CRIBLCON 24

POWERED BY Cribl

Reduce Risk with Cribl and Choose the right SIEM(s)

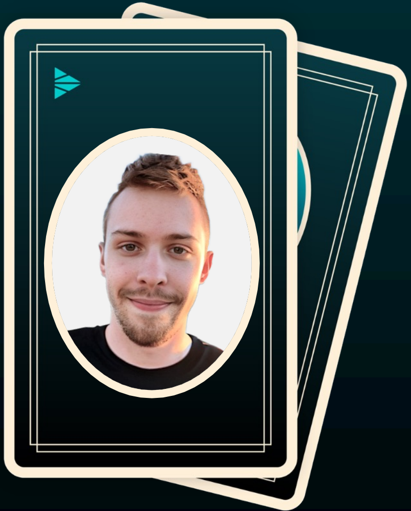
Chris Talbott & Adam McLaughlin
Cyber Security Manager & Cyber Security Engineer, Amex GBT

Chris Talbott

Cyber Security Manager
Amex GBT

Adam McLaughlin

Cyber Security Engineer,
Amex GBT



Parallel SIEM Testing / POC

Cribl Stream played a pivotal role in achieving these goals:

1

Parallel SIEM Testing

- We seamlessly tested multiple SIEMs concurrently, thanks to Cribl Stream's flexible data pipeline.
- This expedited the selection process without impacting our existing SIEM.

Cribl Stream played a pivotal role in achieving these goals:

2

Data Reduction and Increased Visibility

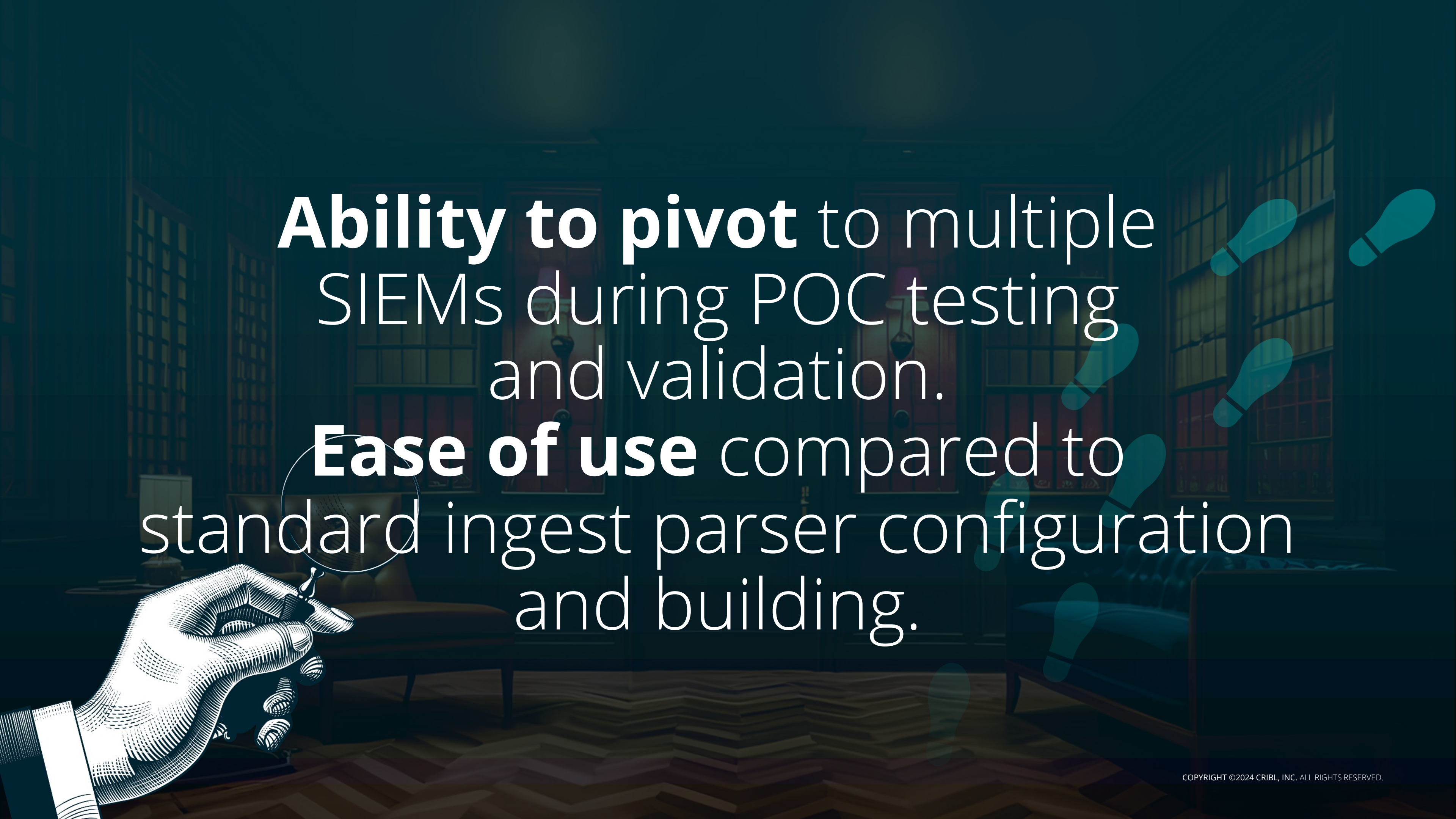
- Cribl Stream efficiently processed and reduced log volume, freeing up valuable resources in our current SIEM.
- This newfound capacity allowed us to integrate additional data sources, enhancing overall security visibility.

