Passive Monitoring or Active Scanning for Operational Technology Environments

Which is the Best Approach?

TABLE OF CONTENTS

I. Executive Summary

Chief Information Security Officers (CISOs) and other security leaders are accountable for the cyber security of the entire value chain that creates and delivers their products. This is especially true for security leaders whose organizations' have undertaken IT/OT convergence initiatives to reduce cost, drive innovation and/or improve sustainability. IT/OT convergence has expanded the attack surface and requires security leaders to consider not only OT assets, but IT assets in the OT environment, and other business systems, such as ERP systems, building automation and control systems, and connected lab environments. However, many security leaders are challenged by lack of visibility beyond the IT environment.

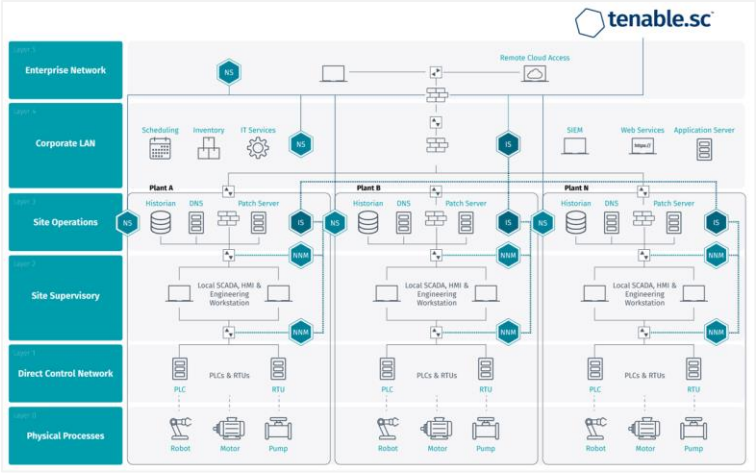
Security leaders require automated tools to inform them with comprehensive and current information. However, not fully understanding ICS operational constraints, they may suggest that IT security tools be deployed in ICS environments to provide a higher level of visibility. Conversely, OT security professionals may automatically resist IT security tool deployments citing unintended downtime as evidence that IT tools don't belong in OT.

Both camps have valid arguments, but neither should take an adamant stance. Rather, they should work together to deploy a mix of passive monitoring and active scanning solutions in a way that maximizes visibility and security without increasing the risk of downtime.

> "Traditionally, VA deployments relied on active network scanning, which can help with point-in-time assessments only. With the expansion in types of assets connected to enterprise network, nonstandard IT assets such as mobile devices, OT and IoT will benefit from passive observation using network-level scanners to achieve real-time visibility. Agent-based scans are suggested on laptops that rarely connect back to the enterprise network, and that would be missed with a network scan; or instances in IaaS that may not be online all the time. Gartner recommends that organizations combine active scanning with passive and agent-based scanning to augment the existing capabilities, as well as to have real-time visibility with improved asset coverage." Gartner, Hype Cycle for Threat-Facing Technologies, 2018, Pete Shoard, 13 July 2018 ID:G00338539

A guideline is to start with passive monitoring at all levels in the Purdue Reference Model, and gradually add active scanning – starting at the higher levels and cautiously moving down. Passive monitoring is not restricted to OT devices and can be deployed at all levels to provide near real-time visibility of assets and vulnerabilities of IT assets. Asset information provided by passive monitoring will inform active scanning's "do not scan" list so active scanning will not scan OT devices.

Active scanning could be initially deployed at level 5 (Enterprise Network) and 4 (Corporate LAN) and added at lower levels. However, each environment's network segmentation, real-time requirements, network capacity and device robustness are unique. Therefore, active scanning should be carefully configured, ICS/SCADA Smart Scanning should be enabled and thorough testing must be conducted prior to deployment in a live production environment.



