Altamaha Bank & Trust

BANKING

About the Client: A community bank with $ 150 million in assets services customers with four branches and an operations center. Their challenge as a small bank has been the need to comply, just like the big banks, but at the scale necessary for their needs and budget. Most importantly, their goal has been to keep up high service standards while ensuring customers and assets are protected.

"Our customers are priority #1. They come to us with an expectation and we want to deliver. The challenge is keeping up that level of service with minimal IT staff, coupled with the heavy need for security and compliance to keep business going."

- Shan Venable, SVP, Chief Technology Officer

The Challenge

"As the CTO of a small community bank, I face the challenge of a very small IT staff of two, whose hands are full ensuring we keep our services up to customer expectations," said Shan Venable, SVP, Chief Technology Officer, Altamaha Bank. With all of the regulations and audits Altamaha Bank faces, as well as reporting needs, Shan knew they would require a Co-Managed Security and Information Event Management (SIEM) solution to allow his small team to focus on business drivers.

Prior to EventTracker, their team faced:

- Limited bandwidth to focus on security, reporting, and compliance needs while balancing the demands of customer needs
- Lack of training and staff necessary for the team to manage security in-house
- Constant audit pressure from the FDIC, the state, and third-parties who required network tracking, account visibility, archiving, and data access for forensics

The Solution – Why EventTracker?

Although security is critical, leadership needed the IT team focused on customers and the business. They started out with EventTracker Log Management, which worked well, but was time-consuming and held the possibility they might miss something. Having a truly co-managed security solution allows the CTO's team to deploy products, train, etc. to help profit the bank and satisfy customers. That is why they needed a partner.

When doing their due diligence, Shan and his team gathered critical business input from key players and looked at offerings that might be a fit.

They considered solutions from TruShield and DefenseStorm, as well as EventTracker's Co-Managed SIEM. Shan said, "The issue was that they were not apples to apples, which was difficult – all aren't created equal." At a high level, Shan and his team were looking for what each could provide in terms of online dashboards, reports, oversight, recommendations, as well as additional features for vulnerability assessments and intrusion detection.

At the time, EventTracker SIEMphonic version 9 was just being touted as the next-gen EventTracker platform. "When you put it all together, EventTracker was just doing a better job in terms of the ability to push the information to us quickly via reports and queries," said Shan. Version 9 set EventTracker apart from the competition in terms of being able to drill down and get to information quickly and easily, then filter to what they wanted to see. "EventTracker 9 has been a game-changer, and their Co-Managed SIEM solution, SIEMphonic, was the clear choice," said Shan.

Shan describes EventTracker's ability to:

- Leverage Elasticsearch, which is incredibly fast with pre-built filters and tagged data elements. "We can click on an element within the graph and it drills down

in a second to the information," said Shan.

- Run fast queries, which means all elements are tagged so you can click and drill down fast. "We don't have to spend time building queries to get to the information to make decisions – that is what sets it apart to us."
- Provide a 24/7 SOC dedicated to a unique partnership, with a team leader who gets to know the customer. "I had concerns at first about the SOC (Security Operations Center) being far away, overseas, but I've worked with EventTracker now for over 10 years and it's never been an issue – they are a responsive team that works U.S. hours."

"I've developed a great working relationship with our SOC team lead overseas," said Shan. "They have great folks over there. Off-shoring gets a bad rap, but that hasn't been the case with EventTracker's SOC and service teams – they are top notch."

Onboarding Experience

Altamaha Bank started with EventTracker SIEMphonic in January 2018. Shan said, "The onboarding process took about 60 days total, but most of that time was spent simply allowing the system to learn our environment. We also were able to get vulnerability assessment and intrusion detection added, which we didn't have before." During this time, they made the upgrade to Version 9 as well.

The system needed time to accumulate data, learn their operations, and know their queries of interest. "During that 60 days, we could filter out all the noise and get what we were really interested in," said Shan. "Onboarding went very well, but you do have to be patient. The system itself is up and running quickly, but it takes time to accumulate and fine tune to get real actionable intelligence, which is what we wanted."

Results

Altamaha Bank & Trust has increased IT productivity by approximately 87%. Shan reported, "Before EventTracker SIEMphonic, I spent 6-8 hours per week reviewing reports, running queries and looking for issues. I now spend 1-2 hours per week reviewing dashboards and looking for those same issues, plus I have a dedicated SOC watching too." When Shan needs further help, he turns to his EventTracker SOC team to get their assistance and input. "The time I gain back can now be put into deploying applications and products for the bank that serve our customers and help us improve profitability," said Shan.

A recap of benefits Shan calls out are:

- **Dashboards:** They give a quick view into network activity so there is less of a need to search reports or run queries
- **Elasticsearch :** This feature is a game changer for Shan... data element tagging, and filtering mean minimal clicks to get to the information you want to see
- **Actionable Information in Less Time:** Shan spends far less time to get more actionable information

Customer "Off the Cuff"

"We went from an EventTracker product that satisfied some of the needs we had, but as we grew, and regulations played a factor, we needed a more enhanced product, plus professional services for oversight to take workload off of us."

"We achieved all of those objectives. I'm able to spend a lot less time on a daily basis digging into log reports to see what's happening on our network.

"I want to give a big thumbs-up to the SOC we deal with overseas, which is very responsive. As an example, we got a call from our team leader because traffic started popping up on our network and he was concerned we had something going. From another vendor, I would have gotten a report or email, but our team lead picked up the phone and called me. We've built that relationship and he understands what's normal and not normal. He's really part of our team. When he saw a trigger on intrusion detection (IDS) – he called me right away because he knows us. We talked and were able to determine what was going on. It was something new we'd introduced that they weren't aware of. It was a false positive but that's a good thing. You never know, but what's important is that Netsurion is on top of it."

"We trust the EventTracker SIEMphonic soution and their SOC, and recommend without reservation."