# 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.

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

splunk> .config

### **Background to AIB Payments Landscape**



**Responsible for the Assurance of Payment Services and Platforms** 



Payments<br/>Business<br/>Activity<br/>MonitoringBAM!2015-2017

#### Critical Payment Services BAM

- E2E Integrity for Payments
- Performance & Volume Trends
- Automated & Independent
- Improved SLA Performance
- Reduced Incidents & MTTR

Business Activity Monitoring

Grow Software Intelligence Capability

Time

2015

-2017

**Assurance Objectives** 

E2E Payment Service Performance

Reduce Operational Risk Reduce Transformational Risk

Reduce Regulatory Risks Become Proactive & Predictive

2015

-2019

Improve Customer Outcomes



## **Machine Learning Journey**



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



Splunk ITSI Machine Learning Pilot with AIB Mobile App 2017

#### Mobile App Splunk ITSI Pilot Capture Mobile Service Architecture 360 Health View of Business, App & Infra Acquire Data Sources (App, OS etc.) Define KPIs & Train using ITSI Machine Learning **Critical Payments BAM Derive Service Health Quality Scores** · E2E Integrity for SEPA Payments Prove ITSI Anomaly Detection • Payments Volume Trends Reduce Incidents and Problem MTTR Processing Performance Trends Automated "4 eyes" Monitoring 2017 Proactive monitoring of Mobile App Reduced Incidents & MTTR

**Business Activity Monitoring of Critical Payment Services** 

Time

2015

-2017



### **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



# **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



# **Drill Down Capabilities**



Customer Service Health "Live Glass Table" View



#### **Technical Health View**



### **Effectiveness Evaluation**



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



### **Anomaly Detected**



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



### Service Insights Rollout 2018-2019

#### Service Insights Rollout with ITSI

- Business, App & Infra "Live" service health
- Channels & Payments Services
- Trusted 24x7 Service "Radars"
- Reduced Incidents & Problem MTTR
- Prevented critical Incidents
- ITSM, IT Operations & ADM Support teams
- Very Positive Stakeholder feedback

Predictive Business Service Monitoring

Proactive monitoring of Mobile App using Splunk ITSI

Time

2018-20

19

Mobile App ITSI Success

• 360 view of Business, App & Infra

Acquired Data Sources (App, OS)

Mobile Service Architecture

Trained ITSI ML Models
"Live" Health Glass Tables

Anomalies Detected

2017

Reduced Incidents & MTTR



# **Outage Prevention Example**



Example of how Service Insights **Prevented a serious Channels Outage** Just **one of many examples** with Mobile, Channels & Payments



