Cribl

>CASE STUDY_

How a national energy company leverages Cribl Stream to support critical infrastructure around the globe

Heading the SOC, CERT Operations, and serving as the Incident Response manager at an energy company is undoubtedly a demanding and multifaceted role. Especially for a national energy provider that operates subsidiaries and critical infrastructure globally, spanning across various regions.

HIGHLIGHTS

- Reduced Splunk license from 1.5TB to 1TB
- Accelerated ability to filter, normalize and tag data
- Accelerated incident detection and response
- Resolved bandwidth issues for international, site-to-site VPN traffic

With enormous amounts of data comes great responsibility — which is why the SOC/Cert manager for this national energy company chose to implement Cribl Stream into their monitoring and security environments.

> **"A pipelining technology that allows you to route data from any log source to any log consumer, and at the same time, filter it, clean it up, split it out, and do all kinds of funky stuff with it."**

Stream is described as: The SOC/Cert manager has been routing data and doing the aforementioned “funky stuff” since the early days of Cribl. They implemented Stream while building the SOC for the organization. The energy company’s team manages and secures an air-gapped data center while partnering with an MSSP for alerting and Tier 1 response. Cribl’s routing capability makes it possible for the right data to get to the right destination to accelerate incident detection and response–ensuring no data is lost in the process.

A pipeline between heavy forwarders and variouss Splunk instances

The energy company has multiple Splunk instances in operation. Cribl Stream serves as the data pipeline that allows them to pump all of their traffic from various geographical locations both to regional instances for compliance and remediation, as well as to their central SOC, and then to their MSSP. Because they have traffic going to and from places all over the world — sometimes from regions with very low bandwidth — they filter data in Cribl to clean data up at the source and contain their Splunk license as much as possible.

In a recent conversation with the SOC/Cert manager, they described how useful Cribl Packs have been to operations across the business:

> **"We're using them for all the firewalls and for Windows – Palo Alto Networks, Fortigate, Cisco ASA. It would have been an absolute nightmare to manage all of them without Cribl Packs."**

> **"We originally tried to do filtering on the heavy forwarders, so we were excited to be able to use Cribl filter packs instead. After a simple plug and play, we were up and running in no time."**

Since they're running multiple pipelines for every data source, they also use Stream to enrich their data, tagging it correctly at ingest so that it ends up at the right index at the end of the day.

Cribl cluster-to-cluster compression

If you're running a site-to-site VPN internationally like the energy company is, compression becomes a necessity — otherwise, you could be wasting bandwidth on data you don't really need. Because of the national importance of the data moving through their infrastructure, the team can't afford to lose a single log, so they have some fairly large Cribl clusters running in various locations.

An added benefit for these regions with low bandwidth is Cribl Stream's persistent queuing feature, which ensures no data is lost if networks go down. Stream spools the data (retention is set to 7 days) and when the network comes back up the data ships to its intended destination.

Cribl Stream's fast time to value

When we asked the team how quickly they were able to see value from Stream, they were happy to share their thoughts:

> **"The minute we started piping stuff everywhere, we saw value instantly. It's a product that has an immediate ROI. To give you context, I previously ran a 1.5TB Splunk license in this environment, and we were able to pull that down to a 1TB license. That's a 33% percent savings, so Cribl more than pays for itself."**

With Cribl Stream in place, the team feels confident that they are getting all the data they need and aren't losing anything important along the way. If you're looking for similar warm fuzzy feelings from your infrastructure, check out our Cribl Sandboxes to learn more about our solutions, and join our community to get support from other Cribl users.

"The enrichment capabilities of Stream makes it easy to tag data correctly at ingest, so it ends up in the right destination at the end of the day."

TL;DR

- This national energy company leverages Cribl Stream to get the right data from its sources all over the world to the right destination.
- Stream allows them to confidently route data locally, to a centralized SOC and an MSSP.
- Cribl reduction and compression capabilities resolved bandwidth issues for remote locations and high-volume sources.
- Stream ensures no logs are lost during network or service provider outages.
- Cribl Packs took away the need to manually code and operate data filters on heavy forwarders.
- Stream's ability to filter data gives the national energy company more control over its Splunk license.

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-0027-EN-1-0724