tenable.ot™

CRITICAL INFRASTRUCTURE CYBERSECURITY

DISRUPT OT ATTACK VECTORS IN THE NEW ERA OF DISTRUST

WHITE PAPER

CONTENTS

THE INDUSTRIAL CYBERSECURITY CHALLENGE

Today's sophisticated operations technology (OT) environments have large attack surfaces with numerous attack vectors.

Until recently, IT infrastructure was front and center for ensuring complete visibility, security and control for your network. That's mostly because this was ground zero for organizational attacks.

For the better part of two decades, this kept CISOs up at night, but that's no longer the full story.

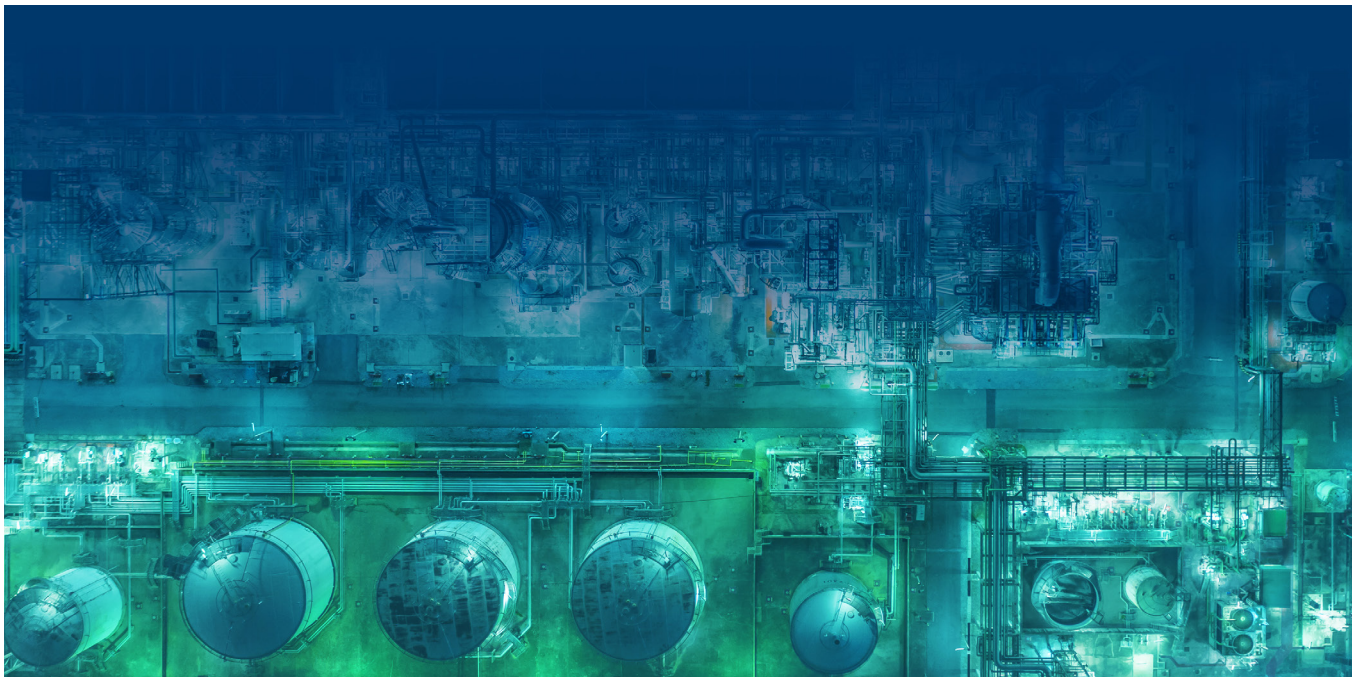
With our world increasingly interconnected through rapidly converging IT and OT environments, industrial and critical infrastructure operations have quickly caught up. They are now lightning rods for new attacks and increased security concerns.

Because OT systems were traditionally segregated and isolated, controllers were not designed to address the security threats or human errors we experience today. Outsiders, insiders and outsiders-masquerading-as-insiders are all potential threat actors that can launch sophisticated attacks with goals to take over machines for nefarious purposes.

