CASE STUDY

Firstmark Credit Union Uses LogRhythm to Monitor Internal Activities

LogRhythm
The Security Intelligence Company

FIRSTMARK Credit Union
Great with people. Great with money.

Organization
Firstmark Credit Union
San Antonio, Texas

Challenges
This regulated financial services company must maintain a tightly controlled environment to ensure that malicious or unintentional activities don't open up the potential for theft, fraud or data breaches. The Credit Union needs to monitor internal user activities and watch for intrusions from the outside.

Solution
An all-in-one LogRhythm XM software appliance provides event management, log management and advanced intelligence for event correlation and real-time user monitoring across the credit union's headquarters and 14 branch locations. The administrators get a single view into all users' activities and unusual behavior with alerting on important events.

Results
Benefits from deployment include:
- Ease of setting up alerts for specific conditions that the Credit Union wants to monitor.
- Quick correlation of events with one-click access to details to aid response to alerts.
- The ability to run tails or investigations on certain computers.
- Rapid reporting to generate firm evidence to review with employees or their managers.

Future Plans
Expand LogRhythm to cover every PC the Credit Union operates. Explore the use of out-of-the-box reports for PCI, HIPAA and SOX compliance reporting.

Times have changed considerably since Firstmark Credit Union was founded in 1932 as San Antonio Teachers Credit Union. What is now the oldest financial cooperative in San Antonio, Texas, had just 40 members and total assets of $475 back then. Firstmark now has 14 branches, manages more than $820 million in assets, and serves the financial needs of more than 93,000 people deep in the heart of Texas.

Growth isn't the only change affecting Firstmark's operations. Like every other financial institution, the Credit Union has become a target for people wanting to exploit any tiny opening in the computer systems that safeguard and manage members' financial accounts. The Credit Union has built a multi-layered barrier around the perimeter of the company's computer systems—but the cyber security doesn't stop at the perimeter. Security administrators closely monitor every type of internal activity on the network to watch for possible signs of an intrusion or other potentially harmful actions taken by trusted insiders.

The Challenge to Know Who, What, When, Where and How

When viewed individually, single activities on a network can seem quite innocuous. An employee resets a password. A worker is prompted to download a software update on his PC. Someone creates an account on a cloud storage application. All are harmless activities, right?

Security experts know that these types of events, when correlated with other activities also happening on the network, might raise suspicions of malicious or otherwise unwanted activity. For instance, that password reset might have been initiated by an unauthorized actor attempting to steal the employee's credentials. That software update might be the means to deliver malware to the worker's PC. And that cloud storage application? Someone might be trying to move sensitive files to an unauthorized off-network location.

The security administrators at Firstmark know it's imperative to collect log files from all types of devices, correlate the events in these files, and raise alerts based on specified conditions. Above all, they need to gain visibility into what is happening, where, and with whom to ensure that confidential customer data is protected at all times. For this reason the Credit Union's IT department places a priority on user activity monitoring.

Firstmark Credit Union operates a very controlled computing environment. Employees are strictly forbidden to do certain things that might be routine at other companies, like plug in a USB thumb drive or watch streaming video. Such restrictions are necessary to limit the potential for malicious activity and to keep

the enterprise network operating smoothly.

Anyone who is familiar with the concept of the cyber kill chain understands that it's just as important to watch for abnormal activity inside a network as it is to prevent attacks at the perimeter. Once a cyber attacker gets a foothold inside a company's computer systems, the potential for a data breach escalates quickly. The best chance to catch an intruder is by monitoring for subtle changes in expected behavior; for example, a user login that occurs at an unusual time of day, or an unexpected update to a system file.

The Solution for Better Visibility

The Credit Union decided a security information and event management (SIEM) system would help network administrators gain visibility into user activities. Network security analyst Christopher Rodriguez says the company installed the product TriGeo SIM (now known as SolarWinds Log & Event Manager). "We initially went with TriGeo for two reasons," according to Rodriguez. "One of our network administrators had experience with the TriGeo system from a previous job, and we needed a product that could do event correlation for us. We had tried using a Cisco security product but it couldn't correlate events."

TriGeo SIM met Firstmark's basic needs for a while—that is, until the security vendor was acquired by SolarWinds. Network Manager Jorge Riojas explains. "With the TriGeo buyout, the new owner wanted us to repurchase the solution we already had. Instead we looked at this as an opportunity to buy a better solution that met more of our needs. TriGeo was a good introductory system for us. I think it helped us evaluate some of the components to look forward to in a new system and what to include in an RFP. From that perspective, we certainly found what we were looking for in LogRhythm."

