Industrial Cybersecurity Services

Portfolio overview

SIEMENS


Digitalization
changes
everything

Cybersecurity is essential for OT environments – but the lack of expertise has far-reaching consequences

Operative challenges

- Digitalization and the growing networking of machines and industrial systems also mean an increase in the risk of cyber attacks. New cybercrime incidents are reported every day. Thus, cybersecurity is essential in today's automation environments.
- There are a lot of cybersecurity standards as well as country-specific laws and regulations, especially for critical infrastructures, e.g. IEC 62443 or the NIS 2 Directive in the European Union.
- Despite the importance of the topic, there is a lack of expertise in the field of IT and cybersecurity for OT environments. This leads to a lack of transparency about potential risks and insufficient protection of the plant.

The advancing digitalization of industry increases the risk of cyber attacks, but there is a lack of experts and protection.

Possible consequences

Increased risk of cyber attacks

Disruption, unplanned downtimes, data theft and extortion or even sabotage and product harm

Significant financial loss and reputational damage

SIEMENS

Challenges regarding security
Productivity, cost pressure and regulations

Protect productivity

Protect against

- Externally caused incidents through increasing connectivity
- Internal misbehavior
- The evolving threat landscape

Reduce cost

Costs

- For qualified personnel
- For essential security technologies

Comply to regulations

Comply to

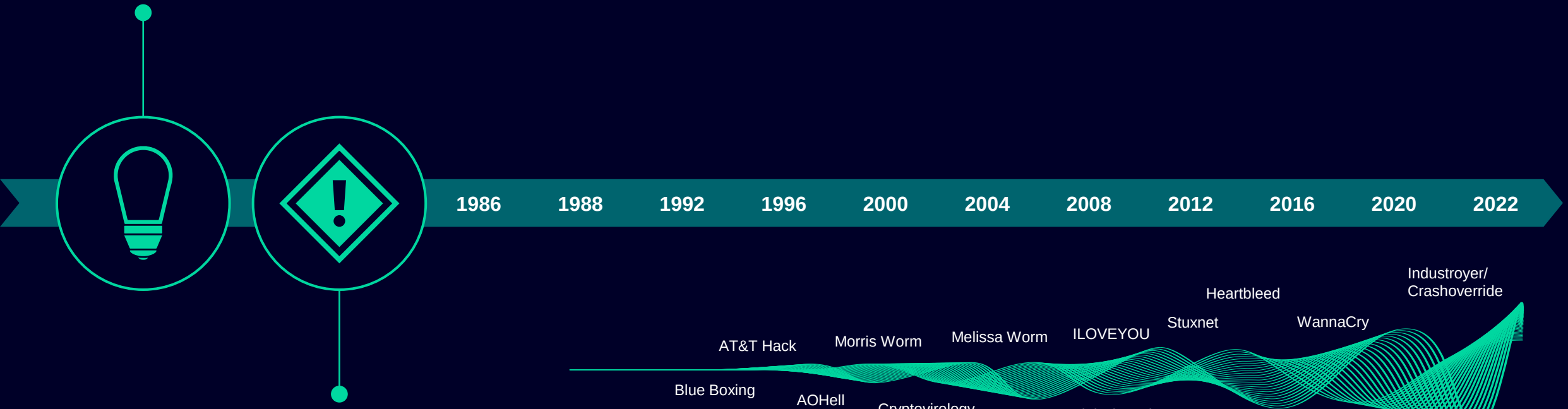
- Reporting requirements
- Minimum standards
- Security know-how

SIEMENS

Evolution of the cyber threat landscape

Opportunities

Billions of devices are being connected by the Internet of Things and are the backbone of our infrastructure and economy.



… and risks

Exposure to malicious cyberattacks is growing dramatically, putting our lives and the stability of our society at risk.

SIEMENS

The security needs of industrial control systems differ greatly from those of office IT

IT Security		Industrial Security
Confidentiality		**Availability and Safety**
3-5 years	**Asset lifecycle**	20-40 years
Forced migration (e.g. PCs, smart phone)	**Software lifecycle**	Usage as long as spare parts available
High (> 10 “agents” on office PCs)	**Options to add security SW**	Low (old systems w/o “free” performance)
Low (mainly Windows 10)	**Heterogeneity**	High (from Windows 95 up to 10)
Standards based (agents & forced patching)	**Main protection concept**	Case and risk based

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

Siemens relies on holistic cybersecurity concept: Defense in Depth

Security threats demand action

Defense in Depth

based on IEC 62443

- Plant Security
- Network Security
- System Integrity
- Industrial Cybersecurity Services

SIEMENS

Cybersecurity for Industry: Offering from Siemens

Defense in Depth

based on IEC 62443

Siemens products and systems offer integrated security

Know-how and copy protection

Authentication and user management

Firewall and VPN

System hardening, continuous monitoring and anomaly detection

Siemens Industrial Cybersecurity Services

- Transparency about the current security status
- Increased security level by closing security gaps
- Long-term protection through continuous security management

SIEMENS

Industrial Cybersecurity Services: End-to-end approach

Plant Security Services

- Security Assessments
- Scanning Services
- Industrial Security Consulting
- Cybersecurity Trainings
- Remote Industrial Operations Services

Network Security Services

- Industrial Next Generation Firewall
- Industrial DMZ Infrastructure
- Remote Platform Software as a Service

System Integrity Services

- Endpoint Protection
- Vulnerability Services
- Patch Management
- Backup and Restore

SIEMENS

Plant-specific security roadmap
with Security Assessments

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

How does it work?

