>CASE STUDY_

The Passport to an Optimized Security Stack at Leading Leisure Travel Company: Cribl Stream

A few years ago, a popular lifestyle magazine underwent a transformation when it merged with a vacation rental and timeshare company. This shift in the company's mission, from print to dream travel experiences led to the creation of the world's leading leisure travel company. This transformation established a global presence and incorporated almost 20 different brands. As a result of their growth, they needed to rethink their observability and security data strategy.

When the travel company expaneded, so did the responsibilities for their corporate security team. They needed to unify and secure their global footprint to maintain their security posture. Upgrading to Crowdstrike Falcon Data Replicator (FDR) met all of their requirements by furthering their Security Operation Center (SOC) with actionable insights from their Endpoint Detection and Response Solution (EDR).

However, after implementation, they found themselves facing an unexpectedly high volume of logs that exceeded the available license space and infrastructure capacity in their Security Information and Event Management (SIEM) tool, Splunk. This put them in the difficult position to prioritize which data they could onboard to drive detection content in their SIEM.

While searching for ways to manage their logging capacity and extract value from Crowdstrike endpoint telemetry data, their Director of Cyber Security Operations, was introduced to Cribl Stream.

> "We worked with Cribl to optimize our FDR logs, and we really liked what we saw. We were able to solve our immediate issue with Crowdstrike FDR, by reducing our log volumes to the expected footprint without losing the context we needed for detection. This would allow us to remain within the licensing constraints for our SIEM." Director of Cyber Security

HIGHLIGHTS

- Able to rapidly get value from Crowdstrike FDR and stay within data limits.
- Initial optimization with Cribl Pack for CrowdStrike FDR opened 50% additional headroom in SIEM
- The team optimized Crowdstrike data while still getting needed context for detection and investigations
- An overall reduction of 72% was achieved.

Operations.

“Stream was a no-brainer. It was extremely easy to use and adopt. After each call we would jokingly increase our desired outcome because we knew the tool could blow it out of the water.”

– Director of Cyber Security Operations

The Affordable Way to Desired Destinations

During the evaluation, the SOC team saw an immediate reduction in log volume, simply by leveraging the free Cribl Crowdstrike Pack. Cribl Packs, which can be found in the Cribl Pack Dispensary, are a set of readily available configurations designed to enable Cribl Stream administrators and developers to quickly reduce, optimize and enhance their Crowdstrike data.

“Using Cribl Packs we were able to achieve an immediate 50% reduction in the logs. From there we had team brainstorming sessions on how to reduce the volume of data without impacting the value. It was tricky, and it took us maybe 5-6 sessions, but we were able to achieve a 72% reduction, while still getting the context we needed for investigations.” Director of Cyber Security Operations.

Making Data Travel Woes a Thing of the Past

After getting their logging volume under control, the team set their sights on the future: optimizing their security stack with Cribl Stream.

“A large part of our strategy is to separate data we would need for alerting purposes into Splunk, while data for retention and compliance purposes was directed towards affordable log retention, Crowdstrike LogScale,” Director of Cyber Security Operations. “We needed Cribl to work seamlessly with both of these solutions.”

“A large part of our strategy was to separate our high-value data into our primary SIEM and our “low-volume data” into a secondary, more cost-effective SIEM, Crowdstrike LogScale. We needed Cribl to work seamlessly with both of these solutions.”

– Director of Cyber Security Operations

It’s important to note that there is no loss of data due to this segmentation. Instead of sending all FDR data directly to Splunk, Cribl is used to easily manage the data pipeline. Reduced, high-fidelity logs helpful for alerting are sent to Splunk, while voluminous raw logs, and logs for long-term compliance are directed to LogScale.

Although the strategy for SIEM Optimization sounds straightforward, the execution of sending the same data to disparate destinations usually requires leveraging each tool’s proprietary ingestion process. Cribl Stream acts as a unified pipeline, allowing several data sources to be modified and redirected, or even enriched with IOC or GeoIP data in flight. The SOC team discovered firsthand just how easy it was to leverage Cribl as part of the optimization process.

New Perspectives for Security

The combination of Cribl Stream’s routing and reduction functions gives the team the flexibility to spend less time managing data onboarding, configurations, normalization and licensing limitations. This provides them more time to focus on their jobs as security practitioners.

> **“With Cribl Stream, we reconfigured the data in one place, with a user-friendly GUI,” Director of Cyber Security Operations. “You can make the changes in a matter of minutes and instantly see results–versus taking hours or days to understand the impact of your changes.”**

Ultimately, the SOC team was able to use Cribl Stream to increase the value of the tools in their security stack in an easily adoptable way.

> **“Stream was a no-brainer. It was extremely easy to use and adopt. After each call we would jokingly increase our desired outcome because we knew the tool could blow it out of the water,” Director of Cyber Security Operations.**

TL:DR

- The World’s Leading Leisure Travel Company uses Cribl Stream to reduce and route security logs.
- Cribl helped the team to optimize CrowdStrike FDR data to stay within SIEM licensing volume.
- Cribl provided easy routing to multiple destinations, based on business needs.

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-0005-EN-2-0624