CASE STUDY

FINRA Levels Up their Data Game without a Steep Learning Curve

CASE STUDY

FINRA Levels Up their Data Game without a Steep Learning Curve

FINRA (The Financial Industry Regulatory Agency) is a not-for-profit organization that regulates one critical part of the securities industry: brokerage firms doing business with the public in the United States. FINRA enables investors and firms to participate in the market with confidence by safeguarding its integrity.

Siddartha Dadana's Security Engineering team maintains platforms for security across all of FINRA's enterprise, and is responsible for all aspects of managing the data generated by their apps and infrastructure --from network, application, metrics, and security. This is no mean feat -- the flow into their analytics platform alone reaches 4TB a day. When they were asked to figure out a way to stream much of that data to multiple different locations to meet archiving requirements, Dadana recalled a demo he'd seen a few months back and began an evaluation of Cribl LogStream.

All of the Grownup Features, None of the Growing Pains

Right away, they were off to the races, getting the right data flowing to the right destinations, in the right formats – within just hours rather than the weeks or months that would otherwise have been needed.

> *"One of the primary things was how easy it was to set up, install, deploy, to just do the basics right. We didn't expect it to be this straightforward!"*
> *— Siddhartha Dadana, Director of Information Security Engineering*

Once those basics were in place, Dadana's team quickly moved on to the nice-to-haves. With LogStream, they are enhancing VPC Flow logs as they arrive from AWS with dynamic, contextual lookups of IP address ownership. This erases the need to manually update Elastic Network Interface (ENI) mappings whenever something changes. This metadata gets added before the data is delivered for analysis – without increasing the cost or complexity of their environment.

> *"We probably would have had to spin up and maintain multiple tens of servers and compute processes to do this otherwise."*
> *— Siddhartha Dadana, Director of Information Security Engineering*

HIGHLIGHTS

FINRA used LogStream to get data flowing to the right destinations in the right formats, right away.

With LogStream, FINRA saves the time and effort needed to manually update ENI mappings.

With reduced complexity enabled by LogStream, the team at FINRA can offer their org access to a wider range of analytics tools.

"WE PLAN TO LEVERAGE CRIBL TO DEMOCRATIZE DATA PARSING BY OTHER GROUPS IN THE ORG, SO WE CAN TELL THOSE TEAMS, 'ANY DATA YOU WANT TO SEND, ANYWHERE TO ANYWHERE – WE CAN SET YOU UP TO ACHIEVE.'"

– SIDDHARTHA DADANA, DIRECTOR OF INFORMATION SECURITY ENGINEERING

Planning for a Smarter Machine

Now that LogStream is delivering on what they needed, the team at FINRA is expanding their usage to drive greater innovation:

> *"When we first evaluated LogStream, we were just trying to solve a single problem...but now we are starting to up the game in terms of what we can do."*
> *— Siddhartha Dadana, Director of Information Security Engineering*

The team is planning to leverage LogStream's real-time processing engine to identify and examine unusual behaviors inside and outside their network, using their own ML tooling to model data traffic and define what's "normal" based on the huge volumes of data they see.

Empowering Other Teams

Many teams at FINRA work with high volumes of data, and Dadana wants them all to have access to the analytics tools they want to use without the hassle that typically goes along with supporting an array of different formats and destination requirements. The solution? LogStream makes it so easy to onboard new data that they're moving toward a self-service environment.

> *"We plan to leverage Cribl to democratize data parsing by other groups in the org, so we can tell those teams, 'Any data you want to send, anywhere to anywhere – we can set you up to achieve.'"*
> *— Siddhartha Dadana, Director of Information Security Engineering*

Find out how your business can implement an observability pipeline to route, restructure, and enrich data in flight, while cutting costs and simplifying operations. Get Cribl, and take control of your data.

ABOUT CRIBL

Cribl is a company built to solve customer data challenges and enable customer choice. Our solutions deliver innovative and customizable controls to route security and observability data where it has the most value. We call this an observability pipeline, and it helps slash costs, improve performance, and get the right data, to the right destinations, in the right formats, at the right time. Join the dozens of early adopters, including market leaders such as TransUnion and Autodesk, to take control and shape your data. Founded in 2017, Cribl is headquartered in San Francisco, CA. For more information, visit **www.cribl.io** or our **LinkedIn**, **Twitter**, or **Slack** community.