tenable OT Security

SOLUTION BRIEF

TENABLE OT SECURITY ACTIVE QUERYING TECHNOLOGY

Business Challenge

Today's converging IT/OT environments have a large attack surface with numerous attack vectors that can take advantage of IT, IoT and OT assets. To reduce the level of risk and cyber exposure in your industrial or critical infrastructure environment, network monitoring is not enough. In fact, leveraging network only detection can miss up to 50% of the information and insights needed to keep your organization safe.

You need the ability to access the details that provide in-depth knowledge and insights both at the network and device levels. Without it, you can only hope that unauthorized activities or external threats do not compromise your industrial infrastructure.

Solution

Tenable OT Security leverages patented active querying technology (US Patent #10,261,489) that employs read-only queries in native device communication protocols. This yields deep details on the state of each industrial asset in a safe manner and without any impact on queried devices.

Active querying is the result of working closely with controller vendors and by performing extensive lab tests with OT devices. Doing so ensures that queries have no impact on the controllers and do not have the potential to cause any disruptions.

Active querying yields a more comprehensive collection of information and helps you:

- **Discover** all assets on your network, including devices like programmable logic controllers (PLCs), remote terminal units (RTUs).
- **Uncover** all "dormant" assets that are not communicating on your network.
- **Classify** each asset based on device type.
- **Collect** all relevant configuration and metadata, including hotfix levels, firmware version, users and backplane info. If a vulnerability or security incident occurs, an alarm gets prioritized and sent to relevant personnel with detailed information.
- **Track** all configuration changes on any asset along with the ability to deliver a complete snapshot that highlights the delta with rich information on the "before and after."

What Industrial Cybersecurity Professionals Need

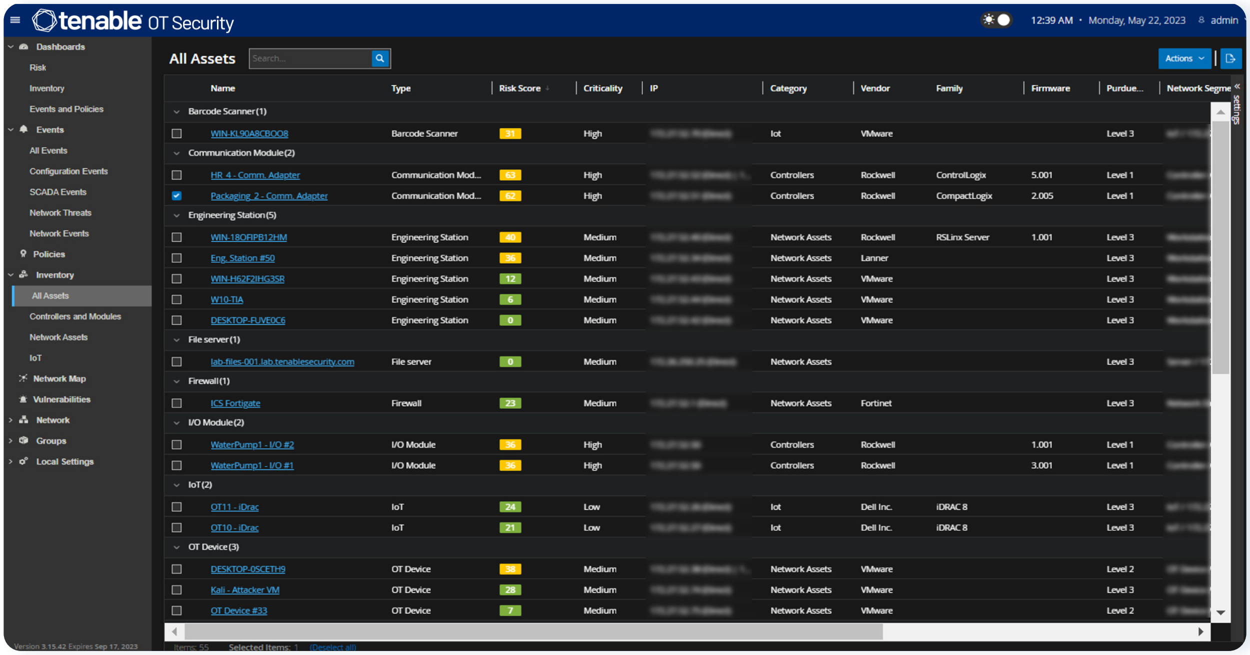
- A comprehensive solution that can scale across converged IT/OT environments
- Vital up-to-date data and situational awareness on all assets and the networks they run on
- Contextual and meaningful alerts with drill down capabilities for root cause analysis
- Alerts to any changes made to control devices
- Ability to address today's OT security challenges with flexibility as requirements change

Value

Tenable OT Security ensures the integrity of your industrial network. It provides deep situational awareness while also tracking every change made to every device in your network. This includes everything from operating systems and software, through firmware and configurations, all the way down to ladder logic.

