CLAROTY
CASE STUDY

WATER UTILITIES

Customer
One of the largest water utilities companies in Europe, operating multiple sites. The customer's main concerns are pollution of nearby water sources due to malfunctioning of automation systems, which will result with heavy fines. The customer has already experienced several non-targeted cyber events that involved infection of various HMI\EWS. Additionally, the customer is aware that as a core critical infrastructure component it may be considered as a viable target for hostile nation states and terrorist groups. As a result, the IT department received the authority of implementing cybersecurity measures throughout the customer's production networks.

Problem statement

Several non-targeted cyber events, that involved infection of various HMI\EWS, have led the customer so believe that the **lack of real-time visibility** into the OT traffic materially impairs its ability to contain and manage such events.
The customer's main concern was the risk of cyberattack on a **waste treatment** facility, leading to for it being accountable to **environmental pollution** which would consequence with heavy fines.
As a result, the IT department received the authority of implementing cybersecurity measures throughout the customer's production networks.

Site
The site chosen for the initial deployment as a 55 years old water treatment plant. The plant automation system has shifted to Ethernet around ~15 years ago. The automation systems are partly managed by external contractor. The customer has defined getting full visibility to all assets and remote activity as a critical need.

Product

- Claroty Continuous Threat Detection
- Enterprise Management Console

Assets

- HMI\EWS (each physical machine occupies both) – 4
- Controllers (Rockwell) – 24
- Remote I\O - ~200
- Other endpoints (servers, Historian etc.) – 61

Networking

- All of the site’s traffic flows through 2 main switches. These switches were connected to an aggregation switch which sends the traffic to Continuous Threat Detection.

Process

- **POC**
    - CTD has captured traffic from the plant’s switches - 1 week.
    - Manual analysis of the PCAPs to generate detailed security assessment report – 1 week
- **Full Deployment**
    - Site preparation for full deployment – configuring all switches to SPAN + connect to aggregation switch + mounting the physical server for CTD – 1 day
    - SOC preparation for installation of the Enterprise Management Console – 1 day
    - CTD training mode – 1 week
    - Shift to operational mode + connection to Enterprise Management Console + connect Enterprise management console to IBM QRadar SIEM – 1 day

End Result

Full visibility to all assets and connections. The customer proactively uses CTD to discover networking misconfigurations and other security issues both on OT and IT networks. A timeline has been set to expand deployment to additional sites.