evening which would have taken HOURS to resolve



09/21/2019, 05:02:00 PM ~

## **Protect – Change Root Cause in Minutes**

Service Insights Glass Table 3.0 🗸



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

AIB						Oracle Private	e Cloud H	lealth					
Omega 12C Host 1				8.90 % CPU %	Omega 12C Host 2				9.20 %				
	% DB Time 🗘	% CPU Time 🗧	SERVICE =	% DB Time 🗢	% CPU Time 🕆	Sql Resp Time(ms)		% DB Time 🗧	% CPU Time ᅌ	SERVICE	% DB Time 🗘	% CPU Time =	Sql Resp Time(ms) 🕆
DBAL901T1	2	22	FraudTest	2.6	11	0.22ms	DBAL902T2	4	11	OBAPITest	4.6	22	0.33ms
DBAL901T1	2.3	6.2	SancTest	1.6	1.9	0.22ms	DBAL903T2	2.3	15.2	BusBankMicroTest	2	21	1.2ms
DBAL902T1	22.93	33	PayServTest	1.8	3.1	0.22ms	DBAL903T2	29.3	14.6	BusBankMicroTest	3	6.3	0.22ms
DBAL903T1	110.47	89.33	PayEngTest	122	55	40.2 ms	DBAL903T2	1.9	20.2	BusBankMicroTest	4.4	22.7	33 ms
DBAL903T1	3	5	TreasTest	2.6	2.7	0.22ms	DBAL903T2	2.9	3	BusBankMicroTest	1.7	4.1	0.14ms
DBAL904T1	7	3	BusBankTest	8.8	2.3	0.22ms	DBAL903T2	4.6	6	BusBankMicroTest	3.4	3.8	0.26ms
DBAL905T1	9	6.6	ServHubTest	11.7	4.2	0.22ms	DBAL903T2	5.5	8.8	BusBankMicroTest	19	7.7	61ms
DBAL906T1	2.5	2.1	BPMTest	3.6	1.8	0.22ms	DBAL903T2	9.1	4.4	BusBankMicroTest	5.2	4.4	0.22ms
Omega 11G Host 1					15.30 %	Omega 11G Host 2				11.40 %			
	% DB Time	% CPU Time 🕆	SERVICE 0	% DB Time 🗘	% CPU Time 🕆	Sql Resp Time(ms) 🌣		% DB Time 🗧	% CPU Time	SERVICE	% DB Time 🕯	% CPU Time	Sql Resp Time(ms)
DBAL801T1	4	11	OBAPITest	4.6	22	0.33ms	DBAL801T2	16	17.5	OBAPITest	2.4	5.2	0.66ms
DBAL801T1	2.3	15.2	BusBankMicroTest	5.5	15	1.2ms	DBAL801T2	2.2	9.4	BusBankMicroTest	3.3	5.1	11.2ms
DBAL802T1	90	70	BusBankMicroTest	7	5.9	0.22ms							
DBAL802T1	90	70	BusBankMicroTest	150	90	200 ms							
DBAL802T1	90	70	BusBankMicroTes	23.7	17.2	0.14ms							
DBAL86 1	4.6	6	BusBankMicroTest	8.8	9.1	0.26ms							
DBAL803	5.5	8.8	BusBankMicroTest	9.3	6.4	61ms							
DBAL803T1	9.1	4.4	BusBankMicroTest	5.2	11.2	0.22ms							

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



### 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



# AIB Splunk MQ App

#### Collect MQ Queue Mgr Statistics

MQ DASHBOARD											
QM Status	5	Listener Status		Channel Status							
qmname \$	status \$	listenername \$	status ‡	channelname \$	status \$						
MQCH1T	RUNNING	SPLUNK	RUNNING	STREAMSVR.TO.MQCM1T	RUNNING						
		LISCH101	RUNNING	CALYPSCYC.TO.HQCM1T	RUNNING						
				MQCLASYT.MQCH1T	RUNNING						
				ABINITS.TO.MQCH1T	RUNNING						
				PRICINGSVR.TO.MQCM1T	RUNNING						
Queue Details											
DDI.QL.OPICS.TEST.DUB.CC.DEAL.DATA	DDI.QL.OPICS.TEST.DUB.WS.DEAL.DATA	SAT.QL.HP.CHAPSFT.OUT	SAT.QL.HP.CHAPSGB.OUT	SAT.QL.OPICS.IN	TPT.QL.CALTITAN.REQUEST						
200 300 100 400 3 00	200 300 -100 400- 0 500 89	200 300 - 100 400- 500 6	200 300 - 100 400- 5 500	200 300 -100 400- 0 365	200 300 100 400- 5 500 19						
TPT.QL.CYCLOPS.RESPONSE	TPT.QL.IMATCH.DEV.XFER	TPT.QL.IMATCH.TST.XFER	TPT.QL.REDLINK.DEV.REQUEST								
200 300	200 300 - 100 400- 0 500 80	200 300 - 100 400- 0 500 158	200 300 - 100 400- 500 6								

- 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.





IK INC.

### **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

#### Splunk Enterprise Cluster

- Splunk Multi-Site Resilient Cluster
- 6 Search Heads, 4 Indexers
- Powerful Physical Servers
- Deployment & Cluster Master
- Heavy Forwarder Load Mgmt.
- 250GB Daily Ingestion
- 250 Forwarders
- Replica Test VM Cluster
- Prioritise Scheduled Searches
- User Access Control Framework