Cribl Stream played a pivotal role in achieving these goals:

3

Smooth SIEM Migration

- Once the new SIEM was chosen, Cribl Stream facilitated a seamless migration by ensuring uninterrupted data flow during the transition.

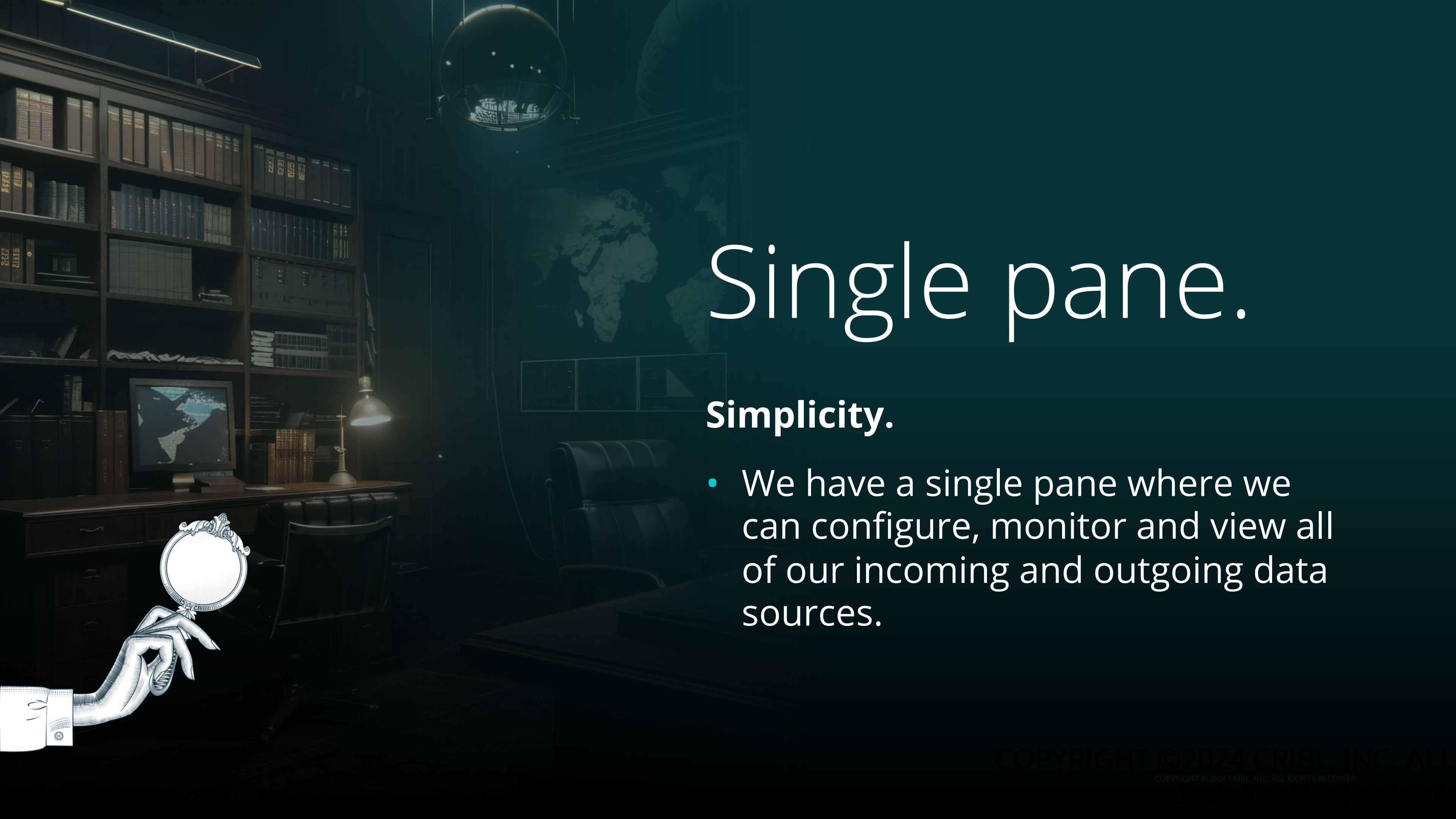


Ability to pivot to multiple SIEMs during POC testing and validation.

