Allied Irish Banks

Monitoring Payments with real time insights using Splunk and ITSI

Damien Perrem, Garvan Power

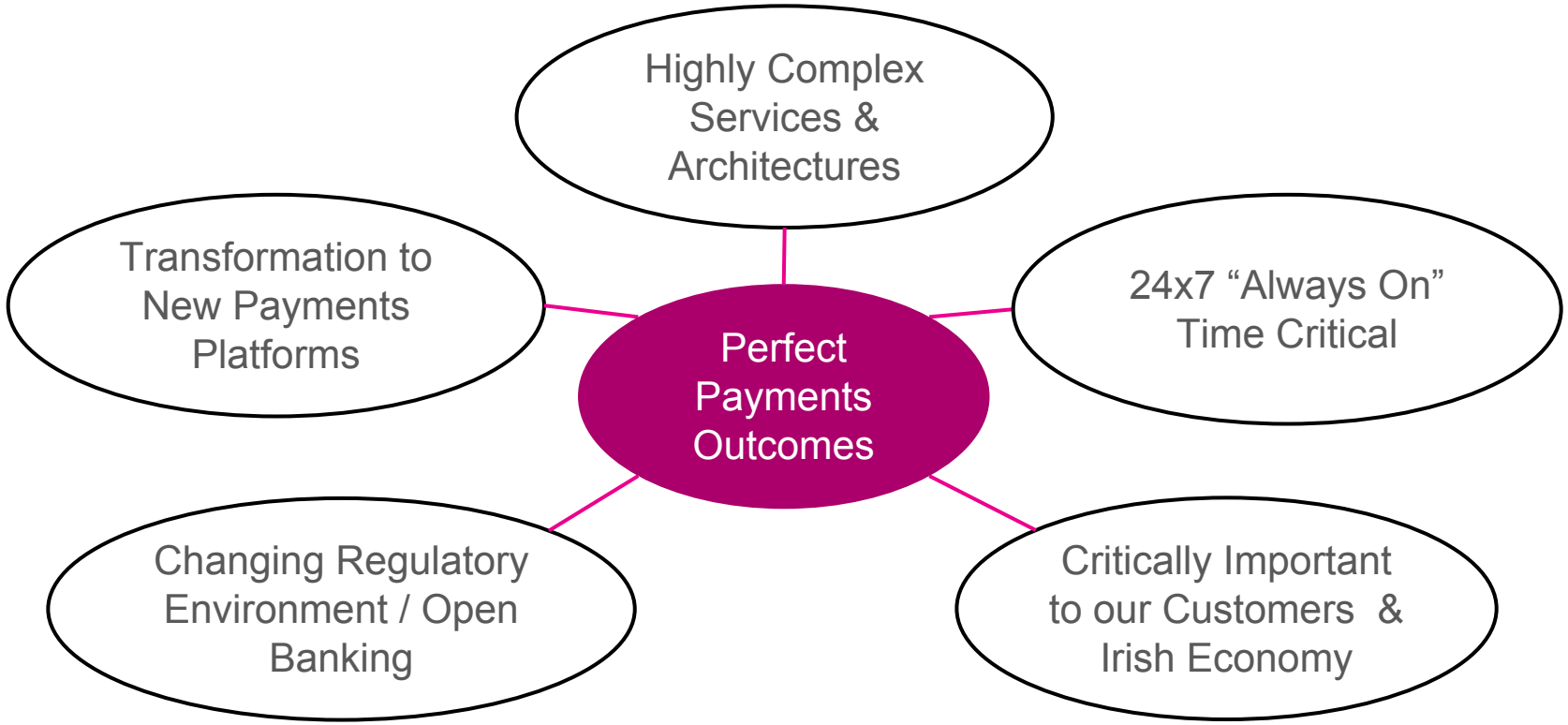
October 2019, Version 1.0

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.

Background to AIB Payments Landscape

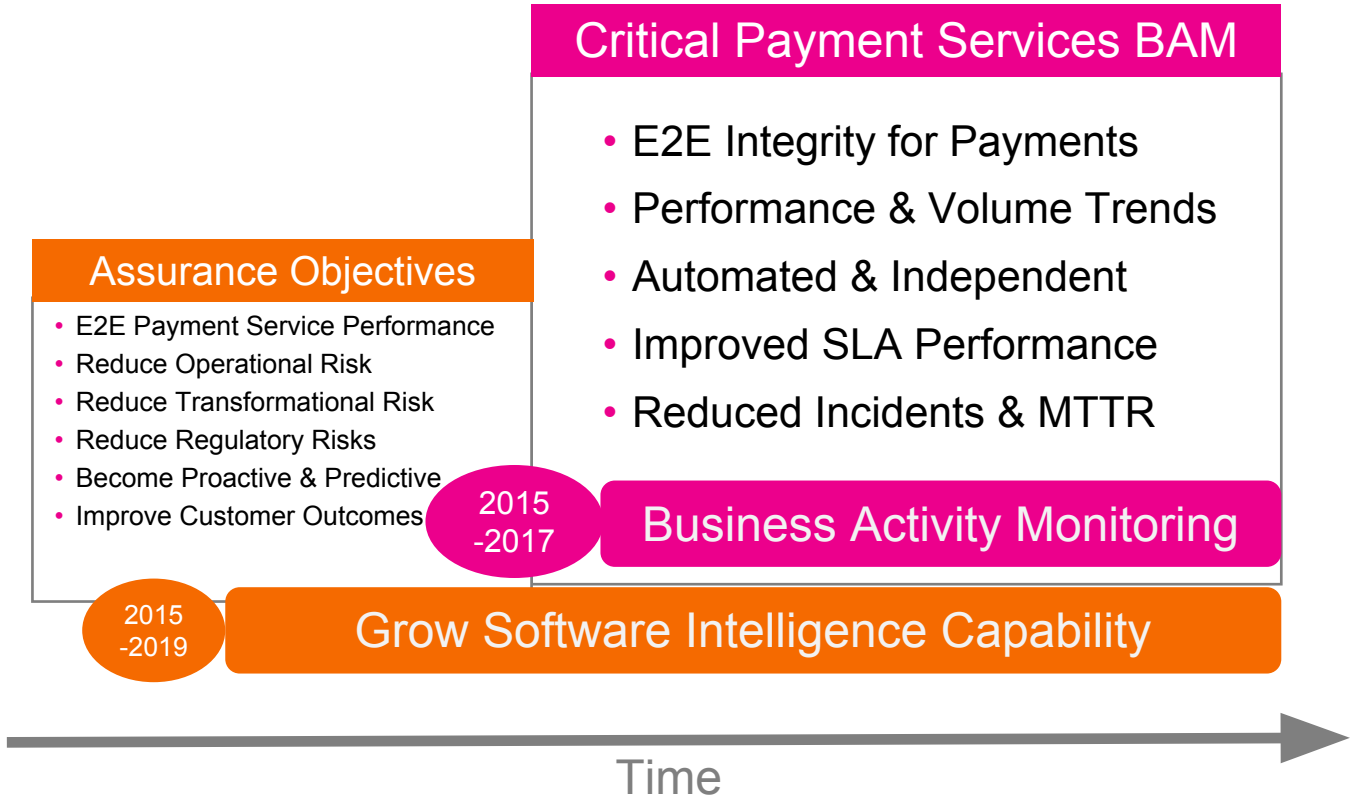


Responsible for the Assurance of Payment Services and Platforms

Payments Business Activity Monitoring

BAM!

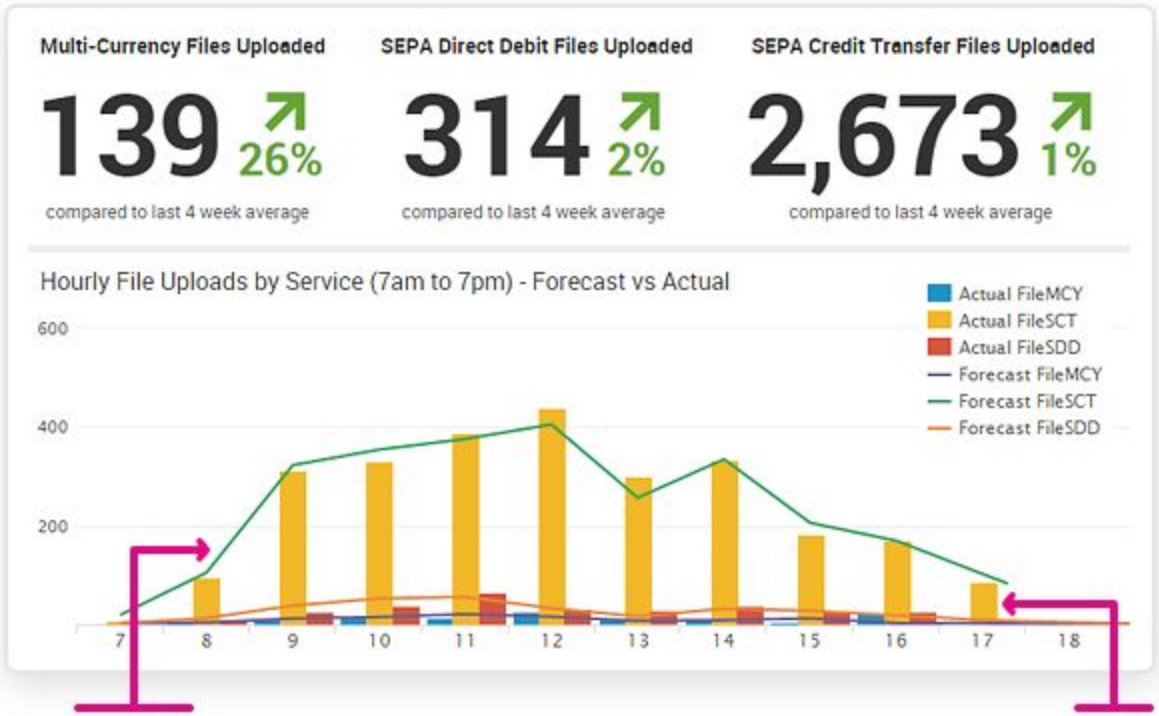
2015-2017



SERVICE INSIGHTS

Machine Learning Journey

Started Machine Learning Journey by **Predicting Hourly File** and Payments Volumes to look for Deviations from Expected Norms

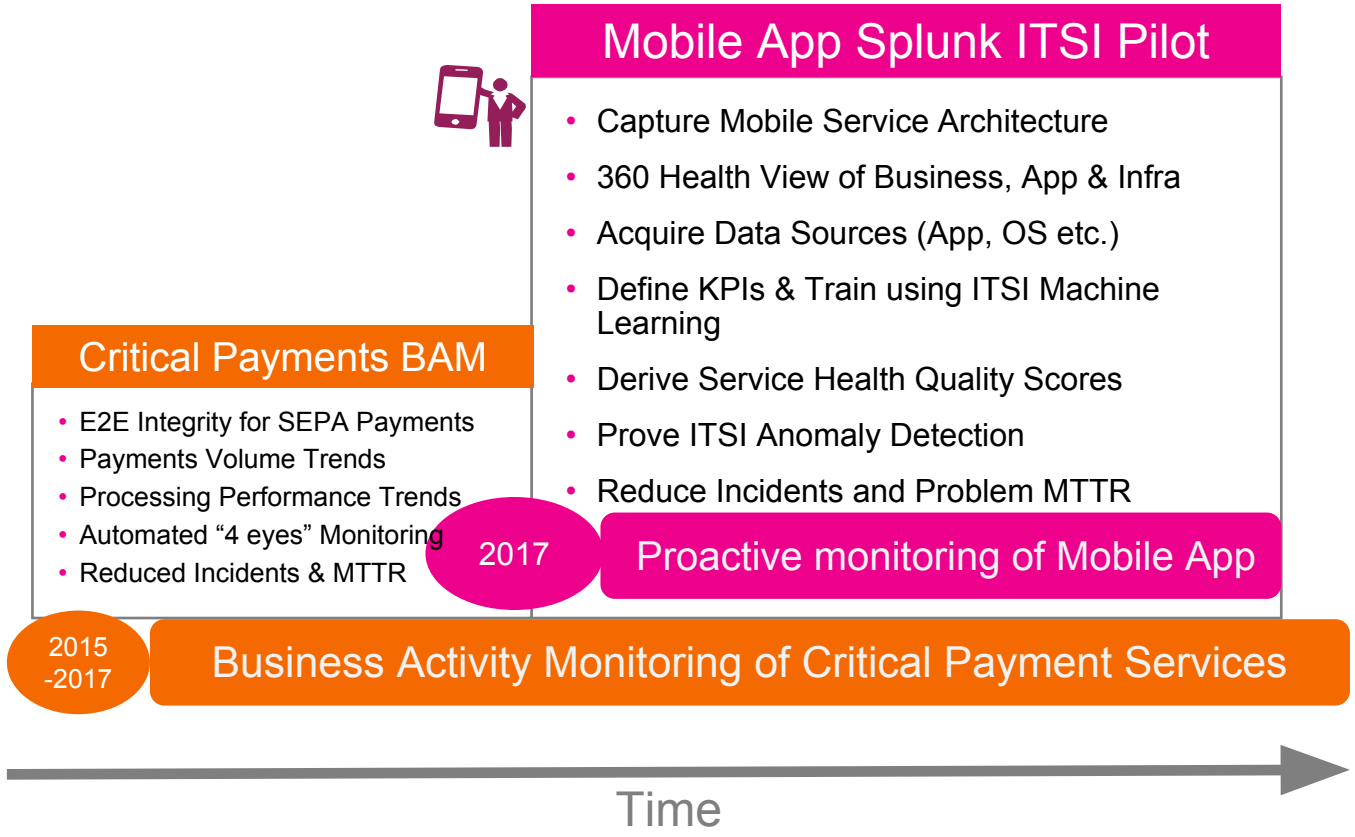


Line is Forecast Payment File Volumes

Bar is Actual File Volumes Uploaded

Splunk ITSI Machine Learning Pilot with AIB Mobile App

2017

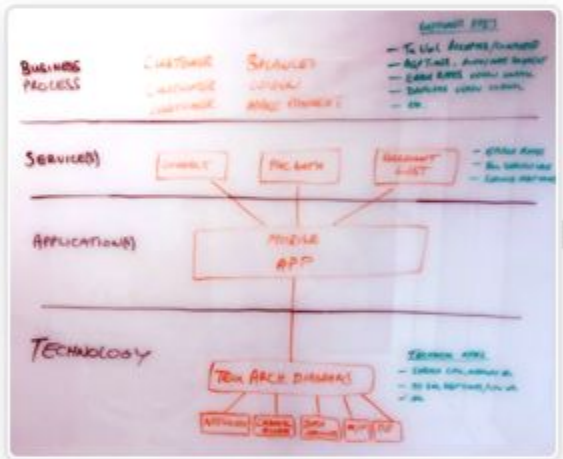


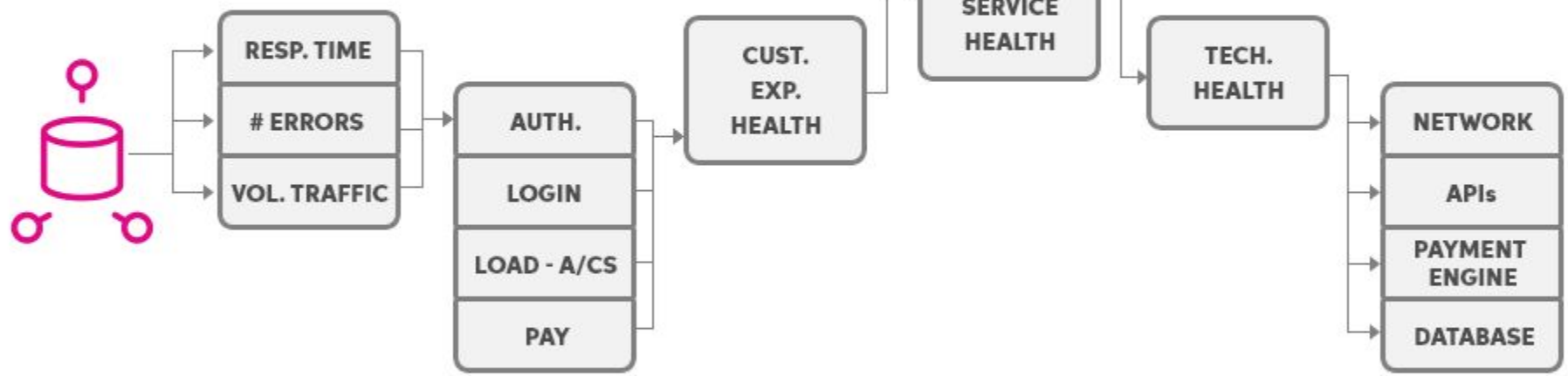
splunk> .conf19

SERVICE INSIGHTS

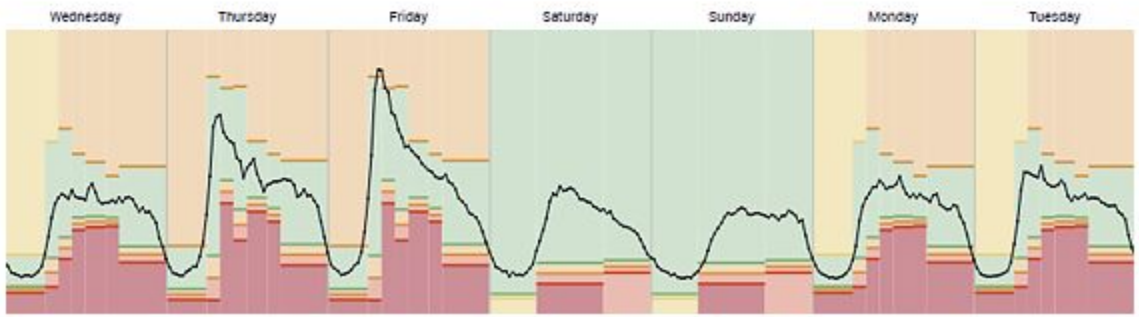
Machine Learning Pilot

Machine Learning Pilot using AIB **Mobile Payments Journey** started by Understanding Key Customer and Technical Health Indicators





Machine Learning to learn what **normal "looks like"** over few weeks



SERVICE INSIGHTS

Predictive Monitoring Of Mobile App

Machine Learning used to **predictively monitor** the **health** of the Mobile App in Real Time to improve Customer Experience

- Solution learns normal App usage and performance patterns based on historical data
- Solution calculates Service Health scores in real time based on the aggregation of numerous customer and technical health indicators
- Solution constantly monitors service health scores and alerts when slight anomalies are detected
- Benefits include reduction in incidents, faster problem resolution & improved customer outcomes

SERVICE INSIGHTS

Drill Down Capabilities

Customer Service Health "**Live Glass Table**" View

Technical Health View

Troubleshooting **Deep Dive**

SERVICE INSIGHTS

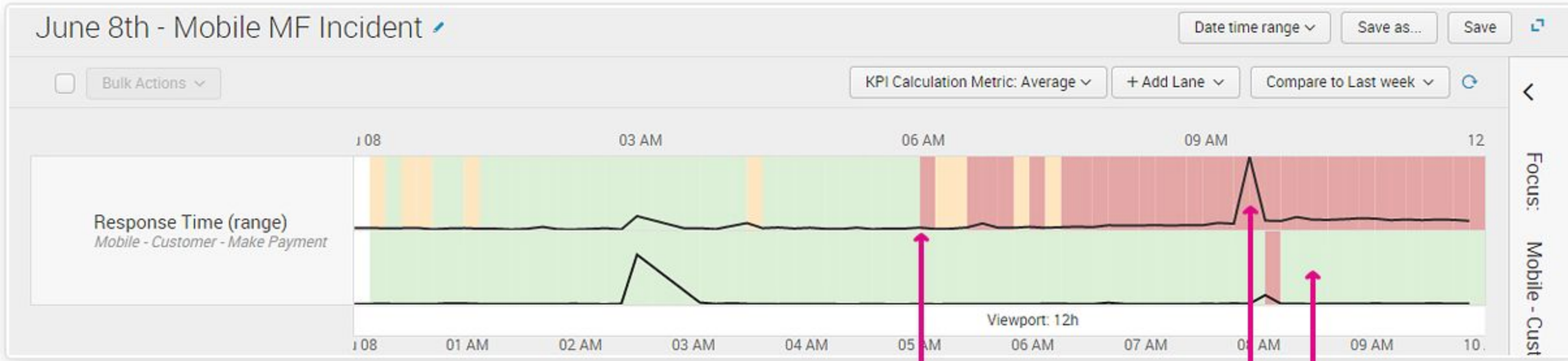
Effectiveness Evaluation

Tested Solution to evaluate **Effectiveness** during a Real Incident **June 8th** 2017 **Mobile Outage** at 9:08am

SERVICE INSIGHTS

Anomaly Detected

Outage 9:08am, **Machine Learning** detected Anomaly from 6am / Proved the **Potential** to **Prevent Incidents**



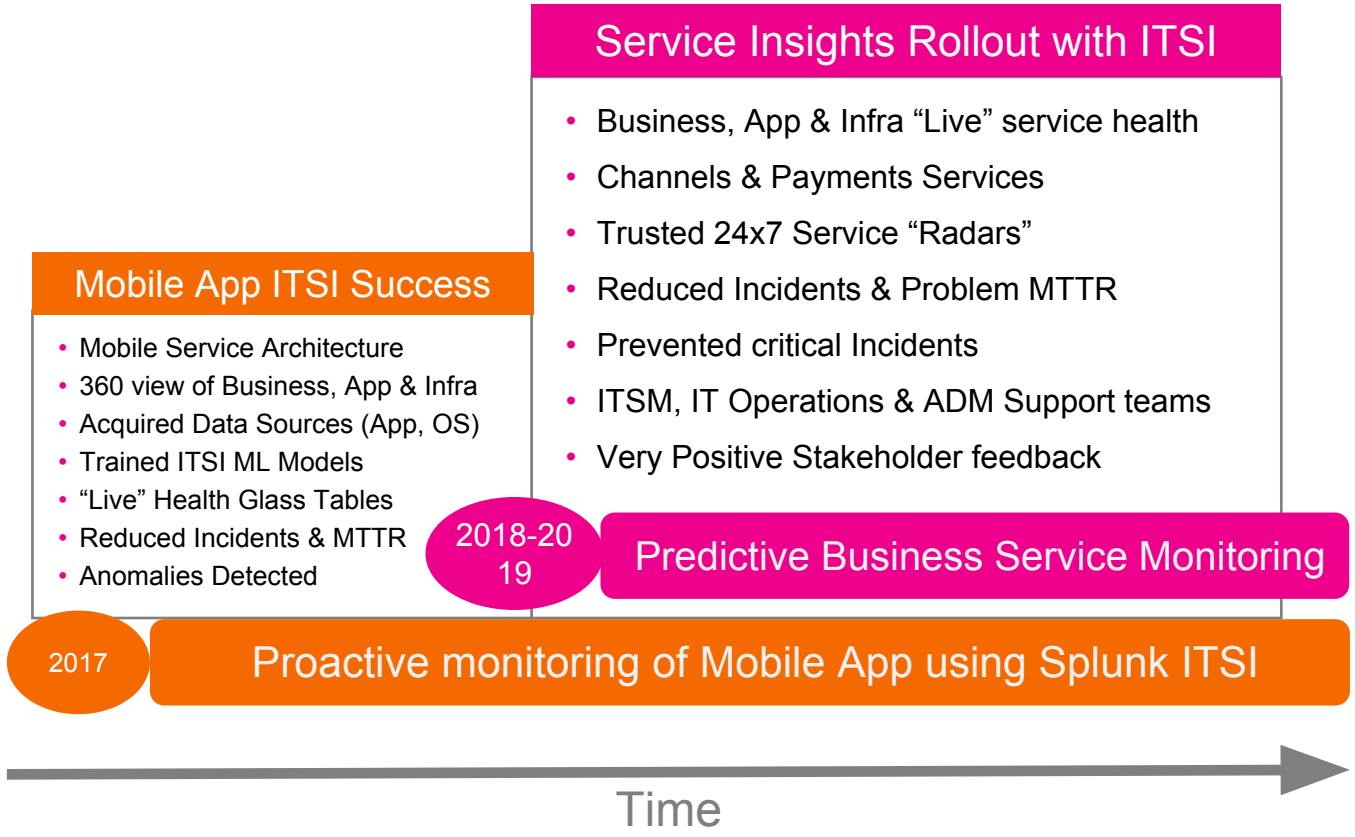
Proposed Response Time KPI detected anomaly **3.5 hours ahead** of the Incident

Incident Time

Compare to 1 week previous

Service Insights Rollout

2018-2019

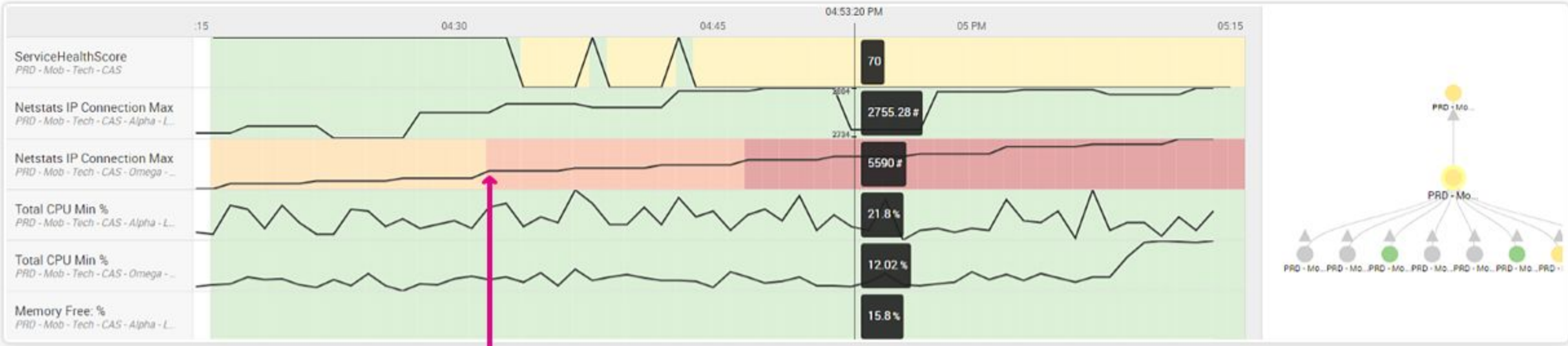


SERVICE INSIGHTS

Outage Prevention Example

Example of how Service Insights **Prevented a serious Channels Outage**

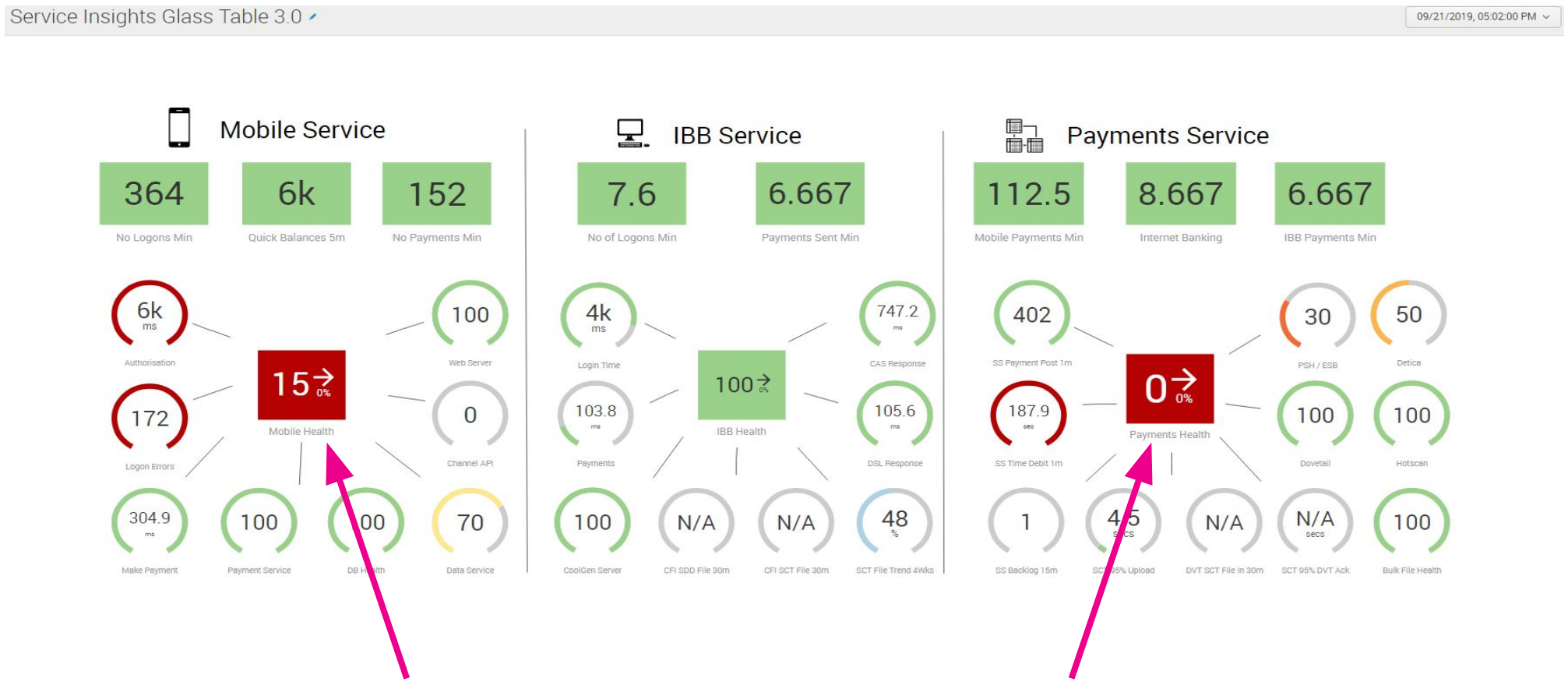
Just **one of many examples** with Mobile, Channels & Payments



Detects issue on Channels Server at 4:30pm allowing **issue to be resolved BEFORE** any customer impact

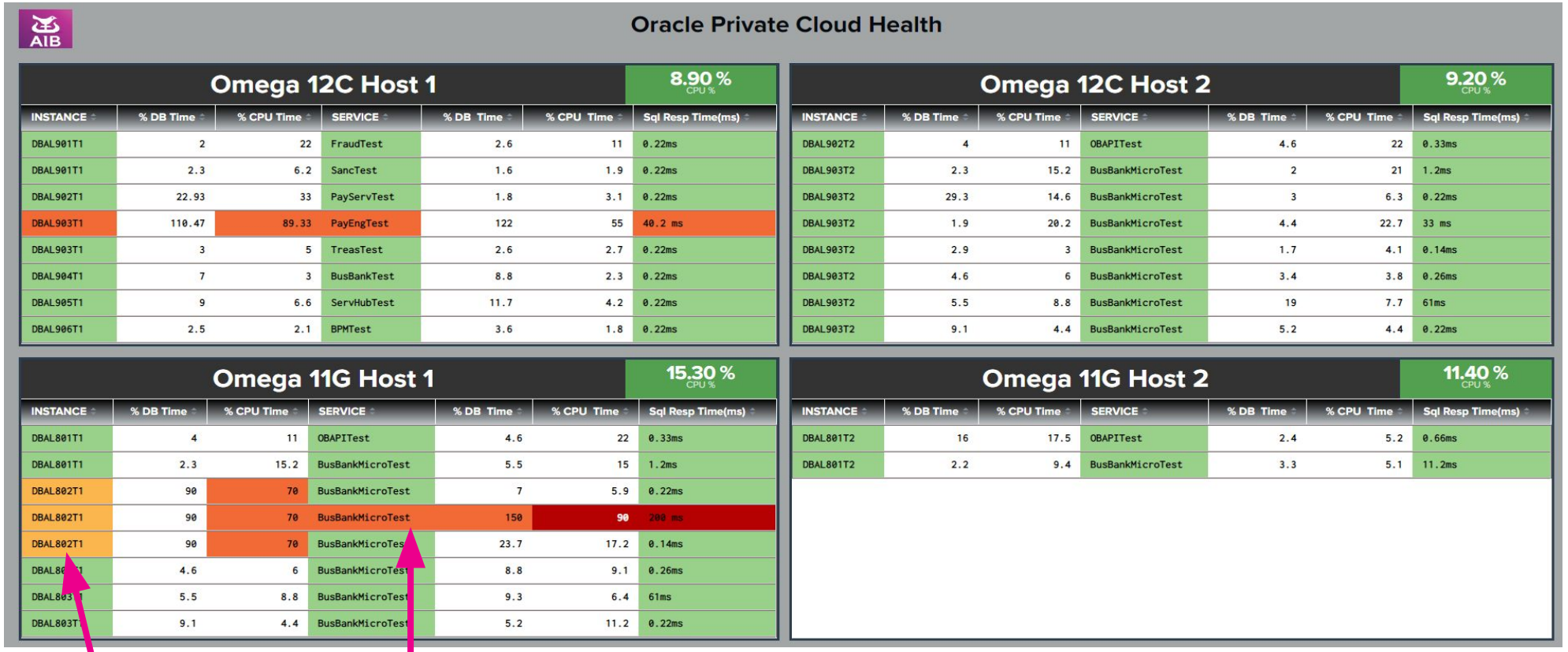
Without the solution, **serious OUTAGE** later that evening which would have taken HOURS to resolve

Protect – Change Root Cause in Minutes



Change causes service impacts leading to reduced health scores and Alerts to Operations teams

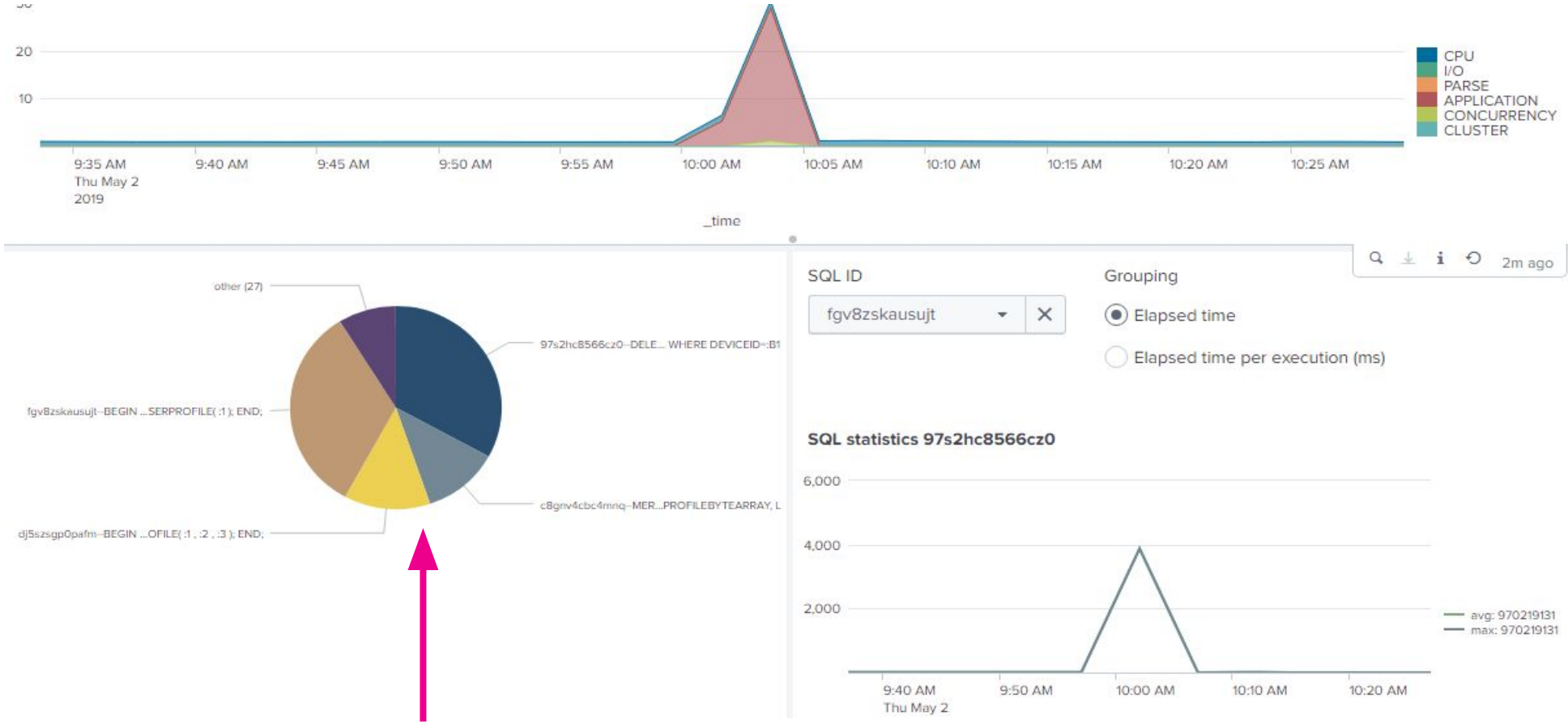
Monitoring Oracle Private Cloud Hosts, Databases & Services Performance using Splunk and ITSI for Dynamic Services



Database and Service performance metrics and health scores monitored in near real time (Test Data for illustration only).

splunk> .conf19

Oracle Service Performance Metrics Captured in Near Real Time for All Hosts, Databases and Services across Oracle Private Cloud

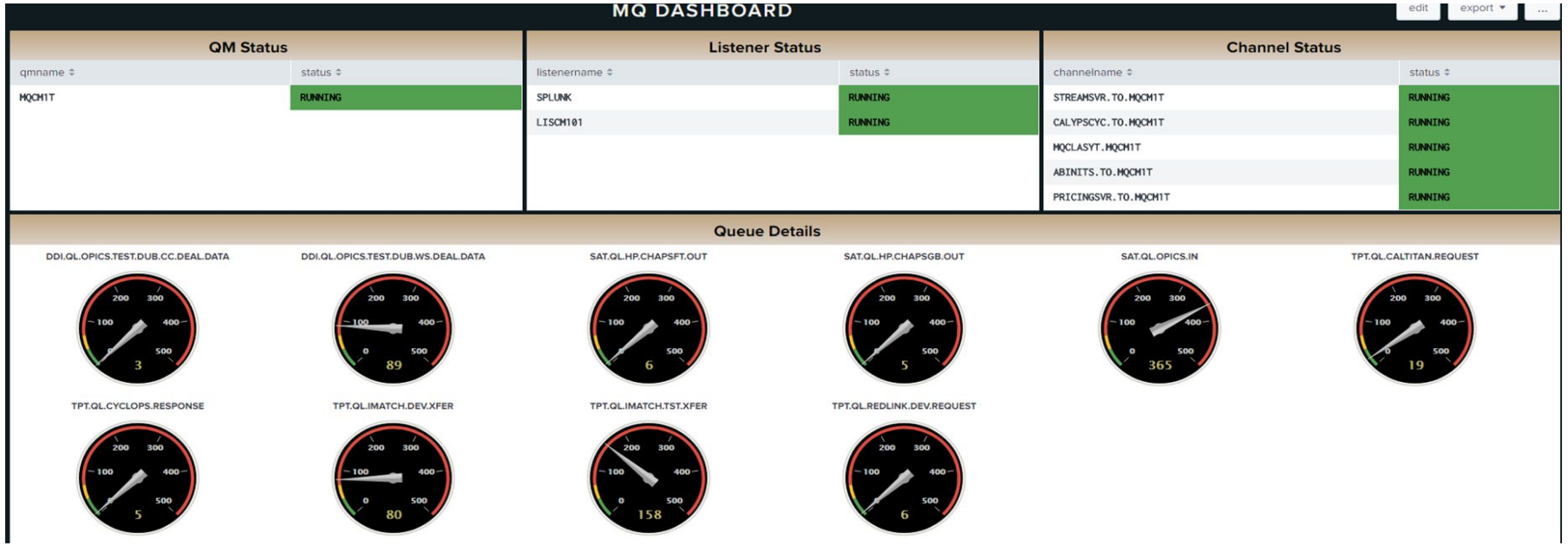


TOP SQL statements running in the Database to find out which SQL statement is consuming most time

splunk> .conf19

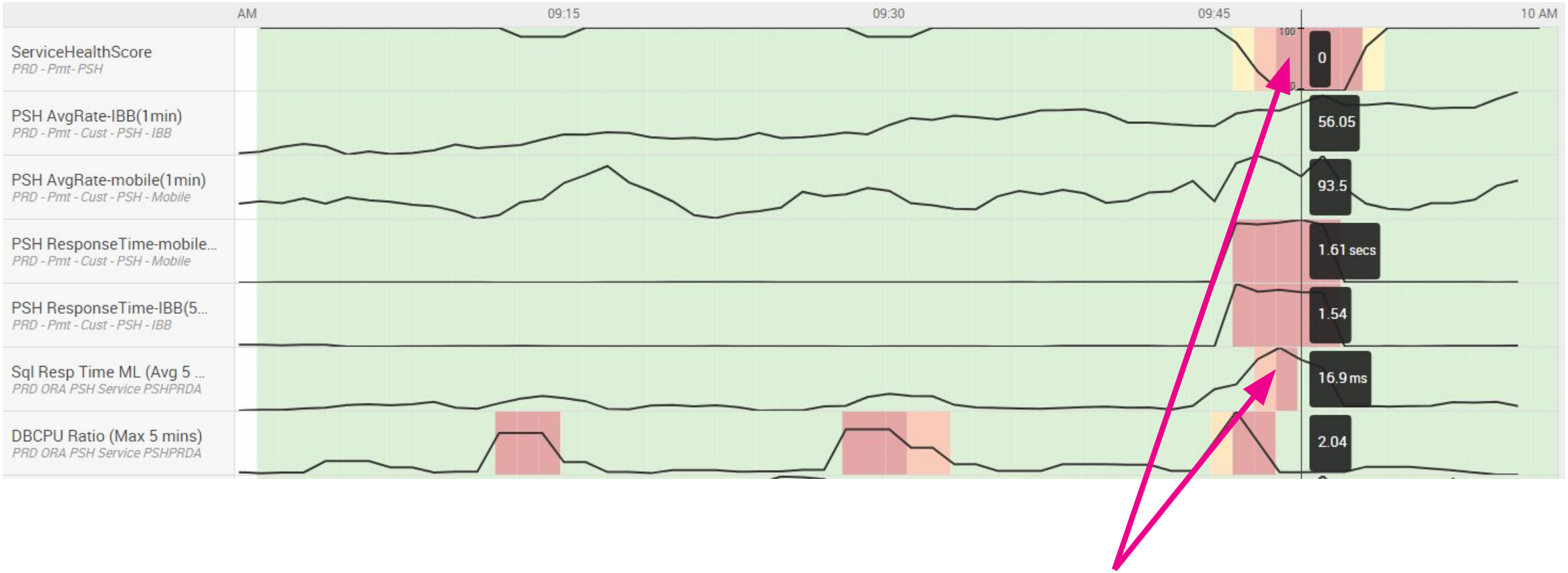
AIB Splunk MQ App

Collect MQ Queue Mgr Statistics



1) Based on Splunk Modular input polling Queue Manager at predefined interval to get two types of data
2) Basic Data: QM Status, Listener Status. Channel Status and Current queue Depth
3) Statistics Data: System Accounting & Statistics queue. It includes gets, puts,puts failed,get bytes,put bytes
4) Can be configured to run inbuilt MQ commands like runqmsc and amqsevt etc.

Protect – DB Root Cause in Minutes



Machine Learned Oracle SQL Response Time KPI Indicating Problem started in the Database

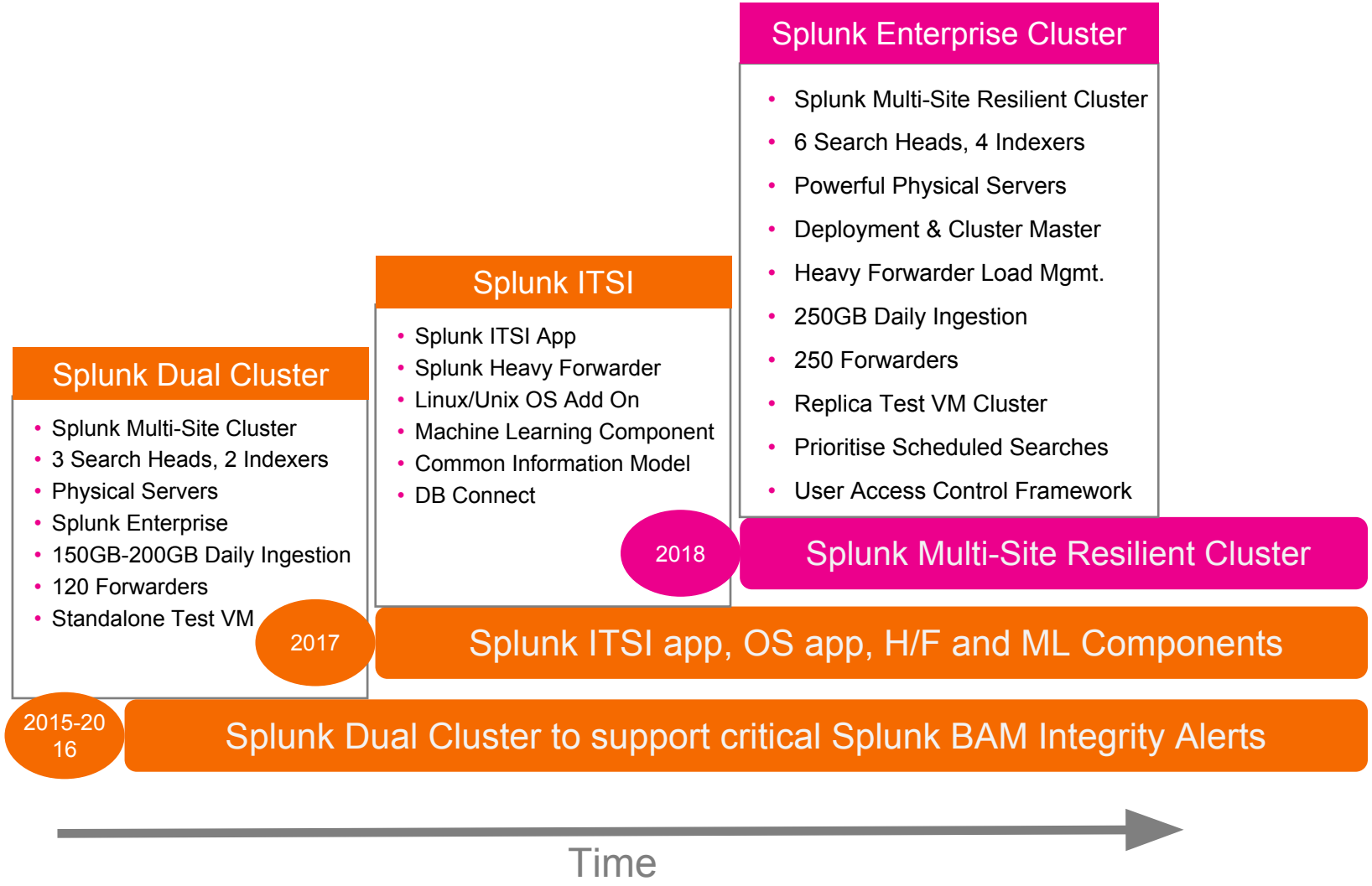
AIB ITSI Journey

Positive outcomes

- ITSI Background
  - >600 services, >150 entities, >1000 KPIS, >20 Glass Tables
  - Critical Services (Mobile, Business Banking, Payments Services etc.)
  - Glass Tables for Service, App & Infra teams
  - “Trusted” for health scores and alerts
- Adopted Good Practice Guidelines
  - Thresholding - Keep it Simple
    - Static where possible, M/L for Volumes
  - Base Searches for multiple KPIs
  - Agree what Critical really means
- Challenges Faced
  - Test data does not reflect production
  - Challenge for training M/L algorithms
  - KPI custom searches impacting performance
  - Filter KPIs to those that really matter
  - Tune prior to rollout to minimise false alerts
- Lessons Learned
  - Use Anomaly Detection only where needed
  - M/L against production data, controls needed
  - KPI weighting biased towards business KPIs
  - Optimise using Base searches
  - Get Buy In, manage data ownership, access

AIB Splunk Infrastructure

From Standalone VM to Resilient Enterprise Cluster



AIB Splunk Implementation

Background & inputs

- Splunk Critical Monitoring Engine
  - High volume of scheduled searches
  - Highly complex frequent correlation searches across multiple indexes – time critical
  - Payment volumes are highly seasonal (e.g. Month End) so trending is tricky
  - Schedule searches based on time and file receipt (event based and not time based)
  - Complex alerting, dedup and throttling requirements
  - Ability to orchestrate Splunk alerts and resolution tasks with external systems

- AIB Points of Interest
  - Splunk COE tunes H/W and SPL
  - Optimised SPL using Stats command and summary indexes
  - Summary indexes with hourly volumes by product for historical trend analysis
  - Alert schedules based on file receipt or event triggered
  - LOGM action with GUI to offer rich alerting and throttling functionality
  - Workflow App to generate/orchestrate Splunk SPL alerts with integration to external scripts / stored procedures

Search Head Cluster

Design & optimization

- 6 physicals across 2 Data Centers
  - 1 Virtual Server on VMWare
  - F5 Load Balancing
  - VM Captain – No Ad-Hoc Search
    - No users can log into captain
    - Allows 6 physicals to run all schedules
    - VM adds extra layer of redundancy
    - Splunk can operate on 40% of capacity

- Over 1K+ unique schedules per hour
  - 25K+ scheduled searches per hour
    - 7 to 10 schedules per second
    - 0% skipped. 0% deferred.
- Optimized for Scheduled Searches
  - All tuning changes deployed as config within custom Tuning TA
  - Search head captain delegates only and does NOT run schedules
  - No priority given to ad-hoc searches
  - Schedules get 100% priority within concurrency (max_searches_perc=100)

Index Cluster

Design & optimization

- 4 physicals across 2 Data Centers
  - Powerful physical servers
  - 128 GB RAM, 64 cores
  - 10 GB network fiber
  - Red Hat 7
  - Local Solid State Drives
- Data Replication design
  - Live Copy present in each Data Center
- Search factor design
  - Allows cluster to run on only ONE server if necessary

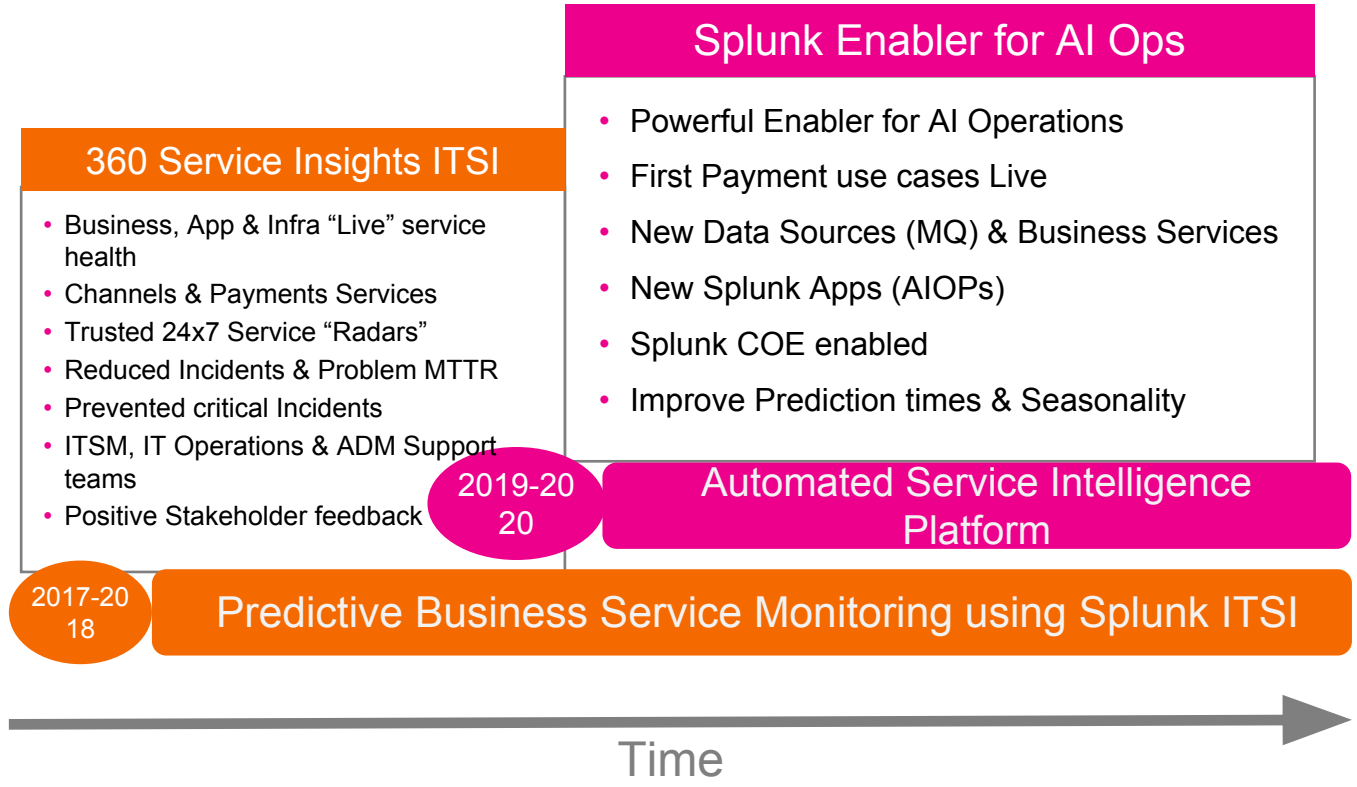
User Data Access Control

Security framework

- Strict control on what data users can see
  - AD Group to custom Splunk role mapping
    - role limits indexes that users have access to view
    - GDPR compliant
  - Customized User roles
    - can’t create schedule or any public knowledge object, restricted search window
  - Customized Power User roles
    - member of the Splunk COE
    - can create schedule searches
    - can create and publish public knowledge objects, ITSI KPIs
- Framework allows us
  - Monitor who can view data in Indexes
  - Control over management and implementation of schedules

AIB Splunk Journey

Next Steps



AIB Splunk Workflow App

Orchestrate tasks, alerts & generate SPL

- Create Workflow based on Business Need
  - Automatically triggered when certain condition meet
- Generation of SPL based on user input
  - No Knowledge of Splunk needed to generate SPL
- User creation of conditional steps
  - Define the inter step dependency as well as branching of steps based on condition
- Creation of scheduled saved searches by just a button click
  - App will generate SPL, create a saved search and schedule it
- Manage workflow processing
  - App user will be able to create, update and delete workflow and steps from Splunk UI

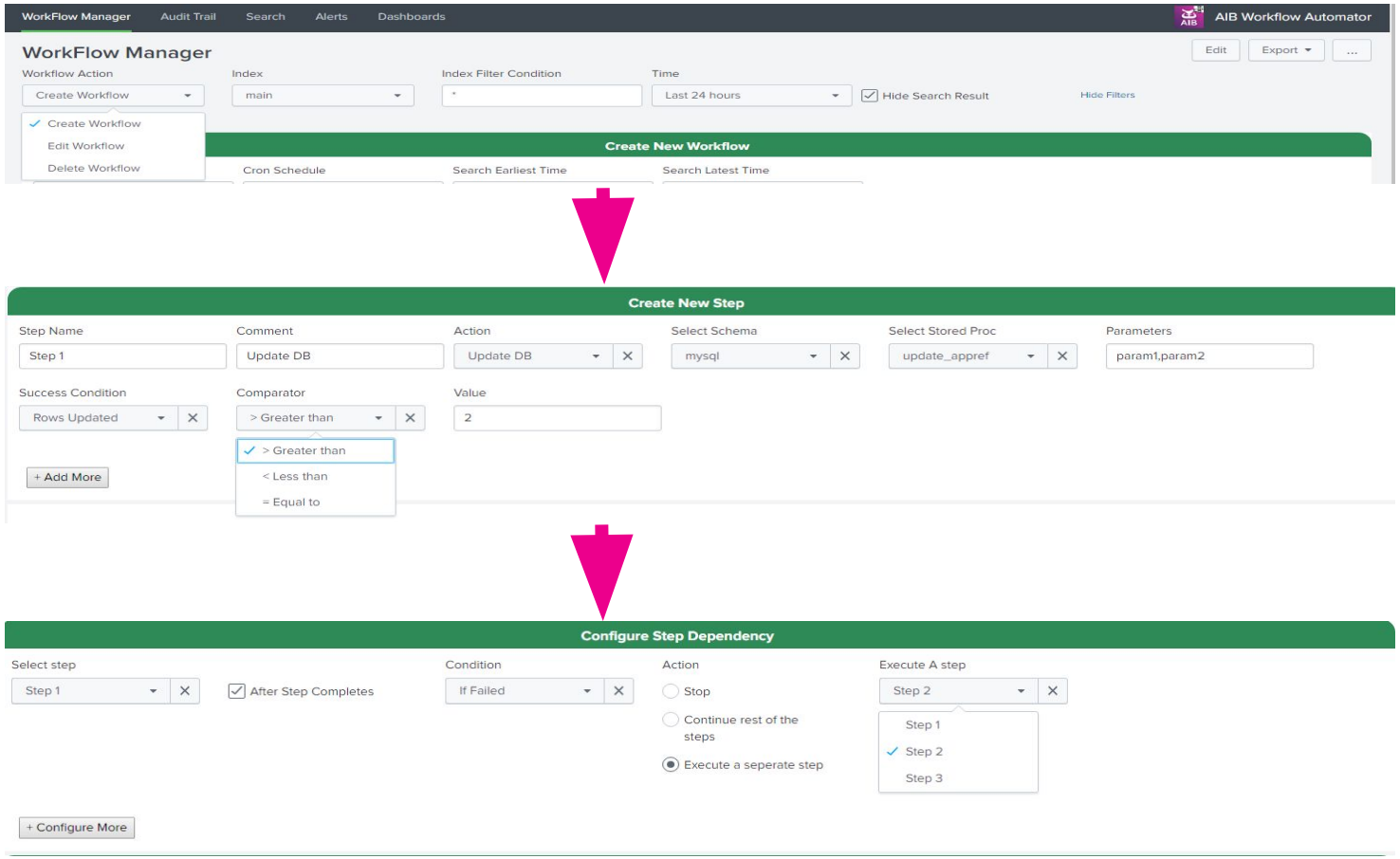
AIB Splunk Workflow App & SPL Generation

Custom Splunk UI to manage workflow

Workflow creation screen

Workflow adding steps

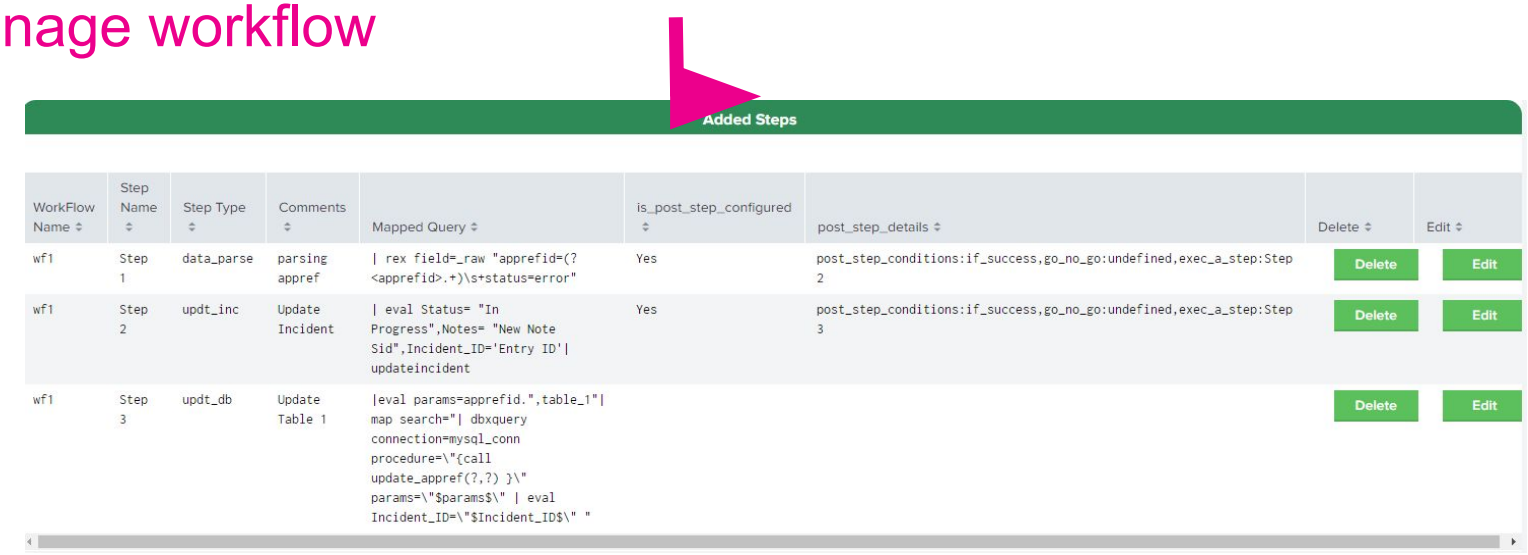
Screen to create step branching



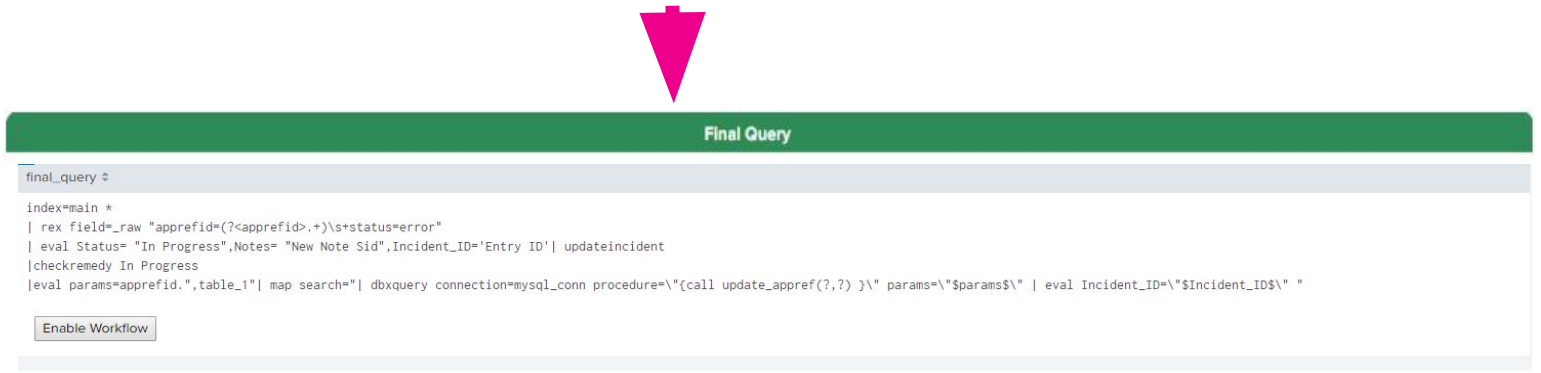
AIB Splunk Workflow App & SPL Generation

Custom Splunk UI to manage workflow

Screen to show the added steps , their dependencies and the generated SPL



Screen to show final generated query and workflow enablement button



AIB Splunk Operating Model

Splunk COE

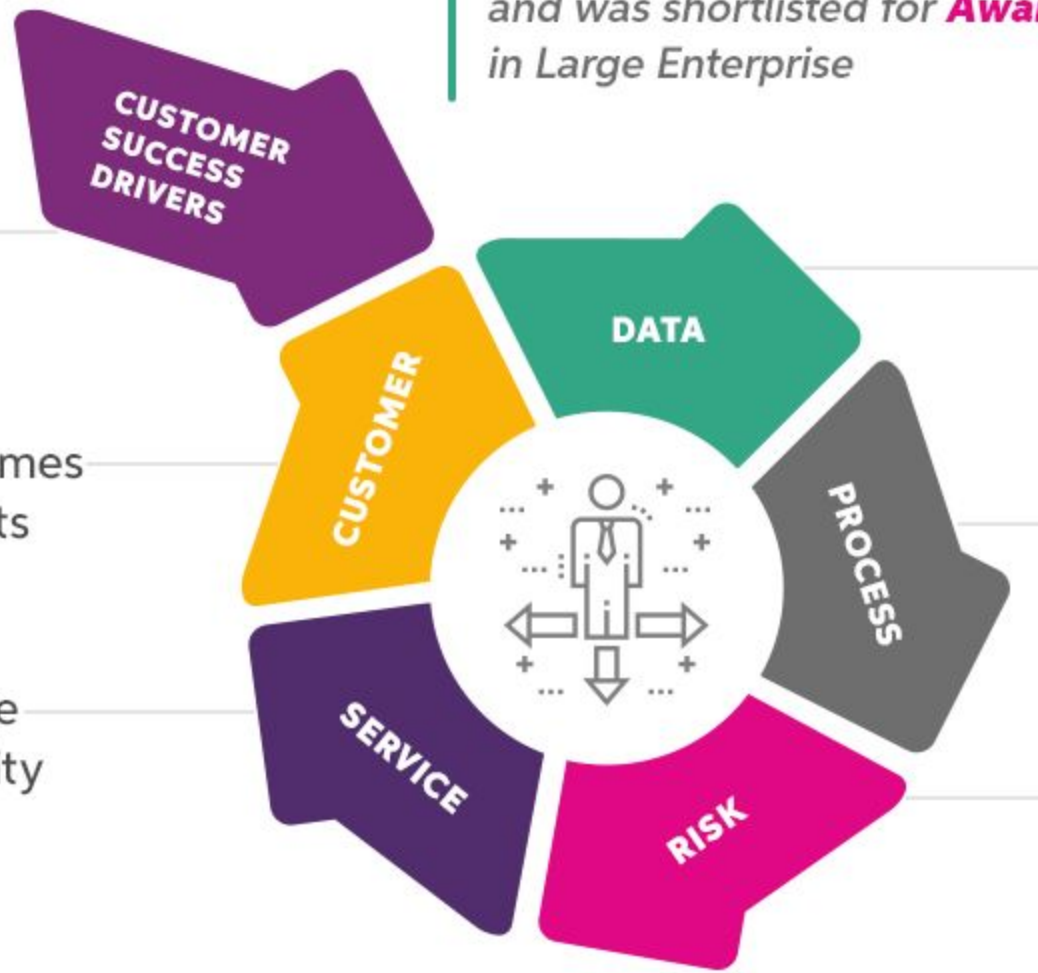
- Splunk Dev COE established (x 4)
  - Support ADM teams with Glass Tables
  - Define Standards & QA
  - ITSI requires different skills to core Splunk
- Splunk Infra Support team (x 2)
  - 1 Architect level
  - Middleware Support Background

- Lessons Learned
  - Deliver value fast, get early wins
  - Focus on business value, not just IT
  - Collaboration is Key, “Win Win” for all
  - Control data access
  - Gather stats (Incidents, MTTR) to prove value
  - Maximize Splunk value visibility with Big Screens
  - Continuously sell benefits to senior stakeholders

SERVICE INSIGHTS

Benefits Realised

*AIB Service Insights Platform is a **leader** among **Global Banks** and was shortlisted for **Award** for **Best Application of AI** in Large Enterprise*



↑ Continual Improvement

↑ Customer Outcomes
Customer Insights

↑ SLA Performance
Real Time Visibility

↑ Capacity Planning
360 Data Insights

↓ Incidents Volumes
Incident Impacts
Change Impacts

↓ Operational Risks
Transformational Risks

WE BACK BELIEF