NextGen IT Ops

A Telco's Journey to Service Intelligence From Legacy and Siloed Event Management Systems

Alexander Romanuaskas | Solutions Architect
Consolidated Communications

October 2018 | Version 1.0

Forward-Looking Statements

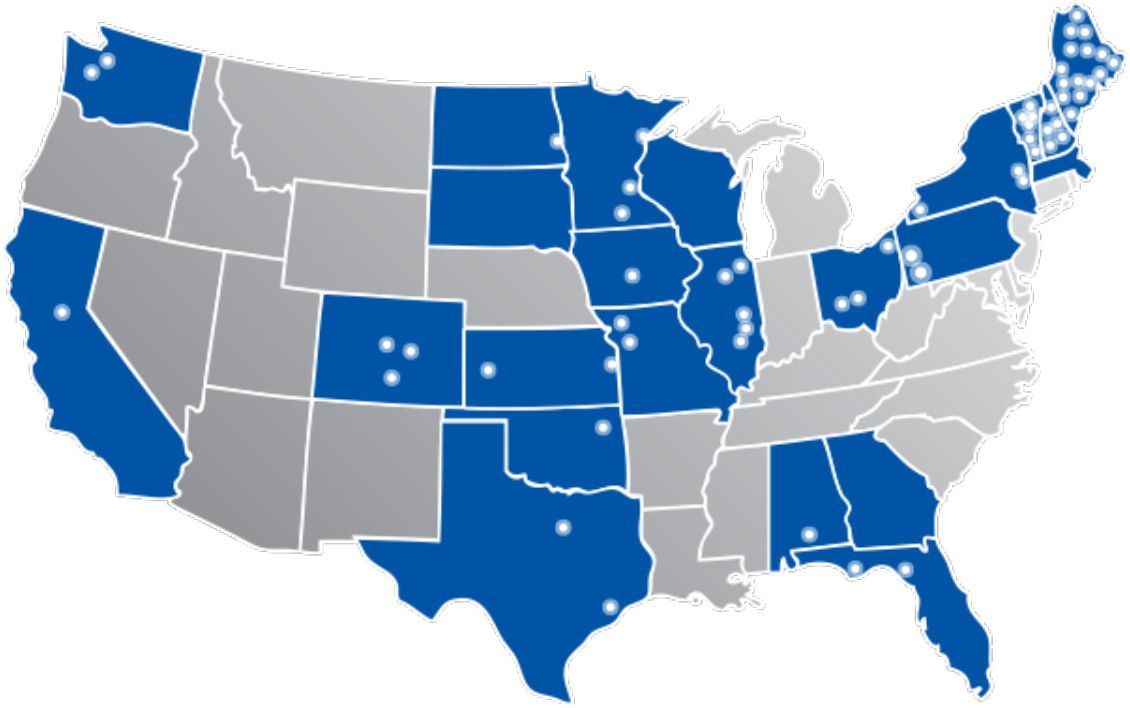
During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

splunk> .conf18

Consolidated Communications

- Founded in 1895
- 9th Largest domestic fiber provider
- Located in 24 states
- More than 36,000 fiber route miles
- 4,000 employees
- Providing data, voice, video, managed services, cloud computing, and wireless backhaul



Alexander Romanauskas

- 23+ Years in the Service Provider industry
- Product Owner of all things Splunk and Network Analytics
- Equal parts Network and System Administrator
- Using Splunk for 5 years
- Splunk Certified Architect

Key Learning Objectives

In this session, you'll learn

1. Common hurdles with legacy tools
2. The problem with siloed information
3. How we used Splunk ITSI to overcome these hurdles and problems
4. Actionable tips for your own implementation, adoption, and success

How It All Began

Many Teams + Multiple Tools = Trouble

Our Motivation For Change

The Core Issues

Maintenance Headaches

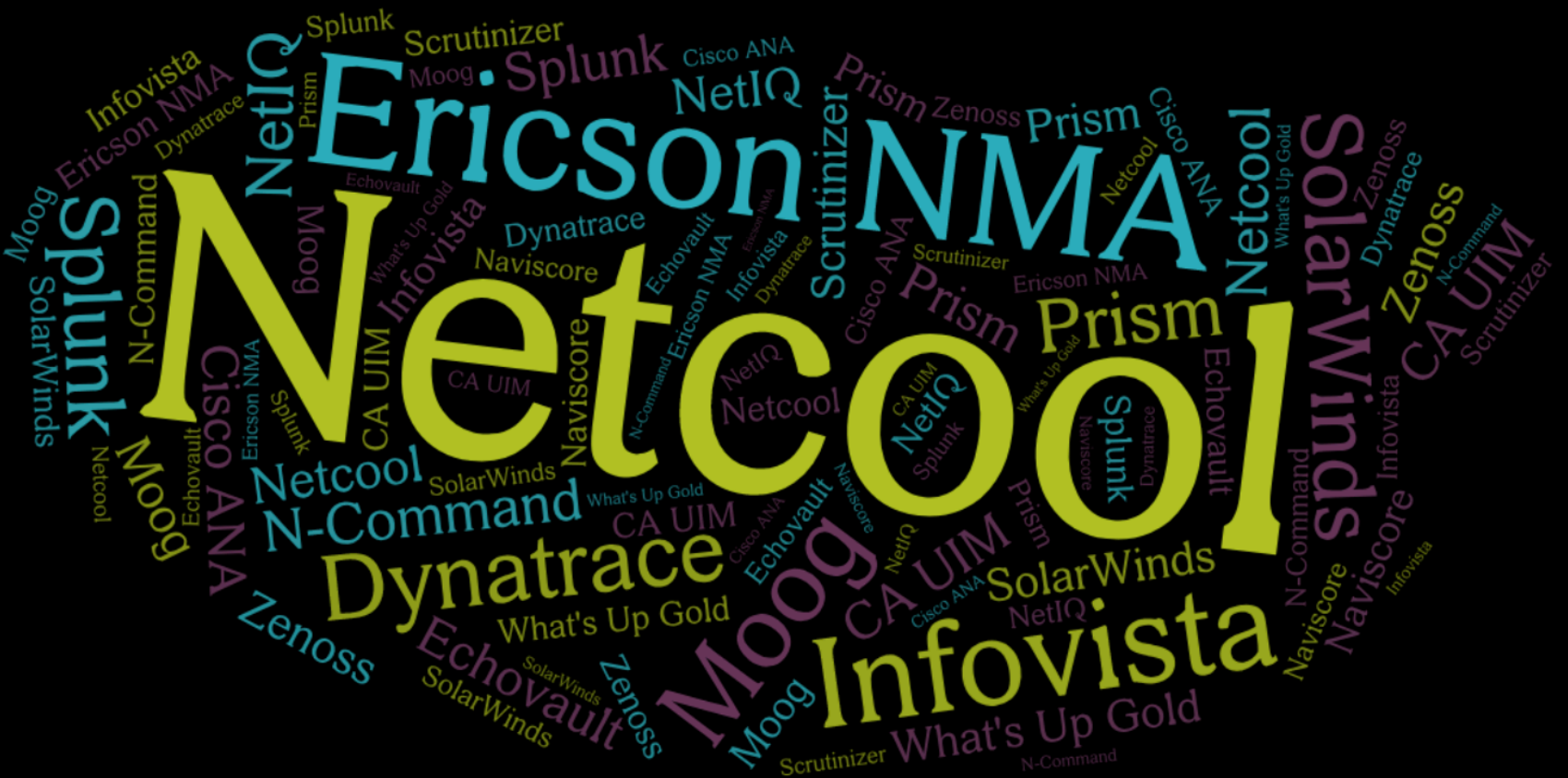
- License Cost
- Bloated Headcount
- Outdated UI Requirements
  - Java Runtime
  - Flash