Legend

- NNM — Nessus Network Monitor: passive monitoring sensor
- IS — Industrial Security: console to manage and display data from NNM sensors
- NS — Nessus: active scanner
- tenable.sc — Tenable.sc on-premises vulnerability management

II. The Technologies

Passive Monitoring

As the name implies, passive monitoring, uses deep packet inspection to analyze network traffic. Passive monitoring can determine which hosts are active on the network, when new hosts become active, which ports/services are active and inter-asset connections. Tenable's Industrial Security™ product, which is based on passive monitoring, also detects vulnerabilities in devices, applications and services.

Passive monitoring sensors must be placed in the network where they can "see" the network traffic to be monitored. For example, sensors could be placed on each network segment in a plant and at the egress point where the plant is connected to the corporate LAN. Typically, passive monitoring sensors are connected to a Test Access Point (TAP) port or to a network switch's Switched Port Analyzer (SPAN) port. TAP ports are preferred because SPAN port operation uses the switch's resources and may degrade switch performance.

Active Scanning

Active scanning, unlike passive monitoring, generates network traffic and interacts with devices on the network. The advantage of active scanning is it provides more information about assets than does passive monitoring. This additional information may include open ports, installed software, security configuration settings and known malware. Several active scanning variants are available, including unauthenticated scans, authenticated scans and agent-based scanning.

Unauthenticated (Network) Scans: Unauthenticated scans, also referred to as network scans, examine devices from the outside-in. For example, they attempt to communicate with each of the IP addresses in a specified IP address range. Once a device is found, the scanner typically attempts to get a response from each of the 65,535 TCP ports to determine which ports/services are open. UDP ports may also be scanned.

Unauthenticated scans can be run externally (from outside of the firewall) to see a network as an outside attacker would see it. Operational control environments should have limited, if any, internet facing systems. However, many instances of control systems being inadvertently open to the internet have been discovered. Unauthenticated scans can also be run by scanners installed behind the firewall. This gives them access to all systems accessible on the selected network segment.

Unfortunately, OT devices such as programmable logic controllers (PLCs) and remote terminal units (RTUs) that monitor the activity and state of machinery (e.g., pumps, valves and motors) and environmental factors (e.g., temperature, pH and vibration) may be too sensitive to withstand active scanning. This is especially true of older devices. Specifically, they may be sensitive for any of the following reasons:

- Limited CPU power: They can be overwhelmed when too many requests are added to their process control duties.
- Real-time communications: The protocols involved often expect an unbroken stream of readings from a device. If they're delayed substantially, they may have issues re-establishing communications. A full vulnerability scan probes many areas of a device very quickly, which can overly burden the limited CPU power and delay communications.
- Custom operating system and software: OT devices generally do not run widely used and widely tested operating systems, such as Windows or Linux. They may include a small HTTP server, but it likely includes a limited feature set. When a vulnerability scanner attempts to check SSL, which may not have been implemented, the embedded HTTP server could crash.

If actively scanned, these sensitivities may result in performance degradation or reboots – causing costly downtime and potentially unsafe working conditions.

Ideally, network segmentation would separate sensitive OT devices from IT-based OT systems, such as Windows-based HMIs. This would isolate them when active scanners probe the IT-based systems. However, in reality, such segmentation may not exist. In this case, the active scanner should be configured to not scan IP addresses belonging to known-sensitive OT devices. If an sensitive OT device's IP address changes or a new sensitive OT device is added, and that device is not omitted from the active scan the scan could disrupt operation.

Tenable Nessus®, an active scanning solution, reduces the risk of an outage with ICS/SCADA Smart Scanning. ICS/SCADA Smart Scanning cautiously probes devices using known OT protocols and default ports to quickly identify OT devices. If a device responds to the OT protocol/port, the scanner immediately stops scanning the device, and it records the device's IP address. At that point, the rest of the scan proceeds as configured for other devices. Subsequently, the scanning parameters can then be updated to exclude the discovered OT device in the future. Note: ICS/SCADA Nessus Scanning should be tested in a lab environment to ensure compatibility with the OT devices it might encounter during scanning.

