SIEMENS

Ingenuity for life

Protecting productivity with Industrial Security Services

Identify vulnerabilities and threats at an early stage. Take proactive measures. Achieve optimal long-term plant protection.

usa.siemens.com/industrialsecurityservices

Comprehensive protection from cyber attacks

Industry-specific and scalable: the optimum protection level for your plants

Quickly growing and continuously new security risks and cyber threats necessitate fast reactions. Production processes in particular are always offering new areas for attacks and therefore require an especially high level of protection. With Siemens Industrial Security Services, companies benefit from comprehensive expertise as well as the specialist skills and knowledge of a global network of experts for automation and cybersecurity.

The comprehensive approach of a customer-specific concept is based on modern technology and thus fulfills the currently applicable security codes and standards. Threats or malware are detected at an early stage, the weaknesses are analyzed in detail and suitable security measures are immediately implemented.

The scalable offer includes comprehensive consulting, technical implementation and continuous service. The portfolio is available for existing Siemens automation technique as well as for components from third-party providers.

Long-term protection for industrial plants: transparency through monitoring and analysis

Surveillance of the overall security health of your production allows early definition of actions necessary to mitigate the potential risk of becoming a cyberattack victim. No matter what industry is involved, a plant-specific security roadmap ensures the best possible security level with a significantly reduced risk.

Continuous monitoring provides plant operators with the greatest possible transparency for the security of their industrial plants, ensuring especially good investment protection at all times. The powerful integral Global Threat Intelligence databases analyze and detect newly developing threats. The corresponding adjustments are made immediately and continuously. Changing threat situations are met with adjustments before threats can develop. The industry-specific, comprehensive and modular portfolio provides security features that are engineered, customized and tailored to your budget.

Industrial corporations trust Siemens Industrial Security Services, whose transparent overview of security status enables plant operators to concentrate on their core business at all times. The sensitive topic of cybersecurity for your production systems belongs in the hands of experienced professionals with world-class automation expertise: Siemens Industrial Security Services.

Assess Security for a risk-based security roadmap

Assess Security includes comprehensive threat analysis, identification of risks and recommendations of security measures to reach your target security level.

Your benefit:

A plant-specific and risk-based security roadmap ensures a comprehensive and consistent security level.

Industrial Security Assessment

- **Based on Siemens Defense-in-Depth concept**
- **Complies with IEC 62443 standards**
- **Analysis derived from Siemens Industrial Security expertise**
- **Compact one-day on-site Assessment**

IEC 62443 Assessment

- **Complies with IEC 62443 standards**
- **Available for plants from Siemens and third-party providers**
- **Inquiry-based**
- **Recommendations for risk mitigation (report of up to 30 pages)**

ISO 27001 Assessment

- **Complies with ISO 27001 standards**
- **Available for plants from Siemens and third-party providers**
- **Inquiry-based**
- **Recommendations for risk mitigation (report of up to 30 pages)**

Risk & Vulnerability Assessment

- **Data-based analysis of threats, weaknesses and gaps**
- **Risk classification and evaluation of system criticality results**
- **Recommendation of risk mitigation measures (report of over 100 pages)**
- **Basis for a risk-based, plant-specific security roadmap**

Implement Security for the steps to minimize your risks

Implement Security provides the implementation of protection measures to improve the security level of plants and production facilities.

Your benefit:

Prevention of security gaps and better protection against cyber threats thanks to technical and organizational measures.

Security Awareness Training

- Web-based SITRAIN training
- Establishment of security awareness among plant personnel: including the current situation and handling of threats, risks and the detection of security incidents

Industrial Security Consulting

- Customer-designed advice to cybersecurity processes and guidelines in the production
- Consulting for the design of automation networks

Automation Firewall

- Automation Firewall classic, based on SecureGUARD Firewalls (PCS7 tested)
- Automation Firewall-NG, based on Palo Alto Firewalls with next-generation functionality (esp. deep-package inspection)
- Configuration and testing of plant perimeter firewall rules

Windows Patch Installation

- Installation of Microsoft® operating system patches using the customer's own WSUS server[2]
- Compatibility evaluation: installation of patches recommended by manufacturers and aproved by the customer

Application Whitelisting

- Installation and configuration of a McAfee Application Control
- Installation of a central management console: McAfee ePO[1] (recommended by more than 10 whitelisting agents)
- Compatibility evaluation for SIMATIC PCS 7 systems