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

Would you like to have a deep **assessment** based on the best-known security standard **for Industrial Control Systems**?	**IEC 62443 / NIS 2 Assessment**
Do you prefer a **compact one-day on-site assessment**?	**Industrial Security Check**

Main value drivers

Evaluation of the current security status

Plant-specific and risk-based security roadmap

Basis for transparent cost estimates

SIEMENS

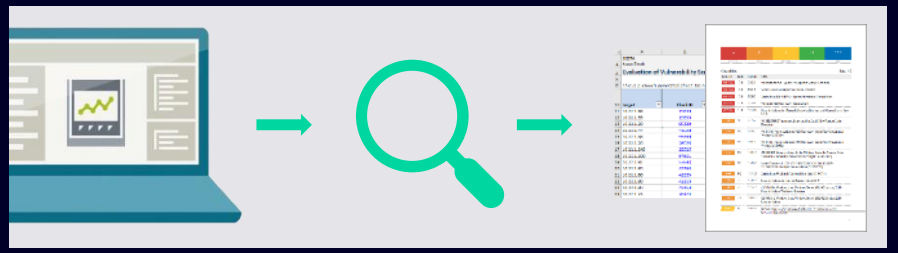
Quick transparency over assets and vulnerabilities
with Scanning Services

Scanning Services

- The growing amount of assets and increasing complexity in automation environments lead to incomplete asset inventory, lack of patching, outdated hardware and software, resulting in increased risk of cyber incidents.
- Scanning Services provide an efficient evaluation method in industrial automation environments based on a broad combination of scan tools and Siemens expertise in industrial security.

How does it work?

- Option 1: Active Asset Inventory Scan
- Option 2: Vulnerability Detection Scan



Main value drivers

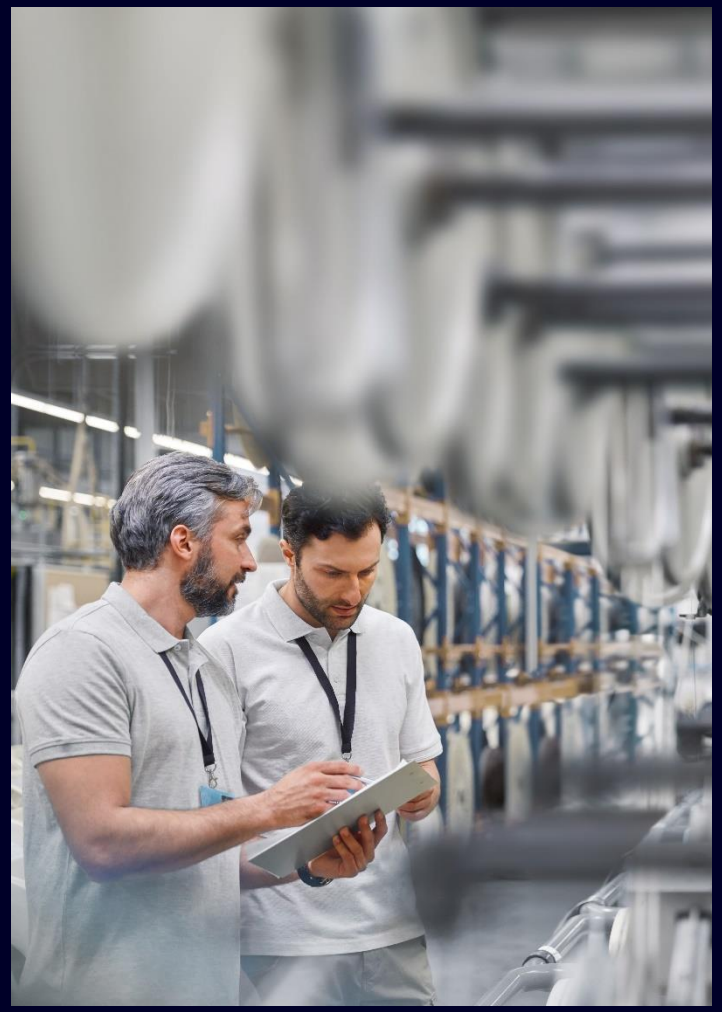
Transparency over implemented assets

Detection of vulnerabilities

Clear guideline to increase security level

SIEMENS

Immediate access to industrial security expertise
with Industrial Security Consulting



Industrial Security Consulting

Operators of production facilities these days cannot afford to do without effective security measures. But industrial security capacities are rarely available.

Industrial Security Consulting provides on-site support through experienced consultants regarding security policies and the plant-specific network layout as well as tailor-made implementation support for the industrial security portfolio.

How does it work?

