Alliant Credit Union Evolves Real-Time Fraud Detection

Alliant Credit Union is one of the largest credit unions in the U.S. It serves more than 335,000 members worldwide and holds over $9.3 billion in assets. For more than 80 years, Alliant has maintained its member-focused mission: to provide members with superior financial value, in the form of award-winning savings and loan rates and few/low fees. Providing best in class cyber security is another way Alliant provides value to its members.

The Business Challenge

Automating Fraud Detection

The Association for Financial Professionals claims that bank fraud activity reached an all-time high in 2015.[1] Transactions involving checks, wire transfers and credit/debit cards pose a risk of fraud for financial institutions the world over.

To combat this threat, Alliant has a department of fraud specialists who regularly scrutinize detailed reports in search of indications of fraud in financial transactions. Fraud analysts often had to resort to a manual process of sifting through transactional information in conjunction with security information from the Information Security team to find patterns and trends. This manual effort resulted in a decrease in productivity and seriously curtailed the fraud team's ability to uncover trends and predict future behavior.

On the IT side, Alliant's Information Security team includes a full-time security staff and a supplemental managed security services provider (MSSP), who work together in a 24/7 security operations center (SOC). Together, this team continuously monitors for signs of compromise on Alliant's network of more than 700 servers, 500 network devices and thousands of workstations and end user devices.

Alliant had a variety of individual tools for both fraud detection and IT security monitoring, but there was a clear opportunity to combine disparate processes with an overarching security information and event management (SIEM) platform. By pulling analytics into a single platform, the security and fraud teams could collect more threat intelligence for both information security and fraudulent activities, and gather intelligence quickly to enable faster response.

"Our goal was to take the things we were doing manually, automate the processes, and analyze them in real time. We wanted to take it a step forward to create a fraud dashboard built from the analysis of patterns and correlations of machine and human behavior. This dashboard provides a single view in which we can see where actions might be happening that fall outside of what we've baselined as 'normal' behavior," said Bill Podborny, chief information security officer (CISO) at Alliant.

ALLIANT

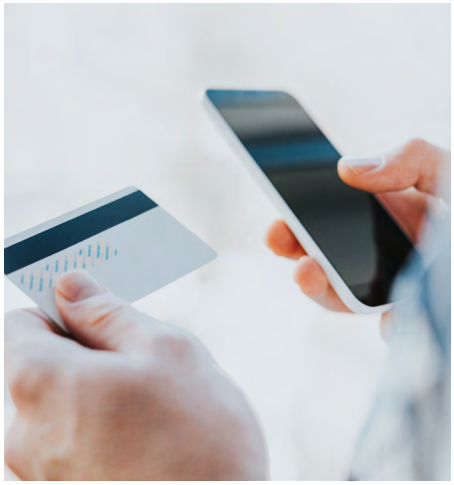
Organization
Alliant Credit Union

Industry
Banking and financial services

Members
335,000 worldwide

Key Impacts

- A single platform to consolidate all machine data from IT events and financial transactions
- Automated analysis of fraud-related patterns and trends in real time
- Fraud dashboard for proactive investigations
- Advanced alerting on security events



[1] 2016 AFP Payments Fraud and Control Survey

The Solution

Financial Fraud Detection Simplified

Alliant conducted a virtual proof of concept (PoC) and, ultimately, they chose LogRhythm. Podborny concluded, "LogRhythm had the most flexibility to build the solution that we need. It was also much easier to implement compared to other solutions. But as crucial as flexibility and ease of use is, the relationship we formed with the LogRhythm team was equally important. Everyone from sales, support and engineering has been great to work with. We felt LogRhythm put the right people behind the technology."

The LogRhythm team helped Alliant replicate the common patterns of fraud that the fraud analysis team had previously looked for manually. They then applied custom AI Engine rules and tuned them to work with financial data. Finally, they applied behavioral analysis to become more predictive, building in automation that will alert on suspicious behavior in real time.

Alliant's deployment of the LogRhythm Security Intelligence and Analytics Platform gathers previously disparate information in one place, correlates it in real time and highlights patterns the analysts had previously parsed through and related manually—saving the team hours of work. What's more, fraud analysts can now be more proactive, as dashboards quickly feature the outliers that they should investigate.

With LogRhythm, Alliant now has a single platform that collects, correlates, analyzes and alerts on IT security and financial fraud incidents. Podborny says the system provides intelligence they didn't have before. "We can now see what our systems are doing at any point in time. We pride ourselves on our efficiency, and LogRhythm has definitely improved ours by helping us automate as much as possible."

"The correlation capabilities and the threat intelligence are like having an instant response. We aren't waiting anymore for someone to notify us, because we can see it as it happens through the LogRhythm console," said David Rebman, senior cybersecurity engineer at Alliant. "Obviously the more information we can gather to put in front of an alert, the more positive we can be in terms of how we react to it."

Looking Ahead

Incorporation of Financial Data and Operating as a Lights-Out Security Operations Center

Podborny has big plans for the LogRhythm platform. Alliant has some mission critical data sources, and the team is looking at pulling those valuable sources of data into LogRhythm to further improve fraud detection capabilities. "We would like to gather any financial transaction information that happens throughout the organization. Having that data in LogRhythm would be a valuable tool to quickly determine if questionable activity is, in fact, real fraud."

A longer-term goal is to use LogRhythm to help the Alliant team operate as close as possible to a lights-out security operations center (SOC). "If we can take what we have learned from current activity, put some additional intelligence into it and put it back into the system, then we can potentially get to a point where the system is running so efficiently that we can be fairly close to a lights-out SOC." Alliant is beginning to experiment with LogRhythm's SmartResponse™ automation framework to help pave the way toward that SOC vision.

> **"We can now see what our systems are doing at any point in time. We pride ourselves on our efficiency, and LogRhythm has definitely improved ours by helping us automate as much as possible."**
>
> David Rebman, senior cybersecurity engineer, Alliant