PROFESSIONAL SERVICES

How secure is your network?

Identify potential vulnerabilities based on IEC 62443 or NIST Cybersecurity framework.

Cyberattacks are on the rise due to sophisticated attackers and increased device connectivity. Assets, equipment, uptime, trade secrets, brand value, intellectual property and even personal safety need to be protected from malicious network intrusions, employee sabotage or accidental manipulation.

To avoid damages and downtime from cyberthreats, it's important to implement a holistic approach addressing the primary components of a security strategy: people, process and technology.

An Industrial Network Security Assessment from Siemens is a smart first step to securing your assets. Each of our industrial network experts has more than 10 years of experience assessing and designing Operation Technology (OT) networks.

SIEMENS

Roadmap for an Industrial **Network Security Assessment**

We examine your ability to detect, prevent, and respond to cyberthreats.

Analysis and Discovery:
Siemens conducts an in-depth evaluation of your network, devices, processes, personnel and current security plans.

Security and Vulnerability Scan:
Siemens network experts use scanning tools to perform a vulnerability scan of your network.

Security Assessment Report:
The report is delivered with a prioritized list of vulnerabilities, findings, recommendations and more.

Who needs to be involved?

IT OT Security

1 Discovery

2 Scan

3 Report

Our certified industrial network security experts, each with more than 10 years of experience assessing and designing OT networks, will begin discussions with you about the facility, network, assets and goals.

Together we identify a security standard to which the assessment will be based. IEC 62443 is an international standard with a focus on Industrial Automation and Control Systems (IACS). The NIST Cybersecurity Framework or other standards can be used depending on the assessment goals. We'll address all areas covered under the chosen standard which may include physical access protection, security policies (process), training (people) and network devices (technology).

After the Security Assessment Plan has been approved by all the stakeholders, Siemens will perform the agreed upon network scanning and any specified intrusive or non-intrusive testing. Scanning tools may include: Wireshark, OpenVAS or NESSUS. Other tools designed for the OT environment may be used depending on the assessment goals.

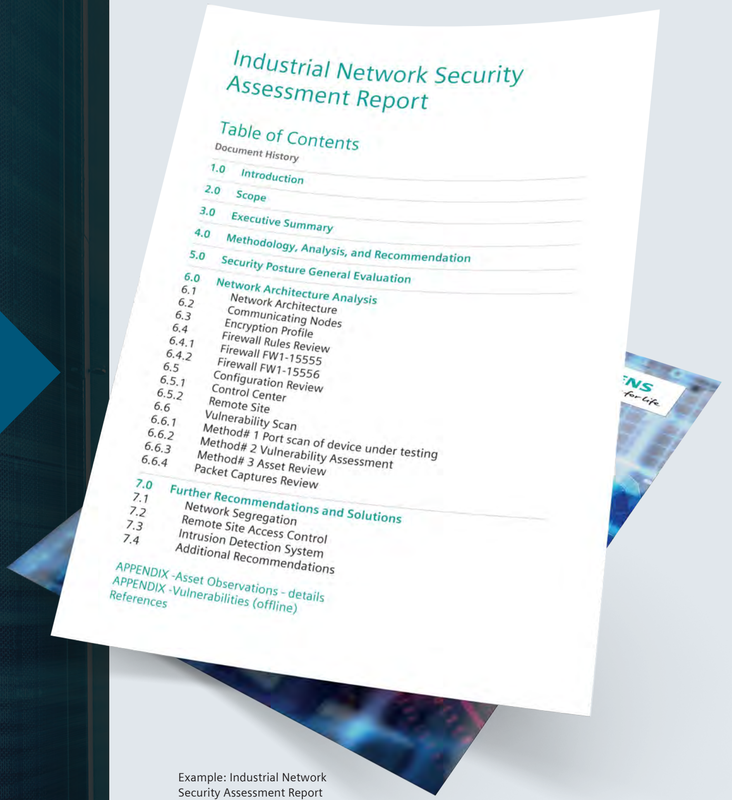
The Security Assessment Report will provide comprehensive insight, analysis and recommendations addressing the people, process and technology that keep your network secure.

Comprehensive evaluation by certified security experts

There is no industrial network too big or too small to implement a security strategy.