- **Incident Analysis:** Immediate support in case of incidents (root-cause analysis, remediation strategy)
- **Policy Consulting:** Review and establishing of policies, processes and procedures
- **Network Consulting:** Support for cell segmentation, network design and firewall rules
- **Implementation Support:** Smooth integration of security portfolio incl. training

Main value drivers

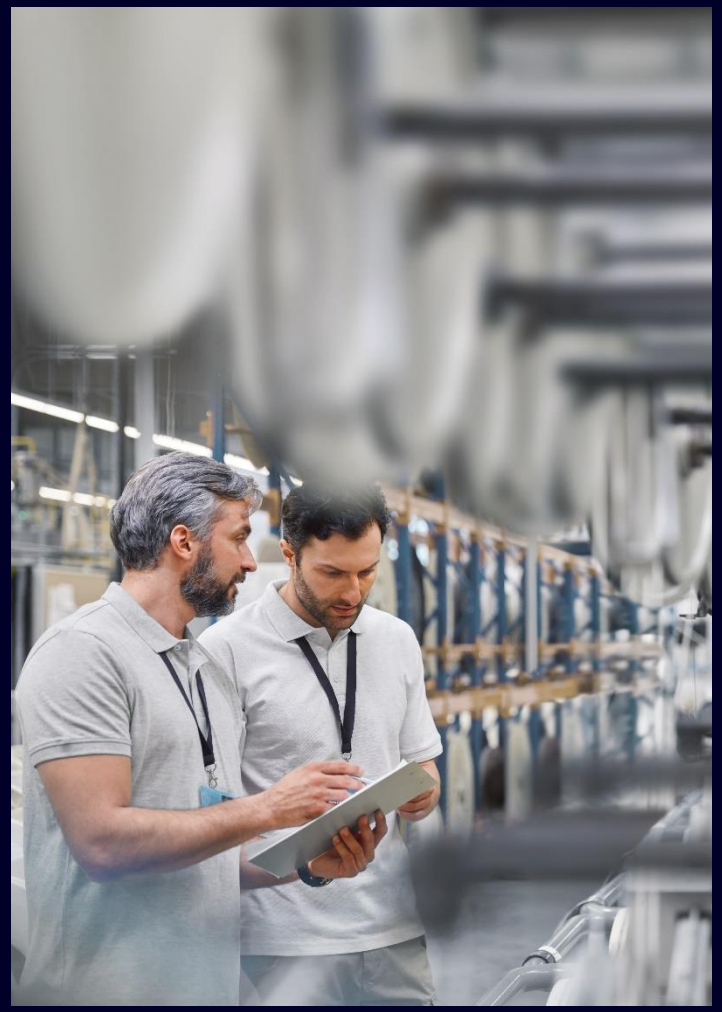
Tailored security policies and concepts

Immediate access to expert know-how

No investment for developing own security capacities

SIEMENS

Fast reaction upon security incidents
with Incident Analysis as part of Industrial Security Consulting



Incident Analysis

In case of cybersecurity incidents, fast reaction is required to close the gaps and keep damage low. But industrial security capacities are rarely available. Who can help?

With Incident Analysis, our Industrial Security experts provide immediate support to close security gaps, restore production, and prevent incidents in the future.

How does it work?

- Collection of forensic information
- Comprehensive analysis of root-cause and criticality
- Recommendation of a proper remediation strategy

1. Detect
2. Analyze
3. Contain
4. Eradicate
5. Recover
6. Post-Incident Activity

Main value drivers

Immediate access to expert know-how

Supporting fast restoration of production

Reduced downtime cost

SIEMENS

Enhance Industrial Security through knowledge
with Cybersecurity Training Curriculum as part of SITRAIN access

Cybersecurity Training Curriculum

Industrial Security plays a pivotal role in protecting critical infrastructure. To address these complexities, education is crucial.

The curriculum within SITRAIN access provides you with the knowledge you need to enhance Industrial Security. It focuses on empowering the learners with the knowledge of following key components.

Content

- **Awareness and vulnerability**: Identify potential threats specific to automation systems and take proactive measures.
- **EU Directive (NIS 2)**: Comply with the European Union directive for robust protection against cyber threats.
- **IEC 62443 standards**: Familiarize yourself with the international standards for IT security within industrial communication networks.

Get the Learning Membership for the digital learning platform SITRAIN access and learn 24/7 anywhere and anytime. Enlarge your knowledge in small steps or at once.

Main value drivers

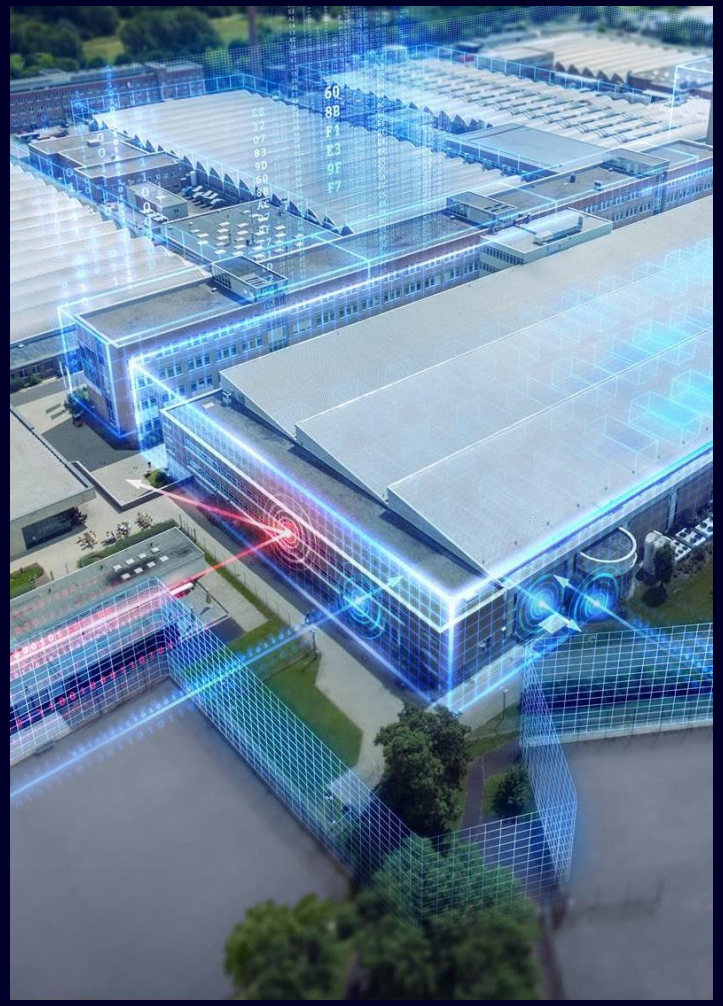
Situational awareness regarding security

