>SOLUTION BRIEF_

FINRA Levels Up Their Data Game Without a Steep Learning Curve

HIGHLIGHTS

- FINRA used Stream to get data flowing to the right destinations in the right formats, right away.
- With Stream, FINRA saves the time and effort needed to manually update ENI mappings.
- With reduced complexity enabled by Stream, the team at FINRA can offer their org access to a wider range of analytics tools.

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 Stream.

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 Stream, 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 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

> **“We probably would have had to spin up and maintain multiple tens of servers and compute processes to do this otherwise. Stream takes that load from my team.”**
>
> **— Siddhartha Dadana**, Director of Information Security Engineering

Planning for a Smarter Machine

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

> **“When we first evaluated Stream, 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 Stream’s real-time processing engine to identify and examine unusual behaviors inside and outside their network, using their own machine learning (ML) 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? Stream 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 that goal.‘ ”**
>
> **— Siddhartha Dadana**, Director of Information Security Engineering

Find out how your business can unlock the value of your IT and Security data with Cribl’s next-generation Data Engine. Get Cribl, and take control of your data.

ABOUT CRIBL

Cribl, the Data Engine for IT and Security, empowers organizations to transform their data strategy. Customers use Cribl’s vendor-agnostic solutions to analyze, collect, process, and route all IT and security data from any source or in any destination, delivering the choice, control, and flexibility required to adapt to their ever-changing needs. Cribl’s product suite, which is used by Fortune 1000 companies globally, is purpose-built for IT and Security, including Cribl Stream, the industry’s leading observability pipeline, Cribl Edge, an intelligent vendor-neutral agent, Cribl Search, the industry’s first search-in-place solution, and Cribl Lake, a turnkey data lake. Founded in 2018, Cribl is a remote-first workforce with an office in San Francisco, CA.

Learn more: www.cribl.io | Try now: Cribl sandboxes | Join us: Slack community | Follow us: LinkedIn and Twitter

CS-0001-EN-2-0524

> "Nam libero tempore, cum soluta nobis est eligendi optio cumque nihil impedit quo minus id quod maxime placeat facere possimus."

ABOUT CRIBL

Cribl, the Data Engine for IT and Security, empowers organizations to transform their data strategy. Customers use Cribl's vendor-agnostic solutions to analyze, collect, process, and route all IT and security data from any source or in any destination, delivering the choice, control, and flexibility required to adapt to their ever-changing needs. Cribl's product suite, which is used by Fortune 1000 companies globally, is purpose-built for IT and Security, including Cribl Stream, the industry's leading observability pipeline, Cribl Edge, an intelligent vendor-neutral agent, Cribl Search, the industry's first search-in-place solution, and Cribl Lake, a turnkey data lake. Founded in 2018, Cribl is a remote-first workforce with an office in San Francisco, CA.

Learn more: www.cribl.io | Try now: Cribl sandboxes | Join us: Slack community | Follow us: LinkedIn and Twitter

CS-0001-EN-2-0524