CYBERSECURITY CAPABILITIES

Custom-tailored service and solutions for securing industrial and mission-critical networks

usa.siemens.com/network-security

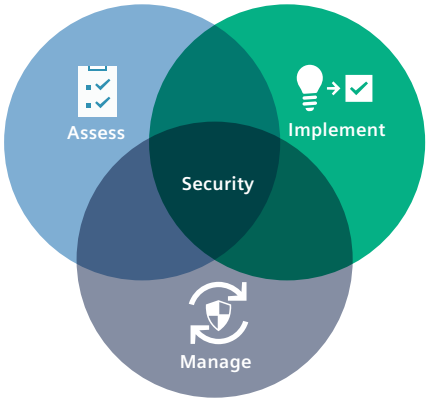
SIEMENS

Why should you **prioritize cybersecurity?**

To remain successful into the future, companies need to seize the opportunities provided by digitalization today. In light of digitalization and the ever-increasing networking of machines and plants, it is key that data security is always taken into account

The use of industrial security solutions precisely tailored to the needs of industry is of fundamental importance and should be inseparably linked with industrial communication. Due to the constantly growing number of convergent networks in companies and the increased frequency of cyber attacks, Cybersecurity becomes more and more important. Cyber attacks can interrupt production, damage physical assets, and even result in injury or death to both, employees and the public. These potential impacts are magnified when the target is a critical infrastructure.

Cybersecurity is a process
A successful strategy for Cybersecurity is a continuous process of **Assess, Implement, and Manage.**



Assessment of the network is the first step and the key to a successful roll-out of Cybersecurity solutions. During this phase, assets are analyzed in-depth to provide insights into security vulnerabilities and risks of a customer's network.

Implementing a Cybersecurity system is more than just an "out-of-box" security system on top of operational technologies. Everything companies do should be 'secure by design'. This includes pre-configuration and testing services as well as training, so staff can play their part in secure operations. Keeping the network secure does not stop with the implementation of Cybersecurity solutions.

Managing the security of a network means staying on top of key areas: monitoring threats, keeping security solutions up to date, and ensuring quick reaction times to identify threats.

"Our mission is to reduce the threat of cyber-attacks in our customers' operations through awareness, thought leadership and knowledge sharing in cybersecurity.

Siemens Defense in Depth concept
To keep industrial plants secure from unrestricted and external cyber attacks, all levels must be protected simultaneously – from the plant management level to the field level and from access control to copy protection. Enter Defense in Depth, an approach to digitalized operations based on the IEC 62443 recommendations for plant security, network security, and system integrity. With Defense in Depth, Siemens provides a multi-layered security concept that involves various levels of protection that detect, prevent and/or mitigate human error or malicious intrusions. It takes attacker motivations and a network's unique design into account to create a unified solution which protects against current and future threats. The result is comprehensive and extensive protection for industrial facilities.

A global leader in cybersecurity
Cybersecurity is an essential factor for the success of the digital economy. Aiming toward a secure digital world, Siemens is the initiator of the "Charter of Trust" and first company to receive TÜV SÜD (German Technical Inspectorate/South) certification based on IEC 62443-4-1 for the interdisciplinary process of developing automation and drives products. Based on the 10 key principles, members of the "Charter of Trust" strive for three goals:

1. Protect the data of individuals and companies.
2. Prevent harm to people, companies and infrastructures.
3. Create a reliable basis upon which trust is established and can grow in a connected, digital world.

Our cybersecurity capabilities

Siemens' heritage is predominantly based on operational technologies and industrial control systems (ICS). Combining this with a deep knowledge of the network and performance requirements for mission-critical applications in harsh environments, our suite of proven cybersecurity solutions and services can address each of the layers in a Defense in Depth strategy.

Cybersecurity technical services

The Industrial Security Services portfolio provides comprehensive support for developing, implementing and maintaining a strategy that conforms with the Defense in Depth concept. Services include:

- Comprehensive discovery of existing network assets and architecture.
- Evaluating the existing security features, conducting a vulnerability assessment of threats, identification of risks, and providing a security assessment report with concrete recommendations of security measures.
- Design and deployment of security solutions and security training of stakeholders.

Cybersecurity technical solutions

- Industrial security appliances
  - Industrial firewall appliances
  - Industrial VPN appliances
  - Anomaly-based Intrusion Detection Systems (IDS)
  - Deep Packet Inspection (DPI)
  - Intrusion Prevention System (IPS)
- Wired and wireless industrial touters
- Secure remote access software
- Security communication processors
- IE RJ45 port lock
- Access control readers

Let's talk.

Your approach to Cybersecurity and ICSs may already rely on Siemens' expertise, experience and our approach to Defense in Depth – along with our proven strategies, software and industrial hardware platforms.

Alternatively, you may be focusing on ICS Cybersecurity for the first time. In either case, a dialogue with a trusted advisor about your ongoing industrial Cybersecurity needs should be on your to-do list.

Contact our Cybersecurity core team for a conversation on how to protect your brand, your business, your ICS processes and your OT networks

Jeff Foley
Chief Technology Evangelist for Cybersecurity
Senior Business Development Manager
Siemens Digital Industries
Mobile: +1 (954) 296-5648
Email: jeff.foley@siemens.com

Chuck Tommey, GICSP, CEH, P.E.
IT/OT Networking Consultant
Cyber | Architecture | Digitalization
Siemens Digital Industries
Mobile: +1 (704) 707-6584
Email: chuck.tommey@siemens.com

Legal Manufacturer

Siemens Industry, Inc.
100 Technology Drive
Alpharetta, GA 30005
United States of America

www.usa.siemens.com/network-security

Order No. NTBR-CYCAP-0923

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 only form one element of such a concept. Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the Internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place. Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit

siemens.com/industrialsecurity

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply 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

siemens.com/industrialsecurity