We have experience working with companies of all sizes in multiple vertical industries. Our certified network security experts will evaluate the security of your operation and provide documentation identifying potential vulnerabilities.

Once we determine the right security standards for the assessment, it will be completed in days or weeks depending on the scope. Armed with a comprehensive picture, you can make an informed decision on how best to protect your assets in the future.



Example: Industrial Network Security Assessment Report

15%

say they are confident in their current abilities to maintain security for IIoT devices and systems

Source: The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns, July 2018

41%

of Industrial Control Systems (ICS) attacked at least once in first half of 2018, up from 36.6% in 2017

Source: Kaspersky Lab, Threat landscape for industrial automation systems, September 2018

$124B

total amount organizations worldwide planned to **spend on cyber security** initiatives in 2019

Source: Gartner, Worldwide Security Spending by Segment, 2017-2019 Report, August 2018

$600B

current estimate that cybercrime cost the world last year, or 0.8% of global GDP

Source: McAfee, Economic Impact of Cybercrime — No Slowing Down, February 2018


Manufacturing


Electric Power


Water & Wastewater


Oil & Gas


Transportation (ITS / Rail)

How to get started

Siemens Industrial Network Security Assessments adhere to well-established security standards. Each assessment is customized depending on the facility size, device quantity and type (i.e. number of machines, servers, routers, switches, firewalls, ports and other factors).

Contact your local Siemens representative to begin initial discussions or e-mail us at: siemensci.us@siemens.com and we can help you get started.

Or visit us online to learn more: **usa.siemens.com/network-security**

Examples of Siemens Industrial Network Security Assessments

Customer: U.S. Industrial Manufacturing Facility

Assessment period: One week

Methodology: A security assessment of network documentation, passwords, architecture, switches, routers, firewalls, encryption, computers, servers and other devices was completed. Data communication was verified with traffic analysis and network health information from all devices was evaluated.

Deliverable: The near 50-page assessment report provided network health results, traffic load of the network, a network validation checklist, data communication results and recommendations on future enhancements to further secure the network and eliminate potential vulnerabilities.

Customer: U.S. Electric Utility Company

Assessment period: Two months

Methodology: The security assessment included interviews with engineers, technicians, IT and management. The security was evaluated for physical access. The network was assessed with packet captures, logs, configuration files and network scanning tools. Systems evaluated included workstations, servers, switches, routers, firewalls, encryption and cellular devices.

Deliverable: The assessment report (less than 100 pages) provided a comprehensive analysis of the current security posture and a prioritized list of recommendations.

Real-world cyberattacks

A leading supplier of aluminum products in North American and European markets, Norsk Hydro, was hit by a cyberattack in 2019. They were forced to shut down several automated product lines. According to the report, "the impact was widespread as several plants in the US and Europe were stopped due to a lack of ability to connect to production systems and customs data."[1]

In recent years, global leaders Merck (pharmaceuticals) and Mondelez (Oreo, Ritz and other food brands producer) experienced cyberattacks. Merck lost nearly $700M and Mondelez over $100M in damages. In addition, they encountered claim denials from Insurers.[2]

Critical infrastructure continues to be a target for hackers. A long-running campaign recently put hackers "inside the control rooms of U.S. electric utilities where they could have caused blackouts." The strategic importance of critical infrastructure to national security and a functioning society can lead to an increase in the frequency and intensity of cyberattacks on those facilities.[3]

These are just a few attacks that have been reported. There are many other examples, some not reported as companies often try to handle them discreetly.

Sources:

[1]www.bloomberg.com, Nordic Metals Giant Restarts Some Systems After Ransomware Attack, March 2019

[2]www.nytimes.com, Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong, April 2019

[3]www.wsj.com, Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say, July 2018

Industrial Networks Professional Services

Certified professionals with the ongoing commitment to continuing education.

Knowledge of Industrial Ethernet standards.

Learn more:

Network Security:
usa.siemens.com/network-security

Professional Services:
usa.siemens.com/industrial-networks-services

Industrial Networking:
usa.siemens.com/future-ready-networks

Published by

Industrial Networking
5300 Triangle Pkwy,
Norcross, GA 30092

For further information please visit:
usa.siemens.com/network-security

Article No.: NTBR-NTSAS-0624
Printed in USA

Follow us:
twitter.com/siemensindustry
youtube.com/siemens