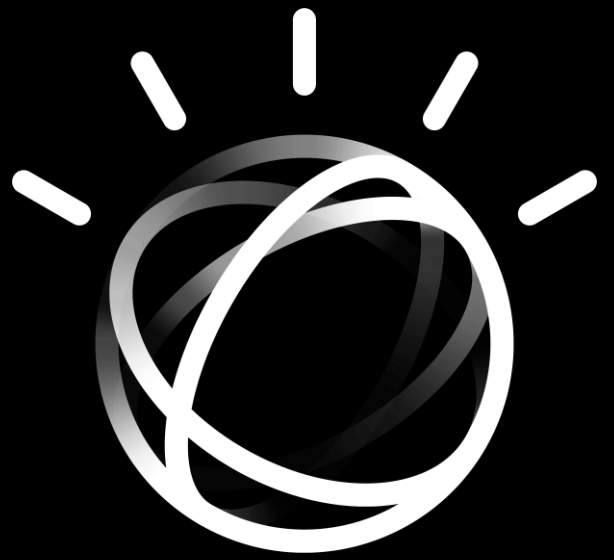
IBM Watson AIOps
Log Anomaly Detection

Leverage Watson AIOps to better predict IT outages from logs.



Watson AIOps

Data channels

Structured data

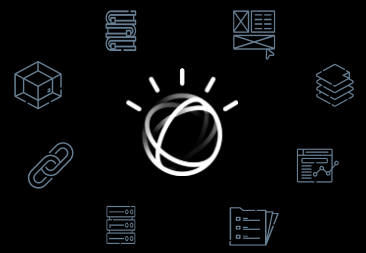
- Events / Alerts
- Metrics
- Topology

NOI, ASM & CP4MCM

Un-structured data

- Logs
- Tickets

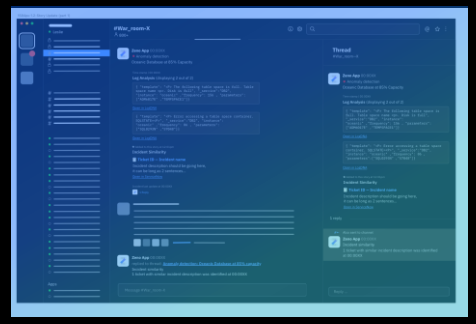
Watson AIOps



Insights & Advise

Insights surfaced via

ChatOps



APIs for process or dashboard integration (future)

Watson AIOps integrates with **Netcool Operations Insights** to ingest events and combine it with unstructured data

Watson AIOps retrieves topology information from **ASM** to map its understanding of location and blast radius.

Watson AIOps retrieves additional data via integrations with **CP4MCM** to deliver additional insights & Next-Best-Actions

Logs


Find a View
EVERYTHING
VIEWS
499error-ts-ui-dashbo…
500 Internal Server Er…
500error-ts-ui-dashbo…
503 Service Unavailab…
demo-view
train-ticket-microserv…
ts-assurance-mongo-…
ts-services
ts-services+UI
ui-view
66d9d8fb-ff78-48de-b1ac-…
IBM-7DAY
Everything
All Tags
All Sources
All Apps
All Levels
Search...
Jump to timeframe
LIVE

Demo

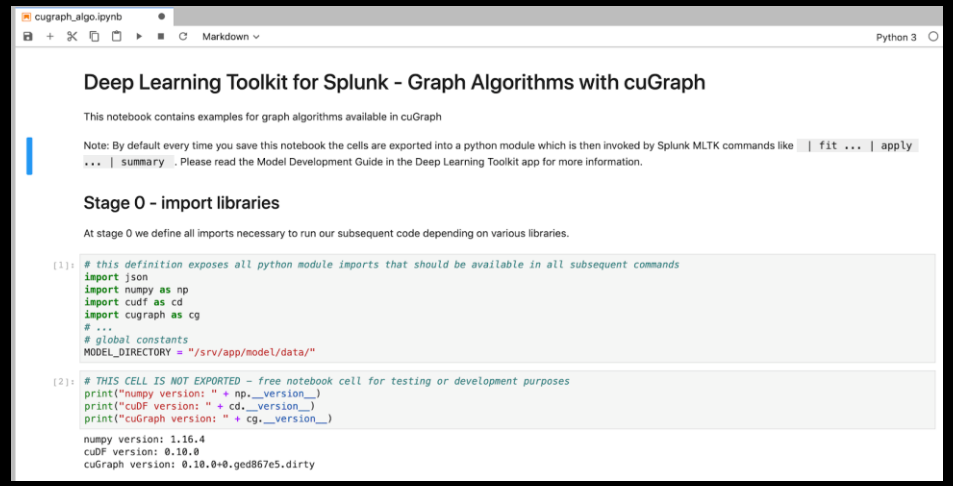
Why Watson AIOps?

Monitoring Metrics Is Not Enough.

Keyword Query Is Not Enough.