Recommendations how to handle cyber risk

Help identifying security incidents

SIEMENS

Secure the “weakest link” in your plant
with Industrial Security Training



Industrial Security Training

Digitalization and the increasing networking of machines and industrial systems increase the risk of cyberattack. Appropriate protective measures are imperative, especially for critical infrastructure systems.

Industrial Security Trainings increase the situational awareness to avoid industrial security incidents caused by human error. Book your Learning Event as a training in a real or virtual classroom or onsite at your plant.

How does it work?

The trainings are based on typical daily situations and sample scenarios as well as statutory requirements and guidelines. Participants are introduced to the dangers of industrial plants in the discrete and process industry, analysis of potential weaknesses, evaluation of risks, and how to protect plants in both industry from attacks.

Different trainings are available:

- Basics of Cybersecurity in the Factory Automation
- Basics of Industrial Security for Process Automation
- Security in Industrial Networks

Main value drivers

Situational awareness regarding security

Recommendations how to handle cyber risk

Help identifying security incidents

SIEMENS

24/7 managed services for your IT/OT infrastructure
with Remote Industrial Operations Services

Remote Industrial Operations Services

Increasing IT/OT system complexity, lack of resources and cyber threats are major risks for productivity losses in operational technology.

With Remote Industrial Operations Services, you have a team of proven experts who remotely monitor and manage your IT/OT infrastructure 24/7, allowing you to focus on your core business.

How does it work?

The modular contracting enables you to select only the services you need:

- **24/7 monitoring** of IT/OT Infrastructure to prevent downtime
- **Managed security services and SOC as a Service** (incl. SIEM) for continuous protection against cyber threats
- **Proactive identification of maintenance needs** in your IT/OT infrastructure and spare parts provision to maximize uptime
- **Expert IT and OT technical support** from one source to rapidly resolve issues

Main value drivers

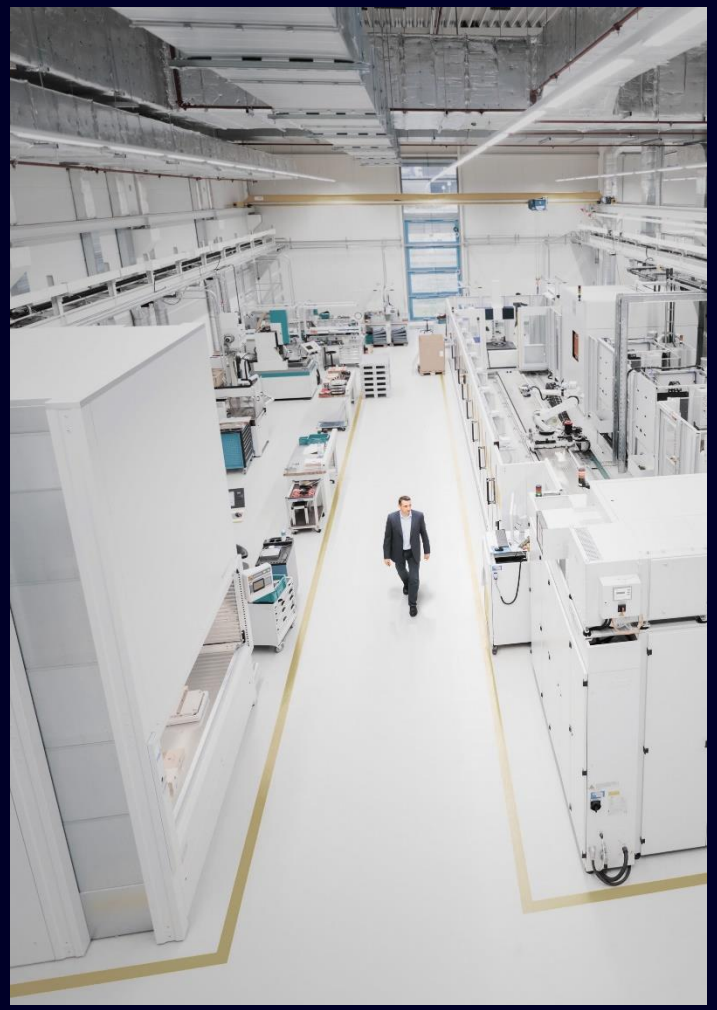
Proven IT/OT expertise by our experts

Operational continuity through 24/7 remotely managed IT/OT infrastructure

Compliance with cybersecurity regulations (e.g. NIS 2)

SIEMENS

Continuous network protection
with Industrial Next Generation Firewall



Industrial Next Generation Firewall

- Shop-floor landscape has changed from isolated islands to highly complex networks without any segmentation from untrusted cyber networks (e.g. office or internet).
- Industrial Next Generation Firewall is a perimeter protection solution in line with security requirements for industrial automation, tested and approved for usage with Siemens process control system.

