Mean Time to Innocence – The Clock is Ticking

Emily Duncan – ITOA Specialist

Franco Ferrero-Poschetto – Sales Engineering

Kirk Hanson – ITOA Specialist

October 2018 | Version 1.0

Forward-Looking Statements

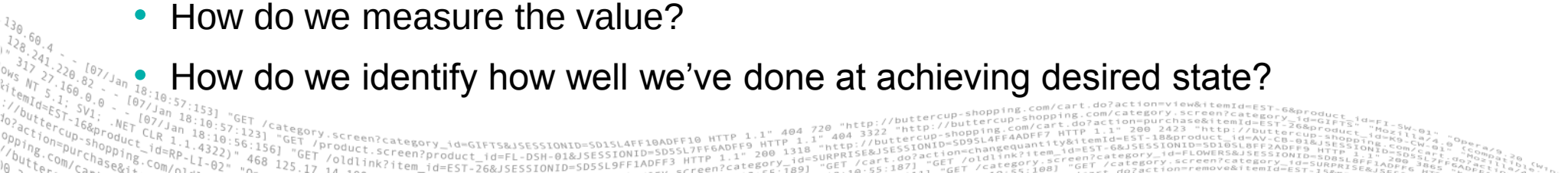
During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results 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

Agenda

- Background and Introduction
- Current State
  - What are we doing now and why isn't this working when it used to work just fine?
- Room for Improvement
  - What exactly needs to change?
- Desired State
  - Where do we want to end up and what Critical Requirements do I need to get there?
- Blueprint for Success
  - What do we need?
  - Where do we start?
  - How long will it take me?
- Realized Actual State
  - How do we measure the value?
  - How do we identify how well we've done at achieving desired state?



Background and Introduction

Who is impacted the most from the current state of things?

Background and Introduction – Service Desk Manager

Who I Am and What Do I Do

- **Who I am?**
  - Kirk Hanson, Manager Service Desk – production support, customer facing applications

- **What do I do?**
  - Oversee 250 support engineers, 200 L1, 50 L2, L3 part of the Digital Retail Application team.
  - Constantly finding ways to improve efficiency, reduce the need to involve L3 engineers
  - Become more proactive, reduce detect issues before customers call
  - Provide metrics and trends to the business and IT department
  - Reduce MTTR, improve SLA's

- **Challenges?**
  - Tickets not assigned to the right support team
  - Still too reactive: customers find out about application issues before we do
  - Too many hours spent in War rooms to detect root cause, high cost of support service

Background and Introduction – NOC Manager

Who I Am and What Do I Do

- **Who I am?**
  - Emily Duncan, NOC manager, infrastructure and applications

- **What do I do?**
  - Manage 30 Engineers in 3 shifts, initial triage of P1 and P2 issues
  - Trying to handle as many alerts as possible with the team I have
  - Responsible for day to day escalations, trying to reduce them
  - My teams have ‘eyes on glass’ which consists of 6 different monitors, each one showing a different type of alerts (SCOM, Solarwinds, Nagios)

- **Challenges?**
  - Constantly navigating in a sea of red alerts, very reactive, and difficult to prioritize work
  - We have 20+ different tools to monitor the infrastructure, issues are very difficult to triage, no end to end view of the environment and applications
  - War rooms are like throwing spitballs at each other
  - Reduce churn in staff

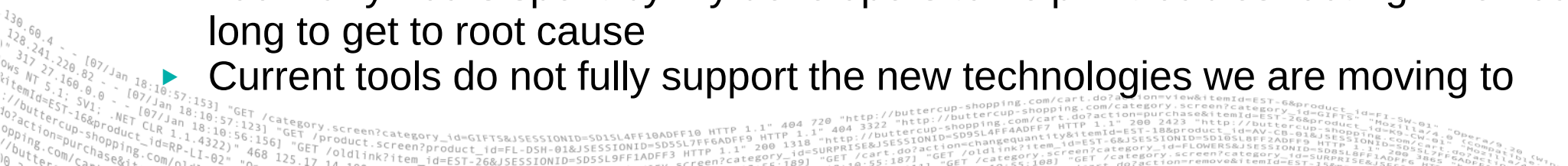
Background and Introduction – Application Owner

Who I Am and What Do I Do

- **Who I am?**
  - Franco Ferrero-Poschetto, Director Digital retail application – dev, test, and prod, responsible for application overall health, and customer satisfaction

- **What do I do?**
  - Manage 156 developers, also act as L3 support when needed
  - Transitioning to Agile methodology
  - Migrating legacy components to the cloud and containerized technology
  - Constantly striving to increase customer satisfaction, reduce MTTR and increase MTBF
  - Provide key statistics to the business

