TENABLE.OT USE CASE

SECURING WATER FACILITIES

2023

complytec.com

BACKGROUND

Water purification and wastewater facilities are critical for the population of the regions and municipalities they serve. Safe and clean water is essential for public health, ecosystem protection and economic strength.

The effective treatment of water and wastewater is also important for population safety and conservation efforts. At the same time, new developments add to the already long list of challenges, including mutual aid agreements between organizations, changing operational paradigms and new regulatory compliance standards. Supporting these important functions requires secured information technology (IT) and operational technology (OT).

To address these requirements, water purification and wastewater treatment operations are increasingly more intelligent, interconnected and digitized. As a result, you need comprehensive network visibility, security and control through the entire water & wastewater purification/treatment processes, the distribution of clean water, the release of treated wastewater, and disposal of harmful recovered waste.

Improving water works operations utilize technological advances that rely on increased interconnectivity and automation. An interconnected network, while creating great efficiencies, also yields a much wider attack surface with the capacity for a security incident to easily move from one provider to the next. Therefore, water industry industrial cyber threats are core risks to safety, reliability and continuity of your critical operations.

COMMON WATER INDUSTRY PROTOCOLS

- BACnet
- ControlNet
- DNP3
- FINS
- HART
- Profinet
- CIP
- DeviceNet
- Ethernet/IP
- GE - SRTP
- Modbus

ComplyTec
IT SECURITY

tenable
PLATINUM PARTNER

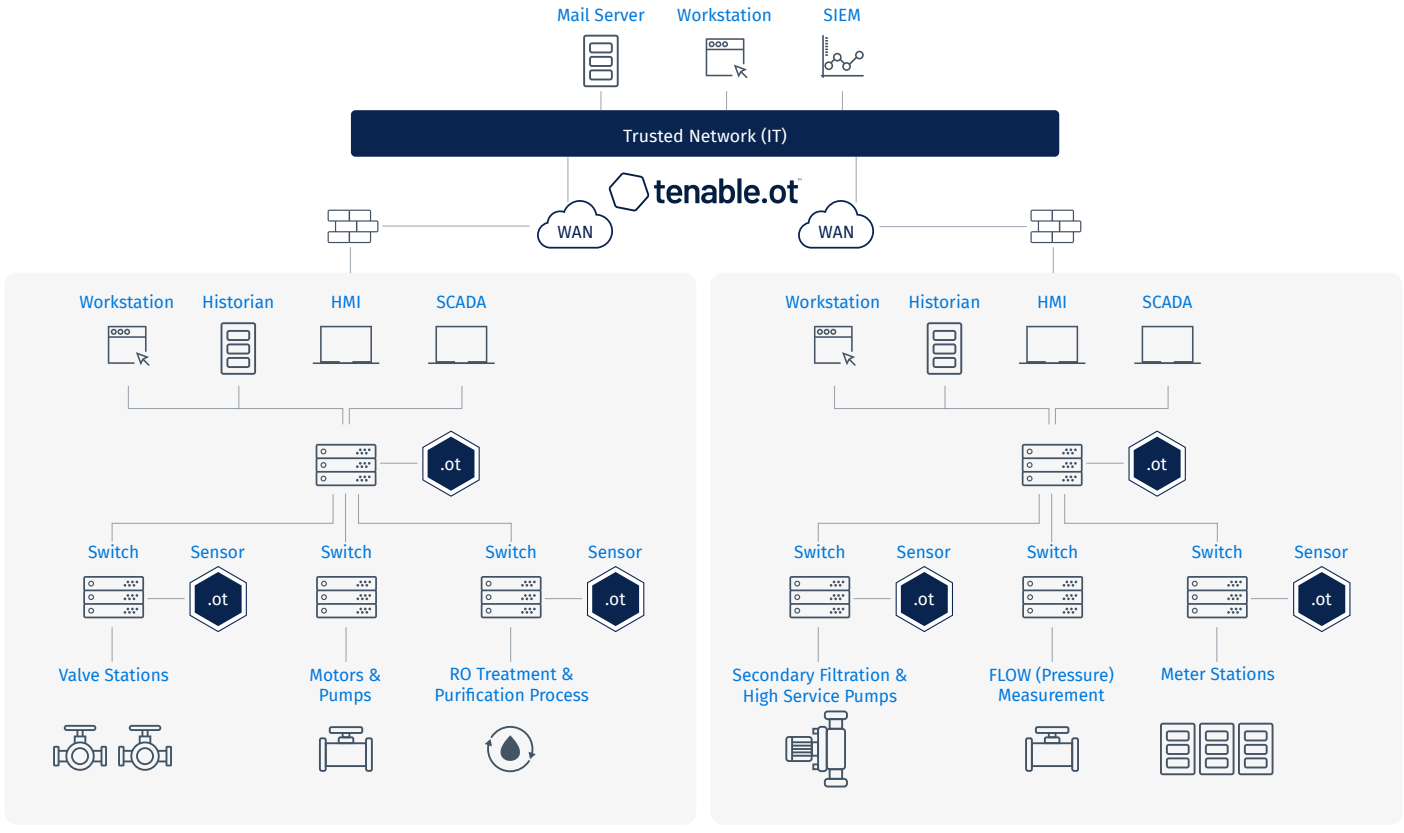
ANATOMY OF A CYBER ATTACK IN WATER FACILITIES

1. Initiate infiltration to the water facilities network.
2. Establish a beachhead in one or more of the assets in the network.
3. Initiate reconnaissance activity to map out targets, vulnerable devices and weak points.
4. Propagate to other assets to reach areas of interest.
5. Launch the "last mile" of the attack ,which disrupts the water treatment or purification operations.

