CRIBLCON 24

POWERED BY Cribl

Next-Gen Logging: Deep Dive with a Large Financial Institution

Raanan Dagan, Principal Solutions Engineer, Cribl
Andrew Duca, Director of Services, Cribl

RAANAN DAGAN

Principal Solutions Engineer, Cribl

DUCA

Director of Services, Cribl

Agenda

1. **Introduction**
2. **Challenge**
3. **Solution**
4. **What’s Next**
5. **Q&A**

Challenge

Financial Institution by the Numbers

Scope and Size

Heritage platform supports Logs and Security

- >25,000 Dashboards
- >15,000 Alerts
- >25,000 Saved Searches
- >15,000 Active Users
- >250 terabytes Daily Ingest
- >60 petabytes Managed Data
- >8,000 log formats

Financial Institution by the Numbers

Design for Growth

Designed to support 2-3X current volumes technically and operationally. Testing multiples beyond targets to understand design limits.

- **Ingest** - Tested to 500 terabytes/day
- **Managed Data** - >100 petabytes
- **Objects** (i.e. dashboards) - >100k

Financial Institution by the Numbers

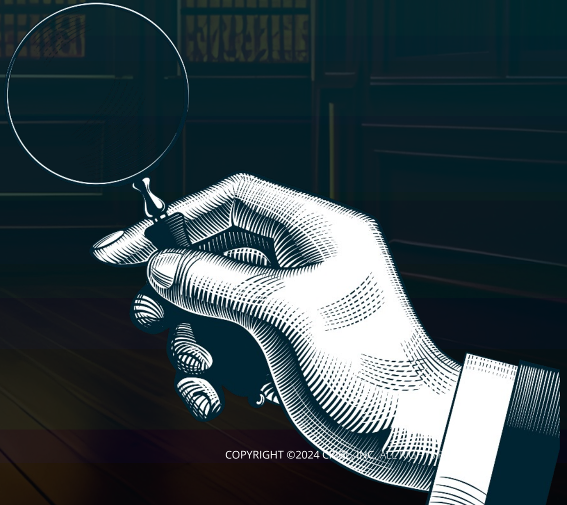
Cribl Partnership Results:

- Ingest Rate increased over 50x in hours
- >30 Cribl enhancements in 36 months
- >~10X increase of data volume
- Forecasting substantial lowering of operating costs over 3 years
- Created an Abstraction Layer that aggregates all traffic regardless or scale or destinations

Why Change

Before Cribl	**After Cribl**
▪ Hard to meet requirements in a timely manner ▪ Access control limitations ▪ Vendor specific knowledge required ▪ Detection accuracy ▪ Built with security as an add-on ▪ Scalability challenges ▪ Expensive to expand ▪ Outdated design ▪ Centralized management	▪ Faster time to market ▪ Fine grain - workload & data isolation ▪ Industry standards ▪ Greater actionability ▪ Independent security platform ▪ Cloud Native at Internet scale ▪ Cost effective dynamic growth ▪ Multi-tier Federated Operating model

Solution



Cribl Architecture Buildout

Planning for Long Term Success

Routing

- Multiple destinations
- Multiple formats
- Enabler for migration (feed old and new)