Ease of use compared to standard ingest parser configuration and building.

Agenda

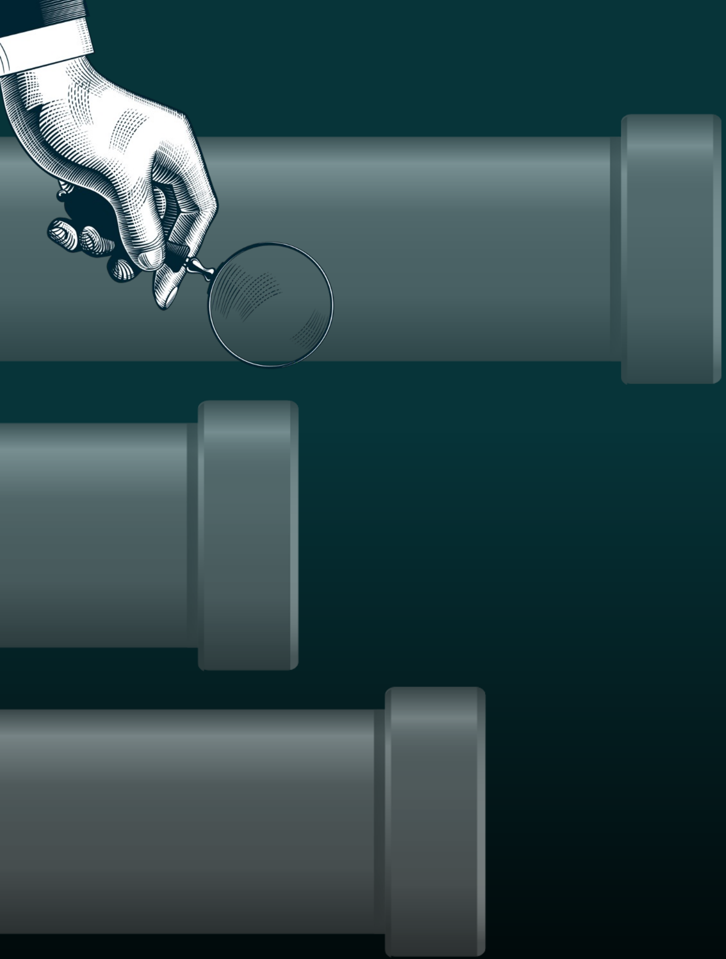
1. SINGLE PANE
2. PIPELINES
3. INTEGRATIONS
4. TAGGING
5. REPLAY
6. REDUCTIONS



Single pane.

Simplicity.

- We have a single pane where we can configure, monitor and view all of our incoming and outgoing data sources.