- **Challenges?**
  - Too many tools, but no complete visibility of the application end-to-end
  - Still too reactive: customers find out about application issues before we do
  - Too many hours spent by my developers to help in troubleshooting when outages occur, too long to get to root cause
  - Current tools do not fully support the new technologies we are moving to



splunk> .conf18

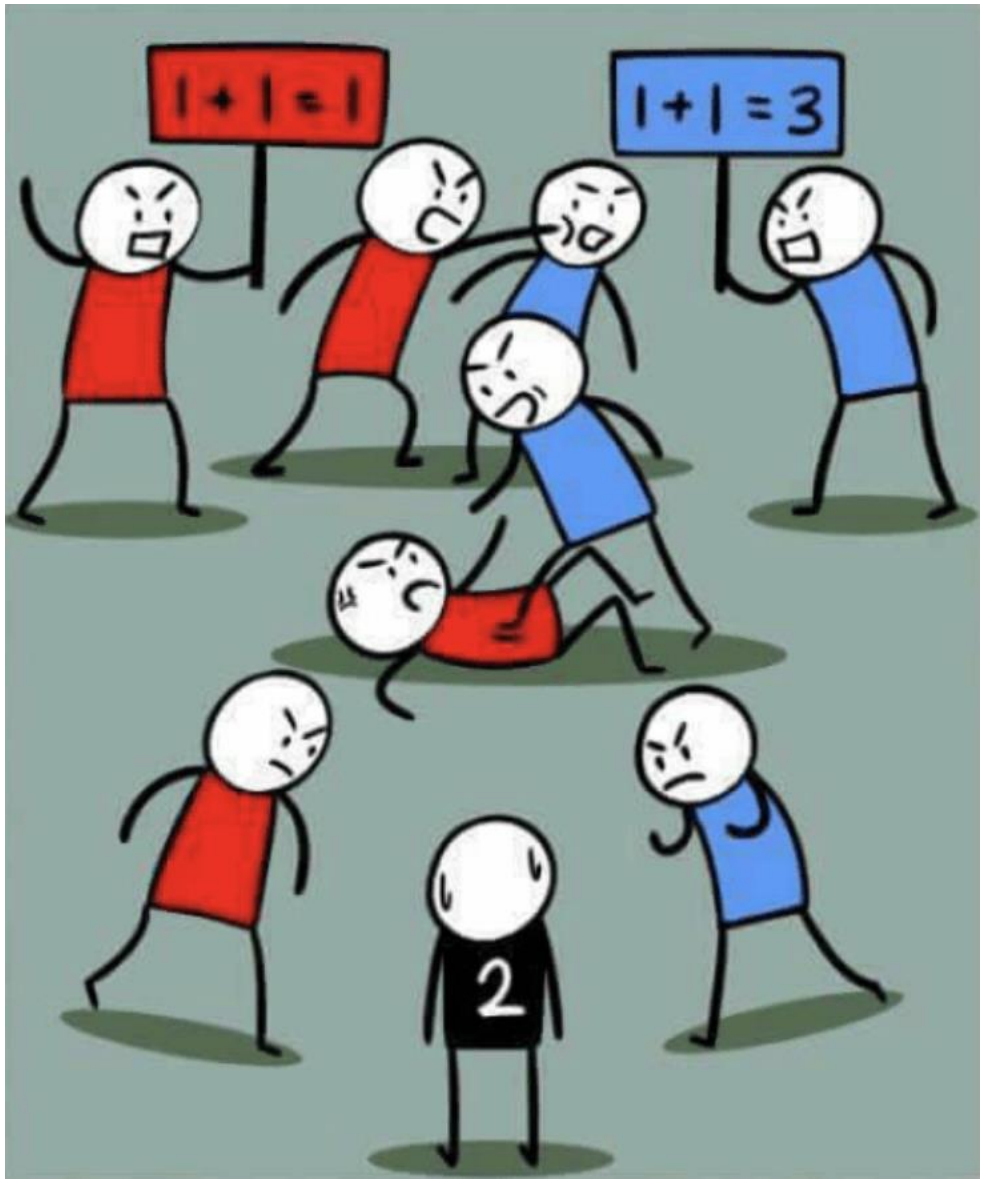
Current State

What are we doing now and why isn't this working when it used to work just fine?