Unique Tools

- Each team trusts their *own* tools
- Inability to share resources
- Duplicate data in multiple places

How It Was Working

Too Many Screens



The Challenge

Keeping It All Together

The Challenge Is

Keeping it all together

- ✓ Combine Performance and Fault Management
- ✓ Reduce the number of silos
- ✓ Use analytics to dynamically detect anomalies
- ✓ Correlate events
- ✓ Simplify the management
- ✓ Enrichment of data
- ✓ Stop the ticket passing

Let's Just Use Splunk

It Can Just Be Some Simple Dashboards

- We already own it
- We have Splunk certified employees
- Unlimited customizations
- Over 1,500 apps currently available
- Machine Learning Tool Kit

Not So Fast…

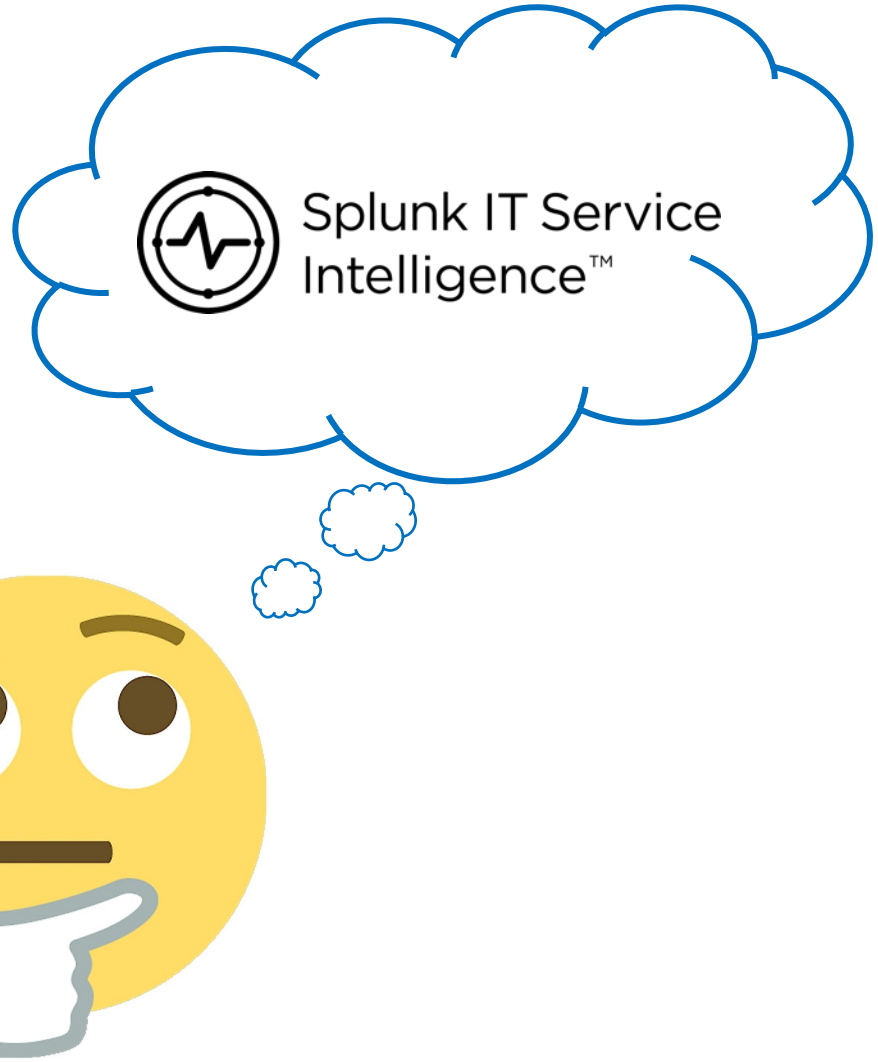
Everyone Wants Customizations

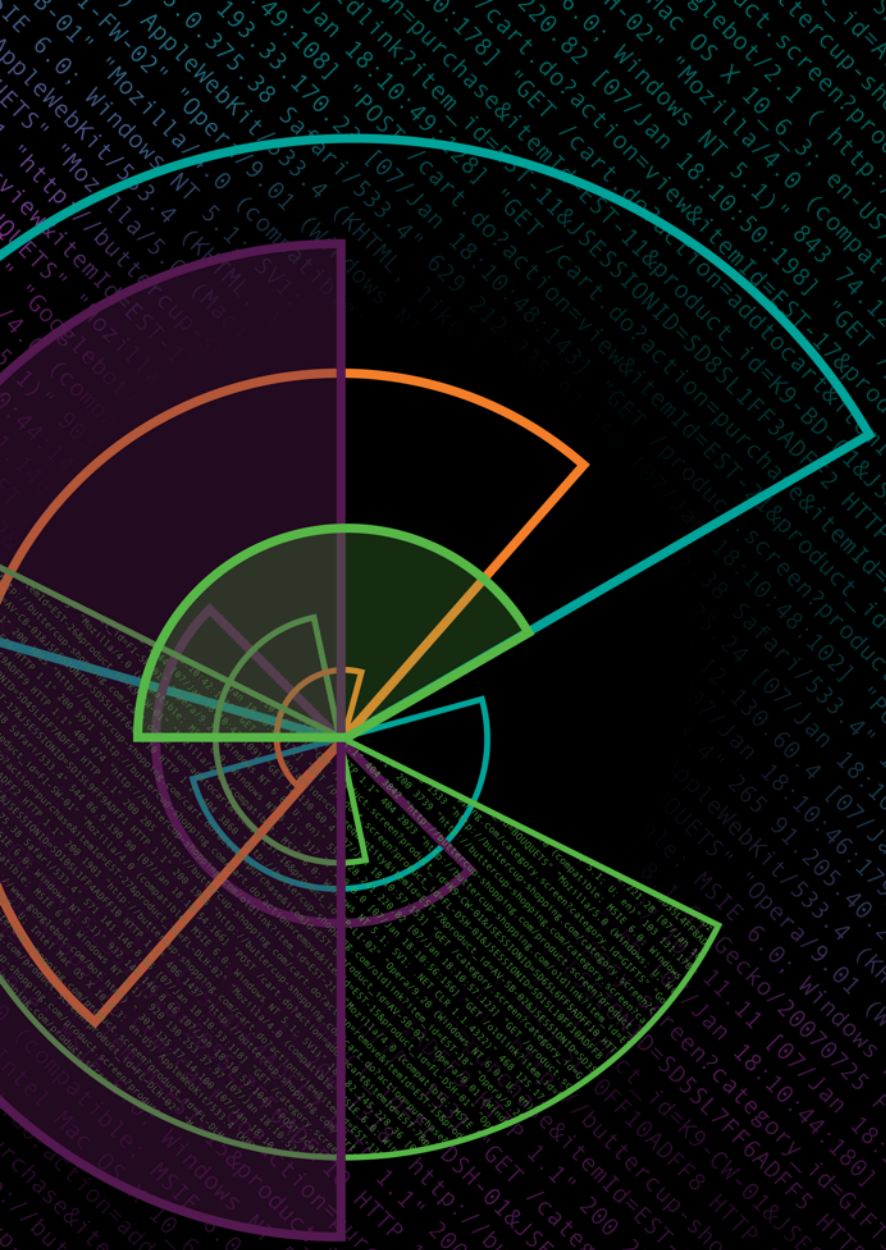
- Road Blocks
  - Splunk resource constraints
    - Too few in-house Splunkers
    - Too much development time
  - Missing IT datasets
  - Mature alerting requirements
  - Ticketing integration
  - Users want *Realtime*

Our Second Thought… Splunk ITSI!

Back To The Drawing Board

- It's Splunk
  - Built atop the Splunk Framework
  - Supported by Splunk
- Components
  - Notable Events
  - Event Grouping
  - Glass Tables
  - Deep Dives





Convincing The Others

Getting Everyone On Board

splunk> .conf18

Splunk ITSI

Buy In

Now that our team has decided on **Splunk ITSI**, how do we convince the others?

- General Splunk Demo and Training
  - Departmental Push Back / Why / What / Too Busy
  - Not all the data is already in Splunk
- Targeted ITSI Demo per Department
  - Resources are not unlimited
  - Not all the data is already in Splunk
  - SME knowledge is required

The #1 Barrier… Fear

Teams Feared New Tools

- Drastic Changes
  - Monitoring dashboards haven't really changed in decades
  - Users comfortable with their current tools
- The Unknowns
  - Existing ticketing integration
  - Legacy processes and procedures

Overcoming Fear Requires Advocates

Stay Calm

- Once you have their attention - get them talking…
  - Uncover and understand *their* processes
  - Identify any integrations
  - Have them assign SMEs
  - GET THEIR DATA INTO SPLUNK!
  - Show them the data

