>CASE STUDY_

Finality Helps Federal Agencies Accelerate Onboarding of New Data Sources, Manage SIEM Licenses, and Meet M-21-31 Requirements

Finality, an IT and Security services consulting firm, helps US Federal agencies meet their log management obligations. When requirements and volume exceed available funding, licensing, and staffing resources, Finality helps agencies find ways to solve these issues.

One of Finality's most common challenges is navigating federal agencies' license limits with their SIEM (security and information event management) providers. As data volumes increase alongside stagnant budgets, this problem becomes more prevalent and difficult to manage.

Eric Jeanmaire, Finality's CEO, was in search of an innovation to address this problem when he was introduced to Cribl Stream in October 2020 — less than a year before the Executive Order on Improving the Nation's Cybersecurity and subsequent memorandum M-21-31 were issued. Significantly greater log collection, retention, and analysis requirements, coupled with the urgency of business imperatives, compelled Eric to implement Cribl Stream within the Department of Homeland Security just one month later.

47% Reduction of Windows Event Logs

Since deploying Cribl Stream Eric has found it easier to fulfill his commitment to his Federal Customers. Agencies can't afford to onboard new system data from a financial perspective, but they can't afford not to from a security perspective — so being able to make room for additional logs was one of the most immediate value propositions.

Cribl Stream allows admins to filter out repetitive or otherwise unnecessary data. Logs can be filtered in their entirety or at the individual field level to remove as much bloat as possible. Eric and his team have seen great results.

HIGHLIGHTS

- **47% reduction** of Windows Event Logs.
- **10x faster** data extractions and data model compliance.
- **250% increase** in SIEM content creation.

> “Being able to get a 47% reduction on average in our Windows Events by dropping repetitive fields is huge – because all of that can go into onboarding additional logs that we need from other systems.”
>
> — **Eric Jeanmaire**, CEO

10x Increase in Data Onboarding Speed

The ease-of-use and scalability of Cribl Stream was a big factor in Eric’s decision to build Stream into the security and compliance stack he delivers for his customers. Because of how easy it is to deploy and scale, Finality has been able to onboard data 10 times faster than before. That increase is representative in accelerating data extractions and making it easier to map data to Splunk’s Common Information Model (CIM), making for better and faster correlations once data hits the SIEM, as well as ensuring data consistency in both the SIEM and in S3 or other cheap storage.

For one of the federal agencies they work with, nothing gets deployed manually — so Stream fits nicely into the automated pipelines of the customer’s environment.

> “Since we’ve adopted Cribl Stream, we’re no longer held hostage to our SIEM TA’s – we can onboard systems much faster now.”

> “I like that Cribl Stream leans towards open source but also adopts a lot of modern architecture best practices. We can scale a cluster very easily and replace or upgrade nodes automatically. Everything is version controlled through Git, so it makes for an easy deployment.”
>
> — **Eric Jeanmaire**, CEO

SIEM License Cost Savings

More efficient data and increased onboarding speed have not only allowed Finality to bring more logs into their customers’ SIEM, but they’ve also been able to shift to a CPU utilization-based model.

> “We’ve shifted CPU-intensive activities-like CMDB and threat enrichment-to Cribl Stream, adding to our SIEM license and infrastructure savings. By doing our data model compliance at the Cribl level, we’re taking away a lot of that compute utilization from our indexers. Savings can still be had, even in the new licensing schema.”
>
> — **Eric Jeanmaire**, CEO

Avoid Downtime or SOC Disruption

Another benefit of Cribl Stream is the ability to capture and analyze production data without disruption to operations. With Cribl’s innovative ability to see data manipulations and changes visually through the UI as they would appear in Splunk or Elastic beforehand, Cribl eliminates hard cutovers, perfect for SOCs that need to collect data 24/7 and don’t want to suffer any feed outages.

Eric and his team take advantage of this by first using Cribl as a catch-all pipeline that simply forwards the data to its destination. Then, they can cut over single feeds as necessary.

> **"With Cribl Stream, we can capture feeds as they're flowing through, create samples, work on our pipeline, QA it, and then turn the pipeline on. From there, we can shift to doing field extraction, normalization, and data model compliance right in Stream, without having it flow through our catch-all."**
>
> — **Eric Jeanmaire**, CEO

Instead of burning developer hours updating technical add-ons (TAs), the Finality team leverages Stream as the universal connector to prepare data.

> **"It's easy to wean yourself off of TAs that need updating by cutting feeds over to Cribl Stream as you're ready. It doesn't have to be one big upfront effort to rewrite all of them on day one."**
>
> — **Eric Jeanmaire**, CEO

> **"Cribl Stream's immediate value propositions were that it aligned well with our architecture, and it provided significant data reduction that allowed us to use our SIEM licensing elsewhere."**

Seamless Firing of Detection Content

One of the architectural, best-practice decisions that Finalty made is to only develop content off of their data models. Cribl Stream makes it easy to transform raw data to your destination schema of choice, to accelerate identification of important Indicators of Compromise (IOCs).

> **"It's easy to get into trouble operating products over time when you have written a lot of content off of raw feeds. You really have to make sure you're sticking to Data Model compliance, and Cribl is a great way to ensure CIM compliance very quickly."**
>
> — **Eric Jeanmaire**, CEO

250% Faster Delivery of SIEM Content

Since bringing on Cribl Stream, Finality's content development time has gone down significantly. Whenever there's a new emerging threat, they have to capture applicable sample data to develop and validate detection content. Before Cribl, they would have to send the data to their SIEM, create field extractions, map it to their data model, write custom correlation searches, and then build the detection content 10 times slower. This process now moves much more quickly.

> **"With Cribl Stream, we've dramatically shortened the content delivery timeline. New source data goes to Stream, and we do field extraction, normalization, and data model compliance all in Stream instead of our SIEM. Then we can start working on detection content and correlation searches much more quickly."**
>
> — **Eric Jeanmaire**, CEO

> “Cribl had immediate value to us and our customers — we know there’s even more savings coming.”

As a result, Finalty has seen a 250% month-over-month increase in the number of new detection rules they are creating. Allowing them to be more responsive to threats, and better controlling Attack Surface Management (ASM).

Maintaining Happy Vendor-SI Relationships

Partnering with Cribl is a great choice for systems integrators looking to enhance their offerings and deliver value to customers. Cribl complements and enhances already-existing tooling, allowing for repeatable, automated management and configurations. Spend less time onboarding data and working with outdated TAs and spend more time delivering value to your customers.

- Create capacity to onboard new data sources at existing license volume
- Accelerate data onboarding and quickly accommodate data format changes
- Accelerate detection content creation for enhanced security posture
- Optimize Splunk CIM/Elastic ECS data model compliance to enhance search performance, reduce CPU load
- Meet M-21-31 requirements while controlling costs

With free training, reference architectures, and sandboxes, SIs can easily develop certified subject matter experts (SME’s) who can leverage Cribl’s capabilities. Our team is well-staffed with a bench of knowledgeable folks willing to help, and a great Federal team that provides support when needed to meet any and all deadlines.

TL;DR

- 47% reduction of Windows Event Logs, making room for more data sources.
- 10x faster data extractions and data model compliance.
- Reduced SIEM license cost and facilitated switch to SVC/CPU utilization license model.
- No hard cutovers and seamless data flow for 24/7 SOC uptime.
- Decreased reliance on outdated TAs.
- Easier data model compliance for seamless firing of detection content.
- 250% increase in delivery speed of SIEM content for emerging threats.

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-0011-EN-2-0624