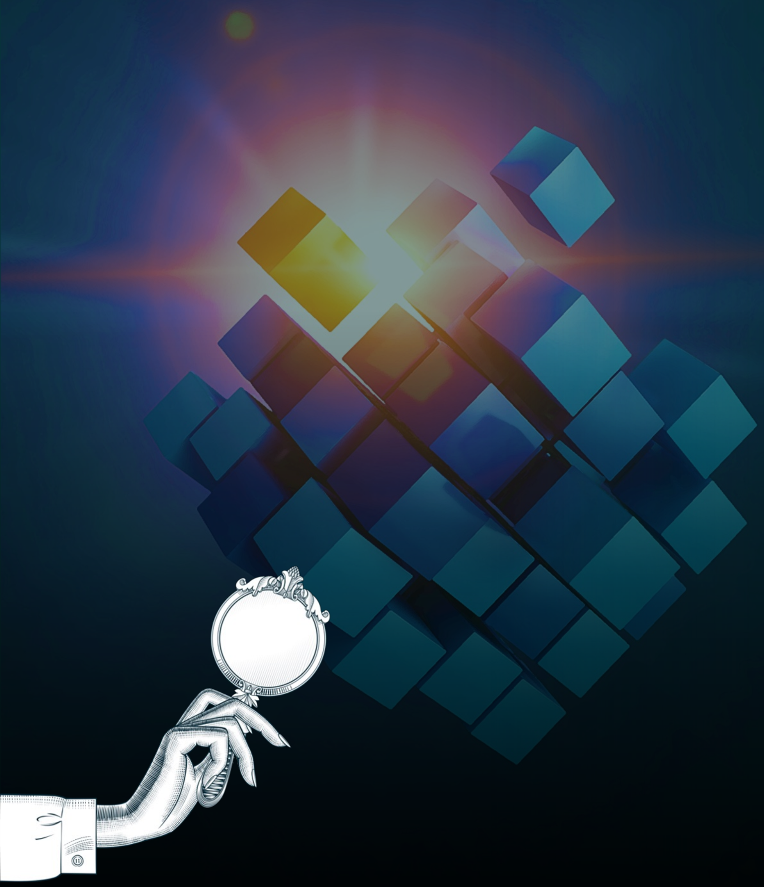
Pipelines.

Mario, “Wahoo!”

Streamlining.

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

COPYRIGHT ©2024 CRIBL, INC. ALL RIGHTS RESERVED.

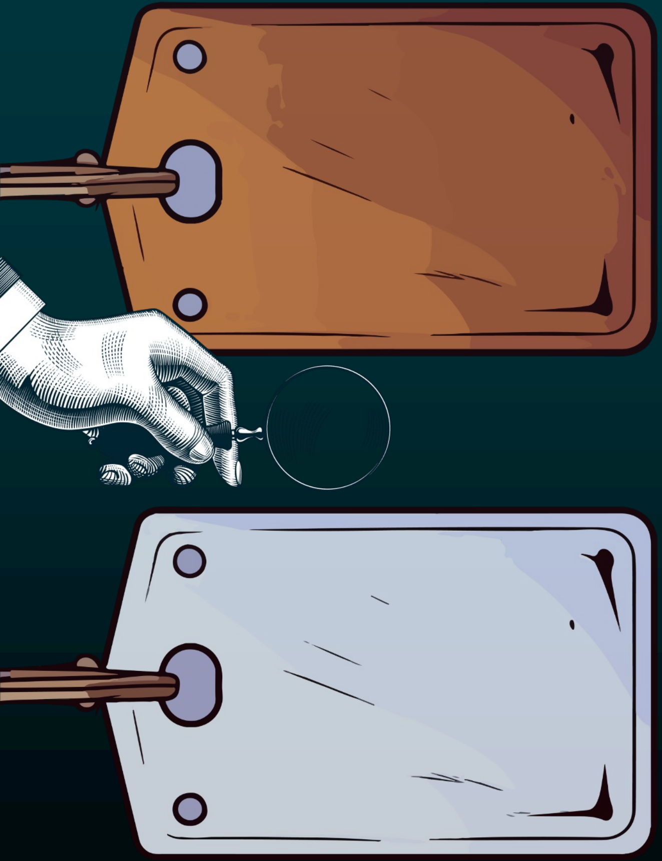


Integrations.