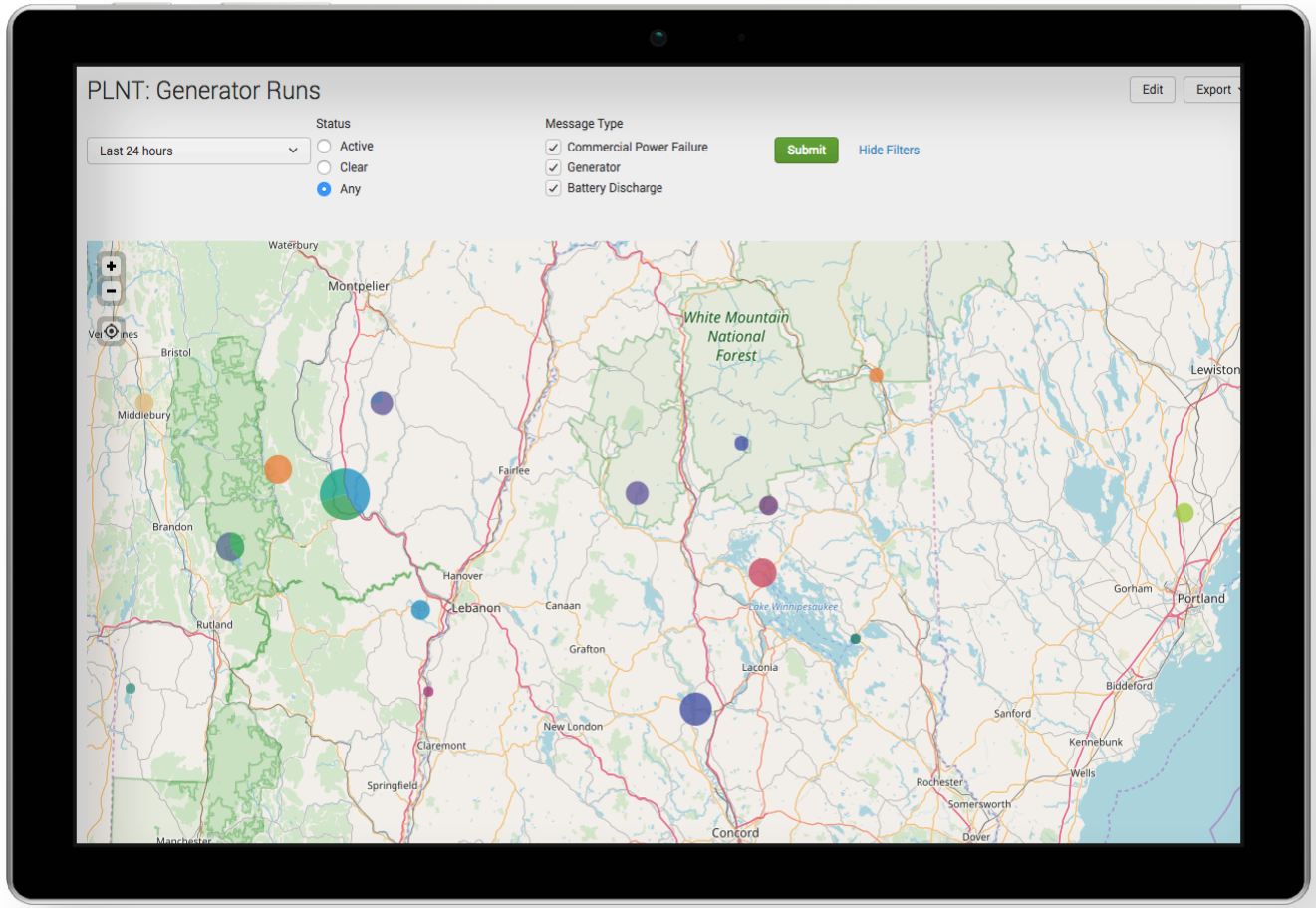
Free Candy

Give Them Something *They* Want

In 6 Hours, Outside Plant had an Alarm Dashboard

What used to be impossible with existing tools was now a single, streamlined interface

- Give them a small sample
- Make it FLASHY
- Listened to their needs



Bringing in the Data

You can’t boil the ocean

splunk> .conf18

Bringing in the Data

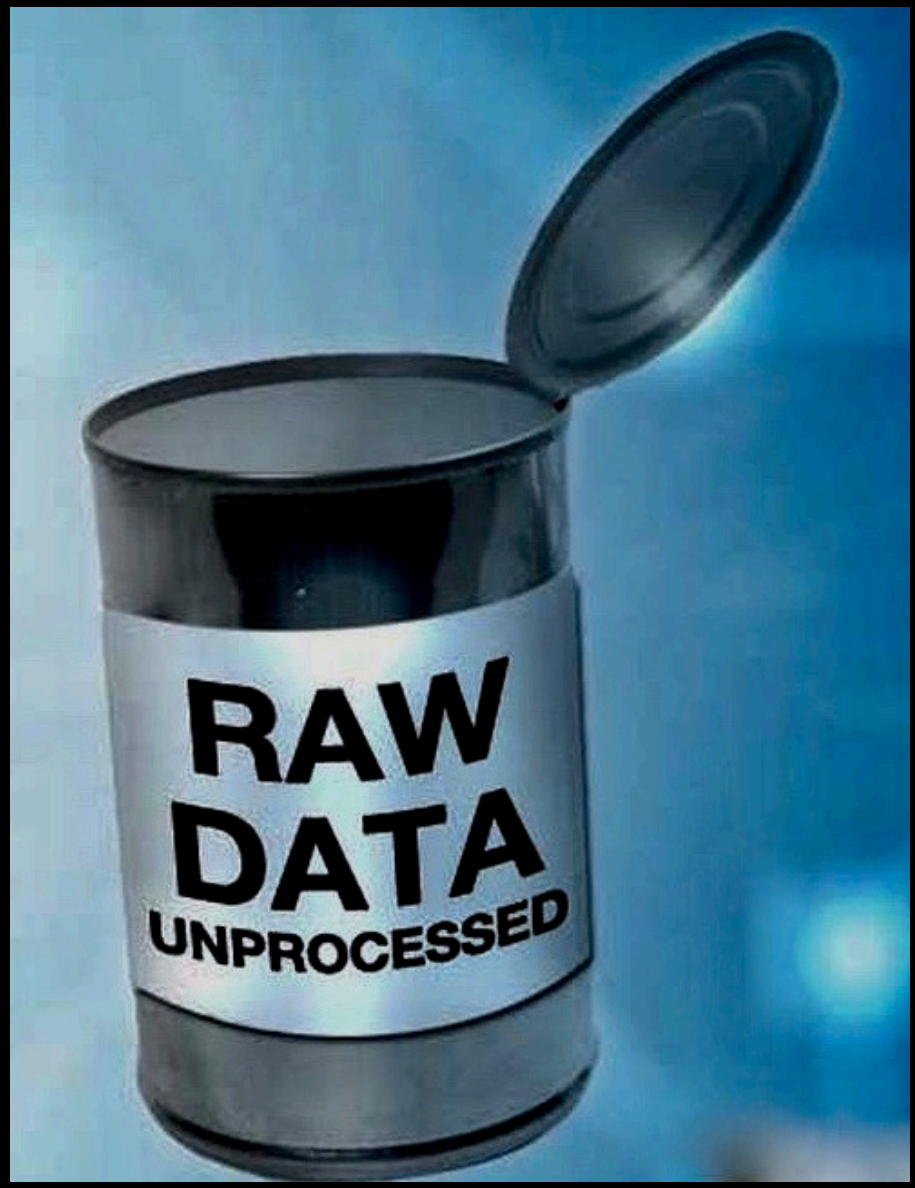
The Quick Way

- Use the existing monitoring systems
  - Forwarded Alerts
  - Poll via API
  - Database Access
  - Internal Logging
  - Export configuration

