Modern
Network Monitoring for the Rest of Us

AusNOG 2017
Tim Raphael

Intro

- Why?

- The current state, emerging trends and technologies

- Barriers for smaller ISPs and enterprises

- An effective monitoring strategy

- How?

Why?

- React to failure situations

- Capacity and service utilisation analysis

- Discover new and emerging trends

- Drive continual improvement

AusNOG 2017

Current State

- Off-the-shelf software and its limitations

- Larger and more innovative organisations tending to build their own due to scale and complexity

- Differences between Silicon Valley-like organisations and "the rest of us"

Technologies

- Push vs Pull

- Time-Series Data

- Event Stream Processing

Push vs Pull

Request (50ms)

Collector → Device

Response (50ms)

Pushed (50ms)

Collector ← Device

Time Series

7

Event Stream Processing

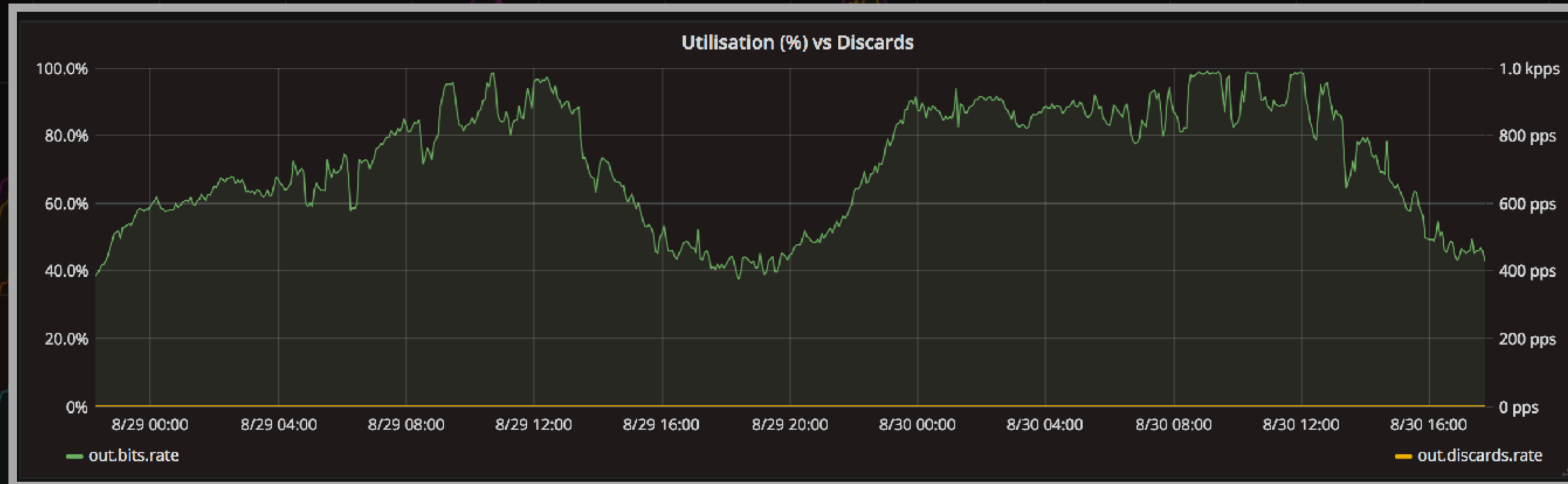**Source** → **Aggregation** → **Threshold** → **Alert**
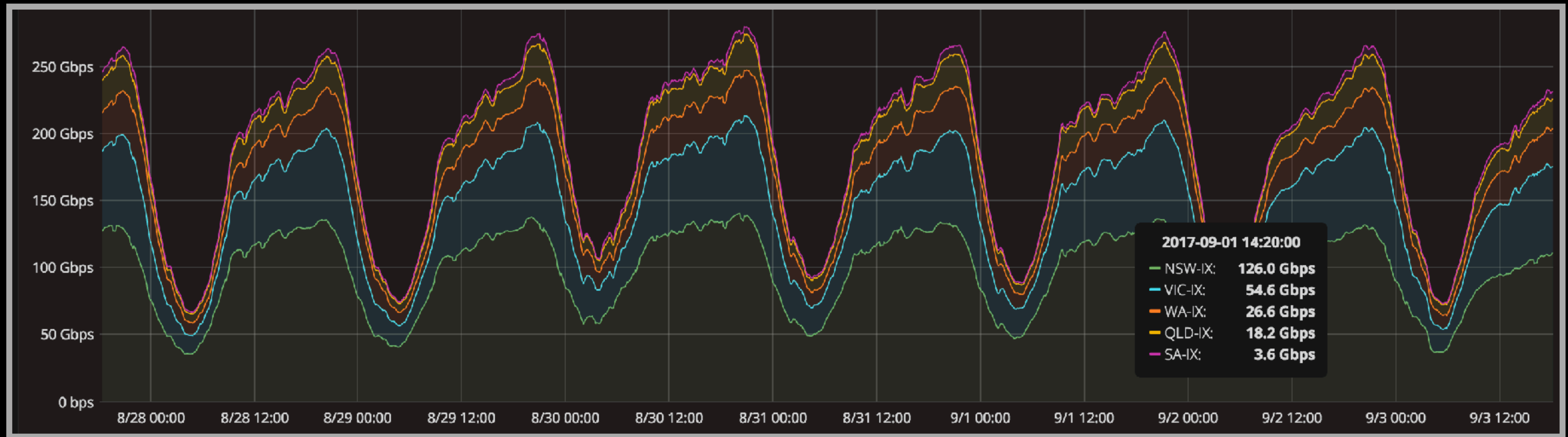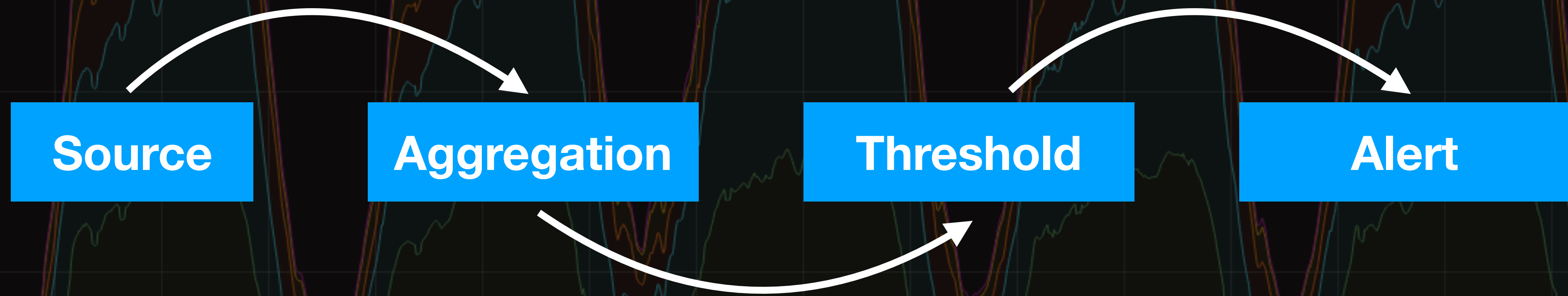
Limitations on the rest of us

