SOLUTION BRIEF

OPERATIONAL TECHNOLOGY ASSET DISCOVERY AND VULNERABILITY ASSESSMENT

What are highest payoff actions you can take to measure and manage cyber risk in your operational technology (OT) environment? Here is a hint. These often overlooked actions are prescribed by virtually every best-practice guide, security framework and compliance requirement. The answer: 1) inventory and control your assets and 2) continuously manage vulnerabilities on those assets.

Continuous asset and vulnerability management are more than good hygiene. They help protect you from the costly operational consequences that can result from cyber attacks.

KEY CHALLENGES

Discovering All Connected Assets

IT/OT convergence is expanding your attack surface. It now includes, not only OT devices, but IT devices in your OT environment and connected business systems. You must manage the expanding attack surface resulting from digitization, and you cannot rely on manual or other periodic asset inventories to inform risk assessment.

Prioritizing Vulnerability Remediation

Most organizations simply cannot remediate all vulnerabilities in a timely manner. The number of vulnerabilities is typically overwhelming, and patching and rebooting happen infrequently. Therefore, you must identify the "must-remediate" vulnerabilities in advance so you can address them during your next maintenance shutdown, if not before.

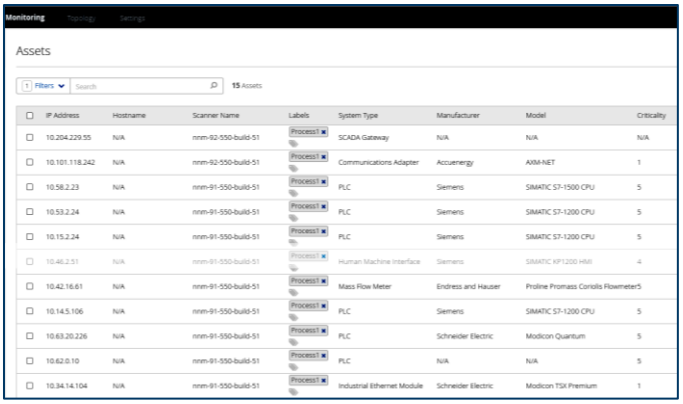
Augmenting Scarce Resources

The global shortage of personnel having expertise in both cyber security and control systems is slowing or even stalling OT risk assessment and cyber security maturation. The result is that organizations may not be able to manage the risk of the digitization projects they must undertake to increase efficiency and profitability.

SOLUTION REQUIREMENTS

Hardware Asset Inventory

Manual inventories are expensive, often incomplete, and quickly out-of-date. Automated approaches are required, and passive monitoring solutions are needed to avoid disrupting PLCs, RTUs, and other potentially sensitive devices. Based on deep packet inspection, passive solutions must be capable of identifying both OT and IT assets that are active on the network. The solution must identify system type, manufacturer and model, and it must support user-defined labels. Additionally, the system should alert when it discovers new assets so staff can confirm the additions were authorized.



IP Address	Hostname	Scanner Name	Labels	System Type	Manufacturer	Model	Criticality
10.204.229.55	N/A	nnm-92-550-build-51	Process1	SCADA Gateway	N/A	N/A	N/A
10.101.118.242	N/A	nnm-92-550-build-51	Process1	Communications Adapter	Accuenergy	AXM-NET	1
10.58.2.23	N/A	nnm-91-550-build-51	Process1	PLC	Siemens	SIMATIC S7-1500 CPU	5
10.53.2.24	N/A	nnm-91-550-build-51	Process1	PLC	Siemens	SIMATIC S7-1200 CPU	5
10.15.2.24	N/A	nnm-91-550-build-51	Process1	PLC	Siemens	SIMATIC S7-1200 CPU	5
10.46.2.51	N/A	nnm-91-550-build-51	Process1	Human Machine Interface	Siemens	SIMATIC KP1200 HMI	4
10.42.16.61	N/A	nnm-91-550-build-51	Process1	Mass Flow Meter	Endress and Hauser	Proline Promass Coriolis Flowmeter	5
10.14.5.106	N/A	nnm-91-550-build-51	Process1	PLC	Siemens	SIMATIC S7-1200 CPU	5
10.63.20.226	N/A	nnm-91-550-build-51	Process1	PLC	Schneider Electric	Modicon Quantum	5
10.62.0.10	N/A	nnm-91-550-build-51	Process1	PLC	N/A	N/A	5
10.34.14.104	N/A	nnm-91-550-build-51	Process1	Industrial Ethernet Module	Schneider Electric	Modicon TSX Premium	1

Comprehensive asset discovery informs security and operations

Asset Connections

Passive monitoring must document asset-to-asset communications so you can identify and investigate unexpected and/or unauthorized connections that could be exploited by an adversary.