Bringing in the Data

Raw Data is better

- Go directly to Splunk
  - Syslog
  - SNMPTraps
  - SNMP Polling
  - Scripting
- Use Splunkbase
  - Over 400 TA
  - Look for something similar



Bringing in the Data

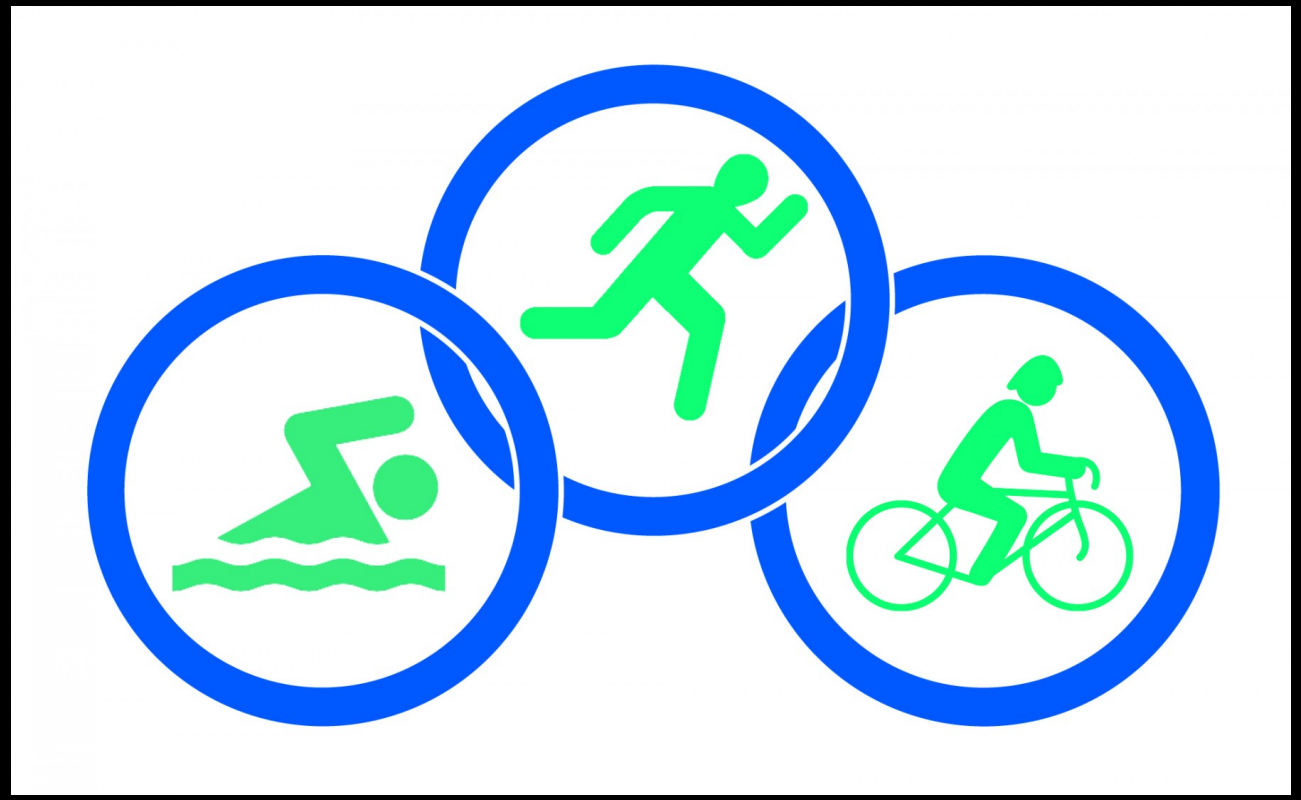
And when direct access is unavailable

- Outside Options
  - Splunk Stream
    - Decode EMS traffic
    - Packet Counts
    - Netflow
  - Opensource tools
    - Cacti
    - Nagios

Adoption & Implementations

If you build it… they may not come.
(… so you get them to!)

