CASE STUDY

CITY OF RALEIGH ENSURES SAFETY AND SUSTAINABILITY OF PUBLIC WATER WITH TENABLE.OT

> "Thanks to Tenable.ot, I can spend less time on inventory management and more time on investigating and remediating actual threats and vulnerabilities."

STEVE WORLEY SCADA
SECURITY MANAGER

ORGANIZATION SNAPSHOT

Organization: City of Raleigh Municipal Government, North Carolina

Constituents Served: 570,000

Water And Wastewater Treatment Plants: 5

Total Volume Processed By The City's Largest Plant :

Approximately 18 Billion Gallons Of Wastewater Per Year

Industry: State and Local Government

Challenges:

- Lack of visibility into all operational technology (OT) assets
- Difficult and time-consuming to manually track OT asset inventory
- Inability to confirm maintenance work performed by third-party contractors
- Need for compliance with new regulatory requirements

Solution:

tenable.ot™ operational technology

Results:

- Enhanced productivity and efficiency with detailed asset inventory management through automated discovery
- Stronger security and control with the ability to know about any change to their network
- Consolidated view with comprehensive situational awareness of all OT assets
- Compliance readiness leveraging detailed audit trails that demonstrate the requirements for regulatory agencies

CITY OF RALEIGH MUNICIPAL GOVERNMENT, NORTH CAROLINA

The City of Raleigh is responsible for providing water and sanitary sewer services to the residents of Raleigh and adjacent areas. These services are managed and maintained by the technical applications group, which is responsible for the supervisory control and data acquisition (SCADA) network operations and security.

Aware of the growing cyber threat to critical infrastructure facilities and the need to comply with new regulations concerning risk assessment and emergency response, the team decided to upgrade its SCADA security solution.

CHALLENGES

To ensure safe and resilient infrastructure and detect security threats that could harm the water supply and disrupt critical services, Raleigh's public utilities department required full visibility and control of changes made to programmable logic controllers (PLCs) and other key devices in their industrial control system (ICS) environment.

The team realized that network traffic monitoring only provides a piece of what's needed to secure their ICS environment. Accordingly, they were interested in adding an active detection component that could work alongside passive network monitoring to provide critical information about the ICS environment that cannot be gathered solely by listening to network traffic.

SOLUTION

After a thorough RFP process, Steve Worley, SCADA security manager for the City of Raleigh, selected Tenable.ot. "We chose Tenable.ot for its unique ability to monitor, proactively detect and alert our staff to any changes made to our industrial control systems that could impact their integrity and proper operation," says Worley.

- **Gain visibility with rich context**

  Tenable.ot's patented active detection technology enabled Raleigh's SCADA engineers to achieve complete security coverage. The solution discovers, classifies and queries all ICS assets and devices – even those not communicating in the network. Native device querying ensures zero impact on network operations. Additionally, asset inventory details and enriched context for alerts helped improve alert accuracy – ultimately boosting efficiency and productivity for their security team.

- **Control and track all devices**

  Tenable.ot automatically maps all controllers and devices on the network, documents their configuration and provides in-depth visibility into their state. The inventory contains unparalleled asset information depth – tracking firmware and OS versions, internal configuration, running software and users, as well as serial numbers and backplane configuration for both PCs and industrial controllers.

- **Stay secure with real-time alerts**

  In addition to the ability to log into a dashboard, Tenable.ot provides real-time alerts for Raleigh with detailed contextual information gathered from devices, including data about suspicious activities and unauthorized changes. This information enables engineering and security to work together quickly, helping them identify the source of potential problems and mitigate risks.

- **Comply with regulations through documented audit trails**

  Tenable.ot provides a comprehensive audit log detailing all engineering activities related to the devices. By capturing the who, what, when, where and how, the audit trail gives the security team full situational awareness, empowering them to quickly pinpoint problems and remediate accordingly.

IMPACT

Since implementing Tenable.ot, Worley has gained full visibility into any change on his OT network and streamlined compliance efforts.

- **Speed and efficiency**

  Given the size and complexity of the SCADA environment, automated asset discovery was a must-have requirement. "Within minutes of installing the Tenable.ot solution, we could automatically collect and display huge amounts of data on our network that would have taken weeks to gather manually," says Worley. The automation provided asset names and IP addresses, MAC addresses and the like, which are useful for network management. Everyone on Worley's team could see these details, as well as access the asset map via the Tenable.ot dashboard.

- **Stronger security with situational awareness**

  The fact that Tenable.ot offered both passive and active components provided real value for the City of Raleigh. Specifically, the ability to actively query PLCs and learn what programming changes had been made, including versioning history, was a major advantage. "Prior to Tenable.ot, we didn't really have a way to get that version information as changes were made. Now, we have a timestamp on when the changes are made and we can determine who made those changes and hold them accountable," explains Worley. This was particularly relevant for monitoring the activities of any third-party contractor or systems integrator who makes changes to PLCs on a regular basis.

- **Regulatory compliance and expert support**

  With the detailed audit trails and the support of Tenable engineers, Worley's team smoothly deployed the Tenable.ot solution within its public utilities' ICS/SCADA network. The initial system was up and running on the first day, providing the City of Raleigh's team with all the data they needed to both meet the requirements and maintain complete visibility and control over all industrial operations.

About Tenable

Tenable® is the Exposure Management company. Approximately 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.

CONCLUSION

Using Tenable.ot, the City of Raleigh now has a comprehensive view of their cyber risk across their OT infrastructure.

The solution also provides automated asset discovery and management, which is key in boosting team efficiency and productivity. The manual processes previously used for inventory management were both time-consuming and error-prone, making it difficult to maintain an accurate inventory of ICS assets, which is crucial for risk assessment and regulatory compliance.

The automated asset management combined with the passive detection, active querying and full audit trail of any change to their network are critical capabilities for their operational reliability and safety. Together, they enable IT and OT managers alike to plan maintenance schedules, track changes made to devices, restore misconfigured devices and comply with new regulations.

MORE INFORMATION

Learn more about Tenable.ot:

www.tenable.com/products/tenable-ot

Contact us: marketing@tenable.com