#### Splunk Multi-Site Resilient Cluster

Splunk ITSI app, OS app, H/F and ML Components

Splunk Dual Cluster to support critical Splunk BAM Integrity Alerts

Time

2018

Splunk ITSI

Splunk Heavy Forwarder

Machine Learning Component

Common Information Model

Linux/Unix OS Add On

Splunk ITSI App

DB Connect

Splunk Dual Cluster

Splunk Multi-Site Cluster

Physical Servers

Splunk Enterprise

120 ForwardersStandalone Test VM

2015-20

• 3 Search Heads. 2 Indexers

150GB-200GB Daily Ingestion

2017



### **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

360 Service Insights ITSI	<ul><li>Powerful Enabler for AI Operations</li><li>First Payment use cases Live</li></ul>
<ul> <li>Business, App &amp; Infra "Live" service health</li> <li>Channels &amp; Payments Services</li> <li>Trusted 24x7 Service "Radars"</li> <li>Reduced Incidents &amp; Problem MTTR</li> <li>Prevented critical Incidents</li> <li>ITSM, IT Operations &amp; ADM Support</li> </ul>	<ul> <li>New Data Sources (MQ) &amp; Business Services</li> <li>New Splunk Apps (AIOPs)</li> <li>Splunk COE enabled</li> <li>Improve Prediction times &amp; Seasonality</li> </ul>
teams <ul> <li>Positive Stakeholder feedback</li> </ul> 2019-20 20	Automated Service Intelligence Platform
<sup>2017-20</sup> <sup>18</sup> Predictive Busines	s Service Monitoring using Splunk ITSI

Splunk Enabler for AI Ops

Time



### **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 Manager Audit Trail	Search Alerts Dashboar	rds			AIB Workflow Automator
Workflow creation screen	WorkFlow Manager Workflow Action Create Workflow Create Workflow Edit Workflow Delete Workflow	Index main •	Index Filter Condition  * Create Search Earliest Time	Time Last 24 hours - e New Workflow Search Latest Time	I Hide Search Result	Edit Export •
Workflow adding steps	Step Name Step 1 Success Condition Rows Updated ¥ X + Add More	Comment Update DB Comparator > Greater than	Cr Action Update DB • X Value 2	reate New Step Select Schema mysql + X	Select Stored Proc	Parameters param1,param2
Screen to create step branching	Select step Step 1 • X + Configure More	✓ After Step Completes	Configure Condition If Failed • X	e Step Dependency Action Stop Continue rest of the steps Execute a seperate step	Execute A step Step 2 • X Step 1 Step 2 Step 3	



### AIB Splunk Workflow App & SPL Generation

#### Custom Splunk UI to manage workflow

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

WorkFlow Name \$	Step Name ¢	Step Type \$	Comments \$	Mapped Query \$	is_post_step_configured	post_step_details \$	Delete ¢	Edit ¢
wf <mark>1</mark>	Step 1	data_parse	parsing appref	rex field=_raw "apprefid=(? <apprefid>.+)\s+status=error"</apprefid>	Yes	<pre>post_step_conditions:if_success,go_no_go:undefined,exec_a_step:Step 2</pre>	Delete	E
wf1	Step 2	updt_inc	Update Incident	eval Status= "In Progress",Notes= "New Note Sid",Incident_ID='Entry ID'  updateincident	Yes	<pre>post_step_conditions:if_success,go_no_go:undefined,exec_a_step:Step 3</pre>	Delete	E
wf1	Step 3	updt_db	Update Table 1	<pre> eval params=apprefid.",table_1"  map search="  dbxquery connection=mysql_conn procedure=\"{call update_appref(?,?) \\" params=\"\$params\\"   eval Incident_ID=\"\$Incident_ID\$\" "</pre>			Delete	E

Final Query

Final Query

final\_query \*

index=main \*

index=main \*

irx field=\_raw "apprefid=(?<apprefid>.+)\s+status=error"

eval Status= "In Progress",Notes= "New Note Sid",Incident\_ID='Entry ID'| updateincident

checkremedy In Progress

eval params=apprefid.",table\_1\*| map search=\*| dbxquery connection=mysql\_conn procedure=\"(call update\_appref(?,?) )\" params=\"\$params\$\" | eval Incident\_ID=\"\$Incident\_ID\$\" \*

Inable Workflow

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



### **Benefits Realised**







### WE BACK BELIEF