MTTI

Mean Time to Innocence

- Everyone is right
- Everyone else is wrong
- Blame game
- Lack of continuity



What MTTI Looks Like to SD Personal

Why Does Mean Time to Innocence Matter to the Service Desk

- Low CSAT
  - *Customers are unhappy with our service*
- Low NPS
- Low Productivity
  - *It takes too many sets of eyes to find and resolve issues*
- Low Morale
  - *People are burnt out and feel they can't ever get ahead of the storm*
- Turnover Rate Increase
- Lower Customer Retention
  - *There are too many competitor options for customers so if we disappoint them there's a line around the corner waiting to take our place*

What MTTI Looks Like to NOC manager

Why does Mean Time to Innocence Matter to the NOC

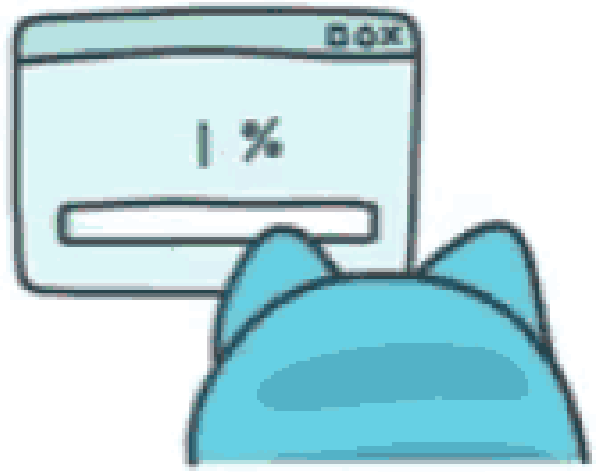
- Everything is a P1
  - Severity doesn't matter, we still have to address it no matter what
- Everything is Down
  - If there is an alert showing on a screen, we have to look at it even if in the end we find out it's not actionable or it's been resolved
- Services are Down
  - We don't know what's impacted or more importantly WHO'S impacted
- Sea of Red
  - Red is always what we see first and there is so much 'RED' it makes it impossible to look at anything else

What MTTI Looks Like to an Application Owner

Why Does Mean Time to Innocence Matter to the Application Teams?

- Is it my application causing the issue?
- Less time to spend actually ‘Developing Apps’ –

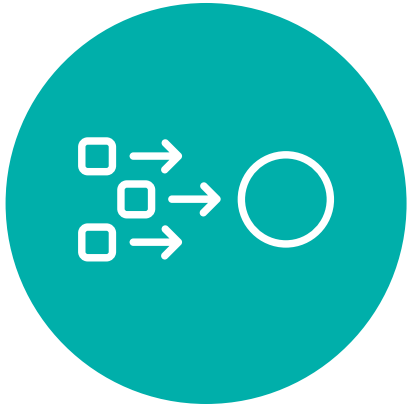
  too much time spent ‘Supporting/Fixing Apps’
- Is my Application playing nice in the production environment?
- App reputation is low means App Developer reputation is low
- Loss of revenue
- Loss of customers



Room for Improvement

What exactly needs to change?

Where Do We Want to End Up?



Reduce Noise

Prioritize Based on Business Impact

Identify Root Cause

Be Predictive

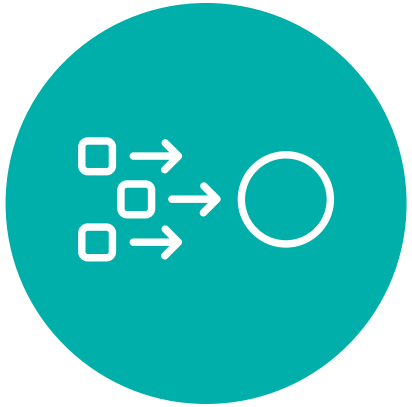
Be Better at All of These!

Desired State

Where do we want to end up and what Critical Requirements do I need to get there?

What are the Critical Requirements We Will Need?

Reduce Noise



Event Correlation cross-stack and cross-tool, remove data silos

Prioritize Based on Business Impact

Service Insights

Identify Root Cause

Root Cause Indication – which alerts are to blame and KPI's (so I can create alerts based on things I know go red when something is bad)

Be Predictive

Alert me in advance if a service is declining so I can fix things before there's wide-spread impact

Be Better at All of These!

Free Splunk led enablement opportunities

splunk> .conf18

Blueprint for Success

What do we need to do? What do we do first, second, last? How long will it take me?

Blueprint for Success

In order to know where you are going, you first have to know where you've been!

1. **Identify where you are in the ITOA Maturity Curve**
   - What is being monitored and by what?
   - Where are the gaps, what can't you do because of the way you are doing things now?
   - Identify what data sources you need to have that 'Single Pane of Glass'
   - Talk to the people who use these alerts to do their job and find out what their looking at (alerts, logs, etc.)
2. **Prioritize**
   - Pick a Business Critical service
     - Identify the data sources monitoring that service
     - Identify 'Who' looks at that data to do their job (this will help you build out what components that service is dependent on)
3. **Correlate on what makes sense**
   - ML can you far BUT you need to talk to the SME's who use this data on a regular basis, understand what they use it for, how they use it, what matters and what doesn't.

splunk> .conf18

Blueprint for Success

In order to know where you are going, you first have to know where you've been!

