

# Real Time Machine Learning and AI Operations

Heather Wighton / Director of Data Insights  
Paul Ireifej / Principal Member of Technical Staff  
October 27, 2020

© 2020 AT&T Intellectual Property. AT&T, Globe logo, and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners



# Agenda

- 1: Intro
- 2: Real-time ML and AI Operations
- 3: Features and Benefits
- 4: Fully integrated ELK stack
- 5: Case Management
- 6: Demo

In corporate America, we operate by the maxim: what gets **measured**, gets **done**. We use data to recognize **trends**, inform our **goals**, and drive our **decision-making** and actions.

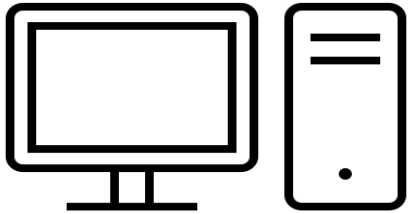
Randall L. Stephenson, Chief Executive Officer of AT&T

This system utilizes **big data**, modern **machine learning** and other advanced analytics technologies to, directly and indirectly, enhance IT operations (monitoring, troubleshooting, and automation) functions with **proactive** and **dynamic** insight.



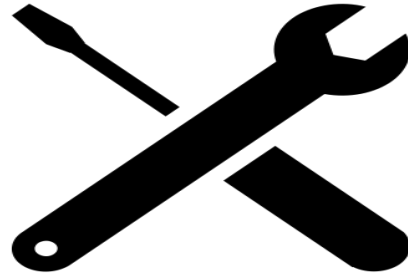
# Features & Benefits

## Monitor applications and systems



- Monitor, profile user behavior and activities

## Real-Time Remediations



- Auto Email & SMS\* Alert
- Auto-generate trouble tickets
- Auto Alert via Instant Messaging
- AutoRun Scripts and Models
- Improved Mean Time to Resolution
- BYOA - Bring Your Own Actions - Extensible capability to integrate new remediation actions

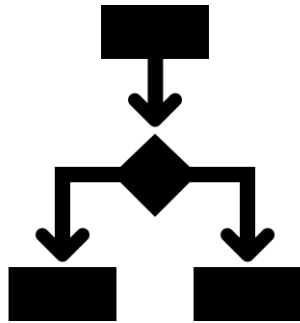
## Machine Learning Models



- Built-In Forecasting Model
- Built-In Anomaly Detection Model
- Built-In Predictive Insights Model
- BYOM - Bring Your Own Model - Integrate your model into the platform

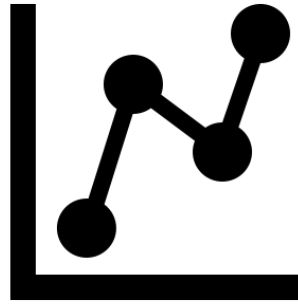
# Features & Benefits (continued)

## Decision Functions



- Dynamic decision function generator
- Update Decision Engines in Real-Time to find events

## Analytics



- Correlation generator based on time span events across data streams
- Volume count threshold based on minute hours and days
- Dynamic Aggregations based on calculations and buckets