Network administrator Paula Reiland says she and Chris Rodriguez saw a demonstration of LogRhythm and were immediately drawn to the simplicity of the user interface and the ease of getting detailed information by drilling down on an event. LogRhythm also offered a very powerful correlation engine to make sense of lots of things happening at once. Says Reiland: "We liked the ability to create alarms based on the tails and the investigations we do instead of having to create a rule from scratch. This alarming capability is easier to do and we can be more specific with our instructions."

LogRhythm Tail is a unique feature of the SIEM that enables real-time search on specific conditions. An administrator can capture conditions to configure alerts to be sent whenever those same conditions occur in the future. For example, Reiland used her own PC to create a tail that alerts on the condition of someone plugging in a prohibited USB drive. "Now we get an alert as soon as someone plugs a thumb drive in and we can investigate it immediately," says Reiland.

> "LogRhythm's dashboard interface is so user-friendly and it's easy to get the information we need without having to stop and run another report on this or that. We can do it directly from one link on the dashboard."
>
> *Paula Reiland*
> Network Administrator
> Firstmark Credit Union

Firstmark Credit Union has implemented a LogRhythm XM license, an all-in-one software configuration that includes Log Manager, Event Manager and the Advanced Intelligence (AI) Engine. "The implementation was seamless," says Reiland. "We had help from a LogRhythm systems engineer who was very knowledgeable about our environment and the product itself. She was able to explain how everything works. Once the implementation was done, I felt pretty comfortable with moving around within the interface, creating the alarms, and where to look for information on events."

Some of the key features that are quite helpful to the Credit Union are file integrity monitoring, which alerts on unexpected changes being made to sensitive files, and extensive reporting. "LogRhythm's reporting capabilities are so important for us," according to Rodriguez. "Our old system needed a whole day to run a report. Now we get them right away."

The security team uses LogRhythm to monitor for and alert on a range of activities; for example, when:

- Any network accounts are created, disabled or deleted
- End users attempt to install any software on their own
- Devices are plugged into or unplugged from switches in a branch location
- A user attempts an excessive number of logins
- Employees attempt to access forbidden websites or applications

These are just a few of the myriad use cases for LogRhythm's event alerting that help Firstmark's security administrators protect the network.

How Firstmark has Benefitted from Using LogRhythm

Since implementing the LogRhythm SIEM just more than a year ago, the Credit Union finds that it gets much better correlation of events than with its previous system, and the significant events are displayed on the dashboard. "I'm not spending as much time digging into an event to find out what it is, where it is, and why it is," says Reiland. "LogRhythm gives me all that information on the screen. If I want to get more information out of an event, it's easy to do that."

> "We really don't have a large team to monitor our network and investigate incidents. LogRhythm has been a big time-saver for us, all the way from alerting us to specific concerns, to reporting and to the actual investigations. It no longer takes us several days to investigate something."
>
> *Jorge Riojas*
> Network Manager
> Firstmark Credit Union

Reporting is also much stronger and quicker—the old system took a full day to produce a report, and LogRhythm generates them very quickly. "If we see something that we need to review with an employee or manager, we can print a report and have hard evidence in hand as to what is happening on our network," says Reiland.

The network managers use the dashboard to get good insight on what is happening, and they can drill down to investigate the details of events. They can run tails to see what is currently happening or initiate investigations to review what has already happened. The administrators have set up auto-ticketing so that when certain activities occur, a trouble ticket is automatically generated in the Credit Union's help desk system to initiate problem resolution.

Network manager Jorge Riojas sums up the benefits: "We really don't have a large team to monitor our network and investigate incidents. LogRhythm has been a big time-saver for us, all the way from alerting us to specific concerns, to reporting and to the actual investigations. It no longer takes us several days to investigate something."

Looking to Do More in the Future

Firstmark Credit Union plans to do even more with LogRhythm. The top priority is to install collection agents on every PC the company operates when the next budget cycle begins. The administrators also plan to explore how they can use the reporting capabilities more effectively. The Credit Union undergoes regular audits by the National Credit Union Administration (NCUA). Riojas says they will be able to generate ad hoc reports as needed by the auditor. The company also will explore how it can benefit from out-of-the-box reporting for PCI, HIPAA and Sarbanes-Oxley compliance requirements.