>CASE STUDY_

How The City and County of San Francisco uses Cribl Stream for smarter cybersecurity spending

The cybersecurity team at the City and County of San Francisco operates with a limited budget, making efficiency a top priority for the organization. They originally brought on Cribl Stream to replace their syslog server, but now use it to evaluate new data sources and tools, save engineering time, and get the most value from their security spend.

As a taxpayer-funded organization, the City and County of San Francisco (SF) makes it a priority to use funds economically and effectively. Their cybersecurity team closely monitors spending so they can allocate more resources to improving security and pass along savings to other department initiatives like public services, infrastructure development, and innovation.

Available spending has also decreased because of the recent economic downturn and migration of many businesses out of the downtown San Francisco area — so having reduced, more predictable expenses is more important than ever. Even as the city recovers, it will still take a few years to replenish their budgets and Cribl Stream has become a very welcome addition to their security infrastructure.

HIGHLIGHTS

- Achieved a 70% reduction in log data, avoiding costly SIEM license increases.
- Streamlined data collection, log optimization, and testing of new security tools.
- Freed up engineering time and simplified training for junior analysts.
- Gained greater oversight and control over new data sources and security tools.

Replaced syslog server for more streamlined data collection

The City and County of SF originally brought in Cribl Stream because their syslog server, which operated on a small virtual machine (VM), was handling 937 different feeds. By using Stream to route, transform, and filter all of that data, onboarding syslog became much more scalable and efficient. It also enhanced the overall performance of their system.

> “We knew we had to replace our syslog server with an enterprise-level solution, so we went out and got Cribl Stream. Not only did it exceed our expectations, but we immediately realized we could do so much more with it.”
>
> — **Manager**, Cyber Data Services

Easy log optimization, transformation, and parsing

Cribl Stream has helped the City and County of SF keep SIEM costs under control and avoid spending more to expand their license. They see about a 70% reduction of their logs. Their return on investment has been much larger than the team expected.

> **“The reduction of data was absolutely huge. I think on average, across our whole environment, we’re cutting about 70% of the raw logs coming through. Avoiding a SIEM license increase took a lot of pressure off of us.”**
>
> **— Manager,** Cyber Data Services

In addition to trimming data they don’t need, the cybersecurity team at the City and County of SF is able to quickly and easily change logs from a raw format, add regex to parse fields, and tag data, which used to be a long, laborious process.

> **“The fact that I can transform raw logs so quickly, and shoot them out in JSON for anyone to read is incredible. Nobody really knows it’s Cribl doing the work, but it makes us look great.”**
>
> **— Manager,** Cyber Data Services

Analysts are happily surprised they can just click on a field and not worry about creating a ticket for someone to regex extract the fields — and the cybersecurity team is happy to have transformed one of their biggest pain points into one of their easiest tasks

More control over tooling spend

Having tackled their initial use case, they’ve moved on to using Cribl Stream to increase oversight and control of new data sources and security tools. The City and County of SF has a review process to evaluate any proposed purchases throughout the organization, which brings security-related tools to the attention of the cybersecurity department.

If a tool replicates a function they already have, they can pause or deny the purchase. They then use Cribl Stream to determine precisely what data a department might need from each source. If a team needs to see performance metrics or get more insight into what their users are doing, the cybersecurity team will also set that up. This approach leads to cost savings and improved efficiency across the entire organization.

> **“Our team knows exactly what we need out of any type of data that is sent to us for incident response. We use Cribl Stream to extract necessary elements from firewall logs, Salesforce data, and any other source.”**
>
> **— Cybersecurity Defense Manager**

A simple, secure way to test new security tools

Another unanticipated benefit of implementing Cribl Stream is the ease of testing out new tools. If another department wants to onboard a new data source, it can be quickly onboarded for a short-term trial and removed if it doesn't make the cut. The team at the City and County of SF also uses Stream to test new SIEMs without completely embedding new companies into their systems.

> **"When testing new tools, we just use Cribl Stream to send them feeds of our data. We can turn the feeds off whenever we want – this has been absolutely huge to us."**
>
> **— Manager,** Cyber Data Services

Now, if they want to test out multiple SIEMs, they don't have to rely on sample data in air-gapped environments and hope that the same alerts come out of each one. Cribl Stream provides an environment that makes it easy to verify that alerts from SIEM A are also coming out of SIEM B.

Save engineering time and empowering junior analysts

Cribl Stream also frees up a lot of time for members of the team to focus on more important tasks. Small projects that used to take hours or days to complete can be finished in just a few minutes.

> **"If our defense side of the house is missing anything from their data, we can go into Cribl and add it back so much faster than before. The other day they were hunting something down on our firewall, but were missing one little field – we added it back in just a few clicks."**
>
> **— Cybersecurity Defense Manager**

It also simplifies the training process for new hires. After a quick intro to the SIEM, they can start working on their own almost immediately.

> **"Since Cribl Stream makes the data coming into the SIEM so much cleaner, our junior analysts are able to go find what they need a lot easier than before."**
>
> **— Cybersecurity Defense Manager**

The City and County of SF currently has data coming in from around 75 sources, and they plan to 10x that amount in the next year or so. In the future, they'll also standardize all their data with a common data model. With Cribl Stream at the center of their data architecture, they're able to offer better services across the board and continuously improve their operations and services — ultimately benefiting all the residents in the area.

TL;DR

- Replaced an overburdened syslog server managing nearly a thousand data feeds with Cribl Stream, improving scalability and efficiency.
- Gained unprecedented control over data and security tool purchases, ensuring smart, cost-effective investments.
- Achieved a 70% reduction in overall log volume, directly avoiding significant SIEM licensing cost increases.
- Streamlined the evaluation of new security tools with easy 1-to-1 testing capabilities.
- Freed up valuable engineering time for analysts, allowing them to focus on higher-value tasks.

Quotes

> “With Cribl we’re as lean as possible and getting the biggest bang for our buck.”

> “We brought it in for syslog, but then we were like, ‘Holy crap, we can do so much more!’ We get that feeling all the time with Cribl.”

> “The support we get from the Cribl Community has been amazing. We don’t get the same thing from our other vendors – the difference is night and day.”

ABOUT CRIBL

Cribl, the Data Engine for IT and Security, empowers organizations to transform their data strategy. Powered by a data processing engine purpose-built for IT and Security, Cribl’s product suite is a vendor-agnostic data management solution capable of collecting data from any source, processing billions of events per second, automatically routing data for optimized storage, and analyzing any data, at any time, in any location. With Cribl, IT and Security teams have the choice, control, and flexibility required to adapt to their ever-changing data needs. Cribl’s offerings–**Stream**, **Edge**, **Search**, and **Lake**–are available either as discrete products or as a holistic solution.

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

CS-0040-EN-1-0825