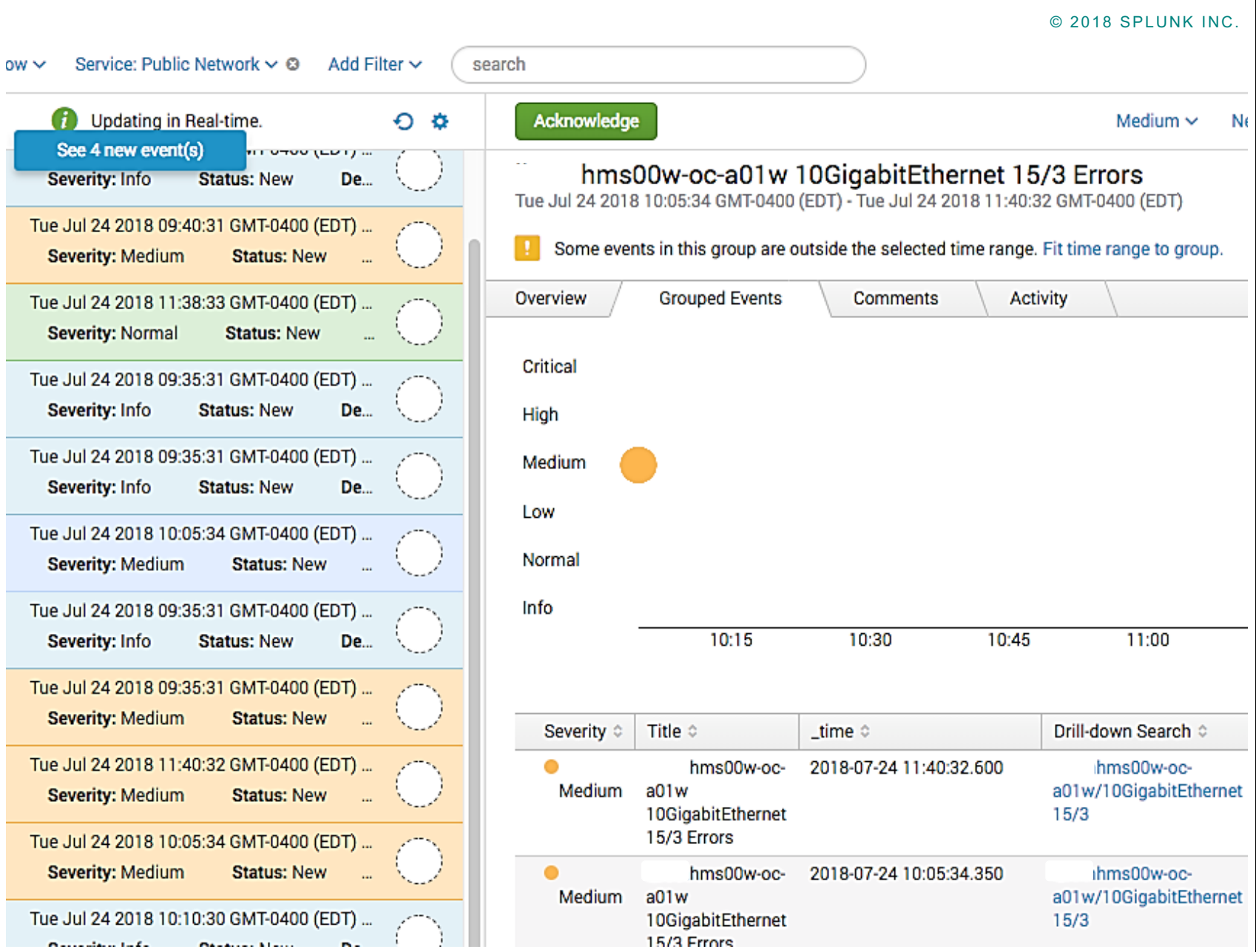
Let The Race Begin



Prepare For A Triathlon Not A Sprint

Make Them Comfortable

