CASE STUDY

tenable

Washington State Public Utility Ensures Reliable Power and Water to Constituents with Tenable.ot

> *"We found that Tenable understood cybersecurity from an industrial control system perspective, not just an IT perspective. And that's what really drew us to them."*

PAUL SIEGMUND
Manager of Automation and
Technology Services

ORGANIZATION SNAPSHOT

COMPANY

Public Utility District #1 of Whatcom County (WPUD)

YEAR FOUNDED

1937

AVERAGE TOTAL MEGAWATTS OF ELECTRIC POWER SUPPLIED

27 MWh

TOTAL GALLONS OF WATER TREATED/DELIVERED PER YEAR

5.4 Billion

INDUSTRY

Power & Utilities

CHALLENGES

- Ensuring capture of any threat to electricity and water services
- Protecting IT/OT networks from sophisticated external cyber threats
- Achieving full visibility into any changes made to industrial controllers
- Expediting network traffic analysis and troubleshooting processes

SOLUTION

tenable.ot
Powered by Indegy

IMPACT

- Gained visibility into all network traffic through continuous packet capture
- Shortened WPUD's learning curve with intuitive user interface
- Improved cyber readiness against remote, local and insider threats
- Boosted accuracy and analyst efficiency through flexible policies and alerts that prioritize real threats
- Achieved peace of mind with complete visibility and control of any configuration change in any controller

PUBLIC UTILITY DISTRICT #1 OF WHATCOM COUNTY (WPUD)

Public Utility District #1 of Whatcom County (WPUD) has countywide authority to provide electric and water services. It currently supplies an average of 27 megawatts of energy to its load customers in the county. WPUD's electric system consists of 15 miles of transmission and distribution lines and three substations.

Aware of the growing need to protect its critical infrastructure from cyberattacks and insider threats, WPUD sought an industrial-oriented cybersecurity solution that would give it better visibility and control of its OT network.

CHALLENGES

Over the past 15 years, WPUD has modernized its electric substations and water plants to streamline operational efficiency. However, the introduction of digitized control systems with remote access and connectivity to IT networks has also raised the exposure of WPUD's operational technology (OT) network to cyberattacks that could potentially lead to equipment failures and power outages.

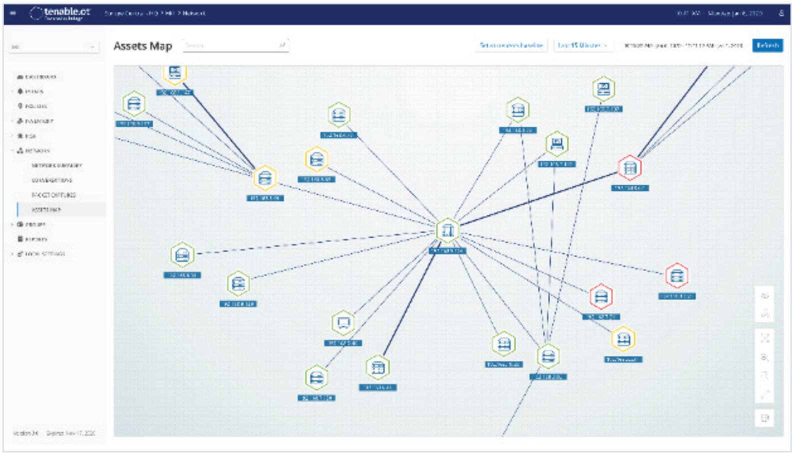
"Cybersecurity has always been one of our concerns, both on the IT side and the OT side," said Paul Siegmund, manager of automation and technology services at WPUD. "We were looking for a solution that could protect us from both remote and local attacks, including insider threats." WPUD's industrial controllers are the crown jewels of its operational network. To ensure service continuity, WPUD required full visibility and alerts on any changes made to controllers and other key devices in its transmission and distribution environments.

