CRIBLCON 24

POWERED BY Cribl

How Cribl saves us 400K a year

Chris Affleck, CISSP
Senior Cyber Security Engineer, Epiq Global

Daniel Wilson, CISSP
Cyber Security Engineer, Epiq Global

Sidd Shah
Staff Solutions Engineer, Cribl

CHRIS AFFLECK, CISSP

Senior Cyber Security Engineer,
Epiq Global

DAN WILSON, CISSP

Senior Cyber Security Engineer,
Epiq Global

SIDD SHAH

Staff Solutions Engineer,
Cribl

CRIBLCON 24

POWERED BY Cribl

How Cribl saves us 400K a year

Chris Affleck, CISSP
Senior Cyber Security Engineer, Epiq Global

Daniel Wilson, CISSP
Cyber Security Engineer, Epiq Global

Sidd Shah
Staff Solutions Engineer, Cribl

The Challenge

Why Digital Transformation?

Leading the way to the Cloud

Regular product evaluations

Ensure optimal client support with the latest technology

Eliminate shelfware waste

Reduce tooling redundancies by streamlining tech stack

Cost analysis

Unlimited ingest w/on-prem hardware vs. ingest cost w/unlimited cloud storage

Why Cribl?

The ideal tool for digital transformation

Essential For Digital Transformation

- Provided the necessary tooling assistance

Supports Maturing Data Strategy

- Ensures compliance requirements are met
- Maintaining full fidelity copies of data

Key Functions:

- Unified pipeline for onboarding logs
- Transforming log formats to destinations proprietary format
- Optimizing logs to enhance fidelity and manage costs
- Running Legacy and new system concurrently

The Data Transformation Journey

Effectively Moving On-Prem Data to the Cloud

Data Integration Needs:

Temporary Solutions

- REST API Collector
- S3 Bucket Pulls
- Azure Blob
- Raw HTTP

On-prem

- Database

Syslog....so, so many Syslog

- Architecture optimization

Data interoperability solutions

- Flexible to any source / destination

The Outcome and How

Starting Strong

Navigating Source / Destination Challenges

No destination? *No problem.*

Cloud SAAS Sources

- Azure Log Collectors
- Microsoft OMS agent

Syslog….so, so many Syslog

- Architecture optimization

Data interoperability solutions

- Flexible to any source/destination

Final Form

Finding a Solution, ***together***.

Executing the strategy

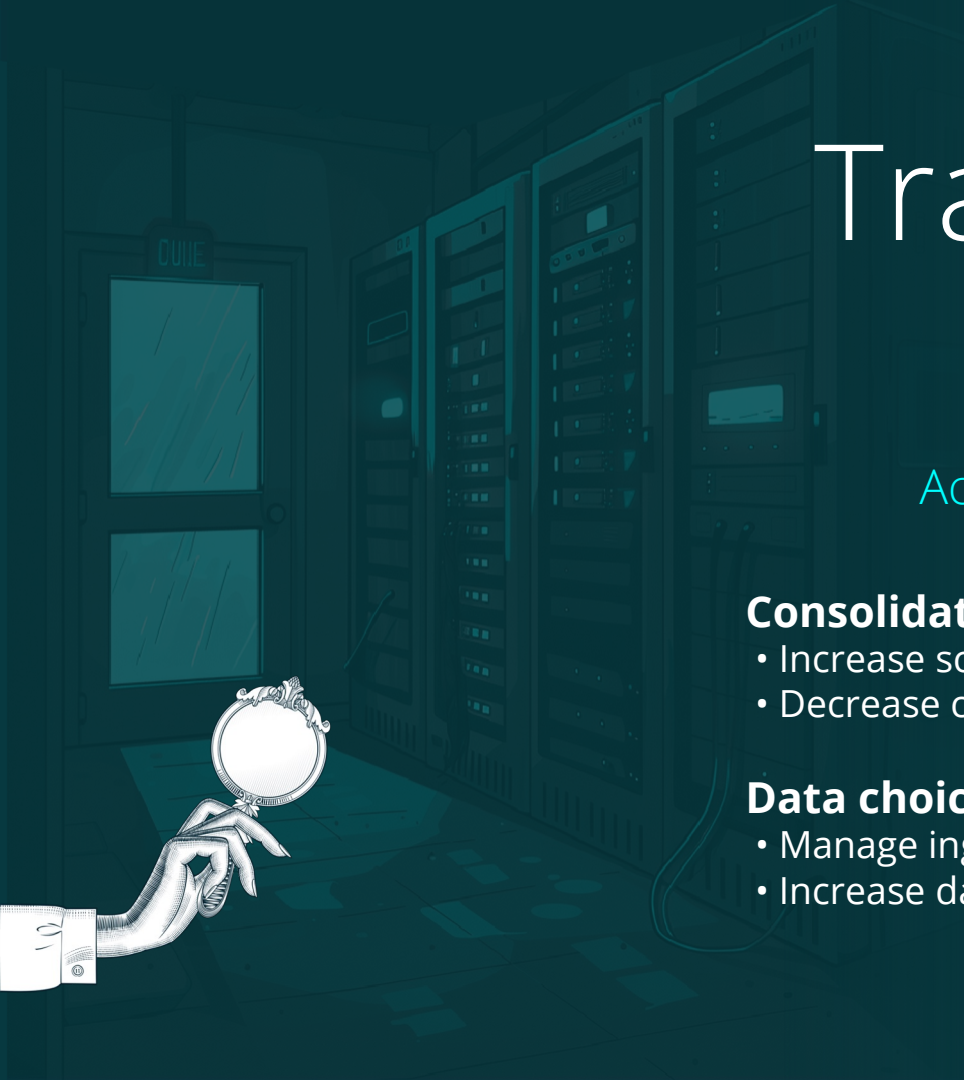
- Customer feedback-driven.
- Goats, helpful and collaborative.