How does it work?

- State-of-the-art Next Generation **Firewall Appliances**
- Additional **Security Subscriptions** for Threat Prevention, URL Filtering and WildFire
- **Support Package** (3 or 5 years) with Premium Support

Main value drivers

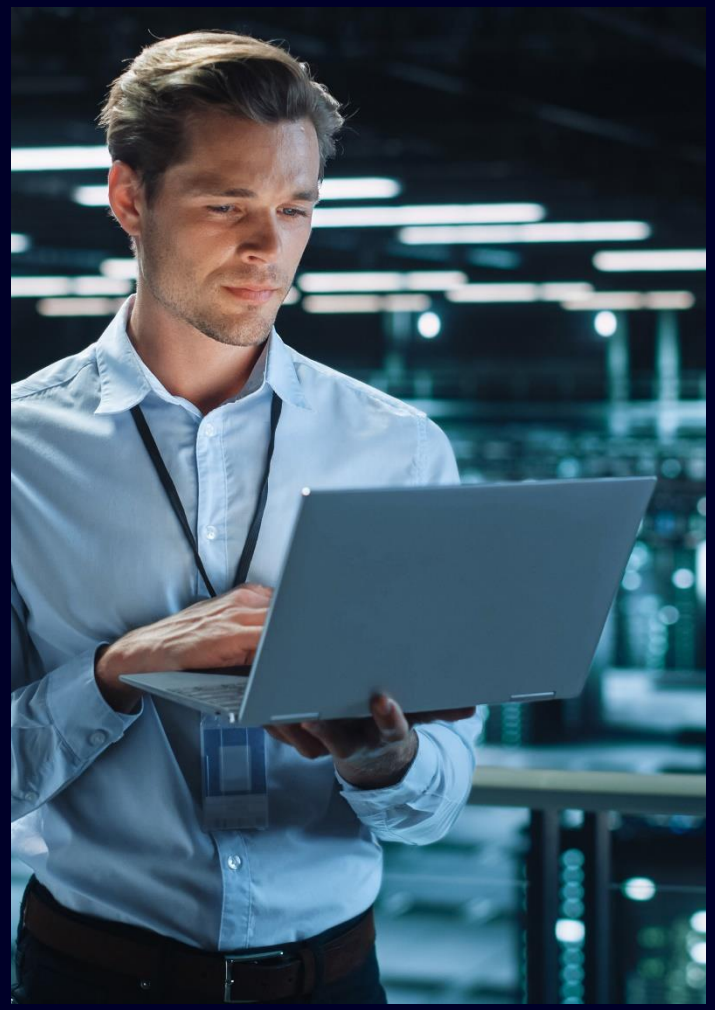
Continuous protection against known and unknown threats

Tested and approved for SIMATIC PCS 7 and SIVaaS

Very good price/ performance ratio

SIEMENS

Secure data exchange between IT and OT
with Industrial DMZ Infrastructure



Industrial DMZ Infrastructure

To protect against cyber attacks, the international security standard IEC 62443 recommends a deeply tiered defense, including network segmentation.

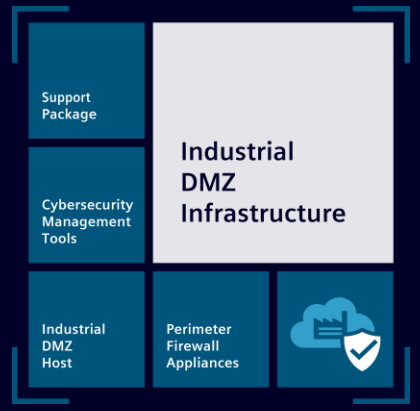
Industrial DMZ Infrastructure is a ready-to-run concept for the segmentation of IT and OT networks with integrated security features in several defense layers.

How does it work?

The concept is based on the principle of the demilitarized zone (DMZ). The applied Next Generation Firewalls protect the automation level from unauthorized access from outside.

Additional highlights:

- Hardware, software and services for network security and system integrity already integrated
- Implementation on the hyper-convergent IT platform Industrial Automation DataCenter