- Time / $

- On-device computing power

- Vendor feature support

- Previous generation monitoring interfaces

Monitoring for the rest of us

- Top-down approach

- Business goals measured by metrics

- Focus on alert conditions to reduce noise and improve impact
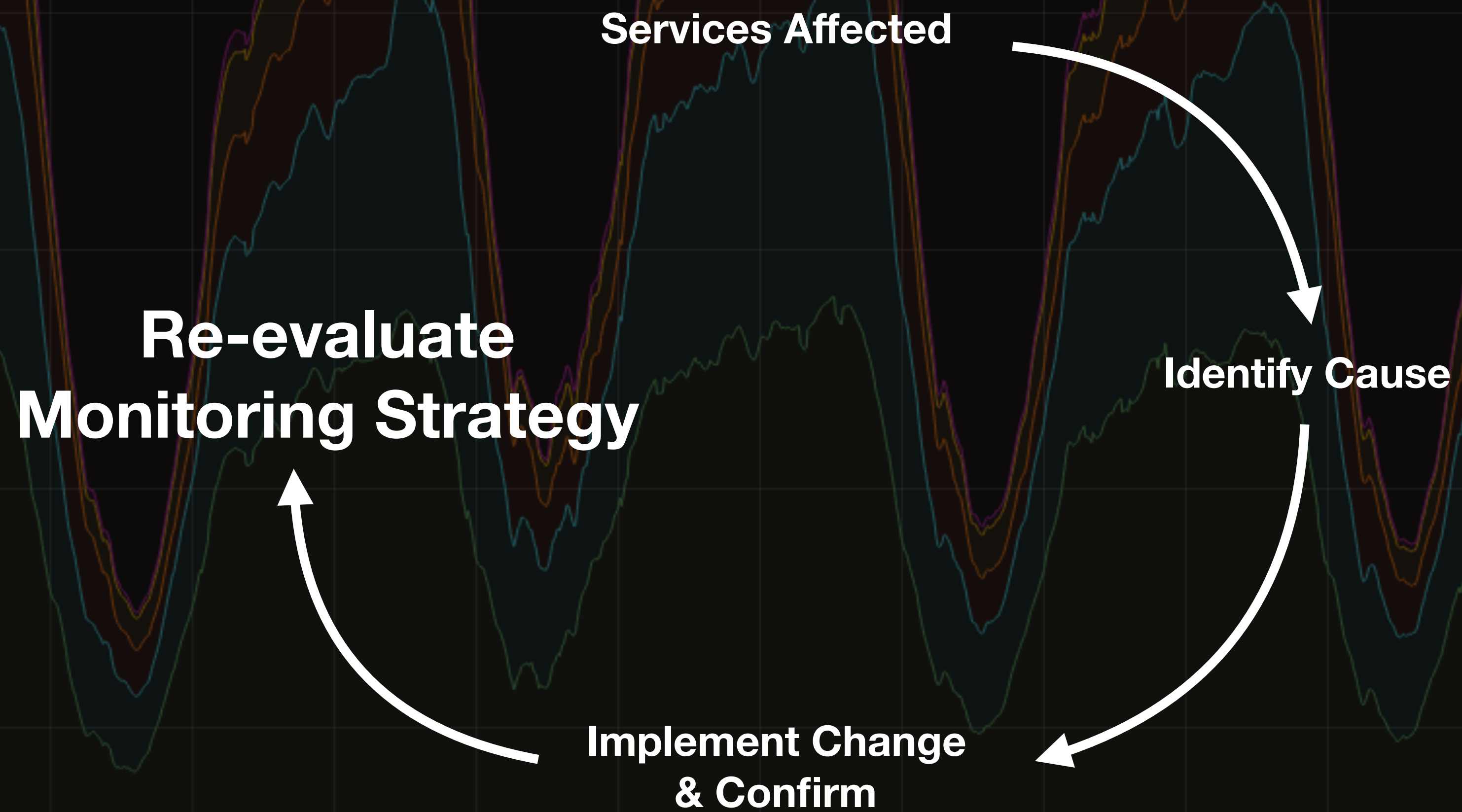
- Continual improvement

Utilisation (%) vs Discards

```
if out.bits.rate > 90% AND out.discards.rate > 0:

    alert: high priority:

else if out.bits.rate > 85%:

    alert: low priority
```

Continual Improvement

Services Affected

Re-evaluate Monitoring Strategy

Identify Cause

Implement Change & Confirm

12

Monitoring for the rest of us

- Use technology available to you

- Design for resilience

  - Put collectors close to the data source

  - Use buffers

  - Store raw values

  - Meta Monitoring

Monitoring for the rest of us

Use technology available to you.

Monitoring for the rest of us

Design for Resilience

Device ⟵┄┄┄⟶ Collector ⟶ Central Datastore

Device ⟵┄┄┄⟶ Collector ⟶ Central Datastore

Monitoring for the rest of us

Meta Monitoring is important

Software

- Storage:
  - InfluxDB, Graphite, Prometheus

- Collection:
  - Telegraf, Collectd, Sensu, Statd, SnmpCollector

- Alert Evaluation:
  - Riemann, Kapacitor, Sensu

- Display:
  - Grafana, Chronograf

Questions

@timraphael215   linkedin.com/in/timraphael215/   www.timraphael.com

AusNOG 2017