Bremer Bank Enhances Security Maturity while Meeting Financial Compliance Controls with Threat Intelligence

Bremer Bank, headquartered in St. Paul, Minnesota, is a privately held, $11 billion regional financial services company. As a trusted provider of banking, wealth management, investment, trust, and insurance products and services, Bremer services customers throughout Minnesota, North Dakota and Wisconsin.

Like any financial services firm, Bremer Bank is required to meet a variety of regulatory compliance requirements. However, Bremer's information security efforts go far beyond maintaining basic compliance to pass regulatory audits. In addition to a CISO, who oversees governance, compliance, and risk, the organization has a chief cybersecurity officer (CCSO) who oversees three teams dedicated to incident response, security engineering and operations, and identity and access management. While focused on different areas of information security, both groups share a common goal: to continuously protect customers and their assets.

The Challenge: Collecting Logs from Across the Environment

Bremer Bank's security and engineering teams faced a formidable task. The heavily virtualized environment consists of 1,000 servers and is actively growing. Bremer also maintains a vast array of networked devices, a robust Citrix deployment, and numerous security applications. Unfortunately, the firm's security information and event management (SIEM) solution couldn't keep up. The SIEM wasn't collecting logs from necessary systems in Bremer's environment—a baseline requirement for any security program. Additionally, it was difficult for the team to run reports and manage the overall solution to get actionable insights.

Bremer Bank's CCSO, Jeremiah Cruit, knew that his teams could better protect the environment if they had more of the right information. "SIEM and log analytics are massively important. If you're not collecting and analyzing all of your logs, you're at a very low security maturity," he said.

Cruit wanted to log and monitor every single device in his environment, while also supplementing his security operations with valuable threat intelligence feeds. These included feeds needed to meet financial compliance requirements, such as those outlined in the Office of the Comptroller of the Currency's (OCC) Cybersecurity Assessment Tool. It was time to make a change.

After evaluating the top SIEMs in the market, Cruit selected the LogRhythm Threat Lifecycle Management (TLM) Platform. LogRhythm stood out from competitors for its ease of use, solution architecture and design, and ability to scale events per second. The ElasticSearch backend storage system would also allow Cruit to perform freeform log analysis and therefore allow other functions within the organization to benefit from the data inside of LogRhythm.

Bremer Bank

Organization
Bremer Bank

Industry
Financial services

Employees
Nearly 2,000

Key Impacts

- Improved ability to collect, monitor, and analyze all logs from across the environment
- Enhanced enterprise visibility
- Automated detection and response
- Improved forensic investigative capabilities
- Gained actionable intelligence from Anomali ThreatStream integration
- Met crucial compliance requirements via threat intelligence

"I've done a lot of SIEM deployments in my career. LogRhythm went in quick, and got up and running fast. Once we started to get logs in, we were able to act on them almost immediately."

"Anomali was up and running in minutes. Starting from the proof of concept—it just worked. To move ThreatStream to production, we simply wrote a check. It was pretty awesome."

—Jeremiah Cruit,
chief cybersecurity officer,
Bremer Bank

The Solution: Immediate Visibility and Response Capabilities

It didn't take long for LogRhythm to help Bremer take a massive step forward in security maturity. "I've done a lot of SIEM deployments in my career. LogRhythm went in quick, and got up and running fast. Once we started to get logs in, we were able to act on them almost immediately," Cruit said.

The Bremer team feeds as many data sources as possible into LogRhythm. "As our SIEM tool, LogRhythm serves as the repository for all the log data across the entire IT environment. So, obviously, LogRhythm is a treasure trove of data. When you analyze that massive quantity of data and tie it in with threat intelligence, you get a lot of benefit."

Improved enterprise visibility is one benefit Bremer realized. Because LogRhythm centrally monitors all logs from across the environment, Bremer's analysts can see more activity than they could previously. This resulted in an enhanced ability to detect and investigate anomalous activity. Whereas before, the team spent valuable time consolidating logs and trying to manually corroborate data points, now they can identify and mitigate suspicious activity before it becomes an issue.

