Siri Varma Vegiraju

# Building Network Telemetry Platform to minimize Security Threats

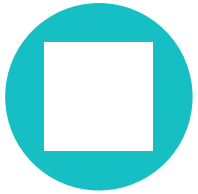
# Agenda

Why Network Telemetry and its need for a platform

Fundamental pieces in Network Telemetry.

Architecture of a Network Telemetry Platform

Improving Network Security



Extensions to the Platform

Conclusion

# Why Network Telemetry ?

Threat detection

Compliance

Anomaly detection

# Need for a Platform

A PLATFORM ISN'T JUST A SOLUTION; IT'S AN ENABLER FOR ENDLESS SOLUTIONS

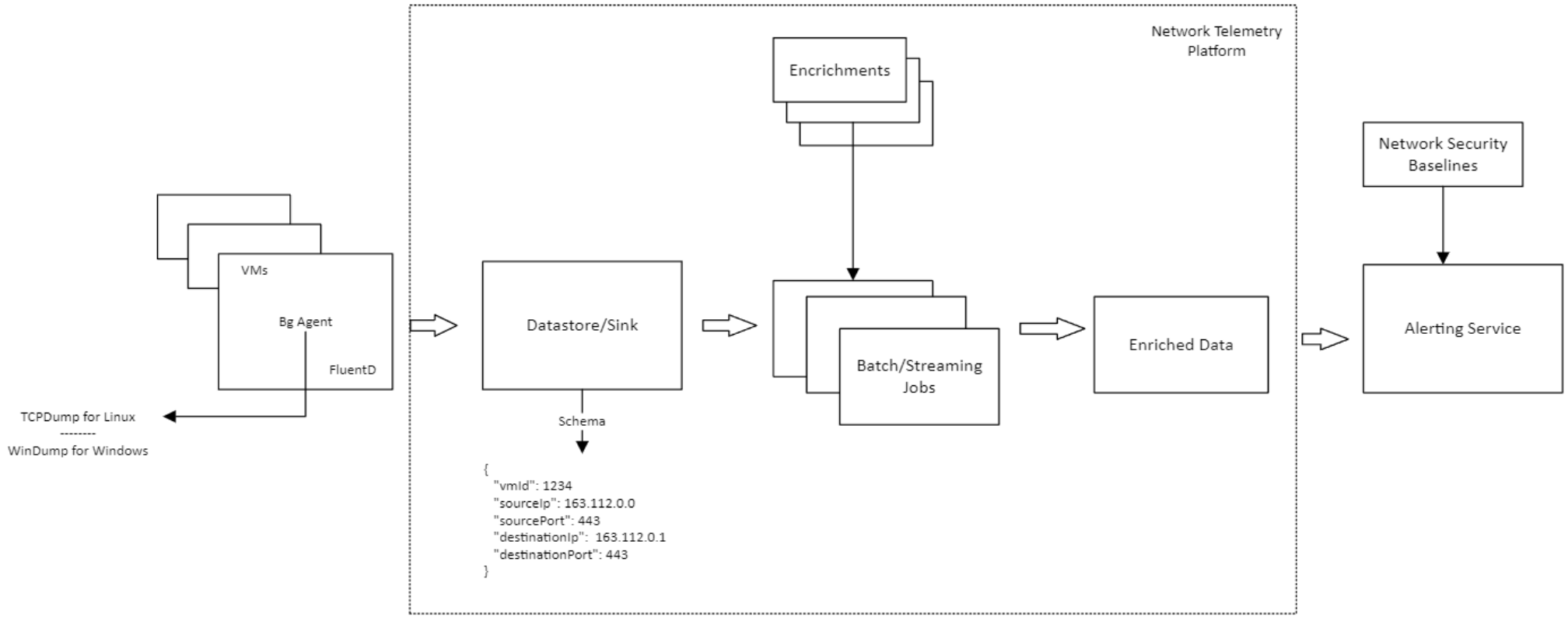
COST SAVINGS

CONSISTENCY AND STANDARDIZATION

# Components in a Network Telemetry Platform

- Collecting data
  - Agents running on VMs
  - TCPDUMP, WINDUMP
- Enrichment
  - Metadata
- Standardization
  - Schemas
  - Versioning

