>CASE STUDY_

Cribl Stream improves the efficacy of Fortune 20 Health Insurance Provider Security Team by providing more structured, relevant data.

This Fortune 20 health insurance provider focuses on an integrated, holistic approach toward improving the health of humanity. They are redefining health, reimagining the system, and strengthening communities along the way. Industry-leading capabilities empower their unique digital platform, and their forward-thinking approach extends to their IT and Security teams. They recently began using Cribl Stream to manage the enormous amounts of data flowing through their organization and are very excited about its capabilities.

HIGHLIGHTS

- 30 to 40% reduction in AWS Cloud Trail data flowing through Splunk.
- Went from 40 million AWS messages in their backlog to zero within 24 hours.
- Cleaning up data to support their security team and improve MTTR.

"Every year, one of our key objectives is to reduce MTTR," says Senior Director, Service Intelligence, who is responsible for health insurance providers' APM strategy, managing their Splunk license, and the support of event management and AIOps for more than 700 apps. With all of that on their plate, they knew that adding Cribl Stream to the toolkit would be beneficial. The early results Stream has produced–namely helping them to better manage Splunk licensing and performance–have already help to reduce MTTR, but they have only scratched the surface of potential benefits.

An information diet for the elephant in the room.

The company employs 100,000 people and serves over 100 million customers, so it's safe to say they're working with massive amounts of data. Because they're required by law to bring all that data into a central log repository, their Splunk spend is through the roof. By putting Cribl Stream in place, they can significantly reduce the amount of data moving through Splunk — they started with AWS Cloud Trail data and have already seen a 30 – 40% reduction in data volume from that source.

More structured data is easy on the eyes.

The Service Intelligence team is also responsible for getting the organization's data in through Splunk and over to its security team for threat detection. Cribl Stream is making that process easier for everyone. The reduction capabilities alone have made it so that there is less noise to sort through, but the team also plans to use Stream to transform logs into metrics.

"Every year one of our top objectives is to reduce our MTTR, Cribl has been instrumental in helping us achieve tangible results this year."

"Reading through logs isn't the most fun way to spend the day — especially if you're dealing with network logs and firewall logs — so that's one territory we're exploring. We're going to put our firewall logs through Cribl, then transform them to metrics that we can put into the Elastic Search platform for our security team."

— **Senior Director**, Service Intelligence

Using Stream to reduce MTTR.

The health insurance company is consistently trying to reduce its MTTR, and this strategy of cleaning up data for the security team will allow them the opportunity to improve it. Normalized, structured data makes monitoring much more efficient and allows security to quickly see if something is going on. Cribl Stream allows them to normalize, and add structure and context in flight so that when it hits Splunk, the data is ready to generate meaningful alerts for detection or evidence for remediation. They also plan on using Stream to improve AIOps — if their event management is intelligent, they can do predictive analysis better and see problems before they happen. Getting the right people engaged the first time around is a priority.

"We created a dashboard to look at how much we're saving in terms of dollars for each data source to get a better view on how we're controlling our overall Splunk expense. This gives us more headroom for additional data sources, and gives us a view of how we're enhancing Splunk performance which contributes to our enhanced MTTR numbers."

— **Senior Director**, Service Intelligence

Wading through the AWS message backlog to avoid losing data.

Another immediately useful application of Cribl Stream came in the form of reducing the burden on the company's heavy forwarders. When they first implemented Stream, they had close to 40 million messages in a queue to be sent to them from AWS. Those messages were on the cusp of expiring, so they were running the risk of losing all of that data.

"When we retired the heavy forwarders and routed everything to Cribl, our AWS message queue went down to zero within twenty-four hours — everything started flowing through, and that potential risk of losing data was gone by the next day."

— **Senior Director**, Service Intelligence

"Once we routed everything to Cribl, we were able to retire our heavy forwarder."

The future is bright.

The team is excited to finally take advantage of all of the capabilities Stream has to offer, and masking PII data is next on the list of use cases. Stream's mask function will help them manage their APM users that have sensitive information in their URLs, and the handful of applications that use PII data in their logs.

They're also going to use Cribl to route data to their SIEM — forking off the data from Splunk that needs to go to Sumo Logic or Exabeam. The Senior Directior also talked about their plan to make use of Stream's ability to keep full-fidelity copies of data in cheap storage. More voluminous logs will route through Stream to into storage where teams can Replay it into analysis tools should the need for longer-term investigations arise.

"I involved our security team from very early on when we first started thinking about Cribl – they understand the simplicity and benefits of being able to send data directly to our SIEM, UEBA tools, or to low-cost storage, and mask PII data in flight, among all the other things Stream can do."

— Senior Director, Service Intelligence

Get Cribl, and take control of your data.

There are many opportunities for the company in its partnership with Cribl Stream. A more cost-effective and performant Splunk footprint, significant improvements in MTTR, and massive cost and time savings are right around the corner.

TL;DR:

- Uses Cribl Stream to route data to their SIEM, UEBA, data lake, AIOps tool, and mask PII data.
- They've already seen big returns, including a 30-40% reduction in AWS Cloud Trail Data.
- Reduced the need for heavy forwarders by using Stream for their backlog of AWS messages.
- Improved the efficacy of their security team by providing more structured, relevant data.
- Filtering data through Stream gives the team the ability to easily onboard additional data sources for more comprehensive monitoring, while also controlling and reducing Splunk costs.

"Cribl's capability to transform logs into metrics made it easy to show those metrics to the right people."