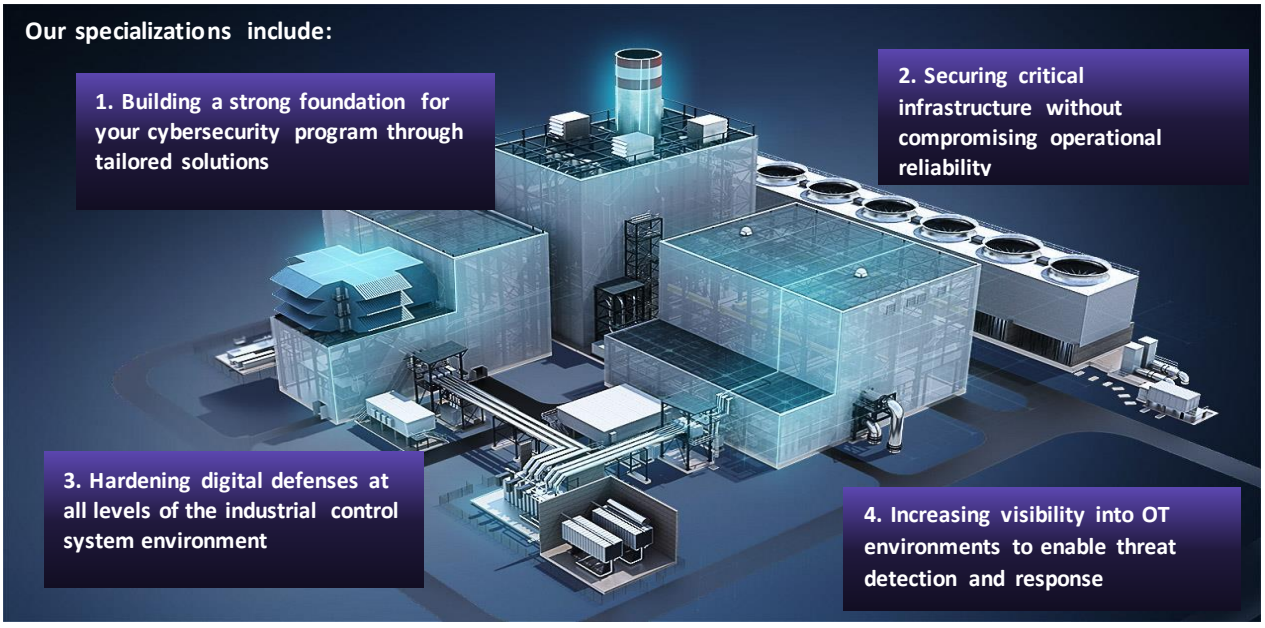
Essential Cybersecurity for Omnivise T3000

siemens-energy.com

Lock your digital door with Siemens Energy's OT cybersecurity solutions

A robust cybersecurity program is critical in today's environment of increasingly potent cyber threats and progressively more stringent regulations. However, most organizations struggle to establish an effective cybersecurity function because they lack the necessary resources, expertise, or direction to do so. Siemens Energy offers a solution. We combine our expertise in operational technology (OT) cybersecurity and industrial control systems with industry leading technology to provide more than just IT-centric tools. We partner with each customer to ***design***, ***install***, ***configure***, and ***service*** cybersecurity solutions that fit the OT environment, thereby mitigating critical risks and establishing the foundation of a best-in-class cybersecurity program that doesn't disrupt safe and reliable plant operation.



Specially designed solutions for a robust cybersecurity program

An effective cybersecurity program must include tools, functions, and services that quickly and reliably address known threats, harden defenses, and enhance visibility into the OT environment. Siemens Energy offers a broad portfolio of OT-focused cybersecurity solutions designed to address customer needs at any level of cybersecurity maturity. These solutions work to prevent attacks from occurring, prepare your organization to properly manage cyber risks, and improve organizational readiness to detect and address cyber events.

Omnivise T3000 incorporates a holistic security concept over the entire product lifecycle and complies with most cybersecurity standards and regulations, including NERC CIP, VGB, and NIST. Additionally, Omnivise T3000 and is certified according to IEC 62443-4-1 and 62443-3-3. By coupling a secure-by-design control system with a comprehensive suite of cybersecurity offerings, Siemens Energy delivers all the elements necessary for an effective cybersecurity program. A sampling of the most critical features and solutions is presented below:

Cybersecurity for Omnivise T3000	
System and Asset Hardening Limit exposure with a system hardened to the latest industry best practices	**Network Intrusion Detection System** Catch attacks quickly through network traffic analysis and custom rule sets
Patch Management Close vulnerabilities with centrally-deployed system-tested patches	**Security Event Monitoring** Enable rapid response to security events with advanced analysis, visualization, and alerts
Malware Protection Identify, report, and remove viruses and malware with an OT-tailored solution	**Configuration Change Monitoring** Validate configurations against regulations and identify deviations from baseline
Application Whitelisting Allow only known, trusted applications to run on your network	**Vulnerability Management** Gain visibility, context, and insights to defend your OT environment with precision
Unidirectional Gateway Ensure OT data crosses network boundaries securely with our data diode	**Remote Expert Center: Cybersecurity (cSOC)** Get 24/7 remote support, event detection, and incident response from OT specialists

Offerings applicable for Omnivise T3000 R8.2 and newer

Siemens Energy's solutions deliver holistic, reliable, and OT-adapted solutions for industrial customers across markets and at all levels of cybersecurity maturity. Whether your aim is to fulfill regulatory obligations or to enhance your cybersecurity posture with more advanced solutions, Siemens Energy will support with the right combination of tools to suit your organization's requirements.

A trusted partner to support your organization's cybersecurity journey

No other cybersecurity solution provider understands the complexities of the OT environment like Siemens Energy, and none bring a 100+ year history as a global leader in energy technology. Siemens Energy's extensive domain experience across the energy value chain means we fully understand the criticality of operational reliability and business continuity in the context of your environment.

Each customer's cybersecurity journey is unique. Siemens Energy tailors each deployment to your organization's distinct requirements, resulting in solutions designed for complex environments across vendors, asset functions, and operational requirements.

Siemens Energy is committed to working with your organization – guiding you on your path to enhanced visibility, capable detection, increased security, and improved reliability.

Contact your Siemens Energy representative or our Cybersecurity leaders to learn how Siemens Energy can help your organization secure its OT environment

For further information:

Leo Simonovich
Vice President and Global Head
Industrial Cyber and Digital Security
leo.simonovich@Siemens-Energy.com

Theodor Rosch
Portfolio Manager Remote- and System Cyber Services
theodor.rosch@Siemens-Energy.com

G. E. Manoranjan
Product Manager Omnivise T3000 Cyber
g.e.manoranjan.ext@Siemens-Energy.com

Manfred Lustig
Product and Solution Security Officer Omnivise T3000
manfred.lustig@Siemens-Energy.com

Published by

Siemens Energy Inc.
Controls and Digitalization
4400 N Alafaya Trail
Orlando, FL, 32826, United States of America