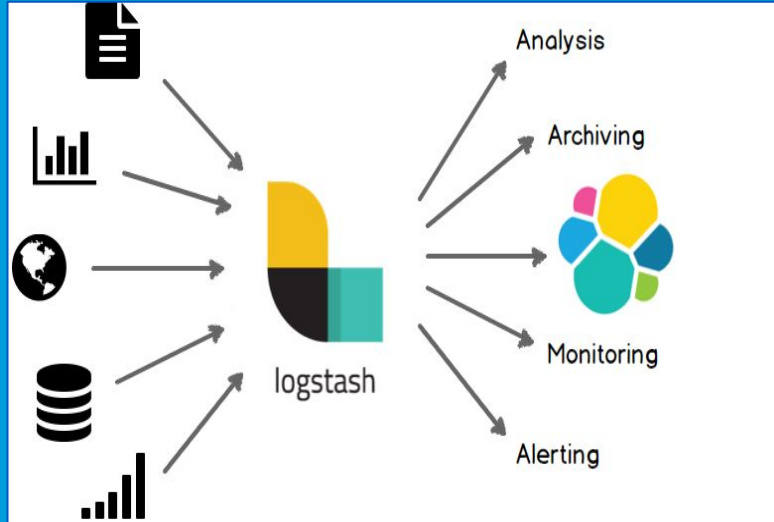
## Data Quality



- Monitor data quality based on the required fields, field length, type of field value and regular expression handling.

# ELK

Fully integrated ELK stack for visualizing real-time and historical events.

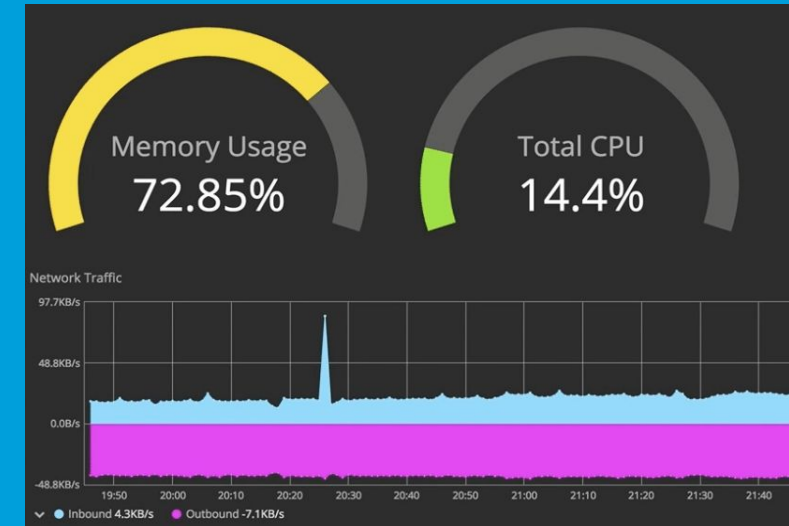


Logstash



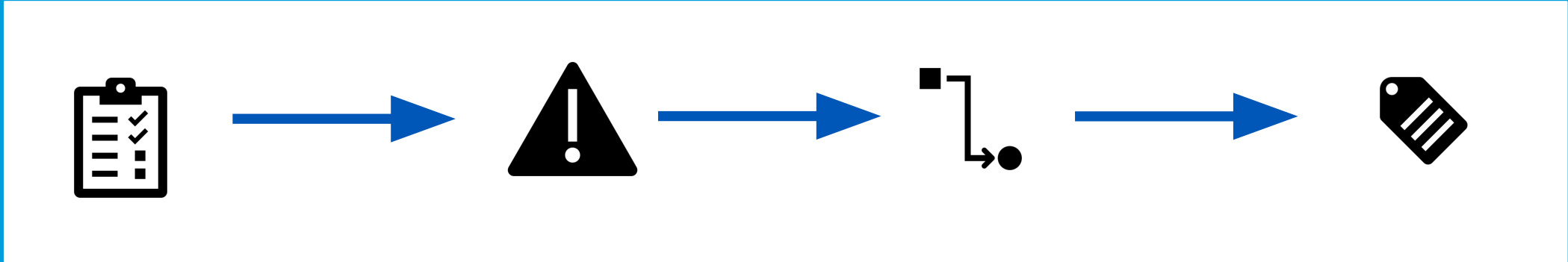
ElasticSearch

Kafka Topics



Kibana visual graphs

# Case Management



- Streamed lined workflow to take alerts to Root Cause closure
- Assign Case to members
- Label severity of the case
- Identify Root Cause and label the incidents.