Anti Virus Installation

- Installation and configuration of virus protection software: McAfee VirusScan Enterprise
- Installation of a new central management console: McAfee ePO[1] (recommended for managing more than 10 anti-virus agents)
- Compatibility verification for SIMATIC PCS 7 systems

System Back-up

- Performance of a one-time backup of critical plant systems using Symantec System Recovery Software (to be provided by the customer)

Industrial Anomaly Detection

- Transparency over data exchange within the plant networks
- Detection of anomalies in communication behavior
- 100 % passive monitoring will not impact the monitored systems
- Available for plants from Siemens and third-party providers
- Based on Siemens industrial Microbox PCs IPC427E

Industrial Security Monitoring

- Continuous oversight of industrial security monitoring scenarios based on SIEM[3] technologies
- Local installation of the monitoring components
- Evaluation of customer-specific applications, e.g. adjustment of the Intrusion Detection/Prevention Systems (IDS/IPS)

[1] ePO – McAfee ePolicy Orchestrator
[2] WSUS – Microsoft Windows Software Update Server
[3] SIEM - Security Information andEvent Management

Manage Security for continuous protection and transparency

Manage Security provides regular monitoring and renewal of the implemented measures through our centralized services.

Your benefit:

You can achieve the greatest possible transparency regarding the security status of your plants and proactively block potential security events thanks to our global security experts and our scalable infrastructure.

Security Vulnerability Information

- **Information on released vulnerabilities of your industrial components and software applications**
- **Deployment via the Security Vulnerability Information App, also available as MindSphere App**

Patch Management

- **System-specific information on known weaknesses and patch availabilities**
- **Recommendations for plant-specific patch strategy**
- **Available for SIMATIC PCS 7 software, and Microsoft® operating systems**

Anti Virus Management

- **Updating of virus signatures and periodic virus scans in accordance with software manufacturer recommendations**
- **Detection of potential false alarms[2] through close cooperation with virus protection software manufacturers**
- **Regularly reports on plant condition regarding malware detection and prevention**
- **Central management possible through ePO[1] console**

Industrial Security Monitoring

- **Continuous analysis and correlation of log data as well as comparison with "Global Threat Intelligence" databases**
- **Detection, classification and immediate notification on the detection of security threats or incidents**
- **Overview of current plant security status with regularly status reports**

Remote Incident Handling

- **Rapid response by Siemens Cybersecurity experts with industrial experience**
- **Collection of information, cause analysis and criticality analysis with tools including intelligence mechanisms, malware sandboxing and monitoring of weaknesses**
- **Recommendations for the correction of any consequential damage**

1 ePO – McAfee ePolicy Orchestrator
2 »False positive«, only for Siemens products

The effective security strategy

Defense in Depth

With increasing digitization, comprehensive security in automation is becoming increasingly important. Industrial security is therefore a key element of Digital Enterprise, the Siemens solution on the route to "Industry 4.0" (the fourth industrial revolution). With Defense in Depth, Siemens offers a multi-layer concept providing both complete and in-depth protection for your plant. The concept is based on plant security, network security and system integrity in accordance with the recommendations of ISA 99/IEC 62443.