Collaborate with Cribl to enhance product:

- Sentinel destination.
- Sentinel packs.

Addition of Cribl Metrics.

- Quantify savings.



Transformation success

Achieving better results, together

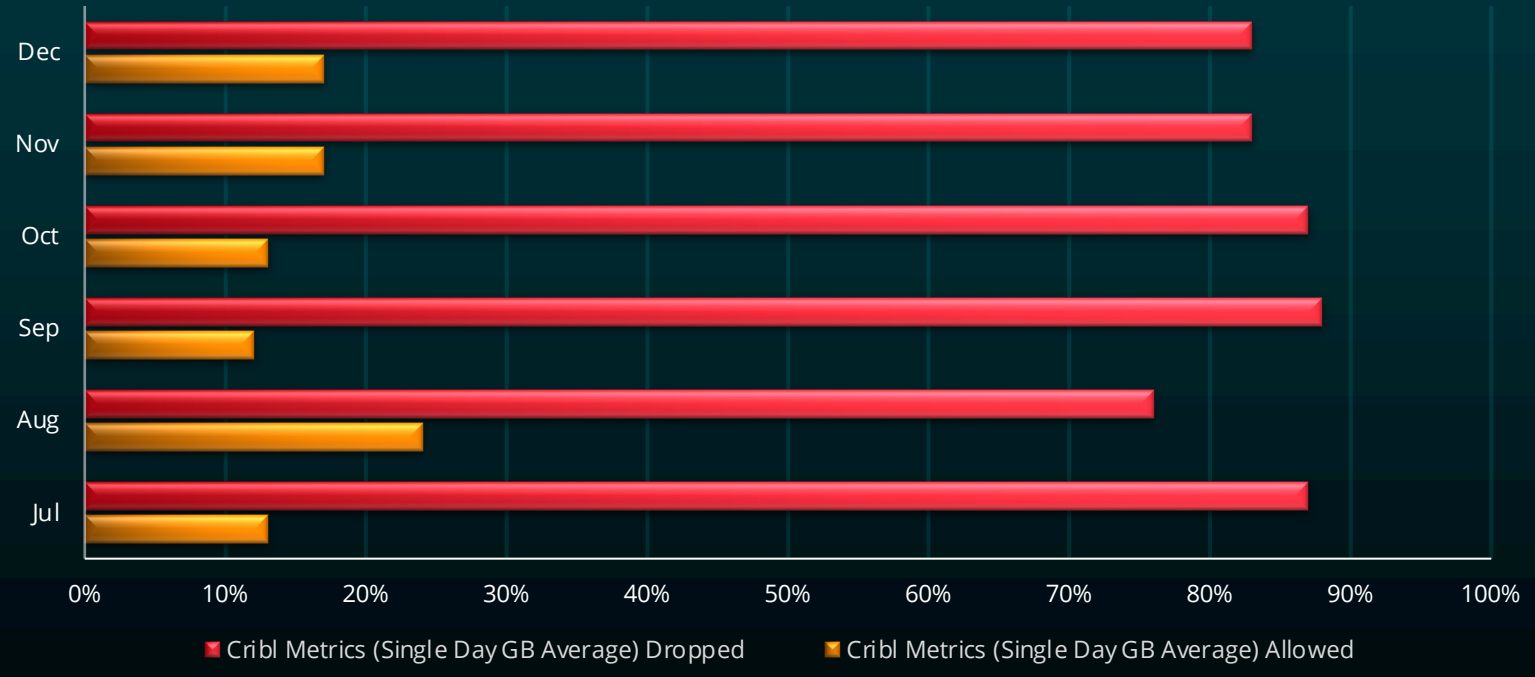
Consolidated tech stack
- Increase scalability.
- Decrease complexity.