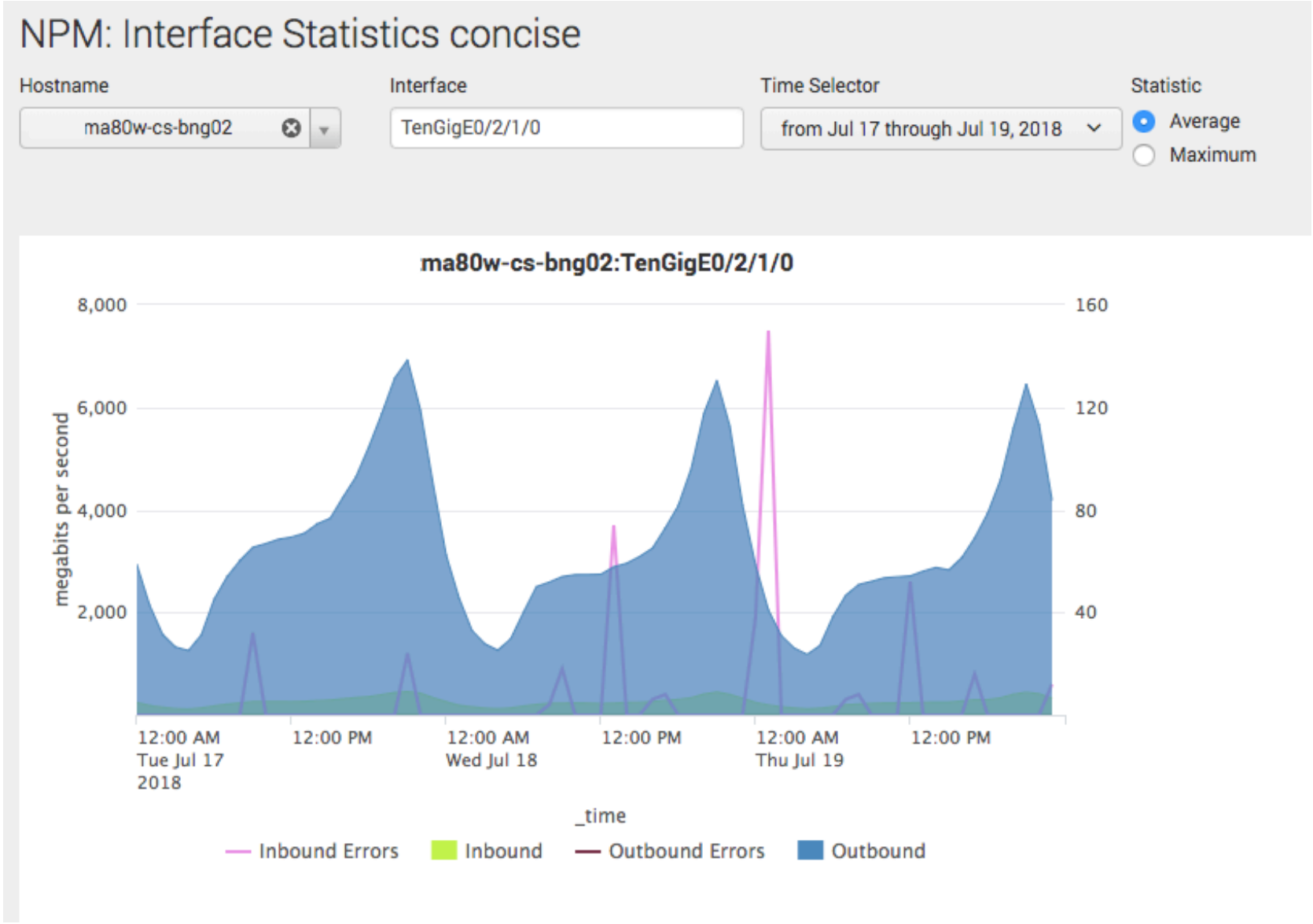
Use Familiar Views



splunk> .conf18

Compelling Visuals…

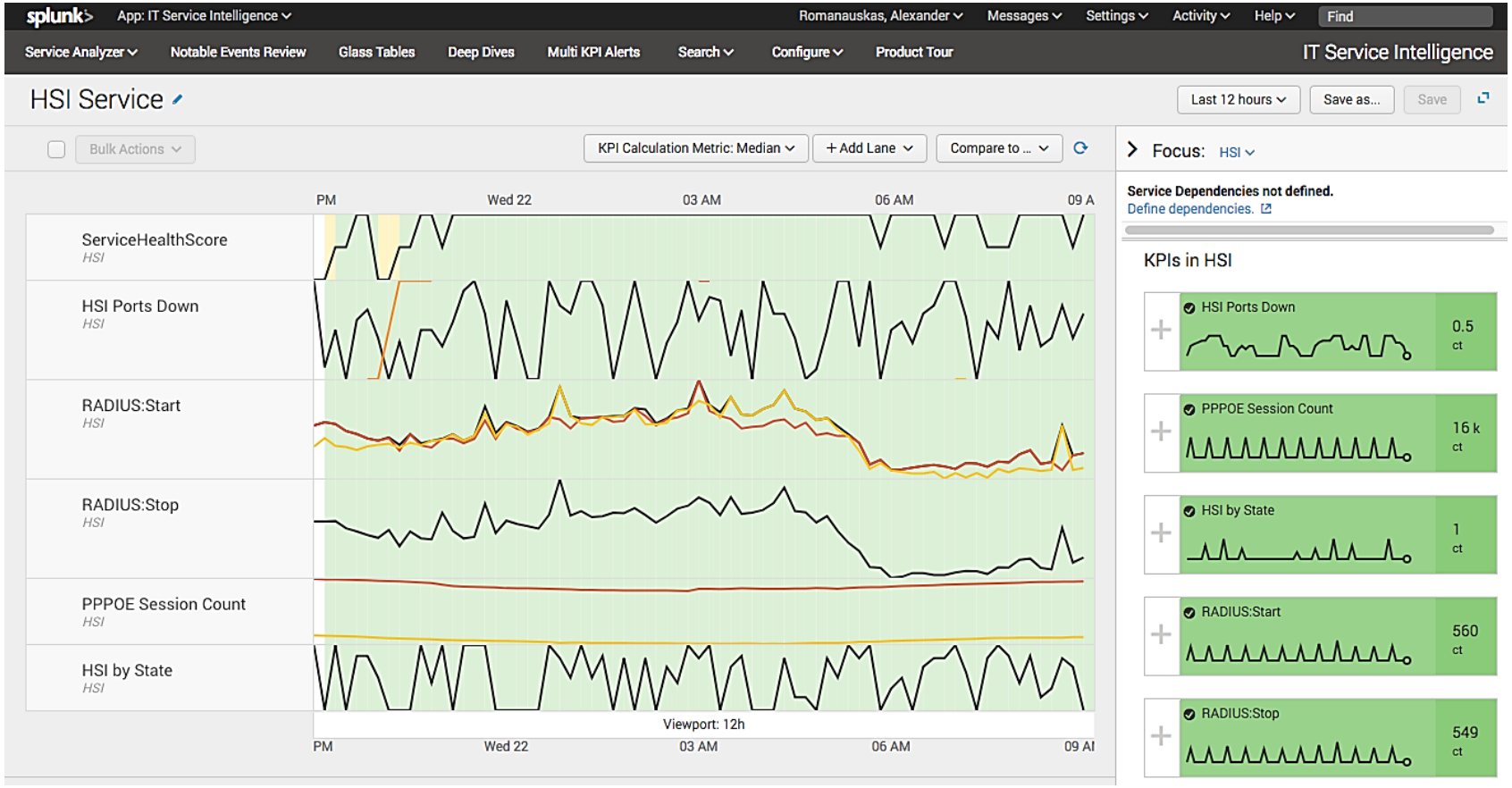