Recently, hackers have evolved from rogue individuals to systematic programs launched by well-funded and highly motivated organizations and countries.

Network monitoring is a good first step to protect organizations, but is not enough to address the new and constantly evolving security threats that specifically target industrial operations. You need visibility into your entire operation including your industrial control system (ICS) environment and your converged IT/OT infrastructure.

You can accomplish this with a forward-leaning security posture.



Here are some ways to identify key elements to progress beyond simple passive monitoring so you can secure your industrial organization from these clear and present threats:

WHERE DO OT THREATS EXIST?

In OT environments, risky behaviors and activities can exist on your network and devices.

In fact, many operations conducted on a device will never traverse your network. Critical asset inventory information such as records of user logins and controller firmware versions—as well as changes to devices made via direct connections—don't typically present themselves in network traffic.

If network monitoring misses an attack on a device, it can remain infected for days, weeks or months without detection. That's because network monitoring only provides operators with 50% visibility and coverage across your OT environment.

As a result, you need an OT security solution to address threats that exist on your network and the devices on it.

SECURITY BEYOND YOUR NETWORK

Go beyond simple network monitoring and include device-based security for significantly better situational analysis for your OT environments.

Active querying surveys devices in your OT network and should provide deep situational awareness down to an extremely granular level. This capability enhances your ability to automatically discover and classify all of your ICS assets—from Windows machines to devices like programmable logic controllers (PLCs) and remote terminal units (RTUs), even when they aren't communicating across your network.

Active querying also identifies local changes in device meta-data (e.g. firmware version, configuration details and state), as well as changes in each code/function block of device logic. For it to be completely safe and not negatively impact queried devices, it is essential the technology uses read-only queries in native controller communication protocols.

Active querying complements network monitoring by collecting information that is impossible to find in your network, yet is crucial for all the benefits described earlier. It is also key in providing additional context for security alerts.

Since active querying eliminates the need to monitor every switch in your organization, it can save maintenance costs while enabling more flexible deployments. If your environment is route-able, you can get information on all devices, with a single appliance.

KEY INGREDIENTS TO SECURE YOUR OT ENVIRONMENT

Not all OT security vendors are equal. Some do not provide any form of active querying functionality because they believe it is "too dangerous."

Of course, anything done incorrectly can be dangerous, but executing active querying is safe and leverages technology built for your PLC or distributed control system (DCS).

Other vendors provide a method for device checks, but if not performed in the device native language, it can make the system unstable. In other cases, checks do not provide the level of situational awareness required and leaves you vulnerable.

When you evaluate OT security solutions, there are some basic requirements you should address at the network level and the device level, including visibility into what is happening, security against attacks, and control over your OT environment.

> Here are some of the requirements for each of these areas:

VISIBILITY

In-Depth Enterprise Visibility

At the most basic level, information flows across your OT network. Devices create data on your network. Thus, maintaining a granular and up-to-date asset inventory is key to help you control your OT environment.

Most importantly, asset data normally does not traverse your network. The device stores can be "dormant"—and don't transmit details such as user logins, latest hotfixes installed on PCs and servers, firmware versions, open ports and lists of controllers.

Active querying solves this problem by querying devices and automatically gathering the most comprehensive and critical information about every asset in your environment.

Capturing "Blind Spots"

Active querying discovers dormant industrial devices connected to your network that are not communicating. Most industrial control vendors support a "find me" mechanism that's built into their controllers and enables detection with a single broadcast of a unique packet. This is how engineering stations (HMIs) can automatically find all controllers in your network.

Active querying uses that same built-in mechanism and ensures your asset inventory is complete and accurate.

SECURITY

Safeguarding From Malicious Behavior and Human Error

It is common for employees, contractors and integrators to connect to control devices with a serial cable or USB. A malicious actor with physical access to your network can also connect to controllers this way.