1. **Identify important metrics**
   - What do you measure or look at to know if something is performing well or badly (THIS IS A KPI)
2. **Identify sources of enrichment**
   - CMDB, architecture diagrams, Event Information (Yes you can even help build a service by the information in an event – hostnames, event messages, fields)
3. **Validate your work**
   - Look at the way events are being grouped (Episodes) and ask the SME's if it makes sense
   - Ask the SME's what is missing, what other information do they need to see to get 80% of the way to know how to resolve the Incident

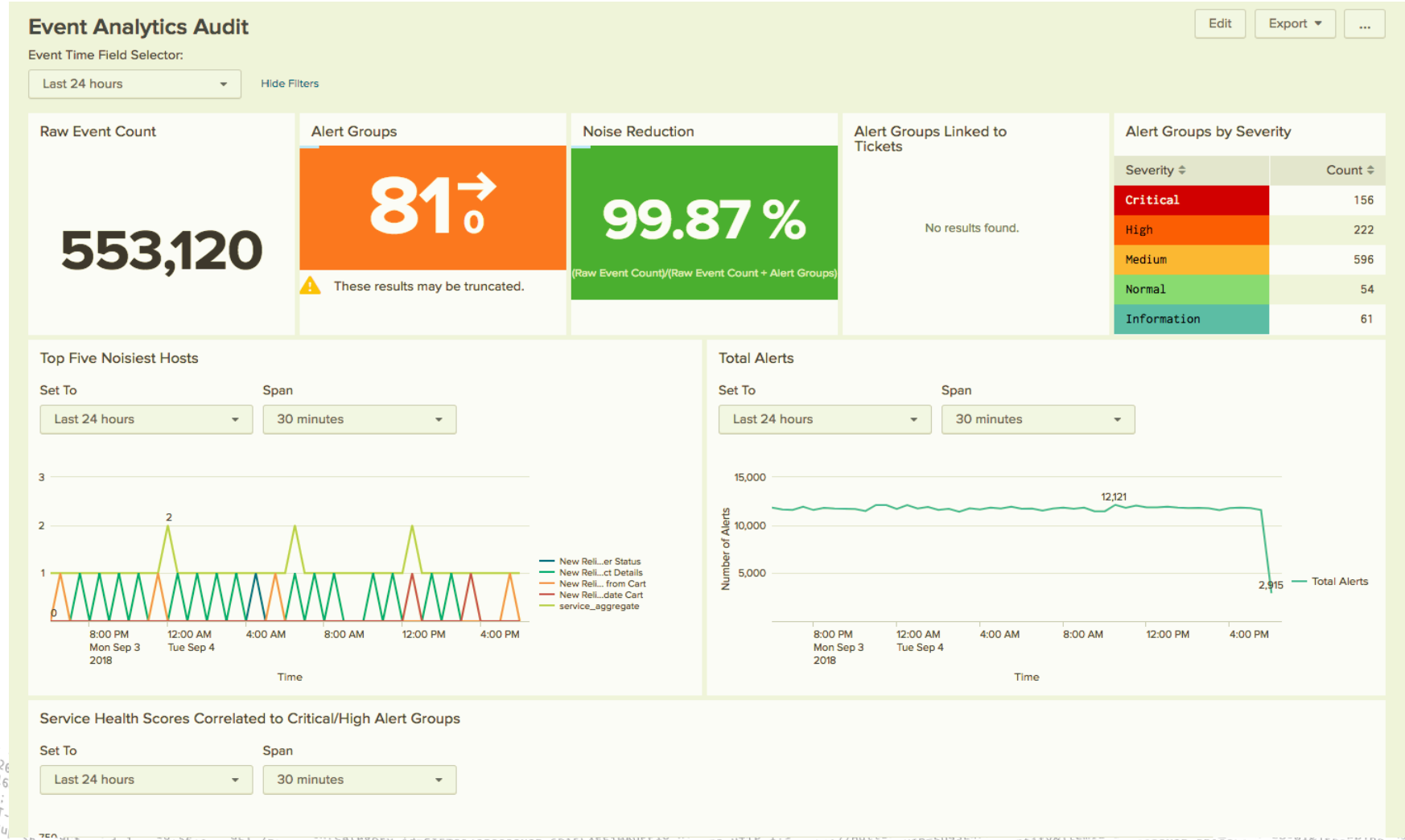
Realized Actual State

How to measure where you are in obtaining your desired state

Measuring Value

Value is in the Eye of the Beholder

Reduce Noise

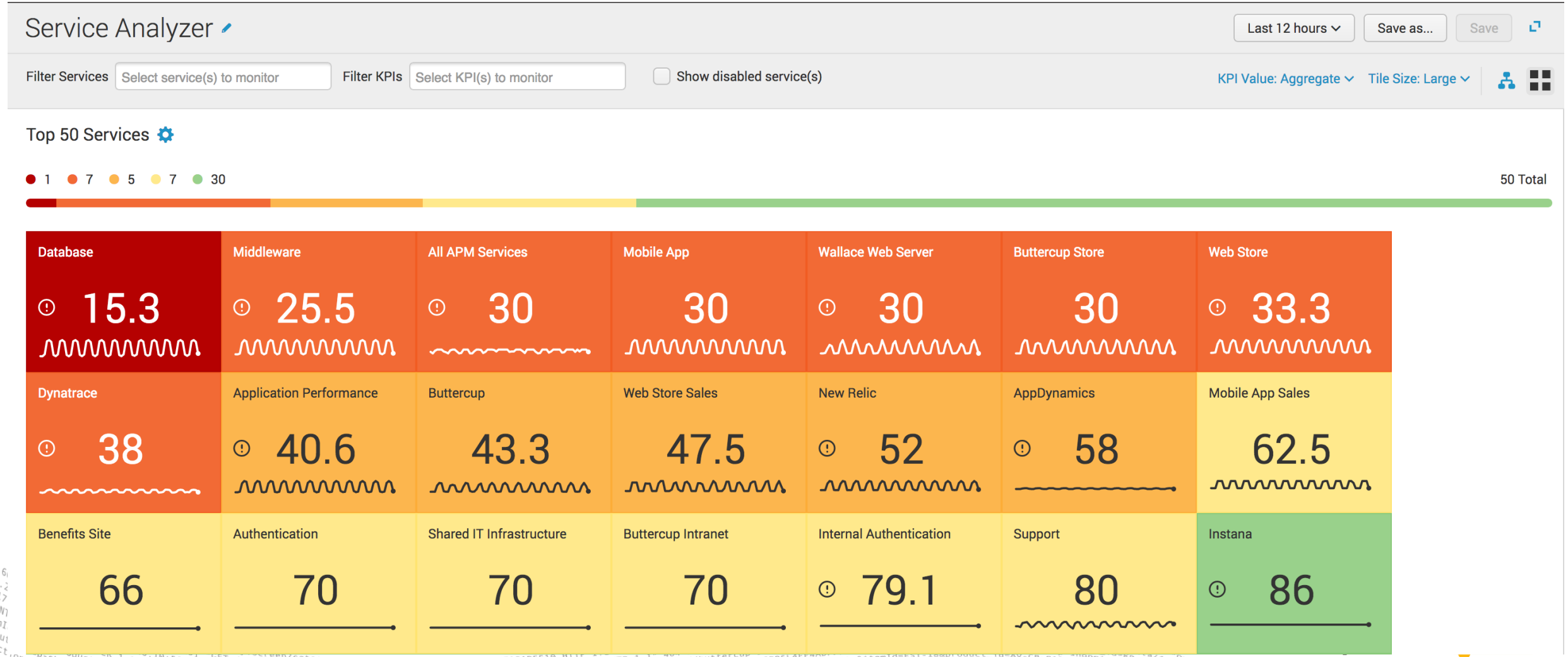


splunk> .conf18

Measuring Value