Take them from an alert to a visual by providing drill down options



splunk> .conf18

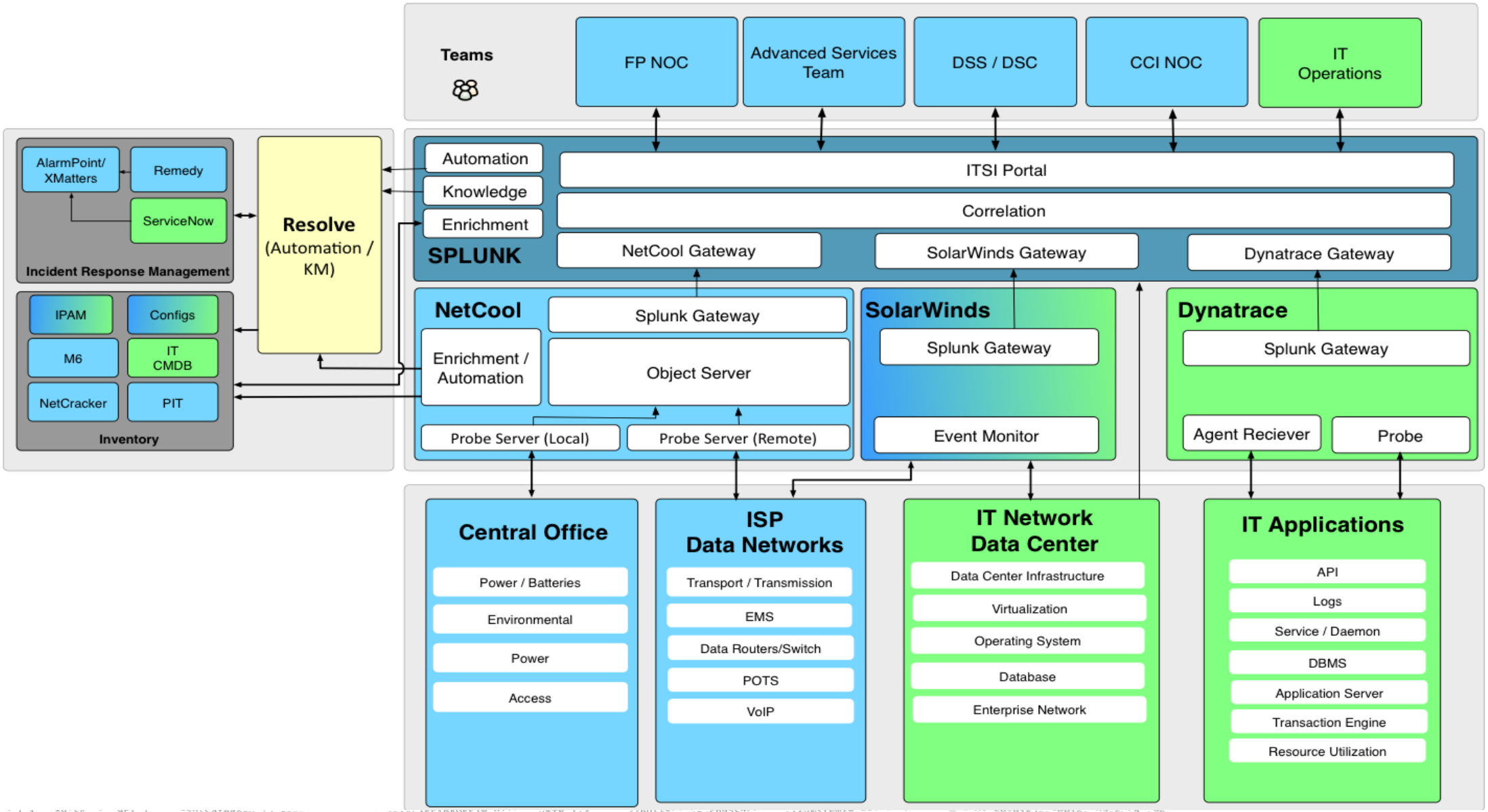
Efficiency!