Recent Events

- **2021 –** Attackers gained access to a Florida water facility from the outside through TeamViewer to a Windows 7 operating system, which was no longer supported. The hacker changed the amount of sodium hydroxide or lye from 100 PPM to 11,100 PPM. Luckily, the incident was caught and reversed prior to public impact.
- **2019 –** The Post Rock Water District in Ellsworth, Kansas experienced a cybersecurity breach when a former employee remotely accessed a Post Rock Water District computer to shut down the cleaning and disinfecting procedures that made the water potable.
- **2017 –** Attackers, believed to work for a nation state, used sophisticated malware called Triton to infiltrate one of Schneider's Triconex safety systems. It's these safety systems that shut down operations in nuclear facilities, oil and gas plants, water treatment facilities and more when hazardous conditions are detected.

LOGICAL SAMPLE DEPLOYMENT: WATER



VISIBILITY ACROSS SYSTEMS

Water facilities contain a host of different industrial operations. For drinking water treatment plants (DWTPs) this includes water source monitoring, initial pumping from it, filtration and treatment and final distribution. In waste water treatment plants (WWTPs), it involves the capture, filtration and treatment of gray water for reuse. For blackwater, it involves settling ponds, advanced filtration, and final treatment, disposition and disposal rendering it harmless to environment.

Each of these processes require an intricate choreography involving IT and OT operations working together. Many organizations have moved to converged IT/OT environments and have also adopted IoT technology to monitor each of the operational elements. The introduction of IP-based devices and the erosion of the air-gap has de-facto opened up new attack vectors in water operations including the "lateral creep" of security incidents that may start in IT and move to OT, or take the opposite route of starting in OT and moving to IT.

For this reason, you need a complete and de-siloed view of your converged environment. Complete 360-degree visibility across your entire infrastructure will ensure you don't have security blind spots that can potentially disrupt or disable operations. You need visibility at the network level to identify questionable or anomalous traffic, and at the device level to find infected IT and OT devices.

INVENTORY AND TRACK ASSETS

Water facilities tend to have large infrastructures. Many different devices spread across a vast area and sometimes across several networks. Networks generally have multi-generations of devices in addition to a variety of makes and models. Your OT solution should be able to combine several discovery methods to create an updated asset inventory of the entire distributed environment.

You also need the ability to track assets to keep your inventory updated and to receive alerts for all unaccounted changes, including visibility into all device types found in water networks such as pump, filtration, valve, mixing and metering stations. Your OT solution should also scale for large networks with many heterogeneous devices. What's more, it should account for dormant devices that are not communicating regularly over your network.

IDENTIFY AND SCORE VULNERABILITIES

Due to the "always-on" requirement for DWTPs and WWTPs, when a vulnerability is discovered it's difficult to stop operations to perform routine maintenance or apply patches. As a result, vulnerability windows can remain open indefinitely and are susceptible to both known and unknown threats.

That's why it's critical to maintain deep awareness of the state and characteristics of all of your devices. This includes accurate matching between specific device condition and the available vulnerability knowledgebase with associated exploits. Because of the dynamic nature of water environments, your OT solution should update this body of knowledge regularly and keep it in sync with newly discovered vulnerabilities. A Vulnerability Priority Rating (VPR) score, for example, can provide a triaged list of vulnerabilities to deal with from most serious to least. VPR is based on a variety of factors such as CVSS score, asset criticality, position in your environment and much more. This delivers an automated, fully vetted, and prioritized list of vulnerabilities you should address to reduce the cyber exposure relevant to your specific environment.

SECURE YOUR INFRASTRUCTURE

To identify events at any stage of an attack, you should employ multiple detection engines, including:

- Attack vectors that can proactively identify weak points before threat actors launch an attack. General traffic mapping and traffic visualization, identification of risky protocols, open ports and vulnerabilities to eliminate risk factors across your infrastructure.
- DPI engines for both documented and proprietary protocols. It identifies activities that break established rules and reconnaissance events and relies on policies that protect against known attacks.
- Anomaly detection identifies zero day or targeted attacks that do not have a signature yet identified. You can use this to pinpoint traffic patterns and behaviors outside of regular daily operations.
- Signature-based detection involves a database such as Suricata. It is open-source and valuable because the greater security community can add new signatures, thus benefitting all OT environments.
- Configuration control tracks malware and user-executed changes made over your network or directly to a device. This provides a full history of device configuration changes over time, including the granularity of specific ladder logic segments, diagnostic buffers, tag tables and more. It enables administrators to establish a backup snapshot with the "last known good state" for faster recovery and compliance with industry regulations.

OT cybersecurity is now widely recognized as a core ingredient to ensuring a reliable, efficient and safe water environment. To mitigate that risk, you need full visibility, security and control into all of your operational assets.

Tenable.ot provides complete visibility across both IT and OT assets. Asset inventory identifies each and every asset in your environment along with deep situational analysis down to the firmware and backplane level. Threat hunting involves proactive attack vectors that identify weak points before threat actors launch an attack. A hybrid detection engine identifies both known and unknown threats when they happen. Vulnerability management prioritizes vulnerabilities with known exploits that are relevant to your specific environment. Configuration control identifies and provides snapshots of any changes made to your OT infrastructure for auditing and rollback purposes, if and when and necessary. Tenable.ot's flexible deployment options and integration with leading IT security vendors will ensure water infrastructures operate safely and with reduced risk.

tenable
PLATINUM PARTNER

ABOUT TENABLE

Tenable 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.

ABOUT COMPLYTEC

At ComplyTec, we've supported organizations with their cybersecurity for nearly 25 years. We're proud partners with Tenable and RSA. For deep expertise and great customer service, we're hard to beat. Try us!

ComplyTec
IT SECURITY