Authorized or not, network monitoring cannot detect changes to the controller code, firmware or configuration. It is also plausible an employee or contractor can unknowingly expose controllers to threats by using a compromised device, for example a laptop or USB drive infected with malware. By periodically capturing device snapshots and comparing them to previous baselines, you can identify changes and validate that no one has compromised device integrity.

Insights Into Vulnerability and Risk

By regularly querying servers and controllers for details such as the OS and firmware version, open ports, latest software, hotfixes, hardware configuration, patch level and more, active querying can proactively achieve complete awareness of the most current vulnerabilities that may put your industrial controllers at risk.

This gives you more accurate risk scoring, which is augmented based on non-networked data. Rather than waiting for the device to pass information over your network, active querying retrieves the most updated and accurate device information and arrests attack propagation before it hits your network.

CONTROL

Greater Efficiency for Incident Response

Alerts can be meaningless without added contextual information, for example: which user is logged into your engineering station at a specific time and the impact of specific activity to the PLC ladder logic.

When detecting a suspicious network event, active querying uses native protocols and automatically queries relevant devices to gather further contextual details. Compared to a network-only solution, this provides more meaningful alerts and results in significantly improved situational awareness and faster forensic and mitigation activity.

Lower Total Cost of Ownership (TCO)

A major disadvantage of network-only technologies is the necessity to deploy them at every intersection and switch within your network that requires monitoring. This can be costly for a large environment with multiple subnets.

The typical method to save hardware and maintenance costs is to deploy fewer appliances in your network. This often results in the sacrifice of control and/or visibility when you use a network-only approach. Active querying technology enables monitoring of all routable sections of your network with a single appliance.

Operations Resiliency

Unless there is backup that traces changes made to control devices, incident recovery can be difficult. With active querying, you can simplify architecture and reduce costs at the same time.

By capturing a complete snapshot of the device including firmware, configuration, complete ladder logic, diagnostic buffer and tag structure, you can keep track of a full history of controller versioning and identify a previously known “good” state.

SAFE, SMART ACTIVE DETECTION

To fulfill requirements noted above, Tenable.ot has patented active querying technology and passive detection.

> With Tenable.ot, you can:

- **Query devices in native language, when positively identified** – Tenable.ot's active querying never uses communication protocols the device might not support or that are not native. It also never "blindly scans" your network looking for devices. Only after positively identifying a specific asset, including vendor model and version, will active querying activate and start querying that asset to gather information.
- **Granular Fine Tuning** – Choose which areas for the network you want to passively scan and which device you want to actively query. Tenable.ot affords administrators the flexibility to define which detection methods to apply and at what interval.
- **Access industrial controllers as they are designed** – Most industrial controllers use different electronic modules for different purposes. Consequently, the network module executes ethernet-based communication with engineering station software, which isn't part of the critical control loop. Additionally, mission-critical I/O activity has its reserved processing resources, which prevents network traffic overload. If the controllers aren't exploited or maliciously scanned, an overload will not occur.
- **Customize schedules and policy settings to your business needs** – Choose your query frequency: every 8 hours, only at specific times of day, for specific subnets, or only by manual activation. With Tenable.ot, you can customize policies to query only predefined sets of IP ranges or asset types. You can also check your network and CPU loads on devices before surveying them.
- **Read-only activity out-of-band** – Tenable.ot's active querying utilizes read-only communication and by design can't change configurations and settings of any of the devices in your network.
- **Apply a tailored approach for each vendor** – Tenable works closely with controller vendors and performs extensive lab tests with physical devices to ensure queries have no impact on controllers and do not have the potential to cause disruptions.

ADDRESS OT ATTACKS WITH ACTIVE QUERYING

When it comes to addressing the next generation of cyber attacks targeting your OT environment, network-only monitoring is not sufficient to reduce risk and keep your environment secure.

By employing a solution that addresses both the network and devices on it, you can see your entire industrial OT system, including converged IT/OT environments, rather than just a portion.

When performed properly, device checks are safe and the only way to ensure complete visibility, security and control for your OT network—today and to scale for the future.

ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. Over 30,000 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 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 30 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.

tenable.ot™