CASE STUDY

Municipal Utility Heightens Security and Vastly Improves Network Monitoring by Partnering with Armis

The Challenge

- Getting a big picture view of the utility's network topology and asset inventory
- Implementing an holistic solution that would not disrupt sensitive OT
- Classifying assets by type, location, number, and other variables
- Improving vulnerability management to minimize risk and prevent potential attacks

The Solution

- Deployed Armis Centrix™ after a successful proof of concept (POC)
- Seamlessly integrated Armis Centrix™ with existing third-party solutions
- Deployed Armis Managed Threat Services (MTS)
- Leveraged Armis customer resources: Resident Architect (RA) and Resident Engineer (RE)

The Results

- Identified top 10 to 12 vulnerabilities each week for remediation
- Built more than 20 team-specific dashboards based on business needs
- Remediated bandwidth and connectivity issues
- Over 1 million gallons of water every day are now better protected from cyber attack disruption, thanks to Armis MTS regularly surfacing the utility's top vulnerabilities in need of remediation

Industry Municipal Public Water and Wastewater

Location Large City

Number of employees 3000

Armis Centrix™ for OT/IoT Security

Armis Managed Threat Services

Background

This municipal utility is responsible for managing a US city's water and wastewater utility (utility), delivering over one million gallons of water every day. Operating over a wide range of businesses, the utility employs over 3,000 employees. The utility has 150 full-time employees dedicated to centralized IT, which manages the IT and operational technology (OT) networks.

The Challenge

The utility IT team was looking for an easy-to-learn solution that would give them a big picture view of the utility infrastructure to help them map the network topology and gain an understanding of how assets were connecting to each other. The team wanted better visibility into the type, number, and locations of their IT and OT assets. They also sought a better way to classify them, troubleshoot issues, and improve the utility's overall risk posture in the face of attacks targeting critical infrastructure.

As a public utility, the utility mission is to ensure business continuity in order to provide essential services to the city's residents and businesses. Vulnerability management has been an increasing concern as the utility deploys more and more OT. Another requirement was that the solution needed to integrate seamlessly with the existing technology stack without requiring agents, which could disrupt the sensitive OT network.

"Most of the competitor's products require some kind of agent. Due to the sensitivity of our OT assets, we needed agentless implementation. Armis provided that and we were able to scale up visibility of assets within our environment without impacting our operation. That's a huge benefit for us."

Director of IT Engineering,
Water and Wastewater Utility

The Solution

The IT team started off with a small-scale POC to determine whether the Armis Centrix™ platform could meet their requirements. They saw the value almost immediately. The rich asset network connectivity data collected by Armis opened their eyes to the possibilities and opportunities the platform could provide across multiple bureaus and technologies. On the OT side, for example, the agentless Armis platform delivered valuable asset intelligence from day one without having any negative impact on operations.

When the team decided to fully implement Armis, they also opted to leverage additional Armis services to gain extra manpower and specific expertise to maximize the value of their investment and assist with configuring dashboards and preparing reports.

With the help of an Armis RA and RE, the utility is expanding its Armis footprint to its entire OT network. The Director of IT Engineering pointed out that a product is only as good as the people that support it and expressed how impressed he is with the Armis RA and RE.

"They're very knowledgeable about the technologies that we utilize within our environment, as well as our infrastructure, our business, and the Armis tool set itself," he remarked. "The RA and RE have helped us create 20 custom dashboards for various bureaus, establish a baseline for normal activity, and more easily identify deviations to enable investigations."

The utility is also using Armis Managed Threat Services (MTS) to supplement its resource-strapped cybersecurity team. MTS helps the utility file reports and manage access and identity using a zero trust approach.

The Results

As the Director of IT Engineering pointed out, Armis serves as a reliable knowledgebase, giving the IT team the visibility it needs and helping it operationalize its data so it can reduce risks in its environment.

All told, Armis has identified and gathered data on approximately 38,000 devices. Some 2,800 of these are switches, firewalls, VPNS, and integrations which are all part of the utility's infrastructure.

On a weekly basis, the RA and RE provide the IT team with a list of the top 10 to 12 vulnerabilities that need to be patched, fixed, or remediated.

Additionally, the subject matter expertise and insights of the MTS team have improved the utility's overall security posture, uncovering the root causes of unusual issues, which enables the IT team to address them more quickly and efficiently. The combined power of the Armis platform and MTS saves the IT team a minimum of three to five hours of troubleshooting time per week.

The Vice President of IT pointed out that MTS is a valuable extra set of eyes to identify ways to reduce risk. "We have the data, but the value is in taking action on the data," he asserted.

When Armis was first deployed, there were bandwidth problems at most of the utility's sites, and "nobody knew why," as the Director of IT Engineering noted. By using Armis data, he was able to trace the problem to a widely used business productivity tool and took the necessary steps to remediate the issue.

In another instance, Armis helped the IT team get to the bottom of network connectivity issues for certain devices by uncovering unsanctioned Dynamic Host Configuration Protocol (DHCP) configurations.

Armis also helps the IT team upgrade or remove applications and services from the network. Armis provides in-depth analysis throughout the process to ensure it goes smoothly across the entire utility.

The RA and RE help the utility solve problems and expand the organization's use cases to get the most value from Armis. With Armis, the utility now has the security posture it has been striving for—and this has been achieved without impacting the utility's operations.

"Armis is so much more than a security appliance. It's a unique all-in-one tool that provides continuous network monitoring, facilitates root cause analysis, and provides real business value for our utility," concluded the Director of IT Engineering.

38,000 assets identified

20+ team-specific dashboards created for specific business use cases

Minimum of 3 to 5 hours per week saved on network troubleshooting

1M Over 1 million gallons of water protected every day

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

Website
Platform
Industries
Solutions
Resources
Blog

Try Armis
Demo
Free Trial