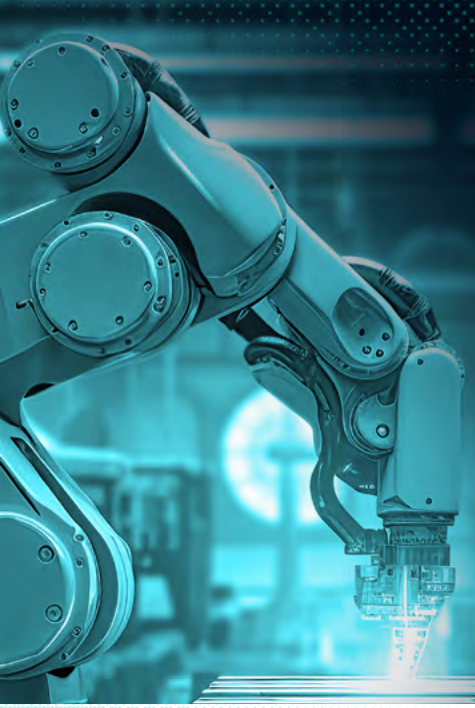

>CASE STUDY_

A Fortune 100 IT Infrastructure and Services Company Improves Threat Detection with Cribl Stream through Faster Optimized Data Onboarding

HIGHLIGHTS

- 95% reduction in development time for custom parsers
- Zero dropped events
- Seamless onboarding of new or unknown data sources

A Fortune 100 IT infrastructure and services company that offers Managed Detection and Response (MDR) as a comprehensive threat detection and response platform helps minimize risk by providing real-time insights that identify and combat threats to your organization, workforce, and customers.

This Fortune 100 IT infrastructure and services company is a specialist in threat detection: they collect and evaluate their customer's telemetry, logs, and alerts from various devices like perimeter firewalls, endpoints, and the cloud, to identify threats. The path from data ingest to Indicator of Compromise (IoC) identification involves multiple steps, each reliant on the one before to keep the process moving as efficiently as possible.

Since bringing on Cribl Stream, the process hasn't just become much smoother — it has also allowed the team to focus more of their efforts on proactive threat hunting instead of solely onboarding and parsing customer data.

> "For us, log ingestion with parsing is just a necessary evil. Now that we have Cribl Stream to handle it, we can have more developer resources focused on threat detection – which is what we're good at and what our customers pay for."
>
> —**Technical Lead**, Office of the CTO

Reduced Dropped Events to Zero

The first step in this MDR team's threat detection process involves collecting their customer's telemetry data. Before bringing on Cribl Stream, events from unrecognized sources wouldn't make it through to their collectors.

Even on previously recognized devices, a firewall port or IP address change would cause events to be rejected and stored locally at the customer's site instead. When local storage locations were exhausted, they would start to cycle data and write over logs.

"We have completely transformed our business and how we collect telemetry data — Cribl Stream is the vehicle we used for that transformation."

"We had a lot of infrastructure built around parsing of telemetry data before, since adopting Cribl Stream we've gotten way better and faster at it."

"If a customer comes to us with a new log source they desperately need to onboard, we ingest it and build it so much faster than before. Onboarding new devices used to take weeks or months, now it takes just a few minutes."

In order to reliably identify IoCs, the team needs to be able to collect all relevant log files, events, and security alerts — this is one of the main reasons they purchased Cribl Stream.

> **"The nature of threat detection is finding the needle in a haystack — we want to make sure we dig through every haystack, so none of the needles get away. If one or two are missing, we might miss out on the final piece of evidence of an IoC that needs to be responded to."**
>
> —Member of Technical Staff CTO

Automatic Parsing of Log Files

For this MDR platform, customer data is collected in an Azure Blob instance that serves as a repository. Next, Cribl Stream identifies sourcetype and routes to the appropriate parser where Streaml normalizes the log to a proprietary common information model (CIM) format. Before Cribl, the team had a monolithic Java application that was home to all of their parsers. Creating a new one or modifying an existing one required Java developers to manually make the changes.

This process proved too labor-intensive and wasn't scalable — and other solutions, like Grok, ate up valuable compute resources and provided subpar results — so the team was thrilled to learn that Stream could solve the problem.

> **"There's no standard format for incoming logs — some may be in key-value pairs, others might be separated by delimiters — it's really all over the map. We use Cribl Stream to take those varied formats and convert them into a standardized one."**
>
> —Technical Lead, Office of the CTO

95% Reduction in Development Time for Custom Parsers

Without having to expend resources on manual updates, the detection and response team can provide more value to their customers by onboarding data sources, faster. The ease of creating custom pipelines in Cribl Stream has made the process of building and modifying parsers more efficient than they could have imagined.

> **"With Cribl Stream, we went from seven or eight weeks of calendar time to produce a parser down to just 15 minutes."**
>
> —Technical Lead, Office of the CTO

The output is a vendor agnostic format that can be ingested by a real-time correlation (RTC) engine. The RTC then correlates the clean data and uses a combination of AI, ML, and human validation to determine the risk level for each result.

"We no longer need to know where customer telemetry data is coming from ahead of time, because we just use Cribl Stream to ingest everything and determine the type of device."

"Our ability to produce and ingest a wider range of data in a shorter period of time allows us to provide a better shield for our customers against bad actors."

"The more we can leverage smarter mechanisms to do our parsing and standardization, the better off we'll be. The way we were doing it was laborious, and Cribl Stream turned out to be the perfect solution."

"In the old days, customers would have to reach out to a salesperson for a quote, then work with our operations team to configure and update each new device. Now that we have Cribl Stream, our customers can just fill out a form for new sources and have their data onboarded in 15 minutes."

—Technical Lead, Office of the CTO

Easy Identification of Unknown Log Sources

Using Cribl Stream to process incoming data has made it easier for this team to identify unknown log formats and sources.

"If we get any sources that we aren't able to identify, we run it through Cribl Stream and have it routed to a bucket for unknown data. Then our team can go in and create new parsers for any previously unidentified sources."

—Technical Lead, Office of the CTO

That previously unidentified data can then be rerouted back through Cribl Stream and sent to the new parser. Data formats that weren't immediately ingestible the first time around will be digested right away in the future. This new process eliminates data loss due to parsing problems, and facilitates a new self-service model.

Cleaner Data = Improved Threat Detection

Since they no longer have to worry about dropped events, and they can identify and parse every data type, the detection and response team can meet their goal of collecting all of their customer's telemetry. There are more haystacks for them to find relevant needles and threat detection is much improved.

"If you were to compare our threat detection capabilities to another company with the exact same algorithm, we would produce superior results — simply because Cribl Stream helps us make the data feeding those algorithms superior."

—Technical Lead, Office of the CTO

TL;DR

- Redirected developer resources away from ingestion and parsing to threat detection, accelerating MTTD and MTTR
- Reduced dropped logs and events to zero
- Developed an automated system for parsing data
- Reduced development time for custom parsers from 7-8 weeks to 2-3 days
- Shifted to a self-service model for customers to onboard their own data
- Created a process to identify and parse unknown logs
- Improved threat detection with an increased quantity of high-quality data