>CASE STUDY_

Building a Scalable Cyber Security Operations Center at a Premier Resort and Conference Center with Cribl and Exabeam

This resort and conference center is a premier, upscale resort destination, bringing in over $1B annually. Because they are also a casino, their cybersecurity team faces very strict regulatory reporting responsibilities and an enormous amount of data to manage. They've leveraged Cribl to dramatically reduce their SIEM spend, route regulatory data to appropriate destinations, and build a fully functional CSOC in 60 days.

When the resort changed ownership in 2022, its cybersecurity team moved away from their existing MSSP to re-imagine their security architecture, tooling and partners, the Executive Director of Cyber Security: Strategy, Architecture & Engineering, knew that Cribl Stream would be a critical element of the transition.

> **"From my vantage point, Cribl Stream is one of the most important tools in the cyber tool chest. I've saved literally half a million dollars a year – they're allowing me to control my own data and make better use of my other investments and tools that have nothing to do with Cribl."**
>
> — **Executive Director of Cyber Security:** Strategy, Architecture & Engineering

HIGHLIGHTS

- $500k annual savings from optimization of data sent to SIEM.
- Increased accuracy of detection content and platform speed with relevant, quality data.
- Re-architected SOC in 60 days.

An Immediate Reduction in SIEM Spend

Inspired by an impending ownership transition, the Executive Director and his team resolved to shift their operational approach. They opted to move from a fully outsourced SOC model to a hybrid SOC, integrating an in-house tech stack with tier one MSSP support. To ensure the transition remained within budgetary constraints and presented a cost-effective solution, the team found it necessary to segregate high-value data intended for analysis and detection from the high-volume data needed for regulatory compliance. Recognizing Cribl's pivotal role in achieving this objective, they determined that prospective vendors onboard with Cribl as a prerequisite.

To get started, they deployed Cribl Stream and Packs from the Cribl Packs Dispensary to rapidly filter logs and normalize the data traveling to Exabeam, their new SIEM and UEBA provider.

> "By using the out-of-the-box filters, we were able to take our data throughput from 1.2 TB down to 800 GB per day. After briefly working with the Cribl team, we got down to 450 GB daily. That process was fast – we recognized the benefits very quickly."
>
> **— Executive Director of Cyber Security:** Strategy, Architecture & Engineering

Instead of just indiscriminately funneling syslog into Exabeam Fusion they worked directly with Exabeam, their SIEM provider, to only send the information needed for Advanced Analytics and to drive detections. Thanks to the reduced data load they've realized by normalizing and optimizing data across all of their sources, the resort's team has not only saved money on data lake storage for their SIEM, but they've also increased the speed of reporting across the platform.

Ease of Compliance With Regulatory Bodies

Large reductions in data and improved performance are the norm for Cribl Stream users, but unexpected benefits are also very common. The Executive Director was pleasantly surprised when the opportunity presented itself to re-think solutions for complying with casino-related data regulation.

> "The number one reason we wanted to use Cribl Stream was the ability to reduce the amount of data ingestion going into the SIEM. But it's more important than that – once we started to learn more about the product, we found that we were able to filter data off, specifically for regulatory reporting, instead of having to pump it into our SIEM."
>
> **— Executive Director of Cyber Security:** Strategy, Architecture & Engineering

Stream made it easy to send concise, masked, scaled-down subsets of information directly to the appropriate regulatory organizations with no concerns about confidentiality or storage.

A Seamless Transition With Zero Loss of Cybersecurity Coverage

It took the Executive Director and his team 60 days from the time they kicked off implementation to stand up a fully functional SOC. Due to heavy industry regulations, they had to run simultaneous coverage during the transition from their old MSSP to the new MSSP.

> "It took us 60 days to fully stand up an MSSP and basically build a fully functional SOC. Cribl was a pivotal part of that."
>
> — Executive Director of Cyber Security: Strategy, Architecture & Engineering

> "Cribl Stream gives me an increased speed of detection and response, as well as the ability to control my own data and reduce my spending. I don't think my own engineering group would fight me if I said it's been pivotal, and it's not going away."
>
> — Executive Director of Cyber Security: Strategy, Architecture & Engineering

> "Cribl had no problem helping us work with our diverse set of cybersecurity tools and data feeds, including syslog. Stream gave us the flexibility to completely control what we were going to send through."
>
> — Executive Director of Cyber Security: Strategy, Architecture & Engineering

> “When you do get a data breach, the incident response folks need the ability to turn back the clock. The Replay feature was also a very attractive capability of Cribl Stream.”
>
> — Executive Director of Cyber Security: Strategy, Architecture & Engineering

> “We would have been severely hamstrung in our ability to provide world-class cybersecurity coverage for our premier casino without Cribl Stream.”
>
> — Executive Director of Cyber Security: Strategy, Architecture & Engineering

> “There were so many issues with our vendors that we would have actually increased our risk by not bringing on Cribl Stream. We would have been forced to stay with them and renew for another year.”
>
> — Executive Director of Cyber Security: Strategy, Architecture & Engineering

> **“We had to have a seamless flick of the switch —Cribl allowed us to take 30 data feeds and fork them to both the new and old platform so that our existing MSSP could continue to provide the service that we were paying them for, while simultaneously allowing us the time and energy to completely stand up a fully operational, brand new architecture.”**
>
> — **Executive Director of Cyber Security:** Strategy, Architecture & Engineering

Ultimately, the Executive Director mitigated the risk of data loss and maintained comprehensive coverage during the transition.

> **“We literally lost zero coverage. We actually gained capability.”**
>
> — **Executive Director of Cyber Security:** Strategy, Architecture & Engineering

Saving on Costs and Engineering Time

Using Cribl Stream to migrate to a new hybrid MSSP model and the Exabeam product suite has created a snowball effect in terms of time and money saved. They were able to reduce their SIEM license, while limiting staff hours spent handling regulatory data, and focus those resources on taking on new initiatives to better service the business. The Executive Director believes that by providing new opportunities to his team–not keeping them mired in data onboarding and repetitive reporting–also helps to address the staff churn so often faced by security teams.

> **“When you’re sitting in my seat or a CISO seat, you’re very concerned with dollars and resource management. Any time you can get a 60% reduction in that bill, and keep your team engaged and challenged, you feel like you’re in control of your own destiny, and that really helps a lot.”**
>
> — **Executive Director of Cyber Security:** Strategy, Architecture & Engineering

Top-Notch Support from Vendors

The resort’s new MSSP does a lot of QA and fidelity checks on the logs sent via Stream, so they’ve also learned a lot about Cribl along the way. The Executive Director describes the relationship between two of his most widely used partners:

> **“Cribl has always immediately helped out. Their expediency and willingness to work with our vendors to solve a very complex problem is unique. Whenever any issues arise, the support team at Cribl has been right there to work with us to help us out.”**
>
> — **Executive Director of Cyber Security:** Strategy, Architecture & Engineering

Since being acquired by a global private equity firm and bringing on Cribl Stream, the resort is considered to have the most mature cybersecurity team out of the hundreds of organizations under the umbrella of their portfolio. And you can bet they'll continue to make strides to enhance their posture.

TL;DR

- Built a fully functional CSOC in 60 days.
- Reduced SIEM license and infrastructure costs by 60%.
- Easily fork off regulatory data to appropriate destinations.
- Zero loss of cybersecurity coverage during the transition to new security architecture and vendors.
- Increased speed of detection and response.
- Recovered lost engineering time from automation of repetitive, time-consuming tasks.

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-0018-EN-2-0624