>CASE STUDY_

Future-proofing Your Security Operations: Evaluating and Implementing Multiple SIEMs with Cribl

HIGHLIGHTS

- 82% reduction for firewall logs; 33% reduction for WAF.
- Seamlessly run parallel tests on four SIEMs.
- Facilitate uninterrupted data flow during the transition to the new SIEM.
- Increase capacity to onboard required compliance logs.

A multinational travel management company provides innovative solutions and exceptional service to businesses worldwide. As a key player in the travel industry, they specialize in comprehensive travel management services, including travel booking, expense management, and travel policy compliance.

For organizations like this one, navigating a complex data landscape requires an innovative approach. With vast amounts of data flowing from various sources, the Cyber Security Manager leading Cyber Security Engineering understood that a traditional SIEM solution wouldn't future-proof their environment in the way they needed.

With many capable SIEMs in the industry, the team faced the massive undertaking of identifying and selecting the right tool to advance their security priorities. In order to be confident in their selection, they knew they would need to evaluate the top contenders in their environment using real data. The team found Cribl Stream was a fast path to get real data where it needed to go in the format required by each SIEM to get as close to an apples to apples comparison as quickly as possible–while not disturbing the data flows to the current SIEM.

> "Everyone touts integrations. But one thing about Cribl, it is basically one tool to ingest them all."
>
> – Cyber Security Manager

> "Cribl Stream played a pivotal role in achieving several of our goals. It allowed us to test multiple SIEMs concurrently, giving us confidence that our final selection would future-proof our security infrastructure."
>
> — Cyber Security Engineer

"Thanks to Cribl's flexible data pipeline, we expedited our selection process without impacting our current SIEM."

– Cyber Security Engineer

A Complex Data Landscape Demands an Innovative Approach

The team didn't just test one or two SIEMs; they took on the monumental challenge of evaluating four different SIEMs simultaneously. Cribl Stream's unique ability to ingest data once and route it to multiple destinations was a game-changer, allowing them to assess each SIEM's performance with remarkable speed and efficiency.

> **"The ability to use pre-built Cribl Packs for the various SIEMs we were testing saved a lot of time and streamlined what could have been a multi-month, if not multi-quarter, process."**
>
> **—** Cyber Security Engineer

Managing specialty dashboards and alerts often requires dealing with log fields that might be extraneous or unnecessary for other SIEMs. By leveraging Packs for data onboarding, the team avoided building custom parsers and eliminated the need for deep expertise in each product. This streamlined approach simplified the data onboarding process and significantly reduced the number of work hours required.

"If you're testing a new source, you can build out as many routes as you need, tailor how you need to, then send it."

– Cyber Security Engineer

> **"Cribl doesn't care what data source you send. You can use Packs to ingest the data, normalize it, and ship it. Then, sit back and watch your dashboards populate."**
>
> **—** Cyber Security Engineer

Single Pane of Glass, Cribl Style

The "single pane of glass" is a familiar concept in cyber security, but the team took it to the next level with a unique, *Cribl-ized* approach. Using Cribl Stream to consolidate their data sources and observe them from ingestion to destination(s), they achieve a unified and comprehensive view of their entire data management pipeline, including each SIEM under evaluation.

"Cribl pipelines gave us the ability to tailor and format all of the log data for each specific SIEM or destination."

– Cyber Security Engineer

> **"We finally have a *single pane of glass*. We can see and monitor all of our incoming data sources. We can monitor them as they traverse through the pipelines to our routes and finally to the destinations. Everybody loves a *single pane of glass* because we don't love pivoting to multiple tools to get the same data. It's awfully convenient to have it in one place."**
>
> **—** Cyber Security Engineer

Cribl Stream's flexible pipelines made it easy for the team to set up precise routes to manage data flow, ensuring choice and complete control over their data paths. With Stream's ability to add fields to data in motion, the logs become easily traceable, enhancing visibility while simplifying troubleshooting and validation.

"Cribl makes troubleshooting SIEM parsers easy and quick. It takes only a few minutes to add new routes and test new destinations."

– Cyber Security Engineer

"Cribl is one tool to ingest them all."

– Cyber Security Engineer

"Logs can be viewed at every stage of the process, from ingestion to pipelines to routes and finally before they hit the destinations."

– Cyber Security Engineer

Tagging, Unsung Hero of Parallel SIEM Testing

Cribl Stream's Ingest-Time Fields, commonly referred to as tagging, can be used to filter and group data. This valuable feature allows you to change incoming events in real-time— critical for parallel SIEM testing.

"Tagging is a super neat feature that Cribl offers. We utilized it heavily throughout our deployment."

— Cyber Security Engineer

By tagging their data, the team stayed organized across their four SIEMs in POV, ensuring that logs could be easily identified and routed. This approach allowed them to trace the impact of any changes made to logs by following an added field through the system, enabling them to pinpoint and address any downstream issues.

"Tagging log sources not only helps us stay organized with routing but also helps with quickly finding specific logs at their destination."

— Cyber Security Engineer

Back to Business, but Better

The team was able to cut through red tape and complete POVs on their own terms and timelines, allowing them to return to their regularly scheduled business much faster than with traditional evaluation periods. The successes for the multinational travel management company have continued, delivering significant improvements in their data management processes.

"Once our new SIEM was chosen, Cribl streamlined and facilitated a seamless migration to the new solution without interrupting the data flows to our existing SIEM. It resulted in a very smooth transition."

— Cyber Security Engineer

Cribl Stream continues to deliver significant efficiency gains in data reduction across key sources, further enhancing their security posture and operational efficiency.

"82% is the average reduction. This was not just tested on firewalls and WAF but on a variety of sources including EDR, Active Directory, and cloud logs from AWS and Azure."

— Cyber Security Engineer

This newfound capacity has allowed the team to onboard logs critical to their governance, risk, and compliance (GRC) teams. They are now including more comprehensive firewall logs and other vital data feeds, enhancing their overall security visibility with their future-proofed SIEM—all thanks to Cribl.

> “We increased overall security visibility by freeing up valuable resources in our current SIEM.”
>
> – Cyber Security Engineer

TL;DR

- A multinational travel management company uses Cribl Stream to test four SIEMs simultaneously.
- Cribl Packs allow quick and easy data onboarding.
- Configure, monitor and view incoming and outgoing data sources with a *single pane of glass*.
- The flexible data pipeline facilitated a faster selection process by reducing data volumes and improving visibility.

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-0033-EN-2-0225