CASE STUDY

Armis Drives Cybersecurity Remediation Efforts for Nationalized European Water Utility Serving 5 Million People

The Challenge

- Managing a vast ecosystem spanning the entire country historically built without a unifying strategic direction.
- Identifying, segmenting, and securing interconnected IT/OT environments Identifying and securing a wide range of makes and models of equipment.
- Complying with strict EU directives governing critical infrastructure.

The Solution

- Implemented Armis Centrix™ for OT/IoT Security.
- In the process of onboarding Armis Managed Threat Services to the security operations center (SOC).
- Plan to integrate Armis with work order tracking application for field workers.

The Results

- Provided data to inform crucial decisions about which systems to replace and remediate first.
- Provided data needed for complying with EU directives and regulations.
- Secured 26+ water treatment plants in 18 months.
- Discovered assets that shouldn't be connected to the sites quickly remediated.
- Helped sites understand their exposure and cybersecurity posture immediately.

Industry: Utilities

Location: Europe

Number of Employees: 5,000+

Armis Centrix™ for OT

Armis Managed Threat Services

Background

In 2014, a European country's government nationalized the country's water utilities. As of January 2024, the government officially took ownership of all the assets from the 31 independent local authorities that had previously been managing and operating the country's water supply, including 2,000+ water treatment plants and 5,000 pumping stations. Assets include programmable logic controllers (PLCs), pumps, chlorination equipment, filters, supervisory control and data acquisition (SCADA) systems, routers, switches, and generally a wide range of makes and models of equipment. The 31 local authorities had functioned independently without any unifying strategic direction and no delineation between IT and OT.

The Challenge

The newly formed national utility had a huge task ahead: bringing all water services, equipment and sites in compliance with the EU National Infrastructure Securities Directive (NISD), the EU Critical Entities Resilience Directive (CER),

Armis has helped us get a handle on our assets and perform preventative maintenance. We have better visibility into the plant now than we ever had before. Armis will be key to our ongoing security strategy, especially on the OT side."

Cybersecurity Manager, European water utility

and the forthcoming directive NIS2. These directives require an organization to understand its assets and the risks associated with those assets and to put remediation plans in place to mitigate those risks. NIS2 extends these regulations to wastewater treatment plants.

Securing the plants from an OT and cybersecurity point of view is a large-scale endeavor that will require multiple years to complete. It is critically important that the process does not jeopardize the delivery of safe, clean drinking water to the population, so the work must be done without impacting any of the plant's operations.

The Solution

The utility's cybersecurity team conducted a review of various tools to remediate vulnerabilities and assist with compliance. After comparing several options and then conducting a proof of value (POV), they chose Armis Centrix™ for OT/IoT Security based on its agility and its non-disruptive, transparent footprint. "Armis was by far the most agile tool that we came across," they said. "The Armis team really understood our issues around asset discovery, vulnerability management, and continuous monitoring—and the tool delivered on these requirements beyond expectations."

The first phase of the project was defining the OT environment at each plant and putting firewalls in place to segment OT from the IT environment. The next phase was to implement monitoring to provide visibility into asset meta data, behavior, anomalous activity and ultimately vulnerabilities.

Armis provides the needed visibility for vulnerability management and compliance. The cybersecurity manager explained that they bring Armis data to the asset operations team to show them which systems impacting the largest populations are nearing end-of-life and need replacement.

To balance the need to protect the population and the need to spend taxpayer money wisely, the utility's executives had to understand the risks associated with its assets. Armis provides the data that drives these crucial decisions.

The utility is also in the process of onboarding Armis Managed Threat Services to its Security Operations Center (SOC). This has opened new lines of communication that are making it easier for the cybersecurity team to do its job.

The Results

After just 18 months, Armis has helped to remediate 26 of the country's largest water treatment plants serving 65% of its entire population. The cybersecurity manager remarked that the project has been a huge success. They hope to finish remediating the top 50 plants that serve 80% of the population by the middle of 2025. Afterwards, the team will work through the remaining 1,950 sites that serve the remaining 20% of the population.

One instance in particular stood out as proof of the value of Armis. The cybersecurity manager shared that they received a call from the largest wastewater treatment plant in the country, saying that there was an asset onsite that exhibited anomalous behavior. One of the PLCs was acting oddly, and the site operator could not get any details on why this was happening. The OT cyber

"The crux of the NISD directive and the NIST framework is about understanding your assets and the risks they pose to the organization. The more we get Armis out there, the more we understand our risk base and our asset inventory and where we need to point our focus."

Cybersecurity Manager, European water utility

remediation team showed up onsite to install Armis, and, within hours, they identified the specific PLC that had the issues and what the issues were and made recommendations on how to fix them. It turned out to be an overloaded DHCP server. While the issue did not surface any nefarious activity, Armis enabled the team to quickly understand the reason behind the peculiar behavior and to put a plan in place to prevent it from happening again—all within a day.

Armis also discovered tablets, digital watches, and mobile phones that should not be accessing these sites. The cybersecurity team is currently building a model that will become the standard network security infrastructure across the country. Every site will have a perimeter of firewalls, a managed remote access solution, and Armis in the middle monitoring everything within the protected environment.

Looking ahead, the utility is working on bringing asset inventory information to mobile workers in the field through integration with its work order tracking application, Maximo. "It will be a game changer for us, as a cybersecurity team, to be able to pinpoint our exposure and say with confidence, 'There's an issue with a certain PLC,'" shared the cybersecurity manager. "We won't have to reach out to our regional managers anymore. Instead, we can just go into Armis and understand our exposure and cybersecurity posture immediately. That kind of efficiency matters a lot to an organization that is funded by taxpayers."

"Armis has helped us get a handle on our assets and perform preventative maintenance," the cybersecurity manager asserted. "We have better visibility into the plant now than we ever had before. Armis will be key to our ongoing security strategy and to maintaining compliance with European directives, especially on the OT side."

60% of the population's water treatment plants are remediated

Remediated 26 plants in 18 months

1 day to identify an asset's anomalous behavior and remediate it

ARMIS.

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011
www.armis.com