Some many applications…

One tool to *ingest them all*.

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

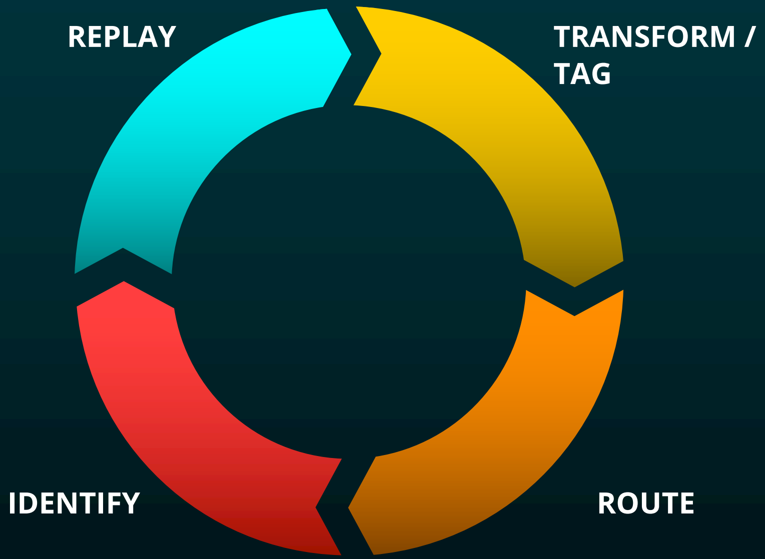


Tagging.

Who am I?

Identify logs with ease.

- Tagging log sources not only helps us stay organized with routing but also aids in quickly finding specific logs at the destination.

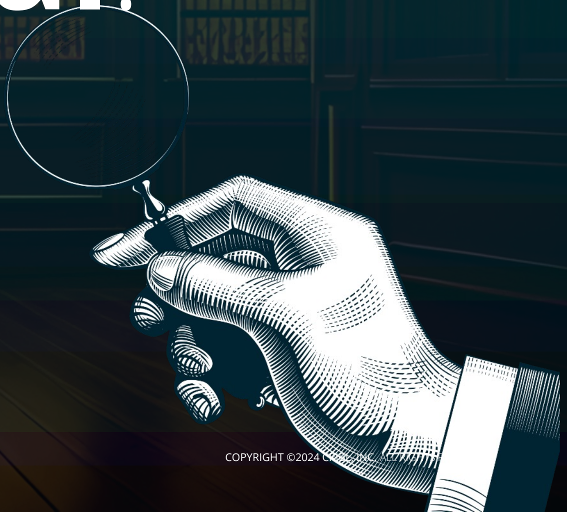


Replay.

