RE-THINKING YOUR SECURITY DATA ARCHITECTURE

Jim Butterworth
Executive Director of Cyber Security—Architecture & Engineering,
The Venetian® Resort Las Vegas

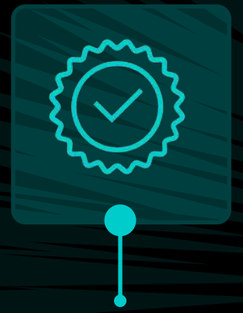
CRIBLERS ASSEMBLE!

CRIBLCON! 2023

WHO IS THE VENETIAN LAS VEGAS?

The Venetian is a marquee property on the Las Vegas strip, featuring three luxury hotel towers that include more than 7,000 all-suite rooms, 225,000 square feet of gaming space, and 2.3 million square feet of meeting space.

WHAT WAS YOUR PRIMARY CHALLENGE?



Build a Fully Operational SOC

- Migrate to Exabeam
- Onboard new Managed Security Services Provider

Improve SIEM Performance

- Improve security tool performance
- Manage risk in heavily regulated environment

Cost Avoidance

- Focus on important data
- Deliver under budget and within 60 days

WHAT'S BEEN THE IMPACT?

Faster Data Onboarding

Fully operational SOC in 60 Days

More Performant Architecture

Enhanced Routing and Filtering

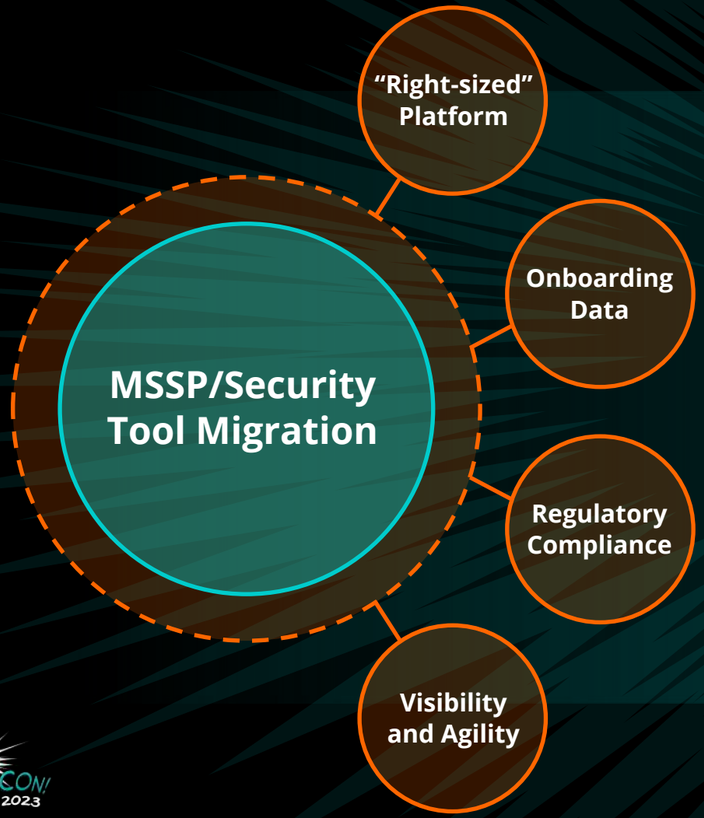
Prioritized data needed to drive detection: Reduced 1.2TB to 450GB without increasing risk

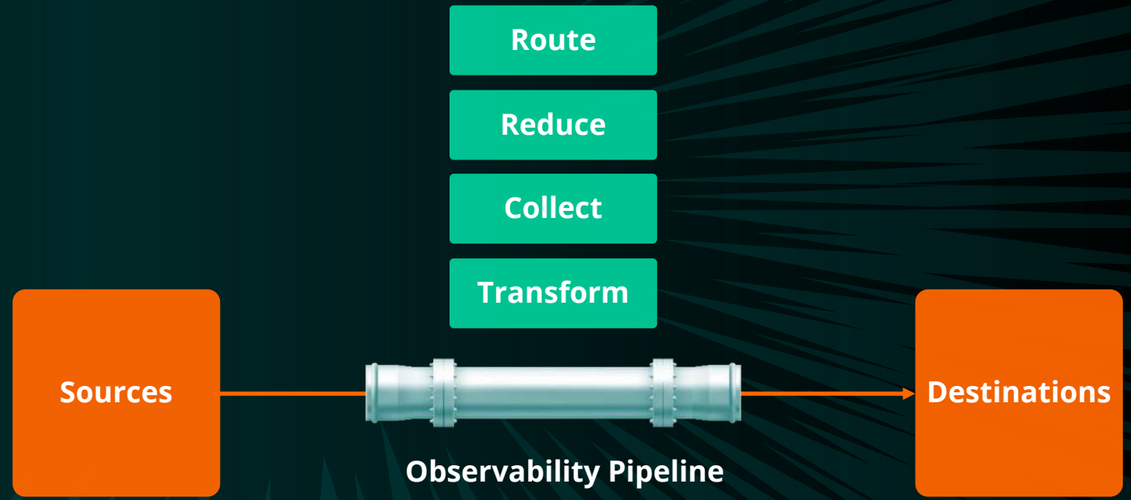
Cost Optimization

Prepared for Growth

Makes it easy to manage Sources and Destinations

WHAT PROBLEMS DID YOU WANT TO SOLVE WITH CRIBL?

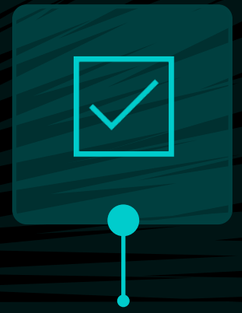




HOW DO YOU DESCRIBE CRIBL?

Enables control of our own data

Allows for better use of other investments and tools

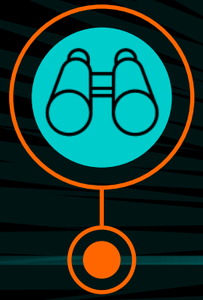


Saved $500k

“Cribl is one of the most important tools in the cyber tool chest”

DO YOU HAVE ANY ROI OR KPIS YOU CAN SHARE?

Accelerated Migration



Better visibility

More data sources, reduced cost, better security posture

Time Savings

3 months to move security tooling

Business Impact

Allowed The Venetian to maintain cyber security maturity due the diversity of the cyber security tools

RECOMMENDATIONS

- 1 Wk of learning from PS
- 1 Wk of Output Customization and Tuning
- Few Days to Dial it in

- Know XML, JSON
- Javascript
- Regex
- Know Your Data

2 dozen data feeds, 100 hours of Engineering and it's been smooth sailing ever since

SUMMARY

- Reduced 1.2 TB of data to 450GB in less than 6 months.
- Due to the nature of the casino business and the stringent regulatory requirements, The Venetian was able to run simultaneous SOCs without interruptions.
- Saved $500K per year and delivered the same risk mitigation they had from a 365/7/24 SOC with 6 FTEs and a re-investment in the tech stack.
- Maintained cyber security maturity due to the diversity of the cyber security tools.

“Cribl allows me to control my own data and make better use of my other investments and tools.”


CRIBLCON!
2023