Data choice and control
- Manage ingestions costs.
- Increase data fidelity.

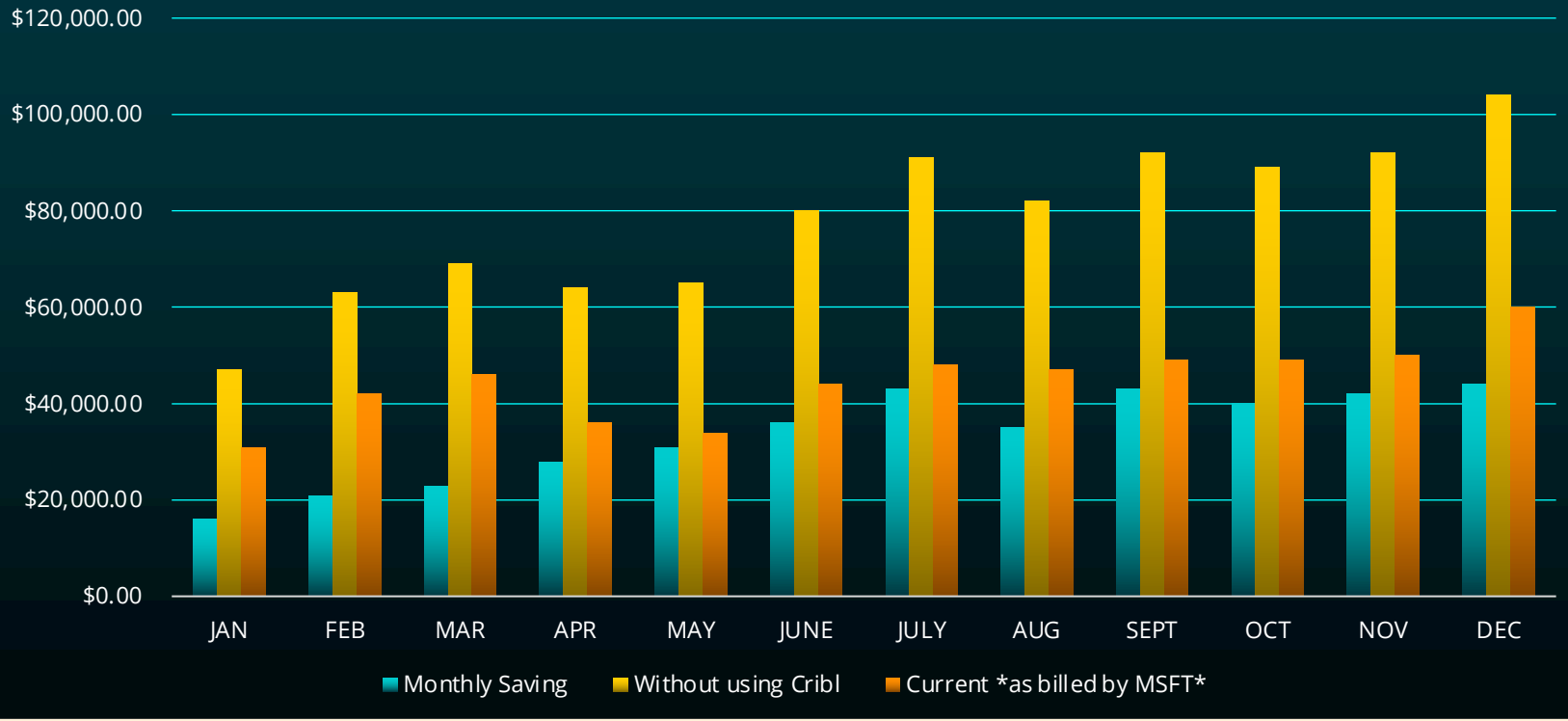
Data segmentation
- High volume, high value.