*This system utilizes big data, modern machine learning and other advanced analytics technologies to directly and indirectly enhance IT operations (monitoring, troubleshooting and automation) functions with proactive and dynamic insight.*

Diagnosis needs –

Real Time Visibility of Health



- Monitor error count of APIs responses
- Monitor Volume per minute of API requests
- Monitor Response round trip to every request
- Alert on anomalies

*This system utilizes **big data**, **modern machine learning** and other advanced analytics technologies to directly and indirectly enhance **IT operations** (monitoring, troubleshooting and automation) functions with **proactive** and **dynamic insight**.*

## Business Benefits

- Decrease MTTR (Mean Time to Resolution)
- Proactive Performance Monitoring
- Drive faster and better decision making



# Real Time Machine Learning and AI Operations

## Complete visibility into your system and resources and applications



### Collect

Metrics and logs from all your system resources, applications, and services that run on-premises servers.



# Real Time Machine Learning and AI Operations

## Complete visibility into your system and resources and applications



Collect

Metrics and logs from all your system resources, applications, and services that run on-premises servers.



Monitor

Visualize applications and infrastructure with dashboards.



# Real Time Machine Learning and AI Operations

## Complete visibility into your system and resources and applications



### Collect

Metrics and logs from all your system resources, applications, and services that run on-premises servers.



### Monitor

Visualize applications and infrastructure with dashboards.



### Analyze

Correlate logs and metrics side by side, apply DevOps rules and Machine Learning techniques to create Cases.



# Real Time Machine Learning and AI Operations

## Complete visibility into your system and resources and applications



Collect

Metrics and logs from all your system resources, applications, and services that run on-premises servers.



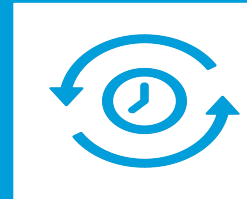
Monitor

Visualize applications and infrastructure with dashboards.



Analyze

Correlate logs and metrics side by side, apply DevOps rules and Machine Learning techniques to create Cases.