Main value drivers

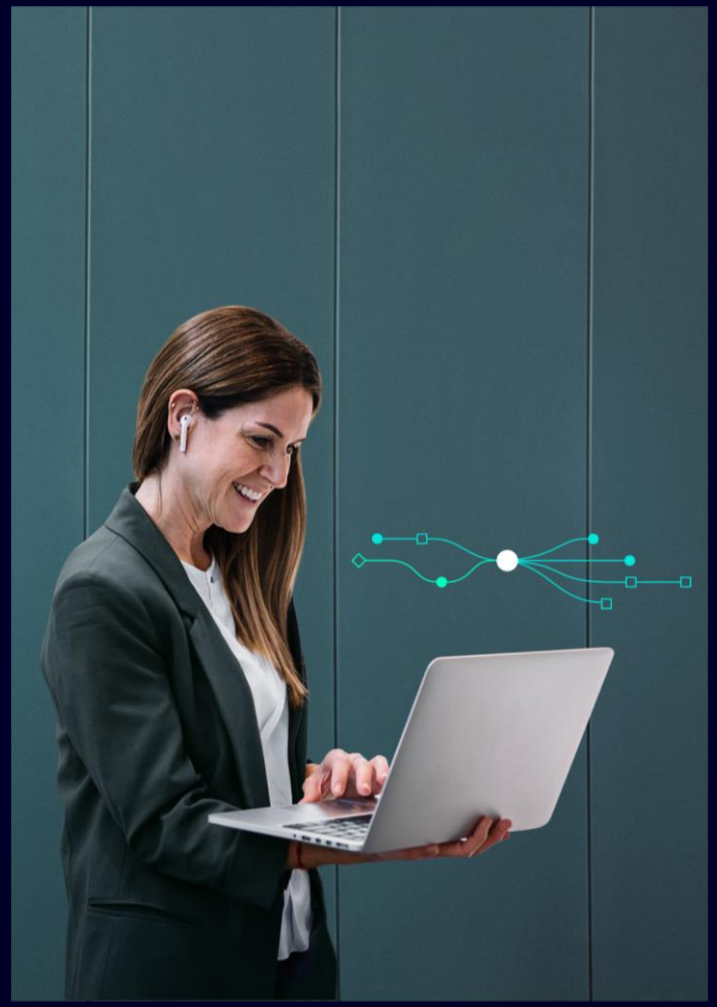
IT/OT network segmentation based on IEC 62443

Defense in depth with security features out of the box

Hyper-convergent IT infrastructure for high performance computing

SIEMENS

Secure remote access to industry devices
with Remote Platform SaaS

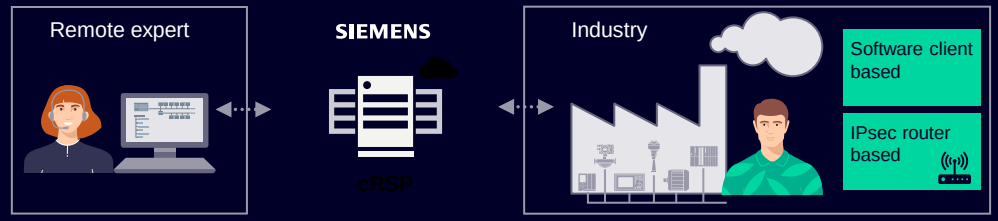


Remote Platform SaaS

Remote Platform Software as a Service (Remote Platform SaaS) provides a highly scalable and secure remote access infrastructure which is operated and maintained by Siemens. The common Remote Service Platform (cRSP) is designed according to industry requirements in line with IEC 62443 and focuses on access to industrial devices.

How does it work?

cRSP is used for implementing remote access and transferring data to IP-based (Siemens and others) devices. The administration and configuration of the remote platform is self-managed or managed by Siemens. Predefined application templates ensure simple workflows for remote experts. After the initial setup, an authorized remote expert can establish a remote connection to the connected devices through secure VPN tunnel via a software client or IPsec router.



Main value drivers

Less travel and reduced downtime lead to cost reduction and contribute to carbon neutrality

Use of Siemens proven and worldwide available remote platform cRSP

State of the art industrial security

SIEMENS

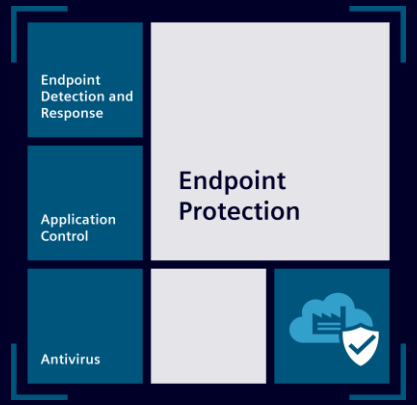
Continuous protection against malware
with Endpoint Protection

Endpoint Protection

- The threat of malware in form of viruses, rootkits and trojans is growing exponentially – also for endpoint devices in industrial environments (e.g. IPC).
- Endpoint Protection provides different approaches – each has its advantages depending on the use case.

How does it work?

- **Antivirus:** The execution of known malicious applications is blocked based on continuously updated signature files
- **Application Control:** Only trusted applications are allowed to run based on a positive list
- **Endpoint Detection and Response:** Interoperability test for the specific configuration of PCS 7 version and 3rd party EDR software version