Compliance, retention
- Product upgrades.
- Sentinel destination.
- Sentinel pack.

Show Me the Savings!

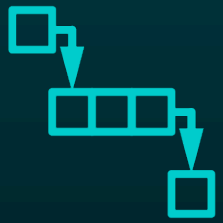


Show Me the Savings!



Lessons Learned / Best Practices

Lessons Learned / Best Practices



Reduce impediments to adoption

- Customer feedback-driven
- Goats, helpful and collaborative

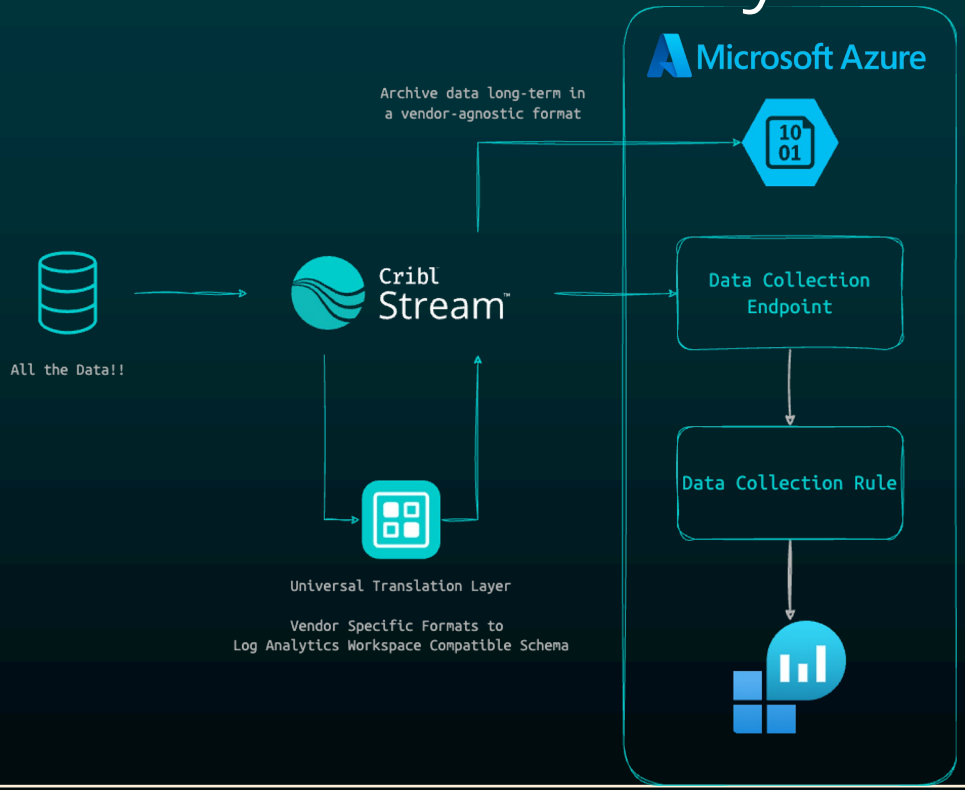
Syslog best practices
Docs

- Separate source devices by port.
- Device class

Use your resources

- **Packs** are where it's at
- Join your local Cribl User Group, **Cribl Community**

The Bits and Bytes



Resources Used

- Packs Dispensary
- Preparing the Azure Workspace | Cribl Docs
- Azure Sentinel SIEM Integration | Cribl Docs
- Cribl Sandbox
- Data collection rules in Azure Monitor - Azure Monitor | Microsoft Learn
- regex101: build, test, and debug regex


Thank you!

Audience Q&A