Value is in the Eye of the Beholder

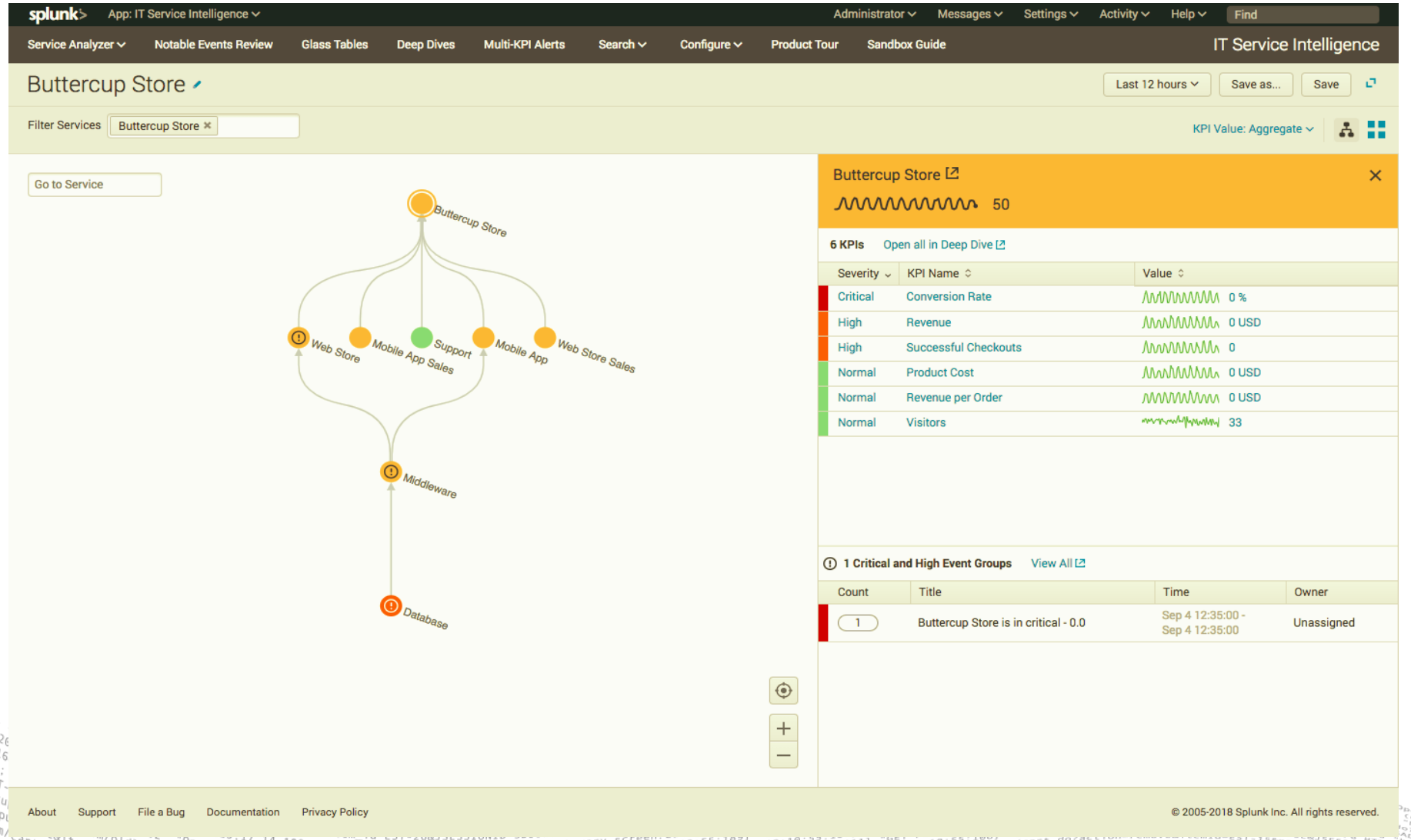
Blast Radius – Service Health View



Measuring Value

Value is in the Eye of the Beholder

Blast Radius – Service Tree View

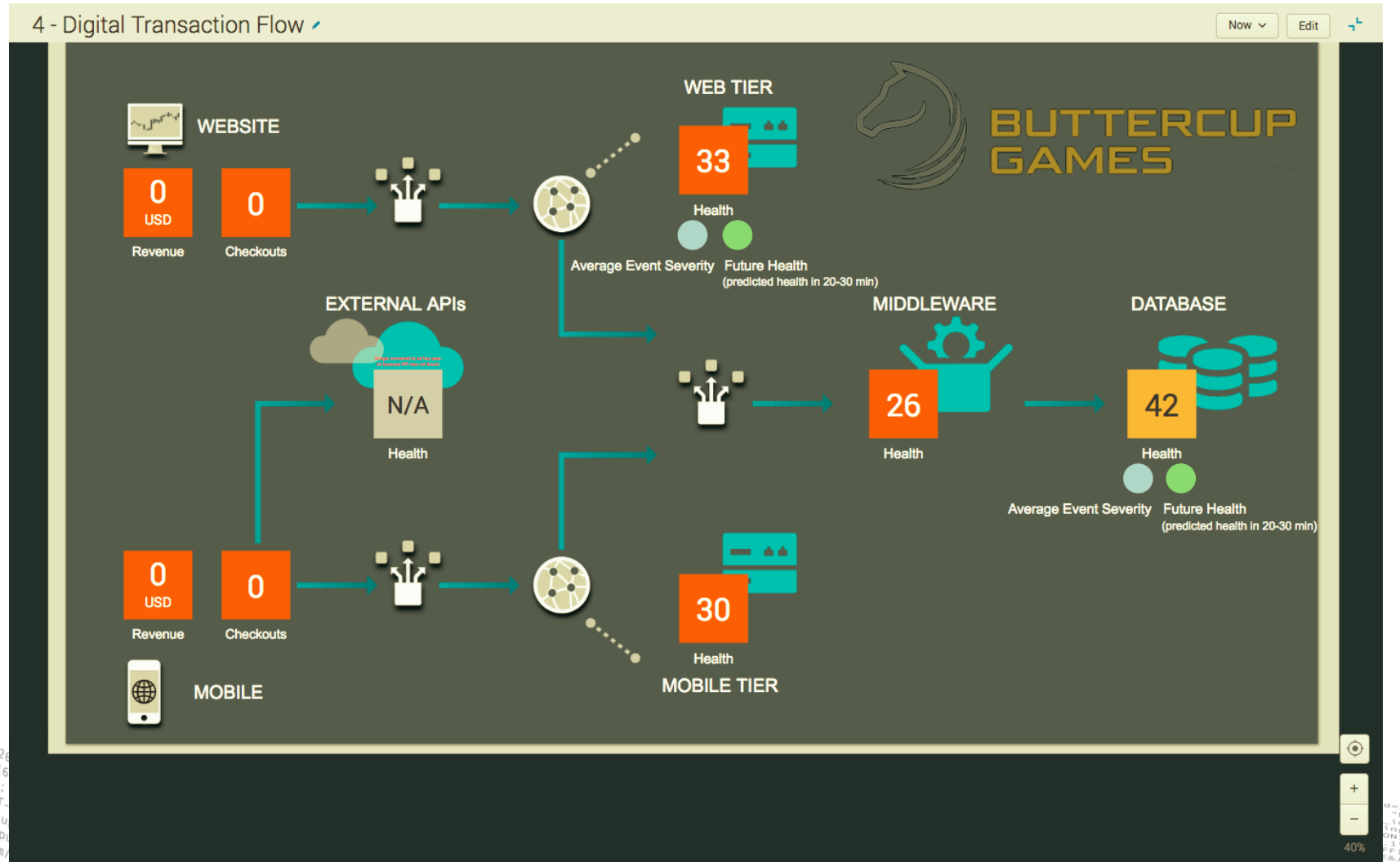


splunk> .conf18

Measuring Value

Value is in the Eye of the Beholder

Be Predictive – Show not only the current health of your service but the Predicted Health 20-30 mins in advance