Continuous Vulnerability Management

A vulnerability management solution must perform two functions well. First, it must continuously detect vulnerabilities in both OT and IT assets. It is very likely that the solution will discover many more vulnerabilities than you have resource to remediate. This leads to the second function.

The solution must also provide a mechanism to identify the most critical vulnerabilities. This mechanism must incorporate your knowledge of asset criticality, and it must rate vulnerabilities with more granularity than Common Vulnerability Scoring System (CVSS) base scores. CVSS base scores are interesting, but you need to details to prioritize remediation. Effective prioritization requires insight about the vulnerability, including knowledge of its impact on availability, accessibility by attackers, and exploitability. This detailed vulnerability information will help you plan remediation to be implemented next maintenance shutdown, if not before.

.

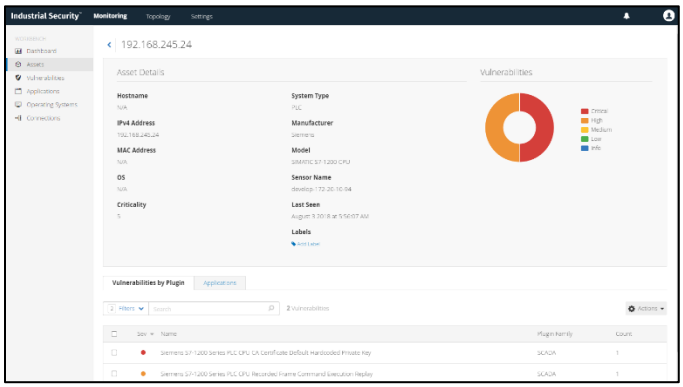
SOLUTION BRIEF

TENABLE AND SIEMENS SOLUTION

Tenable and Siemens are your partners to solve the asset discovery and vulnerability management challenges so you can measure and manage cyber risk.

Tenable 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 sensors to passively monitor network traffic and provide safe and reliable insight. You will know what assets you have, what assets they communicate with and what vulnerabilities you need to remediate.

Covering a wide range of ICS/SCADA systems, Industrial Security's passive monitoring sensors are placed in the network where they can "see" the network traffic to be monitored. For example, sensors could be placed on each subnet in a plant and at the egress point where the plant is connected to the corporate LAN. Industrial Security determines which hosts are active on the network, when new hosts become active, which ports/services are active and inter-asset connections. It also detects vulnerabilities in devices, applications and services.



Asset details include system type, manufacturer, model and vulnerabilities

Siemens Expertise
In addition to delivering and deploying Tenable's Industrial Security software on the control system network, Siemens provide technical expertise:

- Siemens domain experience informs vulnerability analysis to provide insights and context for reported vulnerabilities.
- Prioritization of vulnerabilities to provide deeper transparency and visibility across a plant and complete fleet.
- Translation of insights to remediation plans and actions based on Siemens understanding of operational implications.

KEY BENEFITS

- ***Understand and Prioritize Cyber Risk***
  Visibility of assets, connections and vulnerabilities informs your risk assessment.
- ***Prioritize Remediation***
  Vulnerability prioritization based on factors such as attacker accessibility, availability impact and exploitability helps you focus remediation on what matters most.
- ***Operational Improvements***
  Accurate and up-to-date asset inventories reduce mean-time-to-resolve unexpected outages.
- ***Siemens experts augment asset discovery and vulnerability assessment***
  Ensure consistent reporting, extend resource-constrained operations, and leverage expert advice on how to address cyber risk.

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 www.tenable.com

ABOUT SIEMENS

Siemens combines our deep operational technology (OT) know-how with cutting-edge technology partners to help our customers protect their complete operating environment, from the field to control to the enterprise network. Our broad geographic footprint in 190 countries gives us visibility across our install base. Attackers have no geographic boundaries. Energy companies need an OT provider with global coverage, one that secures its own environment, and understands the threat.