Go forth with confidence

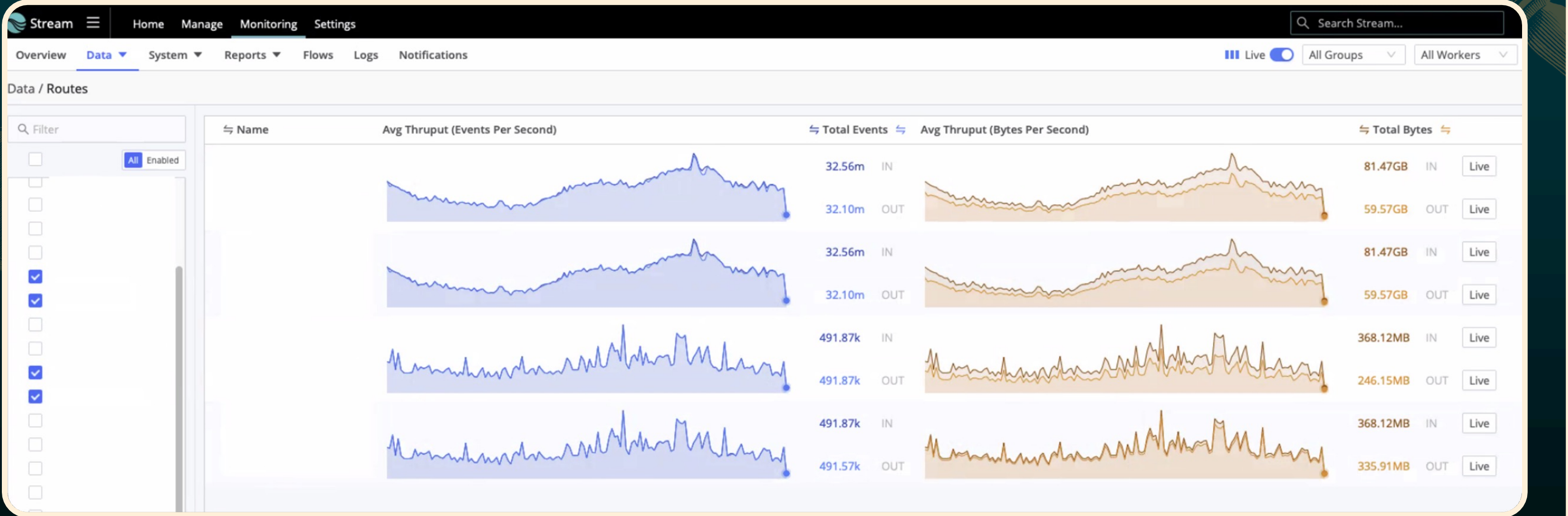
- Full fidelity log data that Cribl kindly sends to S3 can be REPLAYED! if our logs age out of retention in SIEM we can pull them back in and for those oops moments when we removed a very important field. Let's just play it back in.

Now…the **reveal**.



Reductions.

Up to 33% for WAF.