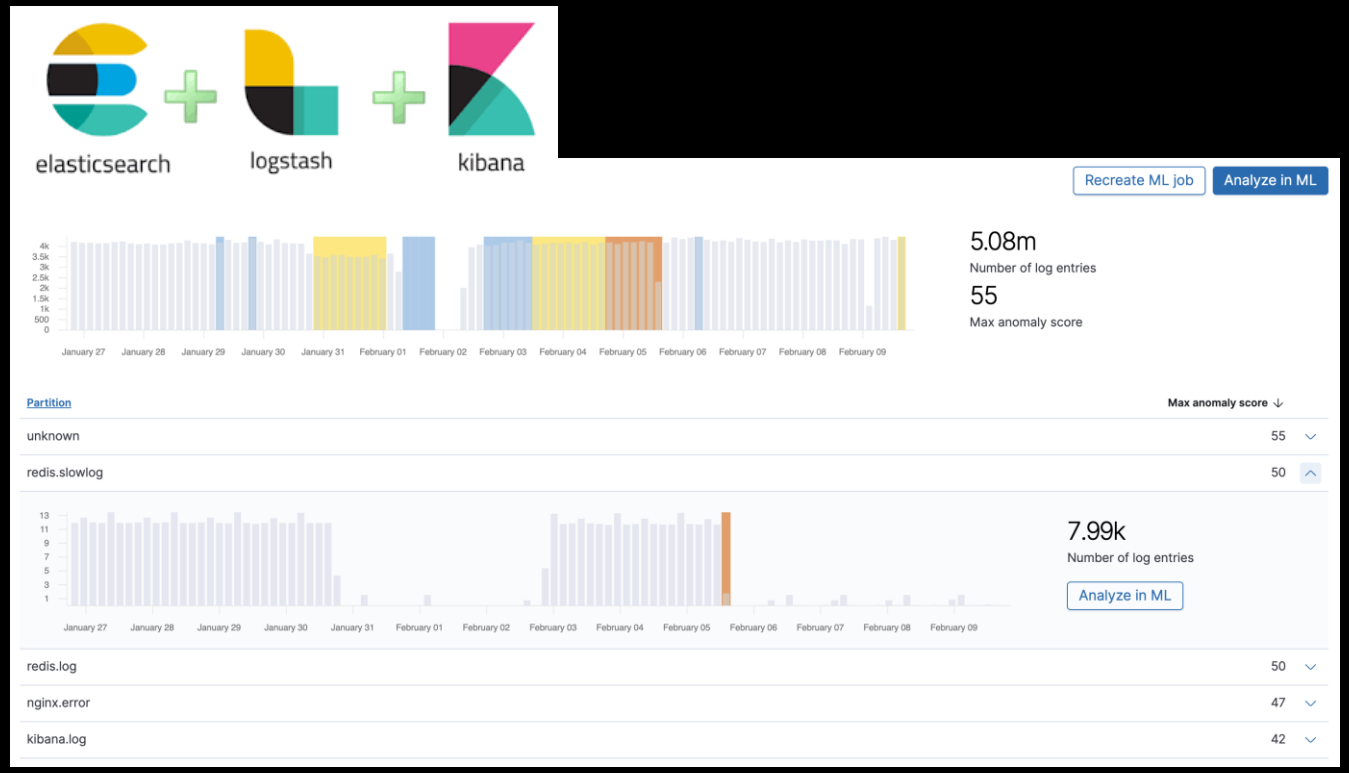
Requiring Data Scientists Is Too Much.