Plant Security

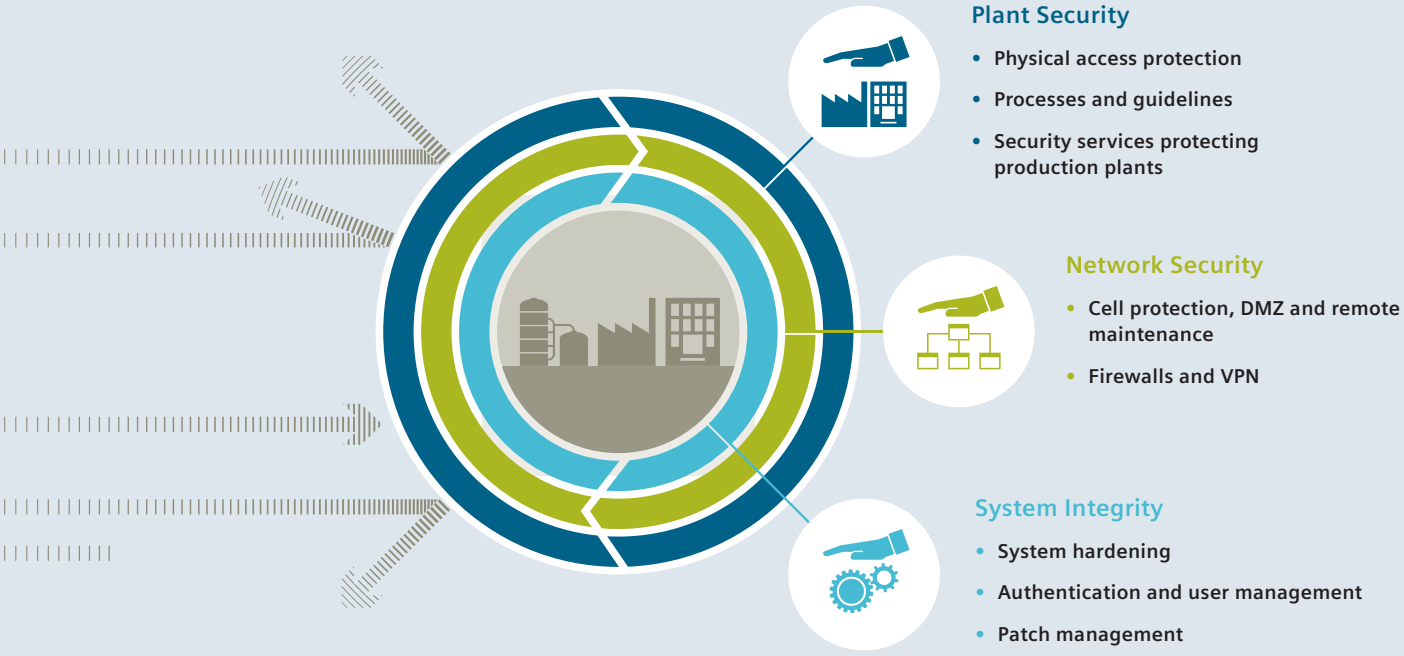
Plant security uses various methods to secure physical access by persons to critical components. This starts with classic building access and extends to the protection of sensitive areas with code cards. The customized Industrial Security Services include processes and guidelines for comprehensive plant security. This includes aspects such as a risk analysis of the implementation of suitable measures and their monitoring up to regular updates.

Network Security

Protecting production networks from unauthorized access is now particularly indispensable at the connections to other networks (e.g. office or Internet). The segmentation of individual subnets such as the cell protection concept with SCALANCE S or the security communications processors for SIMATIC provides additional security here. Data transfer can also be protected using VPN, such as for global remote access to distant plants via the Internet or mobile phone network using SCALANCE M. The firewall portfolio is supplemented by Automation Firewall -Classic or -NG, which are designed to protect the perimeter of your production networks.

System Integrity

The third foundation block of Defense in Depth entails ensuring system integrity. This includes the protection of automation systems and controls such as SIMATIC S7 controls as well as SCADA and HMI systems against unauthorized access or the protection of the information they contain. It also includes the authentication of users and their access privileges as well as hardening of the system against attackers.



Plant Security

- Physical access protection
- Processes and guidelines
- Security services protecting production plants

Network Security

- Cell protection, DMZ and remote maintenance
- Firewalls and VPN

System Integrity

- System hardening
- Authentication and user management
- Patch management
- Detection of attacks
- Integral access protection in automation

Assess Security

- Industrial Security Assessment
- IEC 62443 Assessment
- ISO 27001 Assessment
- Risk & Vulnerability Assessment

Manage Security

- Security Vulnerability Information
- Patch Management
- Anti Virus Management
- Industrial Security Monitoring
- Remote Incident Handling

Implement Security

- Security Awareness Training
- Industrial Security Consulting
- Automation Firewall
- Windows Patch Installation
- Application Whitelisting
- Anti Virus Installation
- System Back-up
- Industrial Anomaly Detection
- Industrial Security Monitoring

Published by
Siemens 2018

Siemens Industry Inc.
100 Technology Drive
Alpharetta, GA 30005

1-800-333-7421
usa.siemens.com/industrialsecurityservices

Subject to change without prior notice
Order No. CSBR-ISS-0618
All rights reserved
Printed in USA
© 2018 Siemens Industry, Inc.

The technical data presented in this document is based on an actual case or on as-designed parameters, and therefore should not be relied upon for any specific application and does not constitute a performance guarantee for any projects. Actual results are dependent on variable conditions. Accordingly, Siemens does not make representations, warranties, or assurances as to the accuracy, currency or completeness of the content contained herein. If requested, we will provide specific technical data or specifications with respect to any customer's particular applications. Our company is constantly involved in engineering and development. For that reason, we reserve the right to modify, at any time, the technology and product specifications contained herein

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/industrialsecurity.

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/industrialsecurity.