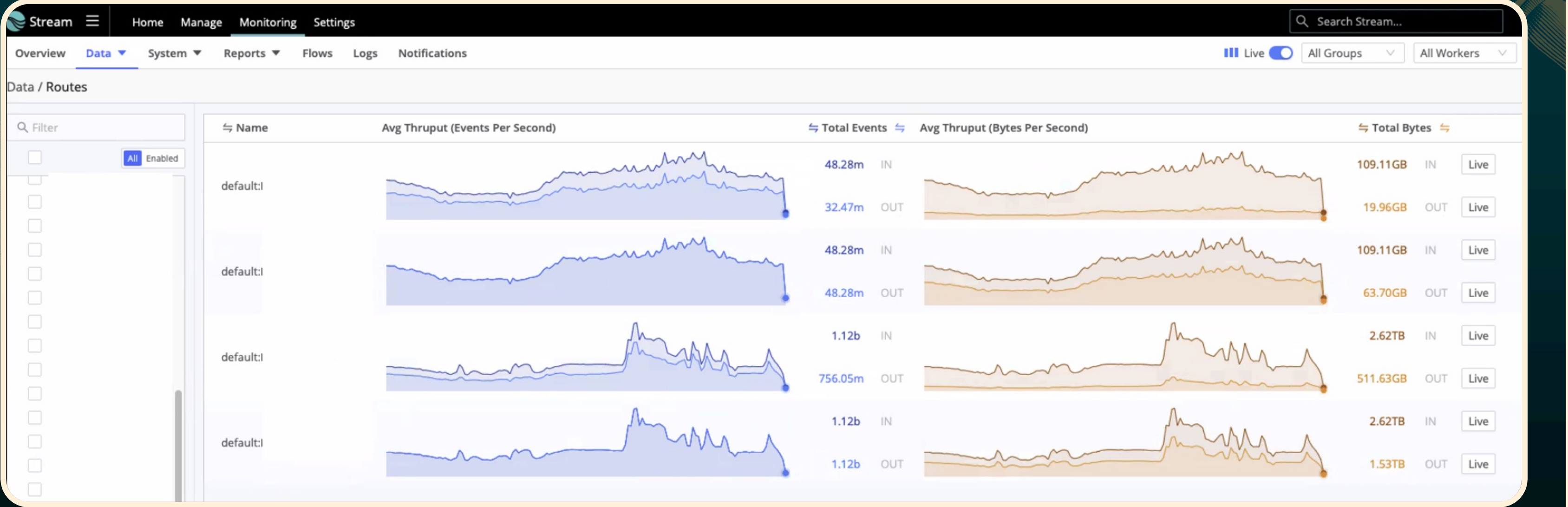


Name	Avg Thruput (Events Per Second)	Total Events		Avg Thruput (Bytes Per Second)	Total Bytes		
		32.56m	IN		81.47GB	IN	Live
		32.10m	OUT		59.57GB	OUT	Live
		32.56m	IN		81.47GB	IN	Live
		32.10m	OUT		59.57GB	OUT	Live
		491.87k	IN		368.12MB	IN	Live
		491.87k	OUT		246.15MB	OUT	Live
		491.87k	IN		368.12MB	IN	Live
		491.57k	OUT		335.91MB	OUT	Live

33% reduction to SIEM 1 and **27% reduction** to SIEM 2 (CrowdStrike).

Reductions.

Up to 82% for Firewalls.



Data / Routes

Name	Avg Thruput (Events Per Second)	Total Events		Avg Thruput (Bytes Per Second)	Total Bytes		
default:l		48.28m	IN		109.11GB	IN	Live
		32.47m	OUT		19.96GB	OUT	Live
default:l		48.28m	IN		109.11GB	IN	Live
		48.28m	OUT		63.70GB	OUT	Live
default:l		1.12b	IN		2.62TB	IN	Live
		756.05m	OUT		511.63GB	OUT	Live
default:l		1.12b	IN		2.62TB	IN	Live
		1.12b	OUT		1.53TB	OUT	Live

82% reduction to SIEM 1 and **42% reduction** to SIEM 2 (CrowdStrike).

~82%

REDUCTION

Across 2 sources and 2 SIEMs

Onboard and Troubleshoot Minutes

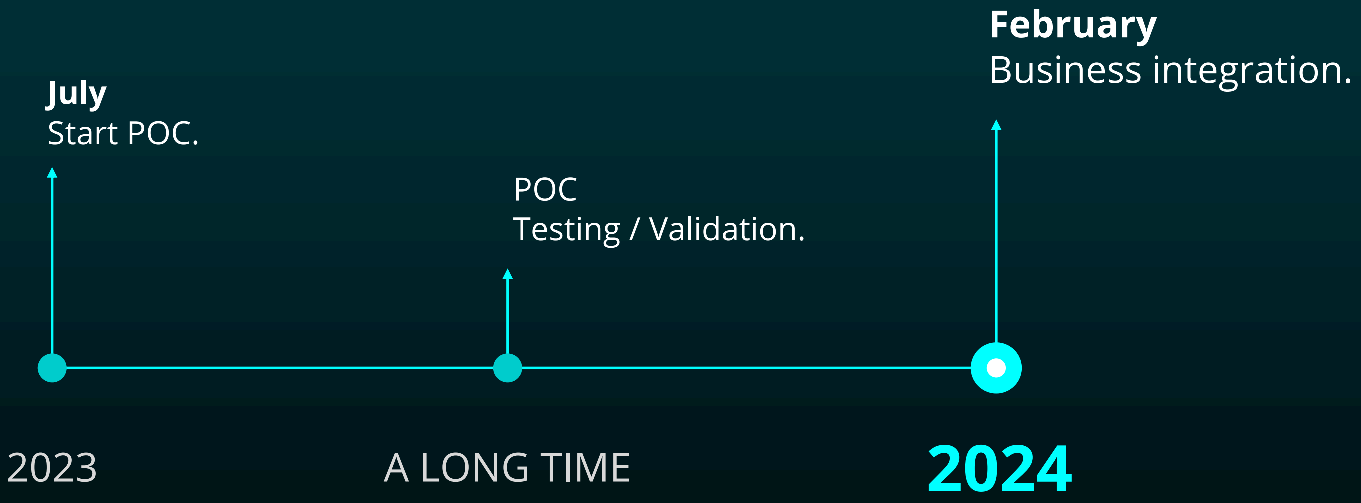
REDUCTION IN EFFORT

Cribl makes troubleshooting SIEM parsers easy and quick. Minutes to add new route and test in new destination.

Improve Security Posture

Added multiple new sources that did not have visibility into before.

How we got here.



July
Start POC.

POC
Testing / Validation.

February
Business integration.

2023

A LONG TIME

2024

Thank you!