CASE STUDY

How South River Electric Membership Corporation Succeeds at IT Security and PCI DSS

South River Electric Membership Corporation, (South River EMC) is a member-owned electric distribution cooperative that delivers electricity to 43,000 members in five North Carolina counties. The cooperative was founded in 1940 and is based in Dunn, NC. South River EMC has 107 employees and is owned and controlled by the members who utilize its services. The cooperative is managed by CEO and Executive Vice President Chris Spears and has nine member-elected directors.

As a cooperative, South River EMC has close relationships with its stakeholders according to Tim Peede, vice president of IT and CIO of South River EMC. "Co-ops don't have customers – we have members and we take that relationship very personally. South River EMC employees are passionate about protecting the infrastructure of which we are stewards."

As an electricity provider as well as a financial entity that bills its members, South River EMC's need for security and monitoring solutions is at the highest level. Like any entity that accepts credit cards, South River EMC must comply with the Payment Card Industry – Data Security Standard (known as "PCI DSS"). The Payment Card Industry is a private group set up by the major credit card companies to define standards for companies that process credit card transactions. PCI DSS is designed to prevent credit card fraud, hacking and other security issues. Any company that processes, stores, or transmits credit card numbers must be PCI DSS compliant or they risk losing the ability to process credit card payments. Secure access to the electric grid as well as members' financial information is an imperative.

Peede was looking for a way to strengthen the Cooperative's security capabilities to meet emerging threats. "Our previous solution was cumbersome when it came to digging through the large volume if data that was generated every day," said Peede. "When I look at the daily report, I need to know what's noise and what is a security issue that I need to address. PCI DSS compliance reporting was of the utmost importance to us as well. So, we began looking for another solution."

"We've been thrilled with what we get from EventTracker and we were thrilled enough to share the great results."

In EventTracker SIEM, South River EMC found a cost-effective security reporting and monitoring platform. "We needed a solution on premises with the right product mix. We wanted the ability to identify and report anomalies in the network, combined with the freedom to have the reporting display and function in an actionable format," said Peede.

South River EMC brought in EventTracker SIEM and as the initial deployment was completed, it began monitoring 250 workstations in the co-op's network. EventTracker SIEM provided a complete view of the IT infrastructure and helped to identify potential threats. Because EventTracker Security Center could classify according to user priorities, it allowed the IT security staff to address the most critical incidents first and reduced the time it took to isolate and correct issues.

EventTracker SIEM correlated with South River EMC's network on a more granular level than the utility had previously experienced. "It could tie a log event to a time of day, and the person who created the event," said Peede. "The hyperlinks it provides in the reporting made it very easy to use and point right to the event in question. It took two minutes to log in and receive a detailed record of what happened today and what connected to the server. Its search capability is tremendous."

The next step was to address a problem common to many co-ops: security staffing resources. Succeeding at SIEM requires more than just buying the platform and running reports. "With EventTracker SIEM, we gained the monitoring and proactive alerting we were looking for, but we have limited IT staff in house, and the team has a lot to do. With EventTracker Siemphonic, we gained an expert who looks at the network every day, makes critical observations, and puts the alerts into context."

This helped South River EMC to realize significant benefits in work hours, and having access to expert security staff. " EventTracker SIEMphonic is one of the few services that I have dealt with that exceeded my expectations," said Peede. "I knew EventTracker SIEM would provide the alerting and reporting we needed, but I was surprised at the speed it allowed through intuitive presentation of information. What I am usually looking for is the 'needle in the haystack' – the one problem that needs my attention is often difficult to locate. EventTracker SIEMphonic finds those 'needles' and then shows me just where they are. It's saved me and my staff lots of time and helps keep the network secure."

Peede considered the collaborative nature of cooperatives across the county. "The co-op community is different than the rest of the business world. When we find a solution that works, we let other co-ops know. We've been thrilled with what we get from EventTracker and we were thrilled enough to share the great results."