VECTRA
SECURITY THAT THINKS.®

CASE STUDY

The power of protection

Tri-State Generation and Transmission Association supplies wholesale electric power to 44 electric cooperatives throughout a 200,000 square-mile service territory across Colorado, Nebraska, New Mexico and Wyoming. Cyberattack threat levels to the national power grid are at an all time high, and protecting critical infrastructure is equally paramount as protecting consumer and corporate data.

Utilities provider detects cyberattacks in real-time

People listen when the National Security Agency and Homeland Security confirm that the national power grid is vulnerable. The threat of a cyberattack shutting down the national electric grid is real, and utility companies are beefing up security measures to keep the lights on and the heat running for households and businesses.

Tri-State Generation and Transmission Association avoids this risk to its power supplies by tracking security threats in real time with the Cognito® network detection and response platform from Vectra®. "Cyberattacks are always a concern from a security perspective," says Dave Buffo, Tri-State senior IT security administrator.

"Vectra gives us visibility into our networks, so we can monitor our internal hosts and address any security issues in real-time."

TRI-STATE
Generation and Transmission Association, Inc.
A Touchstone Energy® Cooperative

Organization

Tri-State Generation and Transmission Association

Industry

Energy

Challenge

Protect Tri-State's corporate and subscriber data and prevent cyberattacks to power grid

Selection criteria

Easy-to-use security solution that provides visibility into internal network and activity on critical hosts

Results

- Provide visibility of internal hosts to halt active network breaches
- Gain real-time insight of real and false threats
- Reduce time spent chasing false alarms

> "Vectra monitors the hosts and shows us real threats. It doesn't get confused by normal traffic that can set off bogus alerts."

Dave Buffo
IT security administrator
Tri-State Generation and Transmission Association

Exposing real threats

Tri-State generates and transmits electricity throughout a 200,000 square-mile service territory spanning four states. The internal networks—that store both corporate information and subscriber data for 1.5 million customers—must be protected. Multiple hosts, or master computers, are located throughout the wide area network and support 1,500-plus Tri-State employees.

These hosts are critical to the utility's business and way too valuable to take any risks with their security. But when it came to understanding the hosts' traffic patterns, the lights were out. Tri-State lacked visibility into the hosts' activity and when potential threats did come up, there was no context to the type or degree of threat, and no prioritization.

"We needed to know what was going on with our internal hosts. We wanted to see what they are doing, what they are talking to, and why they are talking to certain things," says Buffo. "Vectra monitors the hosts and shows us real threats. It doesn't get confused by normal traffic that can set off bogus alerts."

The Cognito platform provides real-time detection and analysis of active network breaches. Cognito provides deep continuous analysis of Tri-State's internal and Internet network traffic to automatically detect all phases of a breach as attackers attempt to spy, spread and steal highvalue data.

The quest for intelligent security

Tri-State battled lots of false-positive threats before adding Cognito. Tri-State relied on firewalls, intrusion prevention systems and antivirus software, but these tools didn't do exactly what Buffo needed. "I was looking for something like Vectra for quite some time and hadn't had any success in finding it."

Tri-State's intrusion prevention system, for example, blocked behavior that wasn't dangerous, interrupting business processes unnecessarily. "It wasn't good for us because systems could be working correctly, but the IPS would still block the traffic. It didn't have the intelligence that we needed," says Buffo.

Staying out of rabbit holes

Cognito stops Buffo from wasting valuable time. Using a combination of data science, machine learning and behavioral analysis, known and unknown threats are proactively detected and automatically scored and correlated. Vectra's Threat Certainty Index™ automatically displays the more significant threats in real time based on contextual scoring so Tri-State can address detections that matter the most.

"We used to go down rabbit holes a lot," says Buffo. "Vectra is smart and knows what a threat is and what isn't." A previous monitoring tool had sent an alert about something that was scanning the network and posed a potential problem. "We used Vectra to identify the host that was making the scan, and it wasn't a safety concern. It was only a managed print service looking at ink levels, so it could order supplies automatically."

> Cognito provides automated detections with context so security analysts have all the information to make fast, informed decisions without wasting time searching for more information.

"I searched for something like Vectra for a long time but had no success until now!"

Everything we need is right here

A coworker's email describing Cognito caught Buffo's attention immediately. He quickly realized Cognito was worth investigating. "We didn't look at any other solutions," Buffo says. "The proof of concept showed us that Vectra was the right choice for our environment."

The two-person security team had no issues deploying Vectra or learning its ins and outs. "Vectra is very clean and easy to use. Everything we need is right here. You quickly understand how to use Vectra and deploy it." platform was straightforward.

Gaining immediate visibility in remote plants

Tri-State has experienced such good results with Cognito in the corporate environment that it plans to expand Cognito network detection and response to the power plants and field locations. The testing is already underway with a Vectra S-series sensor deployed at one remote power plant. S-series sensors passively monitor network traffic, extract critical metadata

and forward the metadata to an X-series appliance for threat analysis. "The sensor was really easy to set up and deploy," says Buffo. "Right away, we could see things going on there." With S-series sensors, Cognito enables Tri-State to extend automated, real-time breach detection to the far corners of its critical infrastructure.

Within a year, Tri-State plans to put sensors throughout its power plants and field locations. "I'm excited to see how this will play out," says Buffo. "Security threats are not going away, and we want to have the smartest and best solutions available to help us stay secure. I searched for something like Vectra for a long time but had no success until now!"

For more information please contact a service representative at info@vectra.ai.

Email info@vectra.ai vectra.ai