CASE STUDY

Energy Think Tank Showcases Armis to Utility Companies as a Key Component of a More Secure Grid

Heightened awareness of cyberattacks helps electricity providers coordinate their defenses across IT and OT networks.

Industry

Energy

IT environment

Approximately 1,000 employees across multiple offices in over a dozen countries.

Introduction

On the heels of recent attacks on energy systems, this U.S.-based think tank is channeling its innovative research and thought leadership into providing utilities with viable solutions for strengthening their cybersecurity infrastructure. The think tank's cybersecurity lab is running simulations and other projects to demonstrate the power of Armis to increase visibility to both the OT and IT attack surface. The think tank foresees a future where utilities will adopt an approach to security that encompasses zero trust, an integrated technology stack, and single-pane-of glass visibility.

This not-for-profit vendor-neutral think tank focuses on all aspects of the energy ecosystem to lower costs, improve efficiency, and drive environmentally sustainable solutions. It has been in operation for over 60 years and has a presence in a dozen countries. The think tank is funded by its more than 1,000 members, who represent primarily electricity utilities that generate and deliver 90% of the electricity in the U.S., along with government agencies, corporations, and other organizations in more than 40 countries. The think tank provides thought leadership and research on everything from improved utilization and delivery of electrical and nuclear energy to environmental sustainability issues.

The think tank currently has three state-of-the-art labs that perform testing, experiments, and technology application research. One of the labs houses a cybersecurity facility that helps utility companies test, simulate, and analyze power grid cyber attack scenarios, such as DDoS and man-in-the middle (MiTM), and come up with mitigation solutions.

Utility companies get serious about escalating security measures

As the cybersecurity research lead points out, the think tank has seen renewed interest in the U.S. on how to prevent attacks that could potentially take down substations and cascade across the grid. This was triggered by several factors:

- The politically motivated Industroyer malware attack, which sabotaged industrial controllers at a Ukrainian power company in 2016.
- The 2021 ransomware attack on the Colonial Pipeline, which caused the Texas-based oil pipeline to shut down operations after it impacted its billing and accounting systems. While the ransomware hit the IT infrastructure, the connected OT infrastructure suffered as a result, as some of the company's OT equipment is administered by computers and other IT equipment.
- Rising utility cyber insurance costs, due to growing threats to operational technology (OT). Insurance companies have doubled down on their requirements and are asking utilities to present complete threat activity logs and demonstrate preventative measures to circumvent future attacks.

Armis offers immediate visibility into insider threats and risky device behavior

The think tank's cybersecurity research lead got wind of Armis when a colleague attended a capture-the-flag exercise, where participants worked with new technologies to identify vulnerabilities and issues. The team was so impressed with Armis that they acquired the platform without a proof of value (PoV). Armis was deployed in the first half of 2019.

While the team was already aware of the 188 connected IT devices they already had at the lab, Armis gave them added visibility to new devices, new protocols, and internet traffic.

"When we first got Armis, our priority was to get as many of our devices as possible talking to it, and that included IT devices, OT devices and IoT devices, like our Honeywell cameras.

Challenges

- Identify device activity associated with unsanctioned insider behavior.
- Get a view into potentially risky interactions between IT and OT networks.
- Help utility companies fortify their defenses against cyber attacks.

Next door, we have a training station for grid operators, which has a number of OT devices, so we've gotten those into Armis as well," said the cybersecurity research lead.

Armis has dramatically simplified asset inventory. Now it only takes about one hour to export device information from Armis to a Microsoft Excel inventory spreadsheet, whereas previously it could take days to sift through log data and pull that information together.

"One of the things we really like about Armis is that it establishes a 'known good' base line against which we can compare anomalous activity or traffic," noted the cybersecurity research lead. "When I remote into Armis from home and don't see any traffic or a flat line, then I know there are connectivity issues. I can then investigate and take action to remediate the situation."

For the lab, the time to value of Armis was immediate. In fact, Armis is among the top five cybersecurity solutions that are showcased when utility companies come in for tours.

"We started showing it off soon after we got it up and running. When we do walk-throughs at the lab, we show people the latest additions, especially cutting-edge solutions like Armis," remarked the cybersecurity research lead.

One of the most important use cases for Armis is detection of insider threats. After Armis was deployed, the lab monitored devices for unusual behavior, especially when people work remotely.

"Armis enabled us to determine which devices were using remote desktop protocols (RDPs) to connect to other systems over the network. It also helped us monitor website traffic and prevent potential datarelated issues by enabling us to look at what leaves the lab or comes into the lab," explained the cybersecurity research lead.