The ability to constantly monitor and capture network packets was another key requirement for WPUD. The open-source tools previously used by WPUD for packet analysis were cumbersome and inconvenient to set up, which hindered its troubleshooting of network-related issues.

SOLUTION

Tenable.ot was initially deployed within WPUD's industrial control system (ICS) network in 2016, providing Siegmund and his team with complete visibility and control over WPUD's critical operations. Since then, WPUD has benefited from the addition of new features that have further enhanced the product.

- **Comprehensive Threat Detection**
  Using Tenable.ot, WPUD can detect and receive alerts on threats coming from external (e.g., malware) and internal sources. Tenable.ot identifies anomalous network behavior, enforces network security policies and tracks local changes on devices so that WPUD is always aware of any threat to its ICS environment. Context-aware alerts with detailed information, as well as a comprehensive audit trail, allow WPUD to quickly mitigate cyberattacks and malfunctions that could impact service continuity or people's safety.



__Illustrative Data:__ Tenable.ot provides a simple-to-use mapping of all OT assets to help you effectively remediate cyber risks.

- **Automated Asset Tracking**
  Tenable.ot automated asset tracking provides WPUD with comprehensive visibility, security and control over its ICS environment. The system gathers and tracks all device-related activities, creating an up-to-date inventory of WPUD's controllers and assets, including dormant devices. Tenable.ot automatically maps all controllers and devices on the network, documents their configuration, and provides in-depth visibility into their state. This includes complete controller code snapshots, with detailed version history, to meet WPUD's backup and recovery needs.

- **Audit Trail**
  Tenable.ot can be set to perform continuous packet capture, as well as provide WPUD with a comprehensive audit log detailing all engineering activities related to its controllers. By capturing the who, what, when, where and how, this auditing capability lets WPUD engineers quickly discover the root cause, identify the responsible party and facilitate remediation.

- **Policy-based Detection**
  WPUD is using the Tenable.ot policy-based detection feature to configure its own customized security rules in minutes. Using a flexible, wizard-based interface, WPUD can modify the pre-defined "best practice" policies or create new ones as needed. Together with anomaly-based detection, these flexible rules help WPUD effectively enforce its ICS network security policies against any type of threat, as well as significantly reduce the number of alerts.

IMPACT

- **Control of All Controllers**
  Tenable.ot lets WPUD's engineers know exactly what's happening in their network at all times. Using both passive and active detection technologies, Tenable.ot automatically tracks every configuration and code change in WPUD's ICS environment – whether performed remotely or locally – along with detailed version control. "The Tenable.ot product assures me that the firmware and the program that's in my controller is what I installed, and that nothing's changed since then," said Siegmund.

- **Flexibility and Ease of Use**
  WPUD is using the intuitive Tenable.ot policy configuration tool to set up security policies specific to its own environment. For example, any time the programmable logic controller (PLC) code changes, WPUD engineers receive an alert with full activity information. Beyond that, the tool allows WPUD to create new policies so they don't get inundated with alerts that aren't important. "The flexibility for configuring the policies is great. It's easy to set up. You don't have to understand fancy rules like you do with most firewalls," said Siegmund.

- **Faster Response Times**
  Prior to deploying Tenable.ot, each time WPUD encountered a sticky network problem, it had to set up complicated mirroring and then hook up other tools to profile network traffic and analyze packets. With Tenable.ot, WPUD performs continuous packet captures which makes it easier for analysts to troubleshoot network events or system alerts.

CONCLUSION

WPUD selected Tenable.ot after an extensive evaluation process. "We probably researched 10 or 20 different vendors before we found what we were looking for," said Siegmund.

Tenable.ot has now enabled WPUD to obtain a comprehensive view of cyber risk across their OT network.

In one case, WPUD suspected that a rogue machine had been plugged into its network. Using the Tenable.ot interactive asset map, analysts were able to quickly see all the different assets the suspicious machine was communicating with to make sure its controllers were not compromised.

Learn more about Tenable.ot | Contact Us: **marketing@tenable.com**