>CASE STUDY_

Creating a Common Operating Picture and Speeding Up Outage Restoration Efforts at a Leading Utility Provider With Cribl Stream

This energy utility company directly serves nearly one million customers, using a variety of fuel sources to generate and deliver power to the residents of their community. They rely on high-quality data and effective monitoring solutions to make business decisions and quickly restore power during outages.

HIGHLIGHTS

- Integrated 50+ disparate data sources.
- Reduced outage restoration time.
- Hit every deployment milestone during architecture redesign.

When their Director of Enterprise Security took over the monitoring, network, and telecom groups, he noticed significant reliability and visibility issues within their architecture. To address this, he initiated a complete redesign of their monitoring program, starting with physical adjustments to their office and a reorganization of leadership.

The company then transitioned to an audit of its legacy tools and the implementation of Cribl Stream as its data pipeline.

> "It's financially untenable to use some of the bigger monitoring solutions because they essentially charge per event – but we still need to collect all of our important data. From a pipeline, capability, and architecture perspective, Cribl Stream was the only tool that met every one of our use cases."
>
> — Director of Enterprise Security

A Common Operating Picture for Streamlined Operations

The goal of this monitoring transformation project was to create a Common Operating Picture (COP) between all parties across the business, changing the way that the organization operates. The team follows the model set forth in the Department of Energy's Cybersecurity Capability Maturity Model (C2M2) to drive situational awareness.

> **"Instead of being a bunch of IT people wearing hoodies, typing away on our keyboards, and operating in silos – we're using Cribl Stream to provide data that allows everyone to understand what's happening in our environment, and use it to make decisions."**
>
> –Director of Enterprise Security

Now that everyone has easy access to the data they need, this utility company can use it to drive business decisions for things like restoration activities. When their monitoring indicates that power and/or communications are down at one or more locations, that information can be quickly communicated to the appropriate teams. Activity can begin promptly and at the right locations, this is especially valuable in times when extreme weather may be affecting their service territory and customers.

> **"From a data pipeline perspective, we're very happy that we don't have to pay as much money to downstream partners."**
>
> –Director of Enterprise Security

> **"We don't look at a Cribl Stream as a tool – it's a platform that enables our growth. All the blinking lights and dashboards in data centers are worthless without being able to see what we need to see and operationalize processes. It's completely changed how we communicate and operate."**
>
> –Director of Enterprise Security

Easy integration of disparate data sources

One of the requirements for the project was the ability to easily integrate any new tools and data sources. Cribl Stream delivers on that requirement. The team's monitoring architecture now includes more than 50 disparate data sources — ranging from commoditized, broad solutions to very specific data sources used for utility-based operations. They expect to have 80 different data streams connected to their data pipeline by the end of the year, including ones that were previously too difficult to integrate.

> **"Ten years ago, we would have to go write collectors or parsers to make integrations between data sources. Getting telemetry from a Linux box to your main monitoring system shouldn't be hard – but it is. Having the integration piece done by Cribl Stream has been invaluable."**
>
> –Director of Enterprise Security

In the past, integrating all of these sources would have required an investment in additional engineering resources. The utility's enablement team was able to spend minimal time focused on creating integrations, and more time making sure that the system kept functioning as necessary. With Cribl as part of the data platform, the project was completed faster than expected.

> **"It's pretty rare to set this type of goal and then to actually hit every milestone. Two-week deployments become risky when they aren't finished six months later. We executed everything exactly as we needed to, and Cribl was a big part of that."**
>
> –Director of Enterprise Security

Higher quality data to feed AIOps tools

The new, fully-integrated pipeline feeds cleaned-up data from all their sources to the organization's downstream AI Ops engine. Over time, the predictive AI will help teams within the company to improve coordination on restoration projects.

> "The first phase where we deployed the Cribl solution was incredibly successful. We hit every milestone we said we would."
>
> –Director of Enterprise Security

> "A monitoring center is often only as good as an on-site analyst. With Cribl Stream's automations, we don't have to constantly rely on one superstar. All of our analysts are equipped to follow documented procedures, and we don't miss a beat. We're not dependent on one person, so it's easier to plug and play resources giving the team more opportunity for learning and growth."
>
> –Director of Enterprise Security

There is a lot of skill required to operate a monitoring center — by making the job less difficult, the electric utility can expand the profiles for recruiting. The team's playbooks and well-documented processes, as well as Cribl's free education helps to nurture less experienced talent to get them productive quickly. They don't have to worry about finding a unicorn that knows everything about the industry, the technology, and security.

Sending logs to data lake for retention savings

This utility is also taking advantage of one of Cribl Stream's biggest value-adds — forking historical data off to cheaper storage instead of eating up license space in a SIEM or AIOps tool. Security events can be much more thoroughly investigated now that they can look back at more than 2 weeks or 90 days' worth of events.

> "If a big event occurs, we know we've got a longer tail of data that we can go back and investigate further. That peace of mind Cribl gives us has been really helpful to have."
>
> –Director of Enterprise Security

Faster Outage Response Times via Event Enrichment

This utility also uses Cribl Stream's enrichment capabilities to add standard information like asset names and IDs to events. They include tags for physical locations, circuits, types of communication paths, and other data that gives a fuller picture of a given incident to resolve issues and restore systems faster.

> "We've got lots of great telemetry and visibility from enriching our data with Cribl Stream. Our custom tags help us determine if particular circuits or communication pathways are affected, and who can address these issues the fastest."
>
> –Director of Enterprise Security

> **"Our service territory has very active weather patterns including tornados that can do incredible damage. Having good data about what's going on in our environment provides us with mission critical visibility. We are able to use that data to help inform business decisions, especially during major restoration efforts."**
>
> **–Director of Enterprise Security**

Information that the security team thinks is interesting today may be radically different than in the future, so they're also happy to have the flexibility to adjust these events if necessary.

The organization's biggest challenge today is making sure to squeeze all the juice out of its new infrastructure. They're working on new integrations with their physical security stack, finding new ways to filter data to avoid downstream license spend, and working with the support team at Cribl to find other ways to improve their common operating picture.

TL;DR

- Completely redesigned monitoring program with Cribl Stream as data pipeline.
- Improved reliability and visibility issues within security architecture.
- Created common operating picture across the organization.
- Reduced outage restoration time due to streamlined operations.
- Integrated more than 50 disparate data sources.
- Feeding cleaned-up data to AI Ops engine.
- Saving on SIEM costs by routing logs to data lake for longer retention periods.