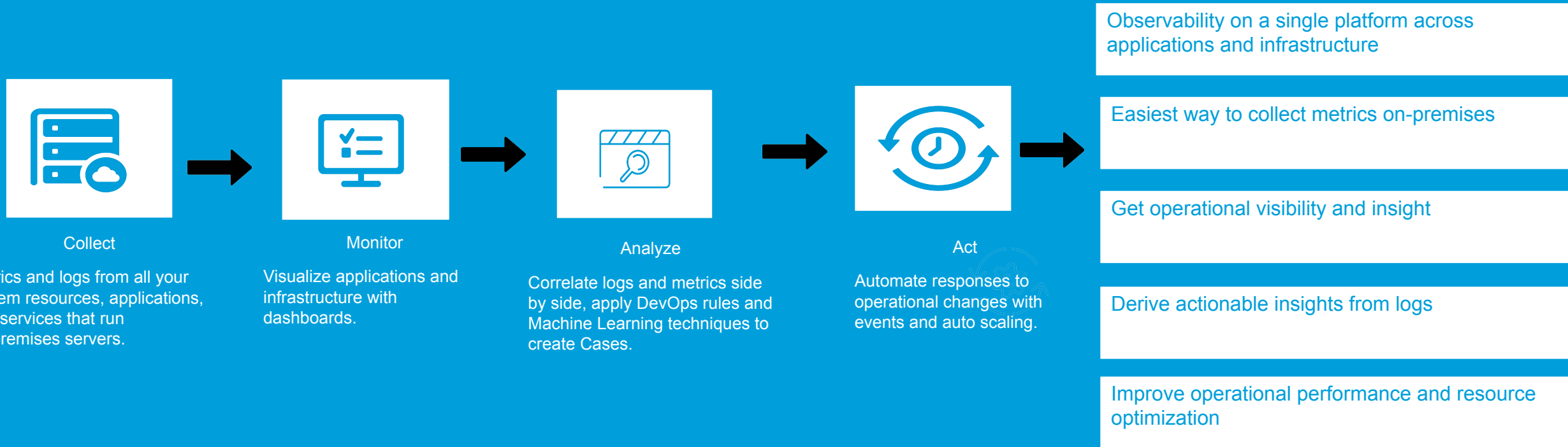


Act

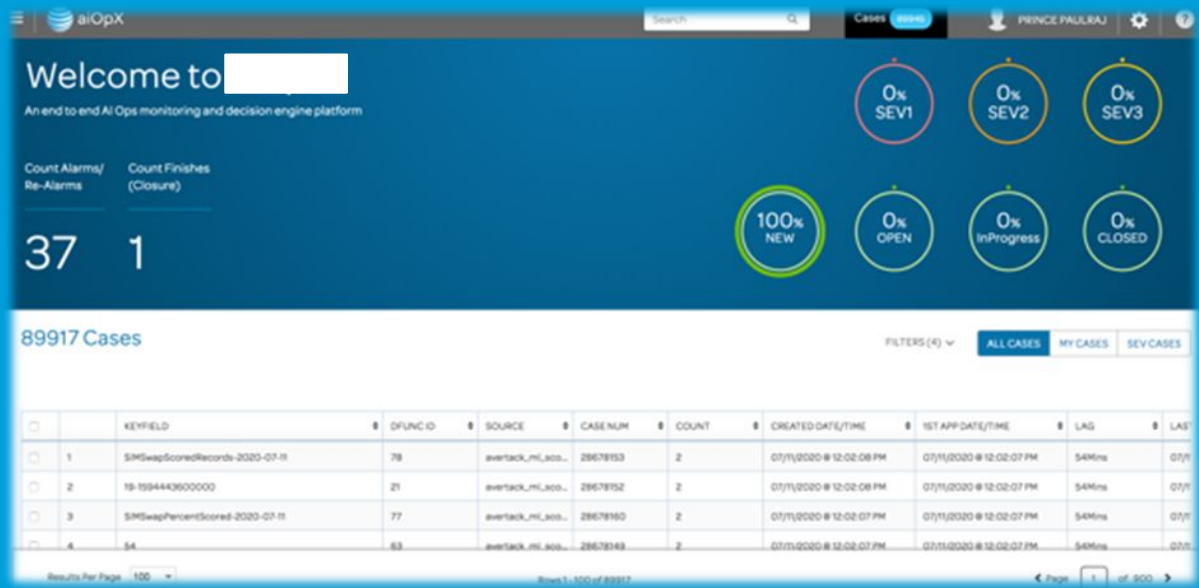
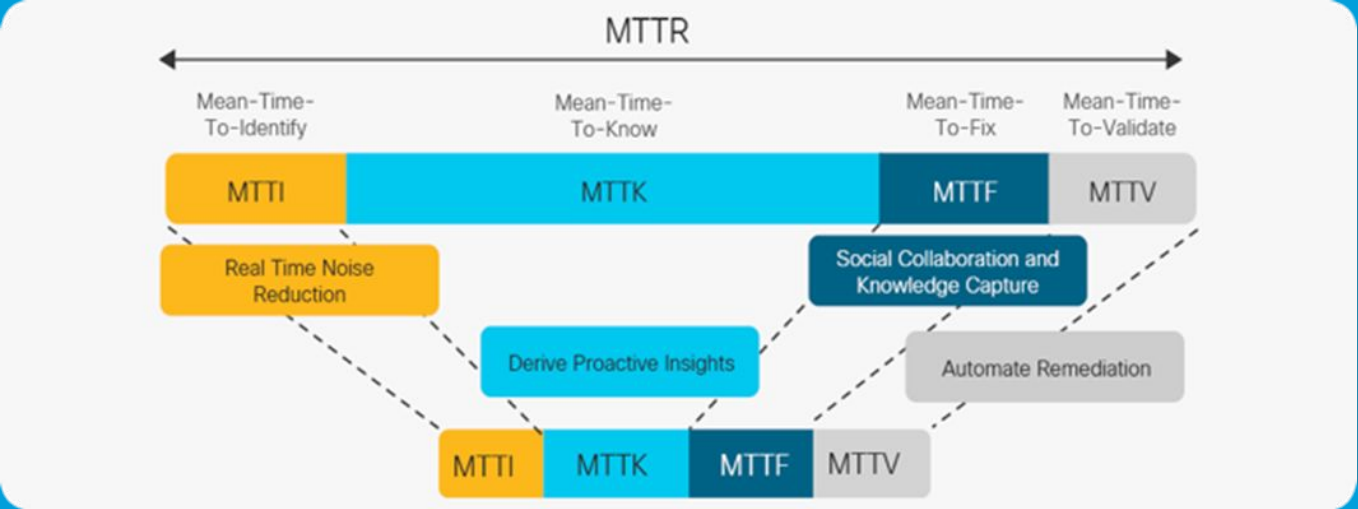
Automate responses to operational changes with events and auto scaling.