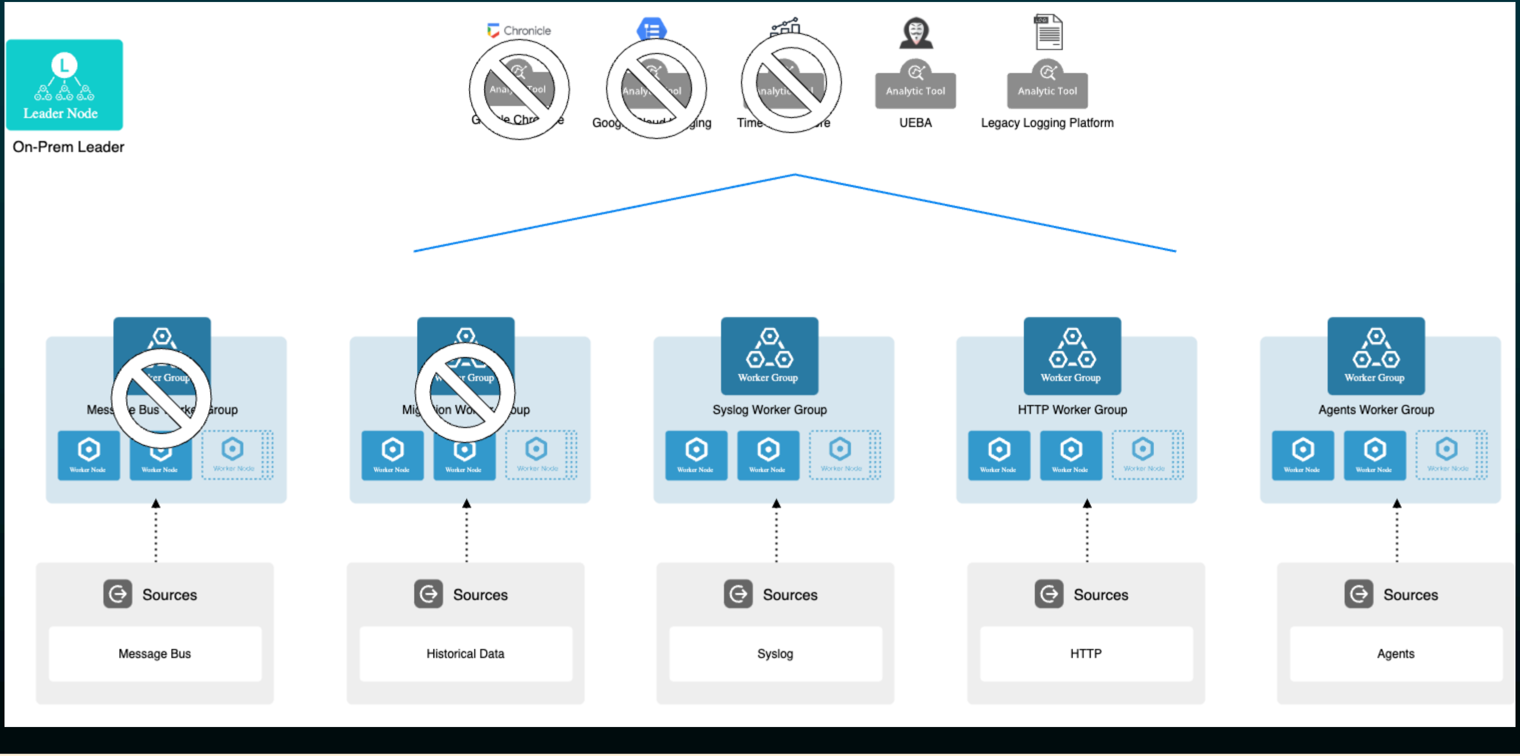
Shaping

- Format conversion
- Event breaking
- TZ improvements

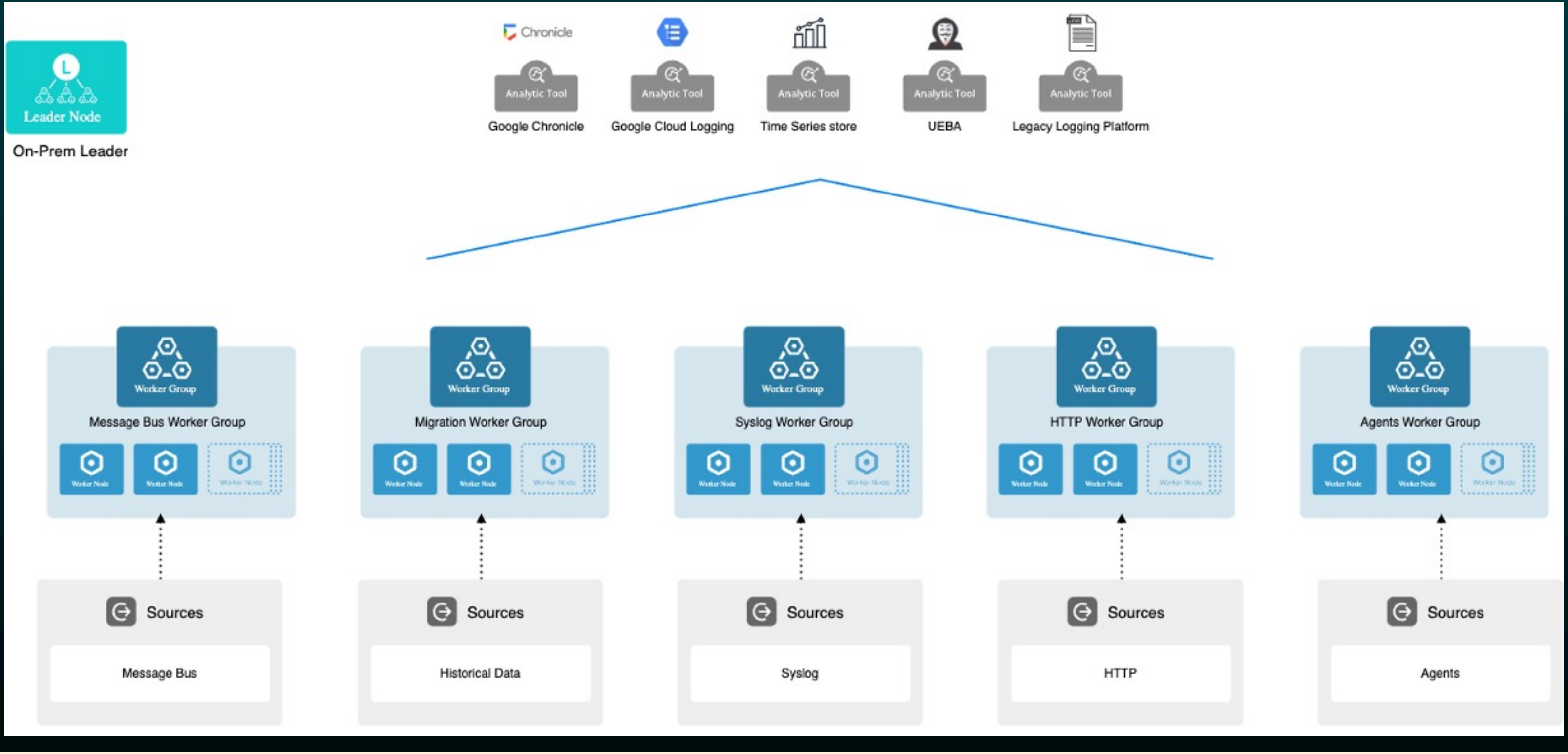
Enrichment

- Normalization of mandatory fields (App id & Env)
- Usage of dynamic lookups
- Metadata for seamless onboarding

Cribl Architecture - Before Migration



Cribl Architecture - During Migration



