>SOLUTION BRIEF_

Federal Law Enforcement Agency Uses Cribl Stream to Accelerate Cybersecurity Investigations

HIGHLIGHTS

- Faster onboarding while enriching and shaping data to accelerate investigations
- Performance enhancement of Splunk and Elastic reduces the burden on users
- Resolving timestamp challenges reduces incorrect IP or geolocation tags

At Cribl, we are honored to work with US Federal Agencies as they monitor and improve national security. One agency, in particular, is responsible for protecting the American people and is often handed enormous amounts of data all at once with the task of quickly making sense of it. Cribl simplifies and accelerates the process of ingesting, enriching, and analyzing those huge volumes of data, enabling investigators to identify specific data points and map them to corresponding Indicators of Compromise (IOCs).

The agency uses Cribl Stream to make it easier to discover the origin of the cyberattacks they investigate. Entities who need help investigating these attacks often share terabytes of historical data with the government agency — most of which end up being irrelevant. According to one of the agency's engineers, "The best way to treat data is to give it an analytical home where it can scale," — with Stream, they can do just that.

Saving Analysts Time by Routing Data to Its Proper Home

Some types of data, like time series or machine data, do really well in a tool like Splunk — while other, more voluminous sources are better suited for a destination like Elastic. Routing larger or text-based data sources to Splunk can cause formatting issues that slow down searches, so it's important that each source ends up in the best tool for the job or team analyzing the data.

> **"Having the flexibility to pivot destinations based on the type of data is really powerful. We're able to give the analysts and the users of these tools a much easier experience and save them valuable time."**
>
> **—Josh Brunvoll**, Consulting Engineer

> "We originally saw Stream as a visually friendly tool for props and transforms on the fly, but it grew from there. With the different capabilities in enrichment and data routing pipelines, it's turned into a tool that's doing a lot of good for us."
>
> – Josh Brunvoll, Consulting Engineer

Cribl Stream makes routing data to the appropriate destination simple, while also giving the agency the ability to filter, shape and normalize the data they receive, so they only ingest the data relevant to each case. Optimized data sets within the right tools make a world of difference in speeding up the investigation process.

Addressing Scale by Enriching Events at Ingest Time

The agency is also using Cribl Stream to enrich data at ingest time to fully replace the custom Python script they currently use. Instead of running that script and dealing with MaxMind lookups and MaxMind database (MMDB) files manually, they use Cribl Stream to add geolocation tags to events.

This strategy will have a number of benefits — enrichment at ingest saves time and processing resources resulting in faster analysis of very large data sources. There are also time savings on the back end:

> **"If you're doing search time enrichment, the extra CPU cycles take a toll on the user. They're going to sit there and wait for searches to complete –but by having appropriate elements already embedded into the events, that time is given back to the user. Multiply that by the number of users we have, and it has a huge ripple effect."**
>
> **—Josh Brunvoll**, Consulting Engineer

Since not all logs come with properly formatted timestamps, the agency will be able to rely on Cribl Stream to ensure they're accurate. Reliable timestamps will assist investigators in creating more precise case timelines as well.

> **"What's really cool is that we can custom build our pipelines to add the different formats and then coalesce them into the output that we want – and it's easy to do whether you're creating your own pack or leveraging one built by Cribl. Once it's in that format, everything's smooth sailing from there."**
>
> **—Josh Brunvoll**, Consulting Engineer

TL:DR

- Federal law enforcement agencies are using Cribl Stream to accelerate cybersecurity investigations
- Stream's visual UI allows them to create props and transforms on the fly
- Stream gives them the ability to address timestamp challenges to ensure accurate investigative timelines and ensure accurate IP geolocation
- Enrich data with specific IOCs before search time, giving investigators better, more relevant data to search through
- Reduce reliance on TAs, Regexes, or configuration files, and reduces low-value, repetitive work for their team
- Investigators can see the right formats and types of data faster, with the right context, in their preferred analytical tool