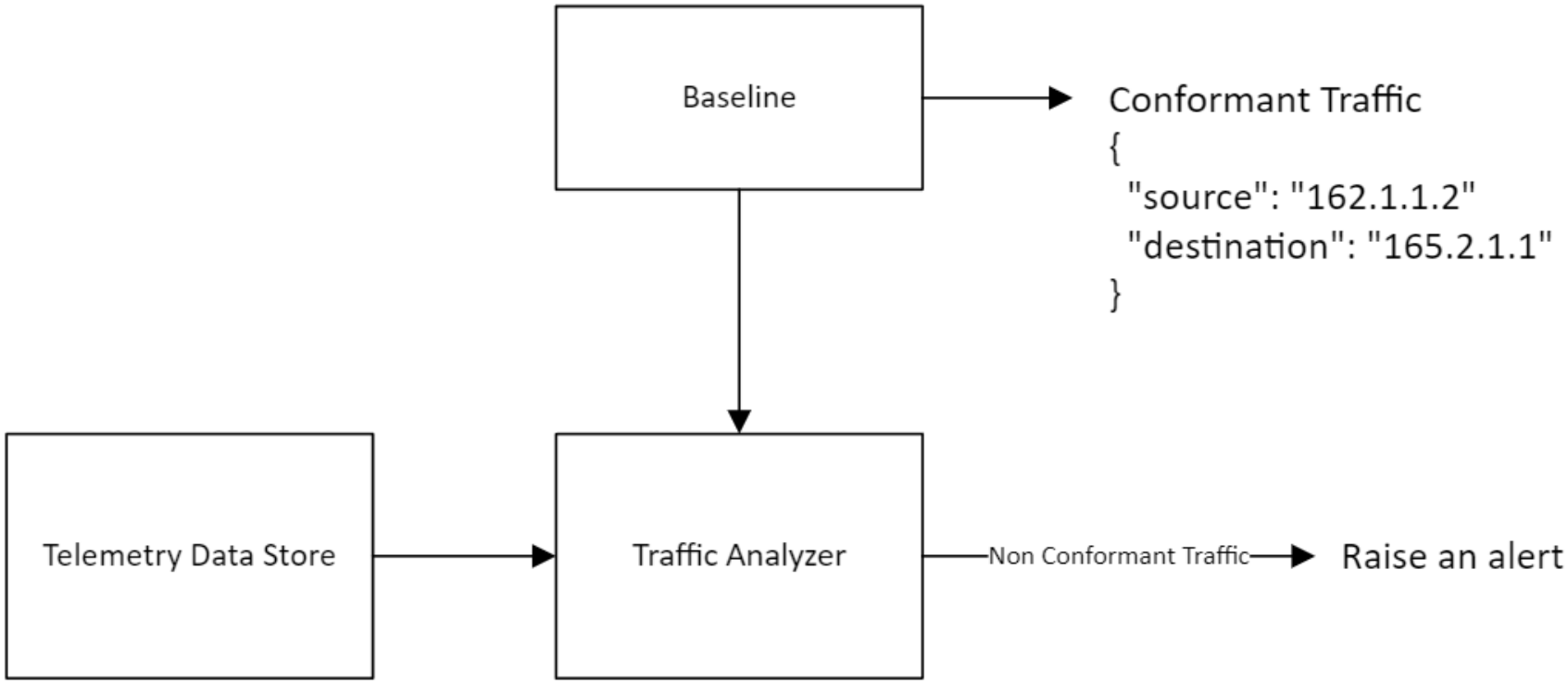
# Telemetry Platform Architecture



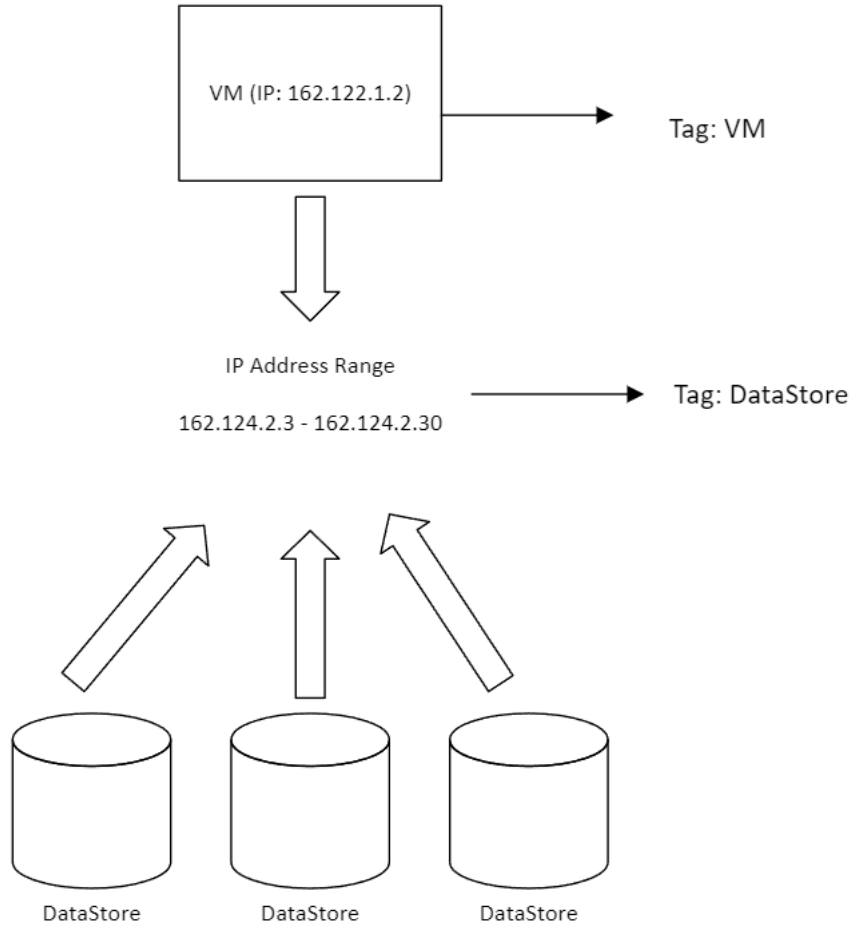
# Improving Network Security

- Implement Baselines.
- Example of a baseline:
  - Database must be accessed using Organization Ips only.
  - Communication to VMs must happen on specific ports.
  - High risk ports like 22 where SSH Brute force attack can happen are blocked.

# Improving Network Security



# Using Tags for Efficiency



# Extensions to the Platform

- Security Recommendations
- Trends in Network Patterns

# Conclusion

# Siri Varma Vegiraju


Software Engineer

Freelance Contributor

Book Reviewer

LinkedIn: /sirivarma

Email: siri.varma@outlook.com

Twitter: @siri_

Thank you