Industrial Security™

Continuous asset and vulnerability visibility built for the most sensitive ICS, SCADA, manufacturing, and other operational systems.

Problem Overview

Industrial Security from Tenable delivers continuous asset discovery and vulnerability detection for safety-critical operational networks. Purpose-built for operational technology (OT) systems, the solution uses passive monitoring to provide safe and reliable insight – so you know what you have and what to protect. Covering a wide range of ICS, SCADA, manufacturing, and other systems, Industrial Security helps IT and OT security, plant operations, and compliance teams enhance security, improve asset protection, and strengthen regulatory compliance. The OT-native solution provides an up-to-date view of systems, applications, and vulnerabilities to help organizations understand their OT cyber exposure and protect operational performance.

Backed by a strategic partnership with Siemens, Industrial Security from Tenable offers expert OT support – including protocol and device coverage for dozens of OT vendors – by passively monitoring critical infrastructure in energy, utilities, and other sectors. This non-intrusive approach gives security and operations teams the only safe way to discover, visualize, and monitor their most sensitive systems.

Benefits

The essential benefits of the solution include:

- See the full set of operational systems, applications and services active on your production networks – and the connections between them

Industrial Security from Tenable delivers continuous asset discovery and vulnerability detection in a non-intrusive manner. It analyzes network traffic at the packet level to provide deep visibility into ICS, SCADA, and other operational systems.

Using patented passive monitoring technology, the solution safely detects vulnerabilities in critical OT systems. For the first time, organizations can get continuous visibility into the exposures in their production networks.

- Safely identify vulnerabilities in sensitive ICS, SCADA, manufacturing, and other operational technologies that cannot be scanned due to the risk of disruption
- Automatically discover and profile new assets added to your networks
- Move from point-in-time vulnerability scanning to continuous monitoring of assets and vulnerabilities
- Immediately identify potential risks to production assets created by new vulnerabilities and new or rogue systems
- Deploy a solution purpose-built for OT networks backed by Tenable and Siemens, global leaders in cybersecurity and operational technology
- Unify your OT and IT security with a single vendor for complete understanding of your modern attack surface

Key Capabilities

Continuous Asset Discovery

The solution continuously monitors network traffic for full asset visibility:

- Identifies hundreds of specific OT assets, covering a wide range of ICS, SCADA, manufacturing, and other devices and their associated communication protocols
  - Provides unified visibility into devices, applications, and protocols across the entire operating environment – including unauthorized software and unmanaged devices
  - Supports systems from dozens of manufacturers, including Siemens, ABB, Emerson, GE, Honeywell, Rockwell/Allen-Bradley, and Schneider Electric
  - Supported protocols include BACnet, CIP, DNP3, Ethernet/IP, ICCP, IEC 60870-5-104, IEC 60850, IEEE C37.118, Modbus/TCP, OPC, openSCADA, PROFINET, Siemens S7, and more
- Detects new assets added to a network
- Passively determines the operating system of each active host
- Displays machine-to-machine connections and "top talkers" communicating on the network
- Supports data export via .nessus, .csv, HTML, and syslog

Passive Vulnerability Detection

Industrial Security from Tenable provides rich insight into cyber exposure across production networks:

- Safely detects a wide range of OT vulnerabilities through passive monitoring (deep packet inspection) of network traffic
- Vulnerability detection spans all OT manufacturers and protocols listed above
- Presents assets and vulnerabilities by severity, count, name, and more
- Delivers information tailored to the needs of OT environments, such as asset role (PLC, PC, server, etc.)

Multi-Site Management

The solution supports distributed operational environments:

- Provides central visibility across multiple sites/plants through the ability to manage and consolidate data from multiple Industrial Security instances

Delivery Options

Industrial Security is available as traditional software for on-prem deployment or as a service delivered by Siemens.

BAKOTECH Group is an official distributor of Tenable Network Security, a leader in Value Added IT-distribution, operating onthe markets of Ukraine (head office), the Baltics, Eastern Europe, CIS and Georgia. As a Value Added Distributor BAKOTECH Group provides a wide range of services such as professional pre-sales and postsales support, trainings for partners and end-customers, PoC, PoV, solution consulting, implementation support, technical support, PR and co-marketing activities.

For additional information, please contact us:
www.bakotech.com, tenable@bakotech.com, +38 044 273 33 33

For More Information: Please visit tenable.com
Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact