Explode your Splunk ITSI Footprint

Automate your Service Decomps!

John Lim
Systems Engineer | Cox Automotive, Inc

Brian Brake
Sr. Systems Engineer | Cox Automotive, Inc

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

splunk> .conf20

Agenda

1) Introduction to Cox Automotive
About us, and what are we trying to solve?

2) Designing Model Service Trees
How did we start building the automation framework?

3) Expanding your ITSI Automation Workflow
Thinking about your customers!

4) SNOW-ify!
Tying your workflow to a SNOW form.

5) What have we learned?
Takeaways from our experience with Decomp Automation.

Introduction to Cox Automotive

Our Splunk footprint

splunk>
turn data into doing™

2.6 B

Daily Unique Event Count

7 K

Total Users

30

Unique Business Units

9 TB

Daily License Usage

splunk> **.conf20**

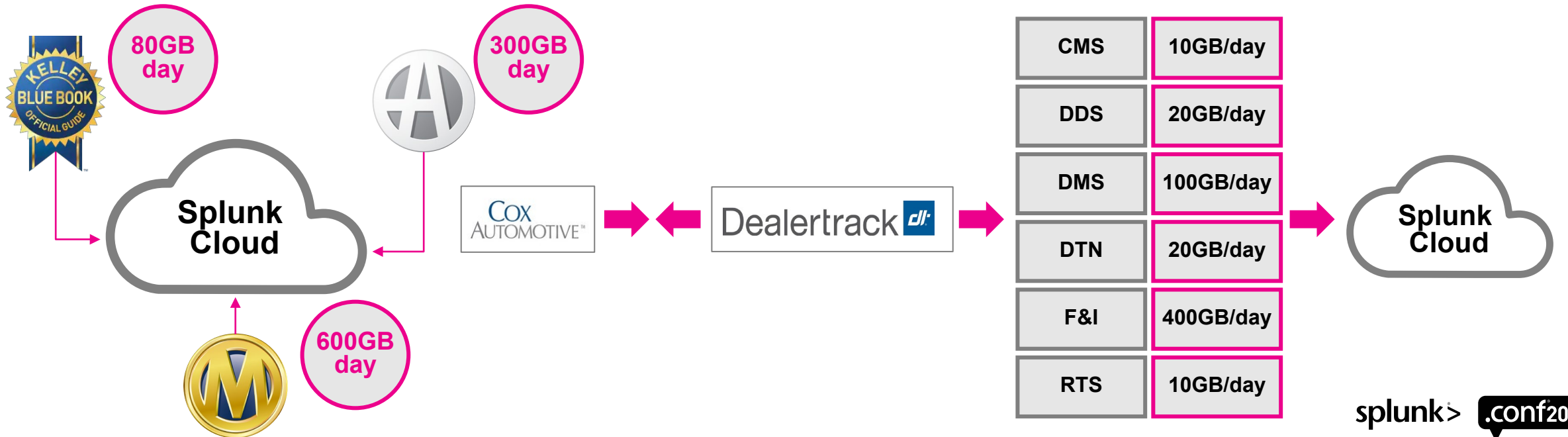# A Quick History–Cox Automotive and Splunk

2014 Cox Auto Splunk Team was formed

2015 Integrate Big 3 Cox Auto Splunk On-Prem Deployments

2016 Dealertrack Conglomerate Acquisition

2018 Integrate DealerTrack Inherited Deployments

2019 All Cox Auto Data in Splunk Cloud

80GB day

300GB day

Splunk Cloud

600GB day

Cox AUTOMOTIVE™

Dealertrack

CMS	10GB/day
DDS	20GB/day
DMS	100GB/day
DTN	20GB/day
F&I	400GB/day
RTS	10GB/day

Splunk Cloud

splunk> .conf20

Implementing ITSI – Scaling Challenge

Resource Constraints

Cox Auto's Splunk Team has 4 engineers.

Small team handles Splunk ops, engineering, and enablement.

Team does not have data ownership and insights into customer's KPI's.

Service Decomps are time consuming and require repeated engagements.

Customer Requirements

There are hundreds of ITSI use cases in Cox Automotive.

Different developers are responsible for different pieces of the application.

Developers have a very rudimentary knowledge of Splunk.

Architectural diagrams are not readily available.

splunk> .conf20
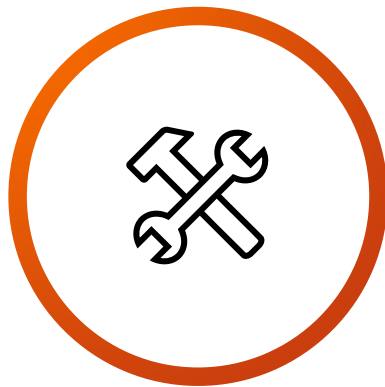
Attacking the Problem

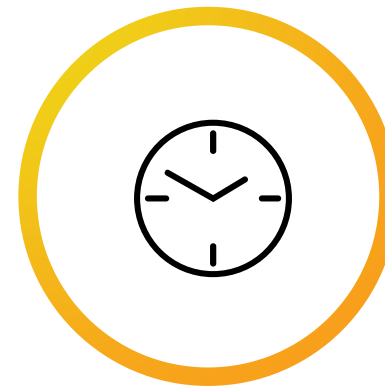How can we scale?

Design Repeatable Models

Re-usable Model
Service Tree,
Decomposition Tree,
Standardize Data
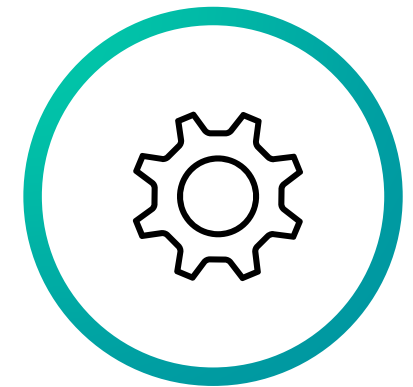Collection
can we scale?

Create an ITSI Automation Flow

Easy for user
to follow along

SNOW-ify

Further automate the
process by
embedding the
automation flow into a
SNOW form

Continuous Improvement

Leverage SNOW's
capabilities to integrate ITSI
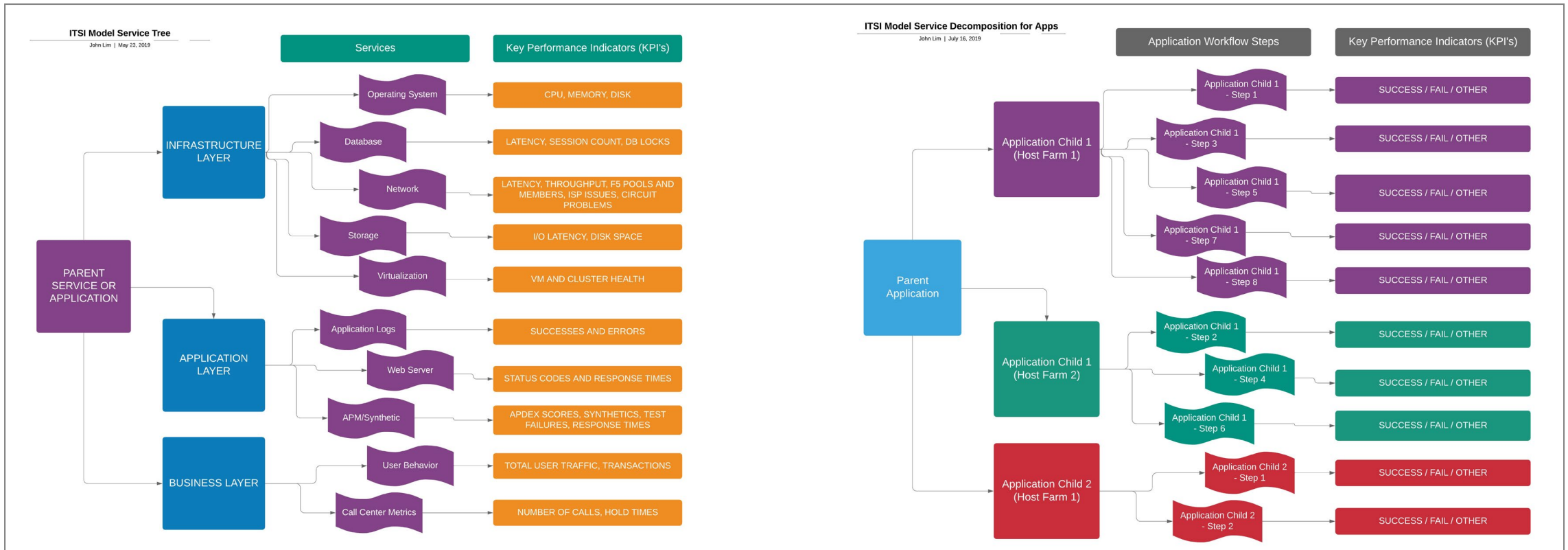with Incident, Change, and
Problem Mgmt

splunk> .conf20

Designing Model Service Trees

How did we start building the automation framework?

ITSI Model Trees

Visualize the decomp for your users

Expanding your ITSI Automation Workflow

Service onboarding phases

The ITSI Onboarding Phases

A user driven interaction
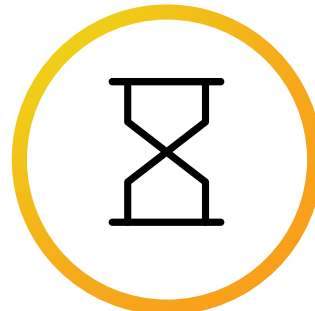
Prerequisites

Opening SNOW ticket, focuses on customer education and data compliance requirements.
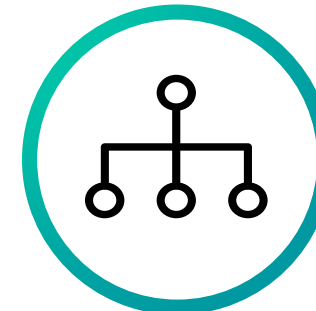
KPI Discovery

Simple workflow design for glass table, Pre-Selected and Custom KPI identification.
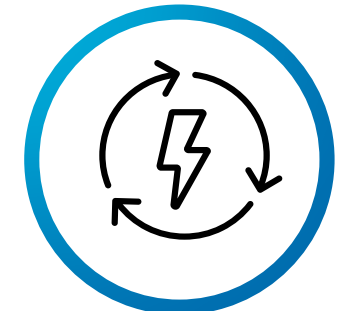
Service Decomp Review

Once user has filled in all requirements, a much shorter Service Decomp Review can occur.

KPI Development

Actual build of the KPI's in ITSI. This can be done either by Splunk Admins or handed off to Professional Services with all the requirements.
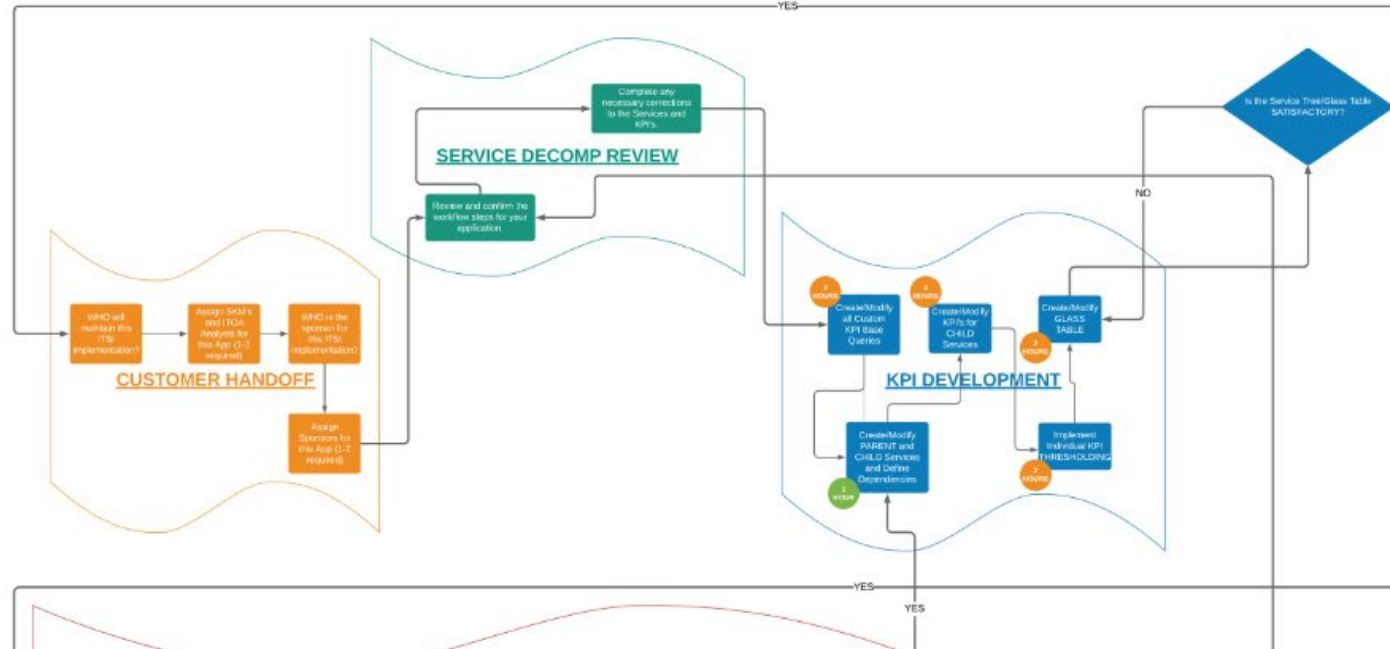
Event Management and Continuous Improvement
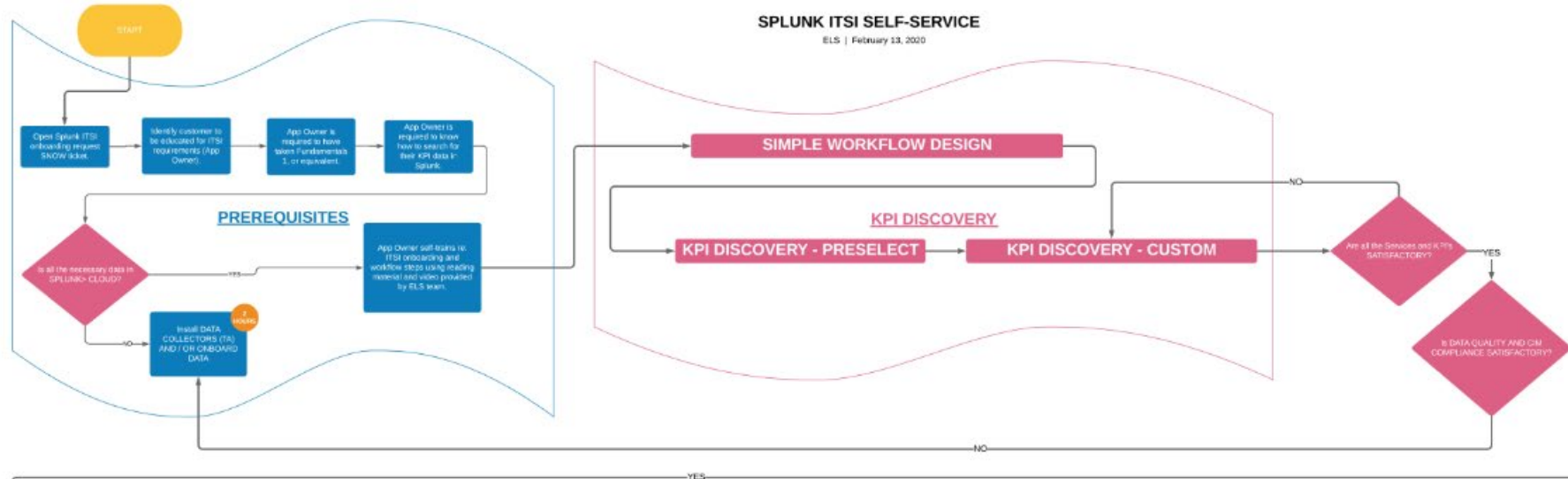
Using completed requirements to drive correlation search creation, filtering criteria, and action rules. Continue to improve via SNOW lifecycle.

splunk> .conf20

So, why do it this way?

1) Cox Auto's ITSI Onboarding Workflow is considered a federated, self-service model.

2) This ensures scalability at an enterprise level.

3) A significant amount of legwork and KPI discovery falls upon the app owner, since the app owner knows their data best.

4) Acquiring a workflow design that simulates the app at a high level (in advance!) helps both the Splunk Admin and the customer. This avoids the lengthiest part of a Service Decomp – the whiteboarding.

5) Letting the customer pre-select KPI templates and using an intake form for the custom KPI's accelerates the process further.

SPLUNK ITSI SELF-SERVICE
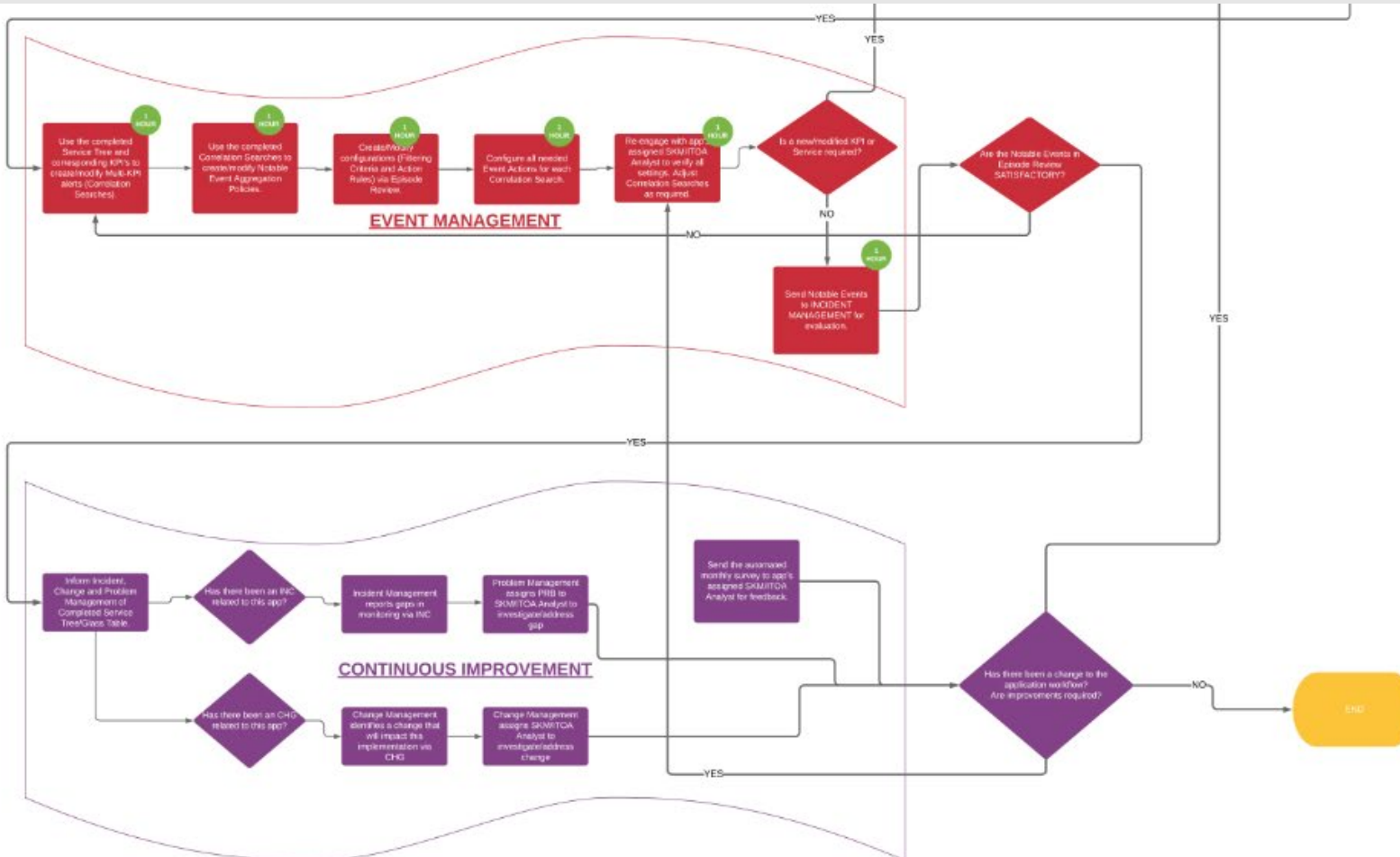
ELS | February 13, 2020

EVENT MANAGEMENT

CONTINUOUS IMPROVEMENT

Tool Integrations
APM (New Relic or AppDynamics)

(PROVIDE EXAMPLES)

KPI DISCOVERY - CUSTOM

Identify your Custom Services and KPI's that are not covered by Step #1.
Use your Simple Workflow Design image to satisfy below requirements.

A - Name of Service (i.e. Step 1 - Application Submit, Step 2 - Application Acknowledged, etc)
B - Name of KPI for your Service (i.e. Success, Failed, Unauthorized, etc)
C - Where is this data in Splunk or logging? Provide a Splunk search string that identifies this KPI.
D - Proposed Thresholds for each KPI (i.e. Static (i.e. Critical >5, High >3, Low 0-2) for Failure)
E - Weight or Criticality of this Service to your Application (static score of 5 (moderate) - 10 (very important))

Repeat process until all Custom Services and KPI's have been identified. There can be up to 3 KPI's for each service. If anything is missing, repeat process.
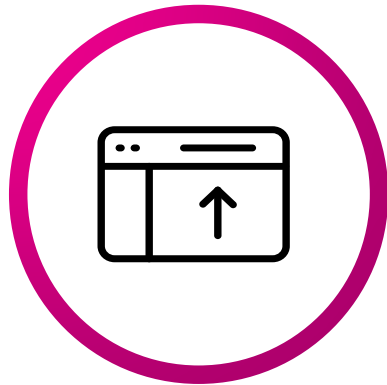
(PROVIDE EXAMPLES)

SNOW-ify!

Tying your workflow to a SNOW form

If you have SNOW, use it!

If your userbase is accustomed to SNOW intake forms, this integration is a game-changer.

Work with Your SNOW Team

Most enterprises that use SNOW have a dedicated SNOW team. SNOW's intake forms are versatile, and you can have your own custom ITSI onboarding intake form.

Ask Pointed Questions
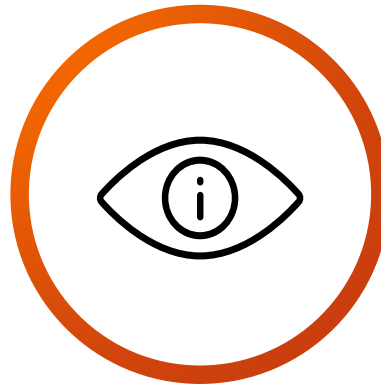
Try not to be too wordy in your SNOW form. Use supporting documents to provide necessary details.

A SNOW Ticket Allows for Tracking and Commenting

When a form is submitted, both the Splunk Admin and the customer can communicate regarding the requirements without the need for a meeting.

splunk> .conf20

* Opened on behalf of this user

🛈 John Lim ✕ ▾

* Please select a Splunk Service:

ITSI Onboarding ▾

* Are you the data owner of this application?

-- None -- ▾

* What business unit are you with?

* Who is the SME for this application?

▾

* What is the name of your application?

* Who is the primary and backup Data owner for your application?

* Do you have a primary/backup Splunk Knowledge Manager?

-- None -- ▾

* Does your application ingest logs into Splunk today?

-- None -- ▾

* Please preselect available out-of-box Key Performance Indicators
that apply to you:

- [ ] Web Server
- [ ] Application Server
- [ ] Database
- [ ] OS
- [ ] Load Balancer (F5)
- [ ] APM

Please fill in requirements for all Custom Base KPI's

* Workflow Step

[   ]

* Service name:

[   ]
[   ]

* Splunk String

[   ]

* KPI Conditions:

[   ]

splunk> .conf20

* KPI Thresholds:

* KPI Weights:

* Describe your troubleshooting process for this 'Workflow Step'

* Who is responsible for troubleshooting this Workflow Step?

* Would you like to add another KPI?

-- None --

📎 Add attachments

Submit   🛒 Add to Cart

splunk> .conf20

What Have we Learned?

Takeaways from our experience with Decomp Automation.

Empower Users!

A guided user experience reduces ITSI onboarding friction.

Phased Onboarding Approach

This approach lets the users be involved in the process from Step 1. They will learn more about their app, along with learning how to use Splunk.

Create Supporting Documents and Guided Intake Form

Don't forget to create your supporting user documents! A guided intake form lets the users take ITSI onboarding step by step. Each piece builds towards the next, and the process is a little less overwhelming.

Continue to Evolve your Process!

Users will always have constant input regarding how the automation can be improved. Use these ideas to build a well-oiled ITSI onboarding machine.

splunk> .conf20

Thank You

Please provide feedback via the

SESSION SURVEY