Solution Brief

Tenable Solutions for Converged IT/OT Systems

Safely Inventory and Protect Critical Infrastructure

The days of air-gapped operational technology assets are gone. Increasingly OT environments interconnect with IT, adopting exploitable assets and protocols. The result: OT systems are exposed to IT threats. Referring to IT devices in operational environments, a SANS survey found, "IT devices such as computer assets running commercial OSes continue to be considered most at risk (70%) and having the greatest impact (46%)".

Additionally, IT/OT convergence is expanding the attack surface, and bad actors who have compromised IT networks may be able to access OT systems from the IT network. For example, bad actors accessing operational technology through the IT network caused the 2015 Ukraine power outage.[1].

Key Challenges

IT/OT convergence is blurring the line between IT and OT environments. However, most security solutions only work in either IT or OT environments, not both. For example, active network scanning products, common in IT environments, are rarely used in OT environments because they can interrupt OT device operation, resulting in costly outages or slowdowns.

Multi-Vendor Device Support
Most OT environments include devices from multiple vendors, and reliance on vendor-specific tools increases training costs and requires potentially costly integration to deliver a cohesive view of security. Security solutions that support multiple vendors' devices are required to streamline security.

Asset Inventory
Virtually all security frameworks and compliance mandates require organizations to maintain an accurate inventory of devices and software. Consider the NIST Framework for Improving Critical Infrastructure Cybersecurity's (NIST CSF). Its "Identify" function starts with the Asset Management category, with three initial subcategories (controls):

- ID.AM-1: Physical devices and systems within the organization are inventoried
- ID.AM-2: Software platforms and applications within the organization are inventoried
- ID.AM-3: Organizational communication and data flows are mapped

Failure to identify all systems creates blind spots where some systems are potentially insecure, thereby increasing downtime risk. If a security incident occurs, timely resolution depends on immediate availability of accurate inventory information, including asset model and version number. Organizations can no longer depend on costly, error-prone manual inventories that may be out of date soon after they are conducted. Automated solutions are needed to identify and characterize converged IT/OT systems.

Vulnerability Management
Because the quantity of vulnerabilities can be overwhelming and timely patching may not be feasible, it is tempting to stick one's head in the proverbial sand and ignore OT vulnerabilities. However, vulnerability management is critical to understanding risk. In fact, it is a key part of the NIST CSF and NERC CIP. Vulnerabilities must be assessed and prioritized, and those creating the most risk must be remediated by patching or with other mitigation measures, such as changes to firewall rules.

Anomaly Detection
Unlike dynamic IT networks, OT networks are fairly static; assets, connections and traffic patterns rarely deviate from a baseline. If significant deviations occur, they must be scrutinized. Therefore, OT networks must be continuously monitored to detect new assets, new connections and unusual traffic; any of which must be investigated to rule out unauthorized activity.

Solution

- Industrial Security
- Tenable.io™

Key Benefits

- Reduced risk of downtime
- Strengthen regulatory compliance
- Reduced Total Cost of Ownership (TCO)

[1] "When the Lights Went Out", Booz Allen Hamilton

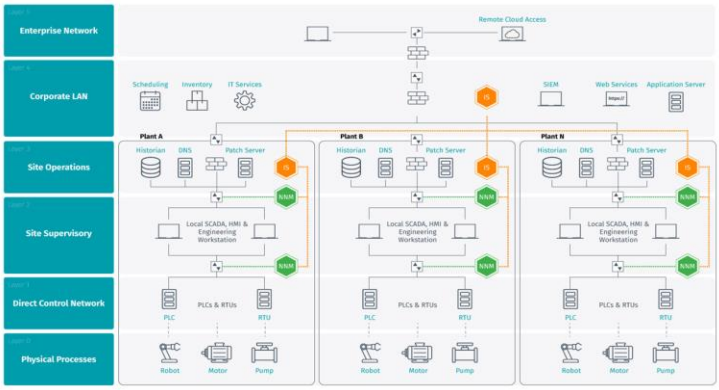
Solution Overview

Tenable's passive and active security solutions enable safe discovery and thorough assessment of converged IT/OT systems, enabling customers to understand and reduce risk.

Industrial Security
Industrial Security from Tenable, in concert with Nessus Network Monitor™ (NNM) sensors, delivers continuous asset discovery and vulnerability detection for safety critical operational networks. Purpose-built for operational technology (OT) systems, the solution uses NNM 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.

Tenable.io
Tenable.io helps organizations manage risk on IT networks connected to OT networks in converged IT/OT systems. Tenable.io includes passive, active and agent-based sensors to discover and thoroughly assess the full range of on-premises and cloud-based IT assets.

Tenable.io's active sensor includes ICS/SCADA smart scanning to thoroughly assess IT-based systems in the converged environment, while reducing the risk that active scanning will disrupt OT devices if they are inadvertently encountered during a scan.



Sample OT deployment of Industrial Security (IS) consoles and NNM sensors

Features and Capabilities for Converged IT/OT Systems

- Support for the full range of IT assets, including servers, desktops, laptops, network devices, web apps, virtual machines, mobile, cloud, and containers
- Support for OT systems from dozens of manufacturers, including Siemens, ABB, Emerson, GE, Honeywell, Rockwell/Allen-Bradley, and Schneider Electric
- Supported OT protocols include BACnet, CIP, DNP3, Ethernet/IP, ICCP, IEC 60870-5-104, IEC 61850, IEEE C37.118, Modbus/TCP, OPC, openSCADA, PROFINET, Siemens S7, and more
- Passive, active, agent-based sensors:
    - Identify and characterize hardware and software to automatically create and maintain an accurate asset inventory
    - Detect and prioritize a wide range of vulnerabilities

Benefits

Holistic View of Risks: A converged IT/OT solution provides a more complete picture of true exposure to better manage risks.

Reduced Downtime: By eliminating blind spots and associated vulnerabilities in converged systems you minimize gaps in protection, reducing potential exploits, downtime and safety risk.

Strengthen Security Framework Conformance and Regulatory Compliance: Asset inventory and vulnerability management are foundational controls in virtually all security frameworks and technical compliance regulations. Implementation of these controls helps demonstrate a robust security posture to business partners and regulatory bodies.

Reduced Total Cost of Ownership (TCO): Security solutions from a single vendor that address both IT and OT environments reduce training, operational and integration costs.

About Tenable

Tenable™, Inc. is the Cyber Exposure company. Over 24,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver Tenable.io, the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 20 percent of the Global 2000 and large government agencies. Learn more at tenable.com.

tenable™

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