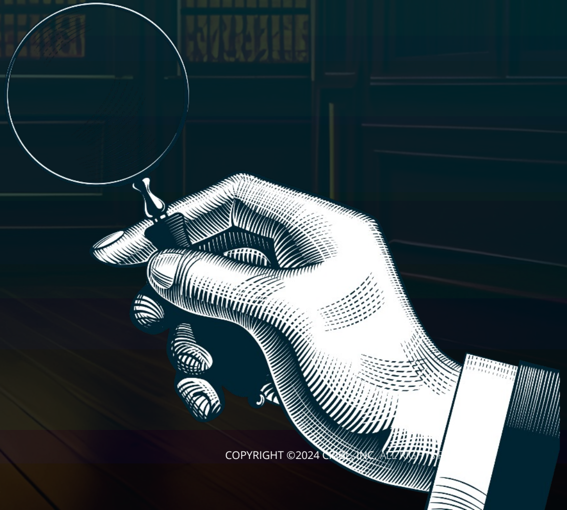
Results for Phase One

Migration Wins and Warnings

- Parity with existing SIEM came quickly
- No interruption of service
- 3 months for first 50% and then 6 months for go live
- Live with Dashboards, Alerts, and Detection on the new SIEM

- Converting detection content is time consuming–not 1:1
- Thousands of configuration files to sift through