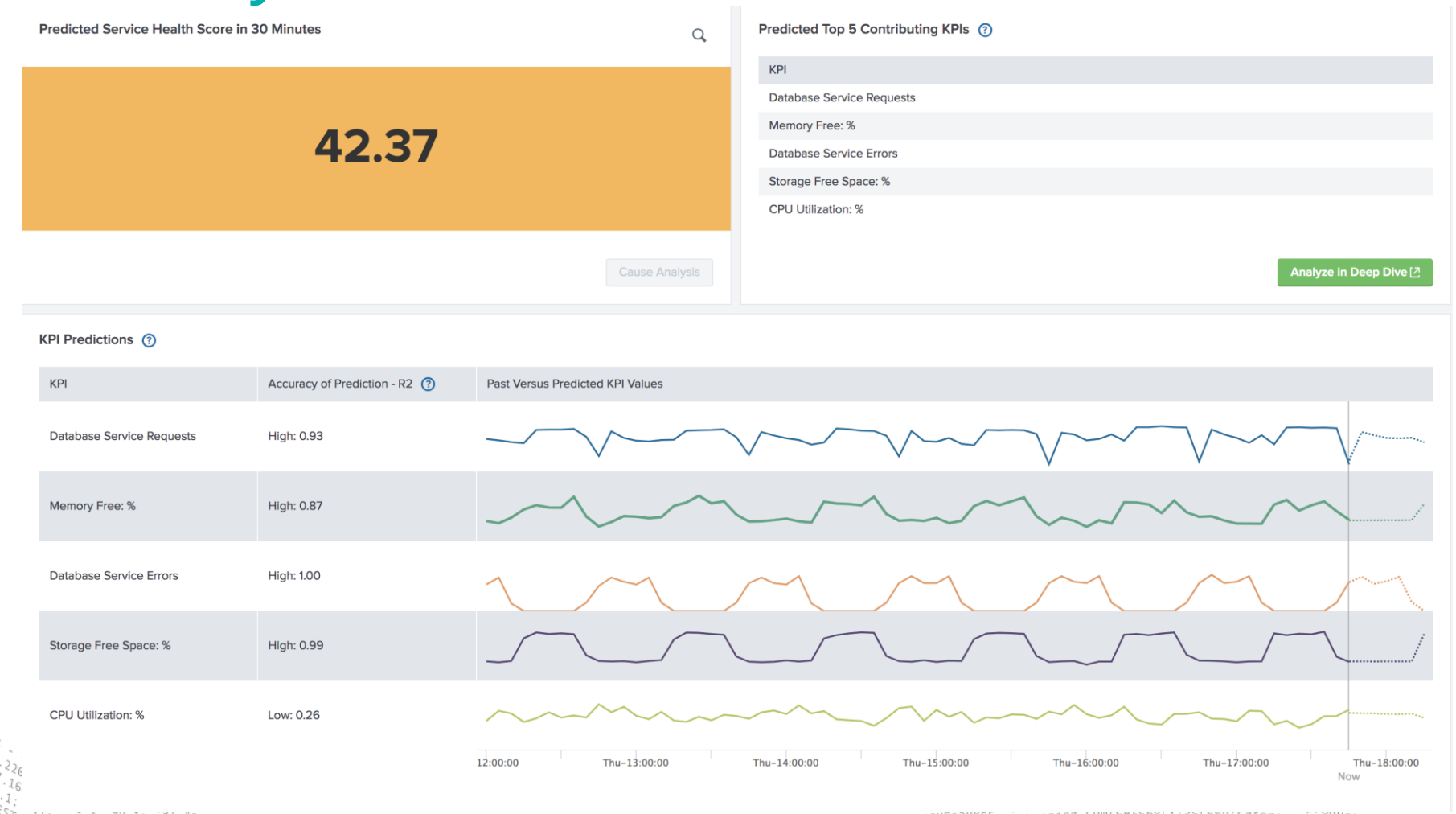


splunk> .conf18

Measuring Value

Value is in the Eye of the Beholder

Identify Root Cause

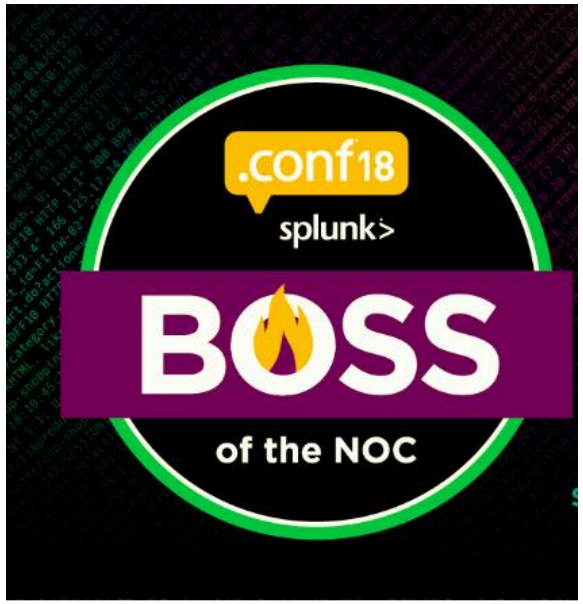


splunk> .conf18

Measuring Value

Value is in the Eye of the Beholder

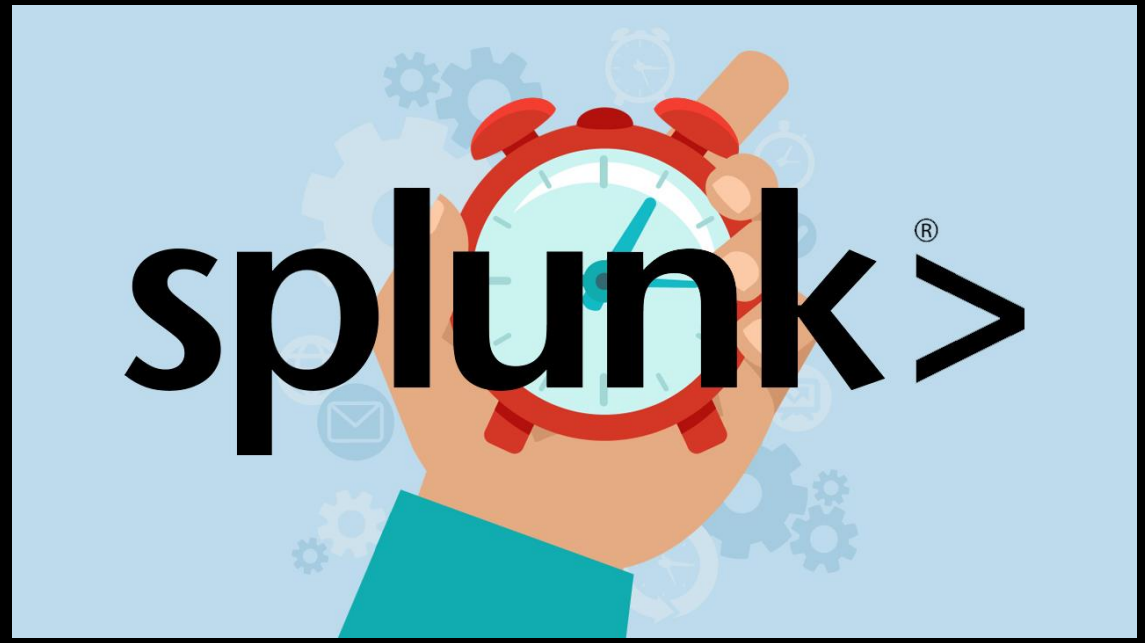
Be Better at All of the Above



Key Takeaways

At the End of the Day…

- Manage the Incident NOT the Event
- Prioritize based on Business Impact NOT Human Decision
- Fire Prevention INSTEAD of Fire Fighting



If you can **visualize it,**
if you can **dream it,**
there's some way to **do it.**

– *Walt Disney*

AZ QUOTES

splunk> .conf18