Main value drivers

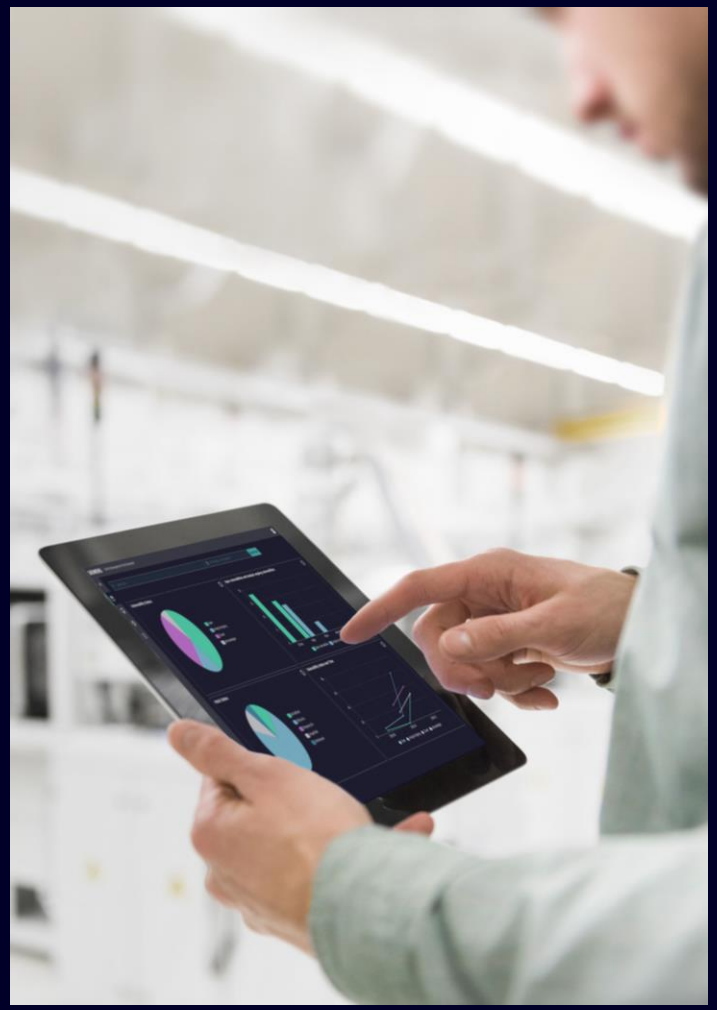
Protection against known and unknown threats caused by malware

Easy, centralized operation via management server

Approved versions with tailor-made configurations for Siemens products

SIEMENS

Efficient handling of vulnerabilities
with Vulnerability Services



Vulnerability Services

Companies need to reduce their exposure to vulnerabilities in the face of a growing number of cyberthreats. Identifying new vulnerabilities as soon as possible is crucial.

Vulnerability Services empower you to secure your product development, infrastructure and product portfolio by providing relevant, actionable vulnerability intelligence.

How does it work?

Based on a unique monitoring approach you receive vulnerability alerts for your individual system.
There are different options – tailored to your requirements:

- **Management Portal:**
  Tool incl. asset import, tracking and reporting
- **API:**
  Seamless integration into existing tools and processes
- **Managed Service:**
  Let us take care!

Main value drivers

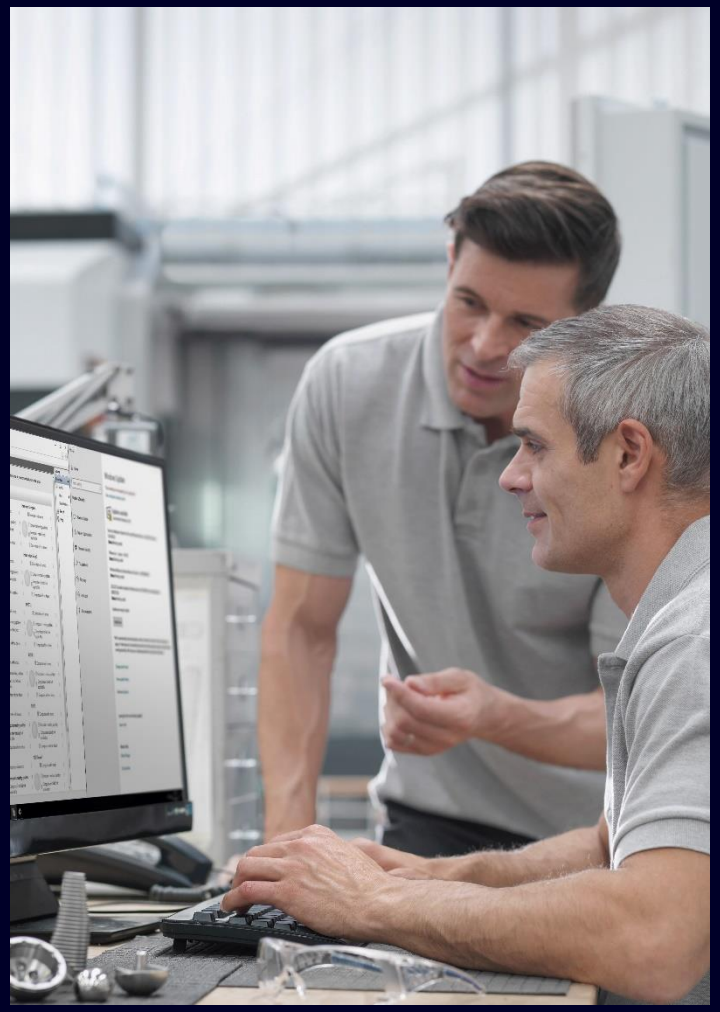
Instant transparency on vulnerabilities and minimized patch-times

Proactive management of cyber risks – easily integrated into your workflow

Reduced risk of costly exploits

SIEMENS

Managing vulnerabilities and critical updates
with Patch Management



Patch Management

- The installation of patches is the appropriate reaction to close vulnerabilities in software. Thus, patches contribute to stable plant operation. But patching is manual work and an incompatible patch can cause unplanned downtimes.
- Siemens offers Patch Management of security patches and critical updates in Microsoft products for SIMATIC PCS 7 to simplify the patch process on the plant.

How does it work?