What’s Next



What’s Next

Security

- Sensitive data support
- Scan and mask
- Shift logic to the edge

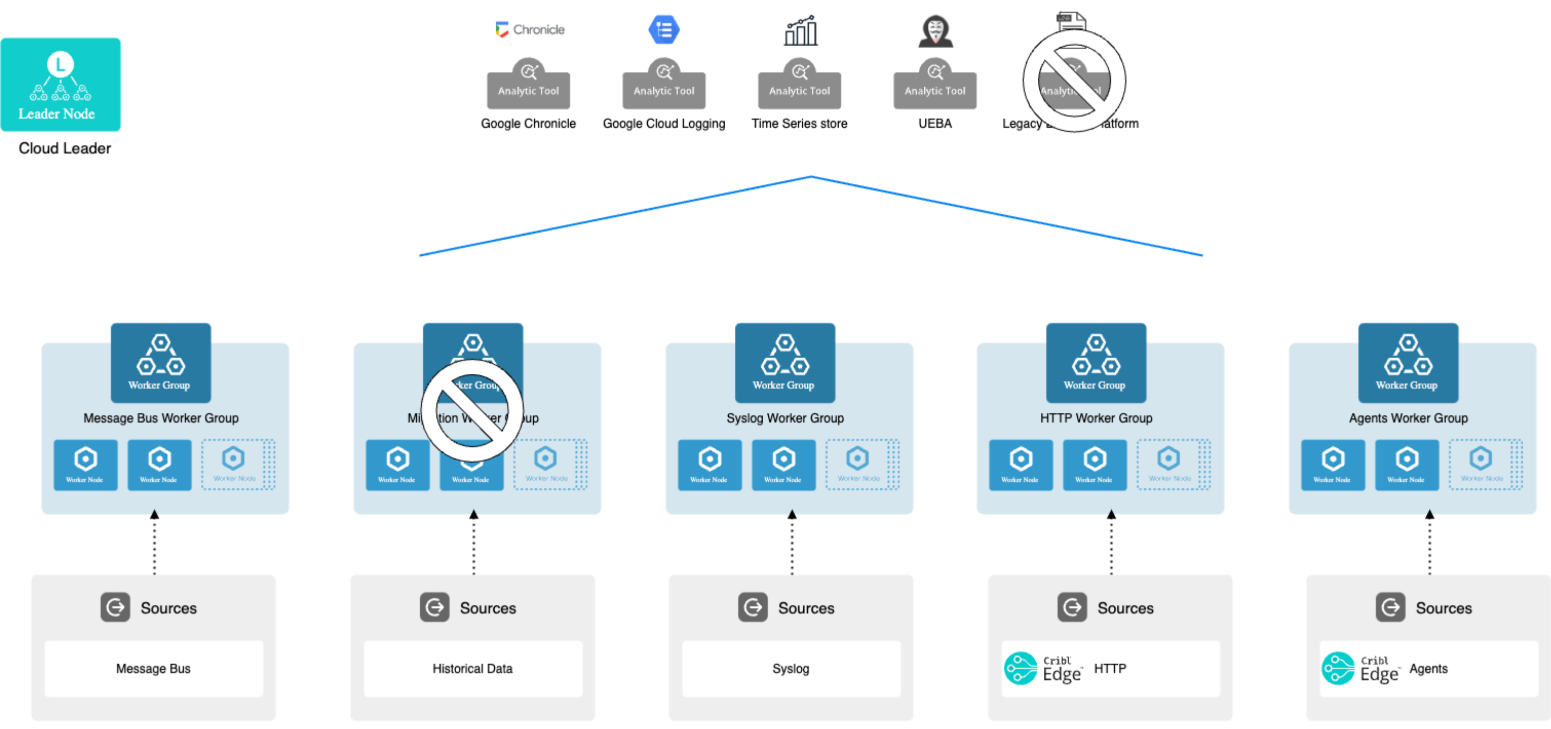
Automation

- Remote GitHub
- Worker group templates

Self Service

- Shift ownership to data owners
- Granular access model

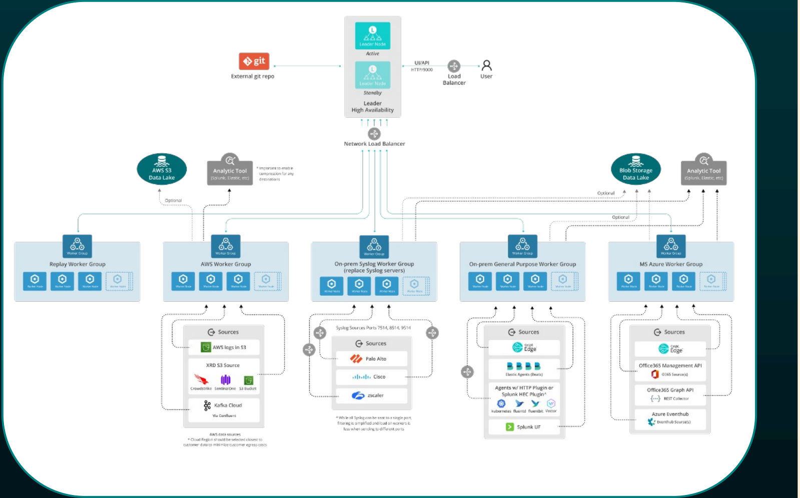
Cribl Architecture - Future State



RESOURCES

Reference Architectures

- Reference Architecture Overview: https://docs.cribl.io/stream/deploy-reference-comprehensive/
- Architecture Considerations: https://docs.cribl.io/stream/deploy-architecture/
- Reference Architecture blog + podcast: https://cribl.io/blog/cribl-stream-reference-architecture/



Thank you!