Authenticated Scans: Authenticated scans, also called credentialed scans, remotely login to devices to examine them from the inside-out. Because authenticated scans interrogate devices from the inside-out they can gather a wealth of security-related information about installed software, security configuration settings and known malware.

Although authenticated scans do not require software to be installed on the target, they use memory, processing power and network bandwidth and can therefore cause degradation and disruption. Authenticated scans are best suited to the IT systems in the upper layers or the OT environment. They are often used in conjunction with unauthenticated scans to deliver both inside-out and outside-in views.

Agent-based Scans: As the name implies, agent-based scans are performed by software agents installed on the target devices. Similar to authenticated scans, agents see the device from the inside-out and can provide detailed information.

Agents are best suited to the IT systems connected to the control environment. The downside to agent scans is that the agents must be installed on a device and will consume memory, disk space, processing power and network bandwidth that will no longer be available to the primary application. This can be mitigated by configuring the agent to minimize resource usage. In some cases, vendor warranties prohibit agent installation or require certification and recertification when an agent is updated. Therefore, agents should be deployed very selectively in OT environments and only after thorough testing has been conducted and vendor warranties have been reviewed.

	Passive Monitoring	***Active Scanning***
Target assets	IT and OT devices operating in the converged IT/OT environment	IT devices operating in the converged IT/OT environment
Information provided	• Discovery and identification of assets that are active on the network • Installed applications and services that are active on the network • Vulnerabilities	• Discovery and identification of assets on the network • Installed applications, services and libraries, including version number and patch level. • Vulnerabilities • Enumeration of user, groups, installed software, running services, etc. • Configuration assessment based on CIS Benchmarks, DISA STIGS and vendor guidance for leading OSes, network devices, virtualization/cloud/container infrastructure, web servers/browsers, databases, and office productivity applications • Detection of default usernames and passwords for leading systems and applications • Malware detection, including known bad file hashes, backdoors • The presence and recent updates for leading AV products • If the asset has a patch applied that requires a reboot to finish

Timeliness	Passive monitoring operates continuously and detects new assets as they become active on the network. The asset and vulnerability information, available in advance of maintenance windows, informs remediation actions to be taken during the maintenance window.	Active scans are scheduled activities that occur at a point in time. The frequency can range from daily to being run only during maintenance windows. The Center for Internet security recommends weekly scans for IT environment. However, if active scans are conducted in OT environments, they are likely to be run less frequently.
Deployment considerations	• Passive monitoring requires TAP or SPAN ports • Define monitored IP addresses and ranges as needed	• Active scanners do not require TAP or SPAN ports • Restrict scanned IP addresses to omit sensitive OT devices • Restrict scanned ports/services to omit those known to be in use • Enable ICS/SCADA Smart Scanning to minimize impact on sensitive OT devices if they are inadvertently scanned
Caveats	• Sensors must be placed where they will "see" the desired network traffic • Will only detect devices that are active on the network	• May disrupt device operation • May degrade network performance and interfere with real-time operation • May conflict with warranties and service agreements

III. Tenable Solutions

Industrial Security

Industrial Security™, in concert with its Nessus Network Monitor™ (NNM) sensors, delivers continuous asset discovery and vulnerability detection for safety critical operational networks. Purpose-built for 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.

Features and Capabilities for Converged IT/OT Systems

- Support for thousands of 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
- Support for a wide range of IT assets, including servers, desktops, laptops, network devices, web apps, virtual machines, mobile, cloud, and containers

Tenable.sc

Tenable.sc helps organizations manage risk in IT assets connected to OT networks in converged IT/OT systems. Tenable.sc includes active and agent-based sensors to discover and gather a wealth of security-related information about installed software, security configuration settings and known malware for full range of on-premises systems.