# Real Time Machine Learning and AI Operations

## Complete visibility into your system and resources and applications



# Mean Time to Resolution





# Conclusion

## Identify and Adapt to Vulnerabilities



As AI becomes more prevalent in fraud detection, it needs to be supported by self learning tools to **identify** and **adapt** to vulnerabilities.

Real Time monitoring systems can mean the difference between an outbreak that last several hours-days to manually remedy, whereas with our solution, we can **detect**, **react** and **mitigate** within minutes.

# Demo: Case Details

## Case Severity, Status, Root Cause, Owner

Case# 33509168

DECISION FUNCTION(S) APPLIED: 81

SLA-RP600T\_CONSUMERRETAIL60DAY-2020-10-26

APPLICATION ID2

Case Severity

Select Severity

Case Status

New

Root Cause

Select Root Cause

Case Owner

AMAND SINGH

Archive Case

CASE CREATED DATE TIME:

10/26/2020 @ 10:42:22 AM

FIRST APP DATE TIME:

10/26/2020 @ 10:42:21 AM

LAST APP DATE TIME:

10/26/2020 @ 10:46:30 AM

0 Case Notes >

Case Details

Case History

avertack\_ml\_ws\_log

status: open tentative suspended cancelled closed

ALL

HOT TABLE

2 Applications-Avertack\_ml\_ws\_log

	VERSION	MODELKEY	PREDICTORAPIEVENTDURATION	MODELVERSION	PREDICTORRESULTS	SERVICEID	RESPONSE MESSAGE
1	1	rp600t_consumerretail60day	30.173	2.0	0.00299328682012856	retail	{modelKey=rp600t_consun
2	1	rp600t_consumerretail60day	17.097	2.0	0.0036153073888272047	retail	{modelKey=rp600t_consun

# Demo: Decision Function

## Monitor zero volume once a day

IF

Add Group

JOIN

Add Join

AND

recordCount = 0

WHEN

09/30/2019 - 09/30/2050, 8:00 AM - 9:...

\*Time Frame

Days

1

Hours

0

Minutes

0

Local Exclusion List

Multi-Inclusion List

IncludeOnceADayCollection

Remediation

Alert

CREATE SCHEDULE

Schedule 1

Start Date

09/30/2019

End date

09/30/2050

Start Time

08:00 AM

Stop Time

09:00 PM

Specific Days:

Sun

Mon

Tue

Wed

Thu

Fri

Sat

\*Decision Function Name

AIOPX - dbmonitor - Zero records per day

\*Description

Monitor zero volume once a day

Instruction

# Demo: Remediation List

## Email

Remediation List			
Remediation ▾			
5001-Email ↑			
Remediation ID	Priority	Remediation Description	Actions
5001	1	Email	{ "email": { "object": { "To": "c@att.com", "Cc": "", "Bcc": "", "Subject": "", "Body": "found an error in LocationServer", "Interval": "OnceEveryNRecords", "IntervalValue": "1" }, "active": true, "value": "", "typeOfValue": "object" } }
5683:AIEM(5683) ↓			
AIOPX - DbMonitor - Zero ML Model Count(5001) ↓			
AIOPX - DbMonitor - Zero rules running(5001) ↓			
AIOPX - Digital Async - Email(5001) ↓			
AIOPX-kafkaMonitor-LagAlert(5001) ↓			
AOTS Ticketing(5004) ↓			
Alert(5001) ↓			

