>CASE STUDY_

How CHRU de Tours Modernized Security Operations and Cut Costs with Cribl Stream

HIGHLIGHTS

- Reduced SIEM ingestion volume by 50%, enabling a lower-cost SIEM license renewal.
- Maintained existing alerts, dashboards, and workflows—avoiding a costly migration.
- Deployed quickly and in parallel with production, minimizing disruption.
- Positioned for scale with Cribl Cloud

As one of the region's largest employers, with 20,000 employees and a rapidly expanding digital infrastructure, the Regional University Hospital Center (CHRU) de Tours operates in a highly complex and sensitive digital environment. Their infrastructure must support mission-critical healthcare systems while protecting vast volumes of personal health data.

Amid increasing cyberattacks on the healthcare sector worldwide, CHRU de Tours needed solutions to ensure operational continuity and safeguard patient trust. However, the combined costs of EDR, SIEM, and managed SOC services quickly exceeded their limited budget, leading CHRU to seek solutions to control spending and manage its expanding data volume.

At the recommendation of their MSSP, CHRU de Tours adopted Cribl Stream, managed through Cribl Cloud, to change how they process and route observability data, enabling them to manage their budget while improving flexibility and visibility.

Modernizing without disruption

Seeking to reduce costs, CHRU de Tours considered replacing its existing SIEM with a custom, open-source solution. However, this alternative would have meant abandoning years of work spent building and tuning alerts, dashboards, and other critical functions. CHRU wanted to consider other options that could still leverage the existing SIEM and investment the team made in content development.

> **"The other solution was to drop all our expertise gained on the current SIEM to build a new one from scratch. This would have taken a long time and a strong effort to reach the same level of knowledge we already had."**
>
> **—Erwan Genestal, Network and Security Architect, CHRU de Tours**

Cribl Stream offered a compelling alternative, enabling CHRU de Tours to modernize its data pipeline and achieve cost savings. Crucially, it did so by preserving the full value of their existing SIEM, so they didn't have to rearchitect or rebuild their entire system from the ground up.

Having found a way to modernize their data pipeline and cut costs, CHRU de Tours now faced a new challenge: a tight, six-week deadline before their SIEM license renewal. The team needed to make a quick decision, which made rapid deployment critical.

Unlike the complex and disruptive alternative of a custom-built solution, Cribl Stream allowed the team to test the new architecture in parallel with their live production environment. This enabled them to quickly and confidently validate the new approach – and cost savings – with zero operational disruption, all thanks to a solution that required no major reconfiguration.

> **"The Cribl solution had the benefit of being tested in a very short time, in parallel with production, so we could see the real gain of the volume reduction without impacting the current solution."**
>
> **—Erwan Genestal, Network and Security Architect, CHRU de Tours**

Cost savings without compromise

CHRU de Tours faced a common security challenge: managing an overwhelming volume of log data from its vast network infrastructure, including switches, firewalls, and EDR tools. The sheer volume was making their SIEM license prohibitively expensive.

> **"Stream is a Swiss Army knife that can do anything we want on the data. We mainly use it to reduce the volume and contextualize the logs, but it can do all the transformation you want."**
>
> **—Erwan Genestal, Network and Security Architect, CHRU de Tours**

By deploying Cribl Stream, the hospital intelligently reduced its overall ingestion by 50%, specifically cutting firewall logs by 60% and Windows Security Events by 50%. This dramatic reduction allowed them to renew their SIEM license under more favorable terms.

CHRU de Tours' success proved that they didn't have to sacrifice data quality for cost savings. They used Cribl Stream to filter out noisy, redundant data and keep only what was critical for security. The security team easily demonstrated that the optimized data set provided the same insights as the original—highlighting just how much unnecessary data had previously gone unnoticed. As a bonus, Cribl Stream also provided a new layer of observability, helping the security team proactively monitor data health and troubleshoot issues.

> **"We kept the original architecture with the forwarders sending directly to our SIEM, and we built a second index with Cribl. That gave us insight into the data profiles, and the proof of concept was quite successful."**
>
> **—Erwan Genestal, Network and Security Architect, CHRU de Tours**

TL;DR

- Cribl Stream helped CHRU de Tours achieve a 50% reduction in log volumes.
- This reduction allowed them to renew their SIEM license under favorable terms.
- CHRU de Tours demonstrated that the optimized data set provided the same insights as the original, voluminous data set.
- The parallel deployment of Cribl enabled quick validation, preserving existing SIEM development work.
- Using Cribl Cloud, they maintain a hybrid infrastructure with minimal maintenance, preparing for future growth.

Faster time to value, less maintenance

By managing Cribl Stream through Cribl Cloud, CHRU de Tours was able to accelerate time to value, reduce operational overhead, and position their team for long-term agility. The cloud-managed approach simplified updates and freed up internal resources to focus on strategic initiatives.

Because Cribl Cloud supports both on-premises and cloud environments, it fits seamlessly into CHRU de Tours hybrid architecture, while also preparing them for a future where more workloads may move to the cloud. This flexibility ensures that as their infrastructure evolves, their observability strategy can scale right along with it.

With Cribl Cloud, CHRU de Tours gained a more efficient, future-ready platform, without the complexity or maintenance burdens of traditional deployments.

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 X

©2025 Cribl, Inc. All Rights Reserved. 'Cribl' and the Cribl Flow Mark are trademarks of Cribl, Inc. in the United States and/or other countries.
All third-party trademarks are the property of their respective owners.

CS-0040-EN-1-0925