Benefits include:

- Timely insights into your OT network, with the most detailed information — operating systems, firmware, configurations, ladder logic and more
- Vital, up-to-date data on all assets, vulnerabilities and security risks
- Alerts to any changes made to control devices
- More contextual and meaningful alerts; fewer false positives



All Assets

	Name	Type	Risk Score	Criticality	IP	Category	Vendor	Family	Firmware	Purdue...	Network Segme
	Barcode Scanner (1)										
☐	WIN-KL90A8CBOO8	Barcode Scanner	31	High	[redacted]	Iot	VMware			Level 3	[redacted]
	Communication Module (2)										
☐	HR 4 - Comm. Adapter	Communication Mod...	63	High	[redacted]	Controllers	Rockwell	ControlLogix	5.001	Level 1	[redacted]
☑	Packaging 2 - Comm. Adapter	Communication Mod...	62	High	[redacted]	Controllers	Rockwell	CompactLogix	2.005	Level 1	[redacted]
	Engineering Station (5)										
☐	WIN-18OFIPB12HM	Engineering Station	40	Medium	[redacted]	Network Assets	Rockwell	RSLinx Server	1.001	Level 3	[redacted]
☐	Eng. Station #50	Engineering Station	36	Medium	[redacted]	Network Assets	Lanner			Level 3	[redacted]
☐	WIN-H62F2IHG3SR	Engineering Station	12	Medium	[redacted]	Network Assets	VMware			Level 3	[redacted]
☐	W10-TIA	Engineering Station	6	Medium	[redacted]	Network Assets	VMware			Level 3	[redacted]
☐	DESKTOP-FUVE0C6	Engineering Station	0	Medium	[redacted]	Network Assets	VMware			Level 3	[redacted]
	File server (1)										
☐	lab-files-001.lab.tenablesecurity.com	File server	0	Medium	[redacted]	Network Assets				Level 3	[redacted]
	Firewall (1)										
☐	ICS Fortigate	Firewall	23	Medium	[redacted]	Network Assets	Fortinet			Level 3	[redacted]
	I/O Module (2)										
☐	WaterPump1 - I/O #2	I/O Module	36	High	[redacted]	Controllers	Rockwell		1.001	Level 1	[redacted]
☐	WaterPump1 - I/O #1	I/O Module	36	High	[redacted]	Controllers	Rockwell		3.001	Level 1	[redacted]
	IoT (2)										
☐	OT11 - iDrac	IoT	24	Low	[redacted]	Iot	Dell Inc.	iDRAC 8		Level 3	[redacted]
☐	OT10 - iDrac	IoT	21	Low	[redacted]	Iot	Dell Inc.	iDRAC 8		Level 3	[redacted]
	OT Device (3)										
☐	DESKTOP-0SCETH9	OT Device	38	Medium	[redacted]	Network Assets	VMware			Level 2	[redacted]
☐	Kali - Attacker VM	OT Device	28	Medium	[redacted]	Network Assets	VMware			Level 3	[redacted]
☐	OT Device #33	OT Device	7	Medium	[redacted]	Network Assets	VMware			Level 2	[redacted]

Version 3.15.42 Expires Sep 17, 2023

Items: 55 Selected Items: 1 (Deselect all)

Figure 1. Enterprise-wide landscape with drill-down details on all assets on an OT

Why You Need Active Querying

- Network sniffing alone cannot collect all relevant information needed to ensure complete OT visibility or security
- Comprehensive and detailed alerts provide full context at the network and device level to give you more efficient and immediate incident response
- Discovery of dormant devices that don't communicate over the network
- Any change, even if done directly onto a device, must be visible
- Detection and tracking of any and all changes made directly or over the network to OT devices
- Stable and highly efficient communication with PLCs and DCSs in their own native language

About Tenable

Tenable® is the Exposure Management company. Approximately 43,000 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 approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies.

Learn more at www.tenable.com.

How It Works

- Query devices in native language, when positively identified
- Active querying never uses commands the device might not support or are not native
- Active querying is read-only and out-of-band. By design, it does not have the ability to change configurations and settings of any devices.

Get Started with Tenable OT Security Today

Passive network monitoring alone can miss crucial device based data and deep situational awareness required to secure your OT environment. Tenable OT Security can reduce your cyber exposure and OT threats by leveraging both passive detection and patented active querying technology.

Visit Tenable's solution webpage to learn how we can help you evaluate your current OT security capabilities, assess gaps in your program and develop a plan to begin your journey to a unified risk-based platform for IT and OT security today.

Contact Us:

Please email us at sales@tenable.com or visit tenable.com/contact