ARMIS®

CASE STUDY

Armis Expands Visibility into University's Facility Automation Systems & Provides Actionable Insights

OT network team builds a better asset inventory while focusing their attention on the most critical issues

Customer profile

State university

Industry

Higher education

IT environment

Approximately 30,000 employees and 100,000 inperson and online students, with an extensive IT and OT environment.

Introduction

Managing and securing building automation systems (BAS) for this high-ranking university's "smart" campus is a big responsibility. After evaluating the security of the OT network, the Facility Automation Systems (FAS) team learned that they needed better visibility into their networked assets. Soon after deploying Armis, the team found thousands of assets they were unaware of previously, and they continue to find more in unexpected places. Armis has also provided them with granular data on potentially vulnerable devices and out-of-date legacy equipment, which helps the team determine what should or should not connect to the network. Thus far, Armis has saved the team a great deal of time and effort, while directing them to issues that deserve focused attention.

Every day, the director of operational technology and his team work hard to make sure the university's connected campuses and buildings are secure, safe, reliable, and functioning at optimal capacity. He likens the campus to a "smart city," where the building automation systems (BAS) are managed by his Facility Automation Systems (FAS) team. According to the director, the smart campus consists of nearly 2,000 buildings—some of them hundreds of miles away from the main campus—including utility plants, water and wastewater treatment, academic buildings, research facilities, museums, and more. While the FAS team operates as a separate entity from the university's central IT security operations, they share some of the same policies and inform IT security when they discover cybersecurity issues outside of the FAS purview.

Audits reveal gaps in the asset inventory

Recently, one of the most critical security challenges faced by the FAS team was insufficient visibility into the BAS network and operational technology (OT) devices. After a comprehensive internal audit and external security assessment, the director realized they needed a more accurate and complete inventory of all assets, both managed and unmanaged, on the highly segmented OT network. Without a proper, detailed inventory, it was difficult to discover vulnerabilities and prioritize them, a key aspect of cybersecurity risk mitigation. During the assessment, the university's OT security analyst looked into how Armis could help the team address this challenge and recommended a proof-of-concept (PoV), which was conducted over a six-month timeframe.

Armis identified multiple previously unseen assets, such building management controllers and old devices that had been on the network for a decade or more. In just one week, the OT security analyst said, Armis found tens of thousands of assets—and that number has increased since more collectors were added to the buildings under the team's purview.

"In the new science building, Armis was able to discover a few hundred devices that our team was unaware of on the core network. Then we added an Armis virtual collector inside the building that could see the devices on the building network, and the count went up to over a thousand devices. Originally, our internal inventory only showed about 175 devices, most of which were for building automation," he reported.

Armis spots anomalies, spurring corrective action

Since Armis has been up and running, the OT security analyst and his team have been able to detect some unusual devices and network activity. At one of the university's facilities, he spent a solid day working with the team to troubleshoot some peculiar issues. It appeared that several anomalous devices were plugging into the network and feeding the team incorrect IP addresses, which made it hard to identify the problem.

Everything changed when the OT security analyst decided to bring Armis into the picture. "I loaded the 'false' IPs into Armis and found out that the device in question was a cloud-managed Cisco Meraki Access Point that was doing Dynamic Host Configuration Protocol (DHCP) on the network but giving out incorrect IPs… Armis gave us that information in less than a minute after I typed the IP addresses into the search bar," he said.

Another interesting Armis discovery was a set of wireless Airtame projectors connected to the network. These are typically used at the university for screen casting (sending what is on a computer screen to a TV, projector, or monitor via Wi-Fi). Armis correctly identified every one of those devices, down to the operating system versions, model numbers, and other relevant and unique data.

Challenges

- Building a more accurate and complete OT asset inventory
- Identifying and prioritizing cybersecurity risk
- Taking corrective action when needed

Armis also discovered a building management server connecting to the network at a university-owned hotel. Armis showed that the outdated server had been reattached to network, along with the name of the server, its Microsoft Windows 7 operating system, and its IP address.

Identifying legacy equipment and mitigating vulnerabilities

Incidents like these have prompted the FAS team to think outside of the IT/OT box with respect to Armis and to use the platform for finding building controls and devices that needed replacing. For the supervisor of FAS application engineering, the biggest use case is accurate identification of the "vintages" and weak points of BAS controllers.

"We receive newsletters from BAS vendors saying that a particular vintage and model of a part has a bad transistor in it. In the past, we had no way of finding those. But, after fine-tuning Armis, we'll be able to very quickly inventory those and concentrate on our 50 hot spots. Then we'll be able to cull the ones that are most at risk and figure out a way to mitigate any issues we see," he explained.

The OT security analyst is also expanding his use of the Armis platform to extract information about outdated or end-of-life (EOL) devices on OT networks. He and his team have found devices that are as much as 20 years old with unsupported operating systems. He is currently building those lists and exporting them into spreadsheets for systems administrators and IT maintenance teams so they can perform necessary upgrades and swap out old equipment with replacements. "Now we can start working on lifecycle planning for building controllers and automation devices, along with the servers," he remarked.

Armis Results

- Quickly discovers and provides detailed data on previously unseen assets
- Zeros in on vulnerabilities and maintenance issues
- Monitors traffic for unusual behavior and connection requests
- Saves time by allowing the team to focus their efforts
- Providing flexible reporting options

Armis makes the team's job easier and directs their focus to what matters most

As the director of operational technology said, a long-term goal for the FAS team is to go deeper with Armis and take advantage of all it has to offer. "I would love to be able to take action based on a condition, so those types of "things are what we want to get to. There's a lot of effort that needs to go into our network before we can do some automation, but that's our ultimate goal," he said.

For his team, intrusion detection was one of the primary drivers in deploying Armis. The agentless Armis threat detection engine uses artificial intelligence (AI) and machine learning (ML) to monitor and alert when devices behave outside their known acceptable baseline, usually due to policy violations or inappropriate connection requests.

"One of my major security concerns is finding out who is on the network and what they are doing. Getting a view into users, logins, and other information gives me a warm fuzzy feeling so I understand what's being done and when," he said.

For the OT security analyst, Armis is not only a huge time saver, it also uncovers valuable insights that he would not have had otherwise. "Armis has made my job easier from a security perspective in terms of finding unknown and random things that pop up," he noted.

Additionally, he pointed out that the versatile reporting capabilities of Armis have cut down on a lot of effort and focuses his team's attention on issues that need to be addressed. With Armis, it has become easier to pull a report, customize it, and understand what needs to stay on the network and what needs to be disconnected or updated.

"As I look at a report for the servers running various operating system versions, I can pick the first seen and last seen servers, so, if a server hasn't been seen for six months, I'll make sure the device has been shut down and decommissioned from the network. I'll then provide that list to the folks in charge of doing lifecycle replacement for those types of servers," explained the OT security analyst.

"One of my major security concerns is finding out who is on the network and what they are doing. Getting a view into users, logins, and other information gives me a warm fuzzy feeling so I understand what's being done and when."

Director of Operational Technology
State University

"In the new science building, Armis was able to discover a few hundred devices that our team was unaware of on the core network. Then we added an Armis virtual collector inside the building that could see the devices on the building network, and the count went up to over a thousand devices. Originally, our internal inventory only showed about 175 devices, most of which were for building automation."

Director of Operational Technology
State University

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets.

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 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