

WÄRTSILÄ GIVES CUSTOMERS OT VISIBILITY TO PROTECT CRITICAL INFRASTRUCTURES WITH TENABLE OT SECURITY



Industry: Marine and Energy

Location: Finland

Revenue: EUR 5.8 Billion

Marine and energy innovator, Wärtsilä, is managing its operational technology (OT) asset inventory collection and providing holistic visibility into its OT environment using Tenable OT Security. The deployment allows Wärtsilä to answer its customers' questions around asset delivery, reducing supply chain risks and taking a proactive stance on cybersecurity.

"The visibility Tenable OT Security delivers helps our customers protect critical infrastructure and adhere to regulations and compliance requirements in a forthright and measured way."

That's how Wärtsilä's Cyber Security Expert, Ross Bailey, describes the value of Tenable OT Security's automated asset discovery to its suppliers and customers.

Wärtsilä and Tenable OT Security

Spreadsheets and Manual Data Entry Led to Errors and Compliance Challenges

A global leader in innovative technologies and lifecycle solutions for the marine and energy markets, Wärtsilä emphasizes innovation in sustainable technology and services to help its customers continuously improve environmental and economic performance.

Building a modern power plant or marine vessel requires hardware and software solutions from a variety of suppliers. Customers need to understand every component, down to the firmware and serial number. Adding to the urgency, the European Cyber Resilience Act (CRA) will impose cybersecurity obligations on all devices that have a network connection.

Wärtsilä set out to address these challenges by creating automated asset inventory collection, streamlining compliance reporting, and enabling OT vulnerability reporting.

In the past, the suppliers who installed the equipment for Wärtsilä's customers created an asset list in an Excel spreadsheet. The manual process was time consuming, error prone, and only relevant for a specific point in time. Technicians had to merge files when new devices were added.

Wärtsilä needed to make the process easy, repeatable, and always up to date for its customers.

Tenable OT Security Automates Asset Discovery and Visualization at Scale

Tenable OT Security enables Wärtsilä to identify assets, communicate risk and prioritize action all while enabling its IT and OT teams to work better together. Knowing exactly which assets exist, their configurations and full situational awareness of both sides of the house, empowers the security team to see and understand the big picture.

According to Bailey, Wärtsilä tested several vendor technologies before selecting Tenable OT Security.

“Many of these asset management tools are passive – they sniff the network by looking at the traffic at the mirror port and using that information to decipher assets. Tenable uses a proprietary approach to query devices in a safe way, PLCs for example, to get rich asset information. And that’s where it really shined for us,” says Bailey.

Tenable OT Security’s automated asset discovery and visualization capabilities provide a comprehensive, up-to-date inventory of all assets. This includes workstations, servers, human machine interfaces (HMIs) and programmable logic controllers (PLCs), including

dormant devices that do not communicate frequently over the network. The latter it uncovers by leveraging its patented active querying capabilities. The results are detailed device information, such as firmware and OS versions, internal configurations, and serial numbers.

Wärtsilä is preparing itself and its customers to operate in a new regulatory landscape. “With regulations like the Cyber Resilience Act coming into law, the need to disclose real-time vulnerability information in a short amount of time adds a huge challenge we’d not be able to meet without a solution like Tenable OT Security,” says Bailey.

As Wärtsilä rolls out the Tenable OT Security solutions across its dynamic environment, the partnership with the Tenable team has been crucial for a successful deployment.

“The great thing about using Tenable OT Security is working with the Tenable people,” says Bailey. “They have great technical expertise, appropriately sizing our environment and positioning us to scale as our licensing needs grow.”

Wärtsilä Helps Customers Visualize Asset Inventory and Protect Key Infrastructures

Now, Wärtsilä has the capabilities to deliver a complete asset inventory to its customers. During site acceptance testing, Tenable OT Security is integrated with each customer’s environment to provide a way to scan the project delivery and existing assets to obtain a complete asset inventory, as well as allow manual asset enrichment for legacy devices. This improved visibility helps customers protect critical infrastructure while meeting compliance requirements.

“There is no silver bullet when asset scanning in an OT environment – you can’t get to 100 percent. Some of these old devices are not compatible with

any proprietary protocols or even Simple Network Management Protocol,” says Bailey. “A flexible tool like Tenable OT Security, which allows for manual asset enrichment, is essential.”

Wärtsilä is also helping its customers save time and increase productivity. Before integrating Tenable OT Security, the asset inventory was tedious and time consuming, taking, on average, two technicians around seven hours per installation. Automated processes help technicians work more efficiently, which increases the number of completed installations each day, with improved accuracy.

About Tenable

Tenable® is the Exposure Management company. More than 40,000 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.

"Automating the asset inventory process saves Wärtsilä's suppliers several hours of tedious work, while improving the accuracy of the inventories for customers," says Bailey. "With fewer errors and more consistency in the data, Wärtsilä is able to standardize and normalize the data."

Tenable OT Security can also create an asset map based on what it senses on the network. As various OT assets "talk" to each other across the network, Tenable OT Security uses that information to gather valuable context. How are the assets connected? What else are they connected to? How are these assets related to one another?

"Our vision is to use Tenable OT Security to create a digital twin – a 3D map of how devices are connected and snapshots of all configuration changes – with near real-time asset visibility," adds Bailey. "In the past, we've done it on an ad hoc basis, but the data is only good for that point in time, the process is time consuming, and we may not get all of the device context we need."

In addition to providing customers with complete and accurate asset inventories, Tenable is enabling Wärtsilä to develop new services that help customers visualize their OT environment. **Tenable Security Center**, a vulnerability reporting engine that gathers and evaluates vulnerability data distributed across the enterprise, will enable rich reports that illustrate vulnerability trends over time, allowing Wärtsilä's customers to assess risk and prioritize vulnerabilities.

"In the future, we will install Tenable Security Center and provide a dashboard and reports to customers through a service we're calling the 'Asset Visualization Service'. When customers don't know what assets they have, we can provide an inventory and a vulnerability report," says Bailey.

Read the [press release](#) about how Wärtsilä is Solving OT Asset Management challenges for its energy customers.