- **Step 1:** The monthly released security patches for Microsoft products are tested and verified for compatibility with SIMATIC PCS 7.
- **Step 2:** This information is published as metadata via a central update server (WSUS – Windows Software Update Services), which sends the information automatically to the local WSUS server in the plant.
- **Step 3:** The customer receives a notification and can download the approved patches directly from Microsoft.

1 Windows Software Update Services

Main value drivers

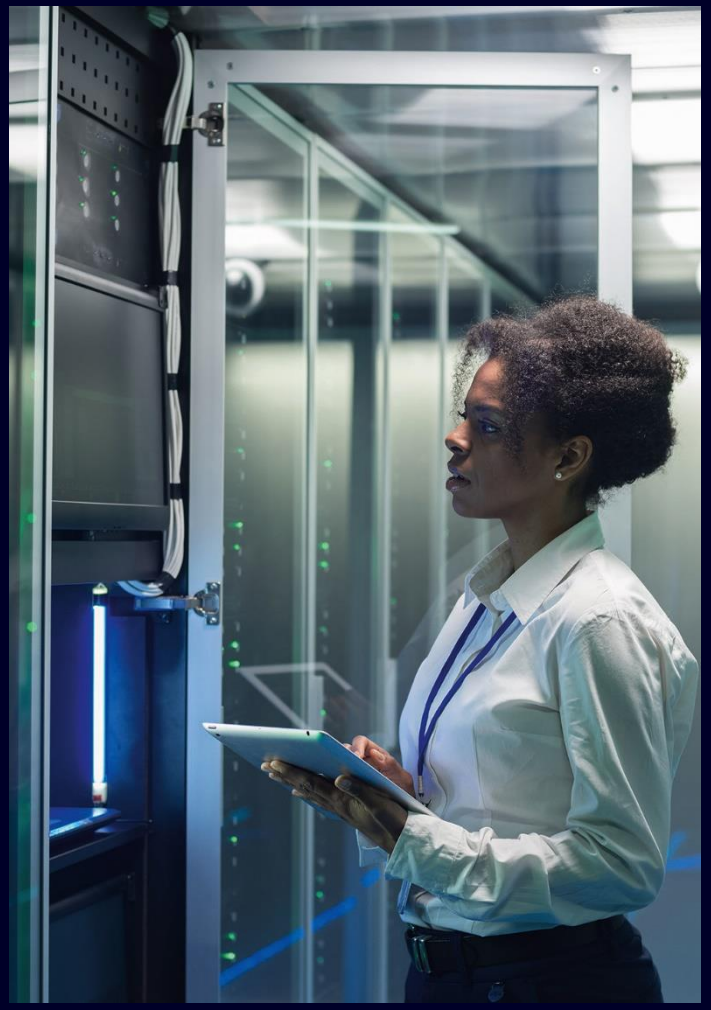
Save time and cost due to reduction of manual work on-site

Minimize risk of human error

Enhanced plant availability

SIEMENS

Pre-configured IT infrastructure for disaster recovery
with Backup and Restore (SIMATIC DCS / SCADA Infrastructure)



Backup and Restore

The right disaster recovery strategy is an extremely important factor to restart production after a breakdown and to prevent data loss. Additionally, new security regulations (e.g. NIS 2 for EU) require operators to have a system for backup, disaster recovery and crisis management in place.

Backup and Restore (as part of SIMATIC DCS / SCADA Infrastructure) provides a powerful and preconfigured IT infrastructure for disaster recovery in industrial environments.

How does it work?

Backup and Restore:
Best in class Disaster Recovery Backup solution, adapted to industrial environments

Support Package:
3- or 5-year service agreement

Main value drivers

- Increased availability thanks to fast disaster recovery and prevented data loss
- Compliance with cybersecurity regulations and improved plant data security in case of ransomware incidents
- Ready-to-run infrastructure with system-tested, pre-configured components

SIEMENS

Industrial Cybersecurity Services @ Industrial Automation DataCenter

SIEMENS

Bridge the gap between IT and OT
with Industrial Automation DataCenter

Industrial Automation DataCenter

System complexity is rising and cybersecurity threats are increasing, whereas there is a lack of know-how and resources when it comes to IT/OT integration.

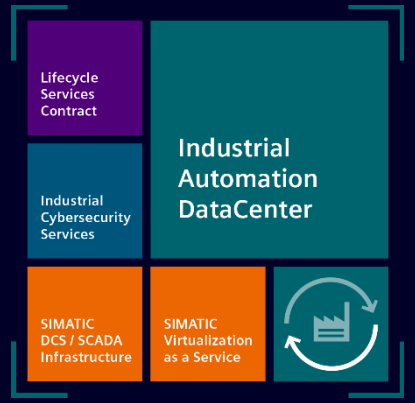
The Industrial Automation DataCenter is a ready-to-run tailor-made IT infrastructure for OT environments – developed by our experts who combine expertise in both fields.

How does it work?

All important core elements of a data center are included:

- High performance computing
- IT/OT network
- Back-up & disaster recovery
- Process data archiving
- Uninterruptible power supply
- IEC 62443 compliant security architecture

The holistic approach covers consulting, configuration and managed services throughout the entire life cycle - from a single source.



Main value drivers

Ready-to-run high available IT/OT infrastructure

High energy efficiency and space savings

Cybersecurity by design

SIEMENS

Let us know if there is anything we can support you with!

You want to find out more?

siemens.com/icss

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.

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

SIEMENS