Tenable.sc can automatically import selected asset and vulnerability data from Industrial Security to help security leaders understand and defend the entire attack surface. Tenable.sc reports and interactive dashboards can easily be tailored to present near real-time status of both IT and OT assets supporting critical operational processes.

Tenable.io

Tenable.io, a cloud-based cyber exposure platform, helps organizations manage risk on IT networks connected to OT networks in converged IT/OT systems. Tenable.io Vulnerability Management active and agent-based Nessus™ sensors discover and thoroughly assess the full range of on-premises and cloud-based IT assets.

Tenable.io's active Nessus scanner can easily be configured to not scan specific port and/or IP addresses.

IV. Implementation Guidance

Note: Tenable cannot guarantee that active scanning will not disturb system operation. Therefore, active scanning should be deployed in a live production environment it has been thoroughly tested and known not to disrupt operations. In some cases, vendor warranties prohibit active scanning and/or agent installation.

Successful implementation requires ongoing communication among IT and IT operational and security staff, as well as facilities personnel. Communication must start during the planning phase and extend through design and into deployment.

Baseline

Using the Purdue model as a reference, IT and OT staff must accurately understand the existing environment, including lines of demarcation, and each required communication path must be documented. It is wise to include area and device owners in the conversation so they can add clarifying details as needed. Planning should identify any devices, VLANs, and other network infrastructure that may need to be reconfigured or moved during the deployment.

Useful questions to address during planning include:

- What networks are isolated/air-gapped?
- Where are switches physically located?
- Are required networking ports available?
- Is there medium or high voltage that may require an electrician?
- What physical communication is available; fiber, copper, wi-fi?
- What electrical power is available?
- Are rack space, ports, cabling, etc. available?

Design

Design addresses sensor placement/configuration and sending data upstream for analysis and presentation. Using the technology discussion above, passive monitoring and active scanning sensors must be placed where they can collect data without impacting operational performance. Data from sensors must be sent upstream, on a non-operational network, where it can be analyzed. Design may uncover the need for:

- Additional or larger switches
- TAP/SPAN ports
- New cable runs
- New telecommunications cabinets.

Deployment

The need for up-to-date visibility provided by the combination of passive monitoring and active scanning is most acute where assets are most dynamic. This often includes supervisory control, process control and I/O devices. Because motors, robots, drives, etc. typically do not change often, they are a lower priority.

Deployment should occur in gradual steps, keeping the following principles in mind.

- Strong communication among all parties is critical. Operational staff must be notified of all pending changes and asked to immediately report any unexpected behavior of the network.
- Passive collection and analysis should be in place until all parties are confident that monitoring has not impacted operations.
- Active scanning should start at the highest level within the network and gradually work down to lower levels.
- Each downward movement of active scanning should have its own evaluation period before further progression is taken.

V. Conclusion

Market opportunities and competitive pressures are driving oil & gas suppliers, utilities and manufacturers to adopt initiatives to reduce cost, drive innovation and/or improve sustainability. The expanding attack surface resulting from these digitization initiatives that span both IT and OT creates cyber risk that must be measured and managed. Passive monitoring identifies and assesses vulnerabilities in both IT and OT assets if they are active on the network and will not disrupt operation of sensitive OT devices. Active scanning identifies and thoroughly assesses IT assets and applications, including workstations, network devices, databases, virtual infrastructure and the cloud.

The ideal implementation is to deploy passive monitoring at all levels of the Purdue model to gain real-time asset and vulnerability visibility and to deploy active monitoring at the upper levels of the Purdue model to gain deeper insight of workstations, network devices, virtualization/cloud/container infrastructure, web servers/browsers, databases, and office productivity applications.

Together passive monitoring and active scanning provide the asset inventory and vulnerability information security leaders must have to measure and manage cyber security risk.

VI. About Tenable

Tenable®, Inc. is the Cyber Exposure company. Over 27,000 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.

7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046
North America +1 (410) 872-0555
www.tenable.com