The LogRhythm AI Engine analyzes incoming data in real time and automatically assigns a risk-based prioritization score from 1 to 100. The enhanced security alerting capabilities have allowed the Bremer team to immediately investigate high priority alarms and remediate actual incidents. The days of manually sorting through logs are over, and the team has realized a "massive time savings by finding incidents earlier and quicker—before they become a problem," Cruit said.

He added, "LogRhythm is helping us find more items of interest, which is great, and my team is doing more valuable analysis. I am able to ramp up my team to focus on the insights coming out of the SIEM rather than other less productive tasks."

Each member of Cruit's team has found value in LogRhythm, whether they're investigating an event or proactively addressing anomalous activity. Information is easily accessible, and reports can be generated without restrictions. "We love the rapid response we get from LogRhythm—the ability to quickly see what's happening and pull logs from systems and view all the logs related to a single user or event," Cruit said.

What's more, LogRhythm's SmartResponse™ feature enables the team to orchestrate automated responses to specific activities. "Whatever you can conceive of happening in the environment, we can build out an automated response to," Cruit said.

Incorporating a Threat Intelligence Platform

With Bremer's security maturity significantly improved, Cruit's next step was to supplement his internal security operations with actionable threat intelligence. Specifically, he was looking to onboard a partner who could provide threat intelligence from the Financial Services - Information Sharing and Analysis Center (FS-ISAC) and other providers to meet compliance requirements, as well as seamlessly integrate with LogRhythm.

Anomali ThreatStream quickly became the obvious choice for Bremer as it exceptionally met Cruit's requirements. "Anomali was up and running in minutes," Cruit said. "Starting from the proof of concept—it just worked. To move ThreatStream to production we simply wrote a check. It was pretty awesome."

Together, Anomali ThreatStream and the LogRhythm TLM Platform help Bremer Bank meet regulatory compliance requirements and further enhance Bremer's security maturity. Threat intelligence is continuously gathered, categorized, and ranked (for severity and confidence) in the Anomali ThreatStream Platform and then delivered to

> **"We love the rapid response we get from LogRhythm—the ability to quickly see what's happening and pull logs from systems and view all the logs related to a single user or event."**
>
> —Jeremiah Cruit, chief cybersecurity officer, Bremer Bank

Bremer's LogRhythm platform to detect security threats in their enterprise infrastructure in real time. For example, what would otherwise be a normal event, such as user authentication, could be escalated if that user is coming from a high-risk IP address flagged in ThreatStream.

Anomali ThreatStream has proven its value in other ways as well. "There are other purchases that I didn't have to make because we bought Anomali," Cruit said. For instance, instead of purchasing an external monitoring service to identify misuse of the Bremer brand, the team uses the similar domain detection in Anomali ThreatStream. By monitoring for variations on Bremer.com, the team automatically found a spoofed site that was being used to mount attacks on a partner.

> **"There are other purchases that I didn't have to make because we bought Anomali."**
>
> –Jeremiah Cruit, chief cybersecurity officer, Bremer Bank

Going Above and Beyond

Seeing the value of SIEM and having the desire to further improve his security maturity, Cruit has developed a strategic vision for Bremer Bank. Going forward, he plans to take full advantage of LogRhythm's security automation and orchestration (SAO) capabilities. By utilizing automation features, he hopes to keep his team's momentum as they move from a reactive to a proactive stance. Cruit is also focused on completely building out LogRhythm's user and entity behavior analytics (UEBA) functionality to detect anomalous user behavior at Bremer. This effort is currently in progress with the help of the LogRhythm Analytics Co-Pilot Service.

"UEBA functionality is likely to become my favorite feature, because looking for anomalous behavior in the environment is probably the most important capability to have today," Cruit said.

Additionally, he plans to invest in large scale log analysis and to make LogRhythm available to other teams within the organization. "Our infrastructure teams, network teams, and applications teams can get a ton of business intelligence out of our enterprise logs," says Cruit, "My goal is to replicate all the data into an Elasticsearch database, and then have a whole stack behind that. LogRhythm will be the front end to feed the database and then we can start getting into heavy-duty log analytics and freeform searching and capabilities that other teams outside of security really enjoy."