Create a Service View that groups all related KPIs together



splunk> .conf18

Our Complete Splunk ITSI Solution Architecture!



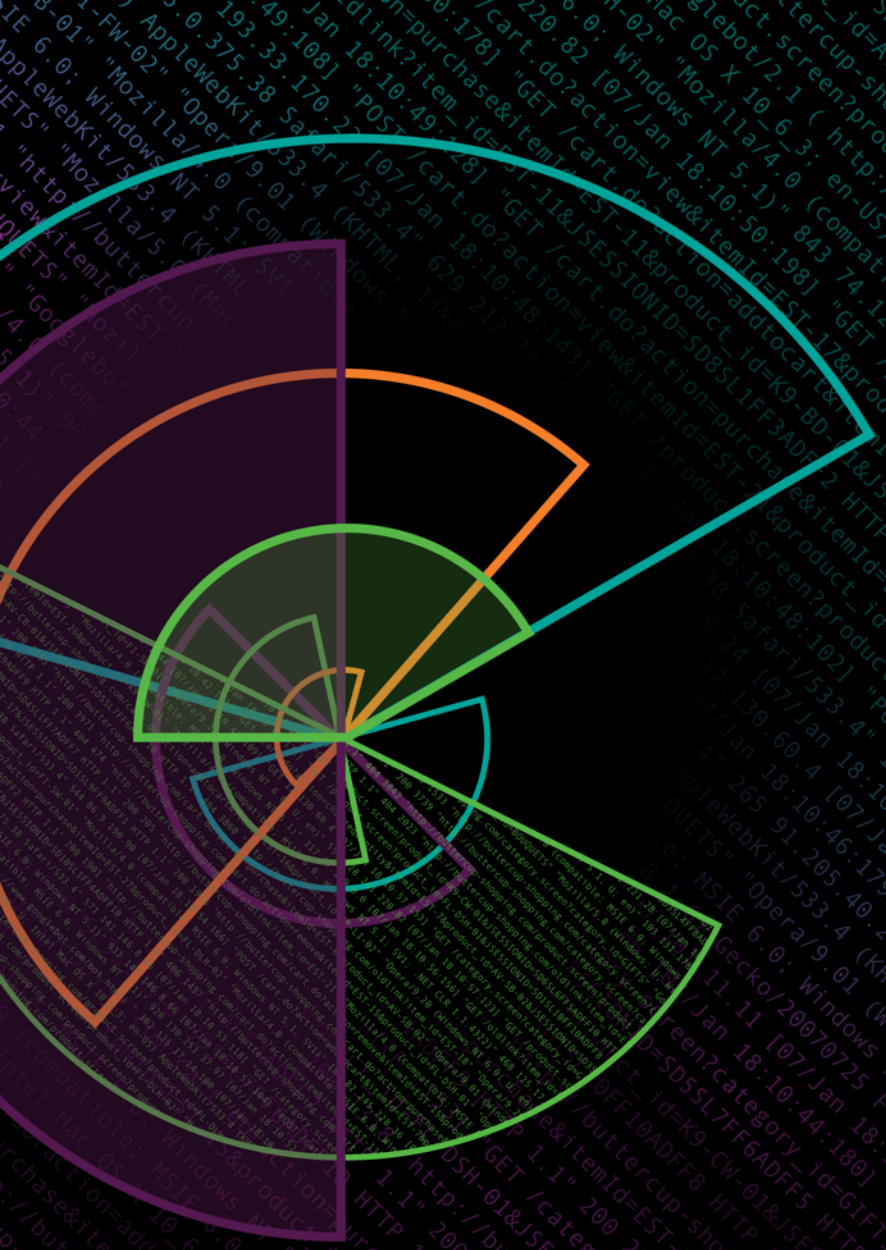
Useful Resources

No need to reinvent the wheel from scratch

SDK for building ITSI actions - https://github.com/splunk/itsi-event-action-sdk

Martin Wiser's ITSI tools - https://github.com/mwiser

Splunk Add-on Builder - https://docs.splunk.com/Documentation/AddonBuilder/latest/UserGuide/Overview



Q & A

Thank You

Don't forget to rate this session in the .conf18 mobile app