For example, downloading a 5 GB ISO file, which is a disc image in the form of an archived file (a CD, DVD, or Blu-ray) is not unusual. However, the cybersecurity research lead does get concerned when Armis sends out an alert after detecting a device downloading or uploading a 20 GB file. Armis even discovered an OT device, a Schweitzer 3355 automation controller running Microsoft Windows that resides in the training room, going to the Walmart website.

In addition, the lab uses Armis to gain insights into suspicious firmware updates, which have been known to contain malware. Armis also provides insights into TCP/IP stack issues, such as misconfigurations, corrupted settings, or vulnerabilities that can cause disruptions in internet connectivity and lead to DDoS, MiTM, or port-spoofing attacks. Based on this type of feedback from Armis, the team has been able to set automated security policies for various scenarios.

Armis Results

- Better visibility into connections crossing the boundaries of OT and IT.
- Comparison of unusual activity against a "known good" baseline.
- Simplified asset inventory.
- Insights into suspicious behavior by insiders.
- Alerts that trigger investigation and remediation.
- Integrations that enrich insights.
- Single-pane-of-glass console to ease management and reporting.

Integrations pave the way for intelligence-sharing

The cybersecurity lab team has integrated Armis to the wireless LAN controller, cyber lab switches, and Splunk. Splunk is an advanced security information and event management (SIEM) system that analyzes and correlates large data sets from sensors, websites, applications, and devices.

The Armis-Splunk integration helps to close visibility and security gaps for both IT and OT environments and can potentially set the stage for communal sharing of threat data for utility companies. Increasingly, electricity providers are looking for a way to see how similar companies are being attacked and what devices are being compromised.

“They want communal sharing of this type of valuable intelligence so that they can stop similar attacks before they reach their system. This level of information sharing will make the overall grid ecosystem that much stronger,” observed the cybersecurity research lead.

“Armis enabled us to determine which devices were using remote desktop protocols (RDPs) to connect to other systems over the network. It also helped us monitor website traffic and prevent potential data-related issues by enabling us to look at what leaves the lab or comes into the lab.”

Cybersecurity Research Lead
Energy Research Institute

Armis plays a prominent role in zero trust strategy for utilities

According to the cybersecurity research lead, zero trust is beginning to gain traction in the world of utilities. In a zero trust architecture, all devices and users are untrusted by default and are scrutinized before being granted connectivity and access to resources. The Colonial Pipeline incident underscored the fact that the boundaries between IT and OT networks are blurring, as IT devices are frequently used as management consoles to control OT equipment.

“No one can say that they are truly air-gapped. Connections between IT and OT devices can still be compromised. That’s why solutions like Armis need to be layered into a zero trust architecture,” affirmed the cybersecurity research lead.

The cybersecurity lead has also observed that, increasingly, energy companies are moving away from a siloed approach to security and leaning toward an integrated security operations center approach with single-pane-of-glass visibility that encompasses both IT and OT. “The Armis platform, with it’s simple-to-use, drill-down dashboard and its integrations with the tools that most utilities already have, is a big step in that direction,” he pointed out.

Hardening utility companies against future attacks and vulnerabilities

Next year, the think tank plans to leverage Armis in DNP3 studies. DNP3 is a communications protocol used in supervisory control and data acquisition (SCADA) systems, which are used in remote energy monitoring and delivery systems at electricity and water companies. DNP3 passes various types of data to and from OT systems, and the protocol is commonly used at utility substations.

“We’re looking into how we can use Armis to detect potential attacks or malformations of DNP3 messages that, up until now, have been undetectable. At our lab, we intend to alter the data in a DNP3 message to make it look like an MiTM attack and then use Armis to detect that the data is out of value. When Armis sees that the data has been tampered with, DNP3 should send back a message saying that the data is invalid. If our experiment works, we foresee that utility companies will be integrating Armis into their zero trust security stack,” said the cybersecurity research lead.

In addition to the DNP3 project, the think tank plans to build out a fourth cybersecurity lab on the West Coast and will deploy Armis to help regional utility companies conduct OT cybersecurity simulations.

The cybersecurity research lead is also looking to deploy Armis Asset Vulnerability Management (AVM), which provides vulnerability information for all assets and fills in the gaps on scanner-identified assets. This is valuable not only for the lab’s internal operations but is also vital for electricity utility companies, as it will help them prioritize risk and remediate issues faster to prevent outages or grid failures.

Finally, the cybersecurity research lead is committed to cultivating an ongoing relationship with Armis to help both the think tank and their members stay up to date on the latest technology advancements. It’s all part of the organization’s mission to benefit society by helping energy companies maintain a resilient and reliable grid that everyone can depend on in their daily lives.