Security Services

Siemens Plant Security Services offer complete protection against cyber-threats, based on the three clusters of Assess, Manage and Implement. Industrial enterprises benefit from Siemens Plant Security in multiple ways: A global network of automation and cyber-security experts makes its in-depth knowledge available to you for your individual production infrastructure.

Siemens AG
Digital Factory
P.O. Box 48 48
90026 Nuremberg
Germany

Article No.: DFPL-B10031-00-7600
Printed in Deutschland | fb 7185

siemens.com/plant-security-services