# Demo: Metrics

## Third party server

Metrics						
	AuthenticID-Server					
	Internal	3rdParty	MongoDB	Internal	Kafka	
<b>API Internal</b>						
<b>API Internal Timing</b>						
Average API Timing	✓			✓		
Average Overhead (Total - Running - Loaded)	✓			✓		
<b>API Internal Status</b>						
System Health	✓			✓		
API Calls	✓			✓		
API Timing	✓			✓		
Total calls last 1 hour (Dynamic Timing)	✓			✓		
Errors last 1 hour (Dynamic Timing)	✓			✓		
API Server Errors by Type	✓			✓		

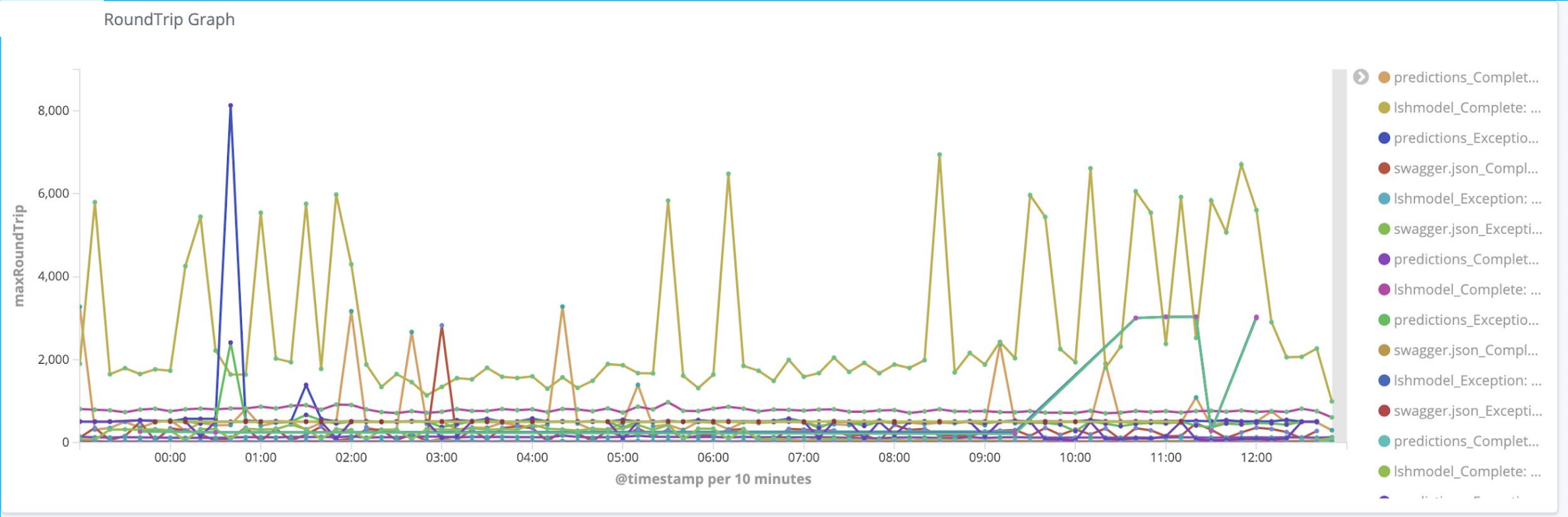
# Demo: Kibana

## API Exception and Transaction Volume



# Demo: Kibana

## RoundTrip Graph





# Thank you!

## Questions?