splunk>

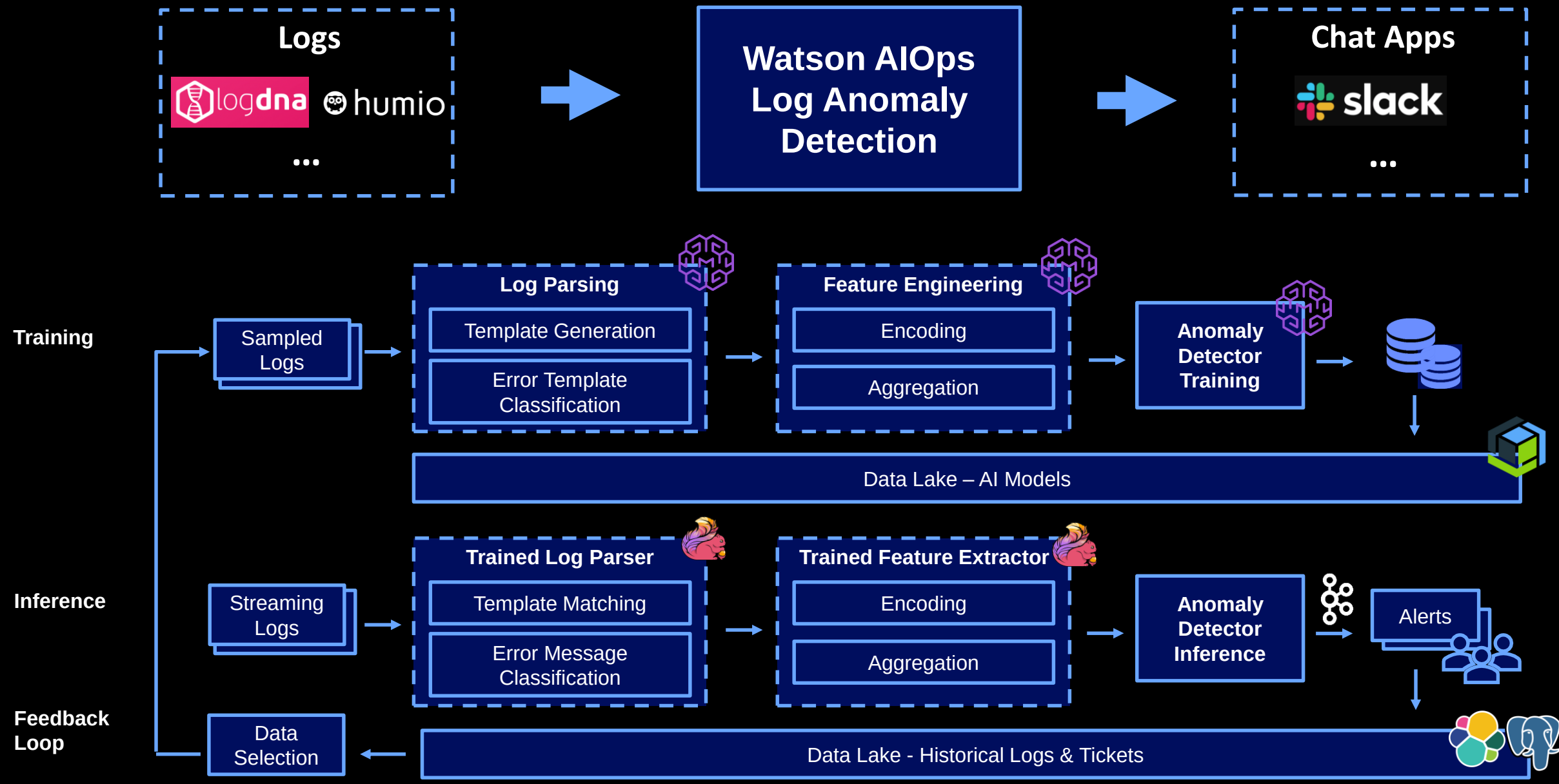


DATADOG

Prometheus



Log Anomaly Detection



Template Generation

```
/*  A logging code snippet extracted from:
    hadoop/hdfs/server/datanode/BlockReceiver.java */

LOG.info("Received block " + block + " of size "
    + block.getNumBytes() + " from " + inAddr);
```

Log Message

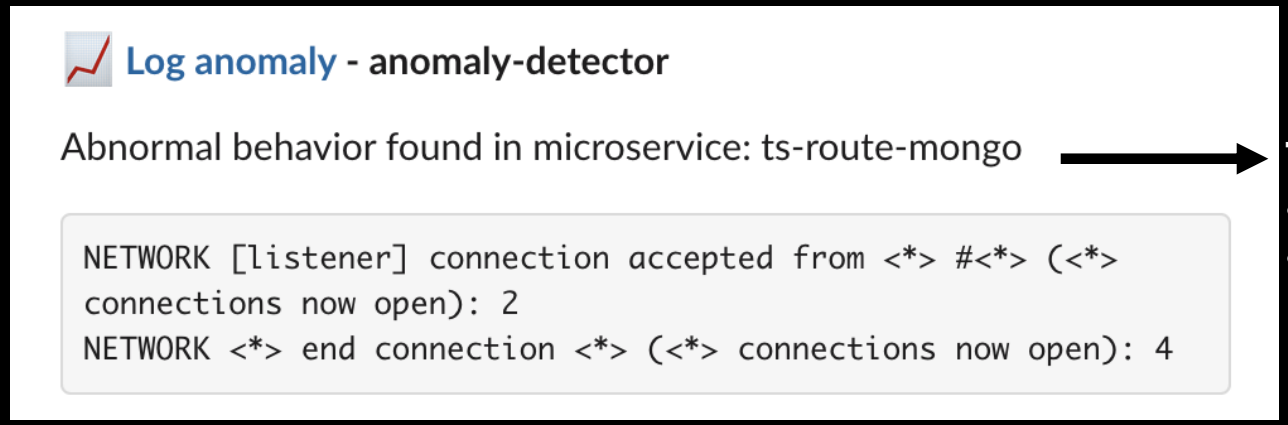
```
2015-10-18 18:05:29,570 INFO dfs.DataNode$PacketResponder: Received
block blk_-562725280853087685 of size 67108864 from /10.251.91.84
```

Structured Log

TIMESTAMP	2015-10-18 18:05:29,570
LEVEL	INFO
COMPONENT	dfs.DataNode$PacketResponder
EVENT TEMPLATE	Received block <*> of size <*> from /<*>
PARAMETERS	["blk_-562725280853087685", "67108864", "10.251.91.84"]

Explainability

Generate Human-readable Titles for Log Anomaly



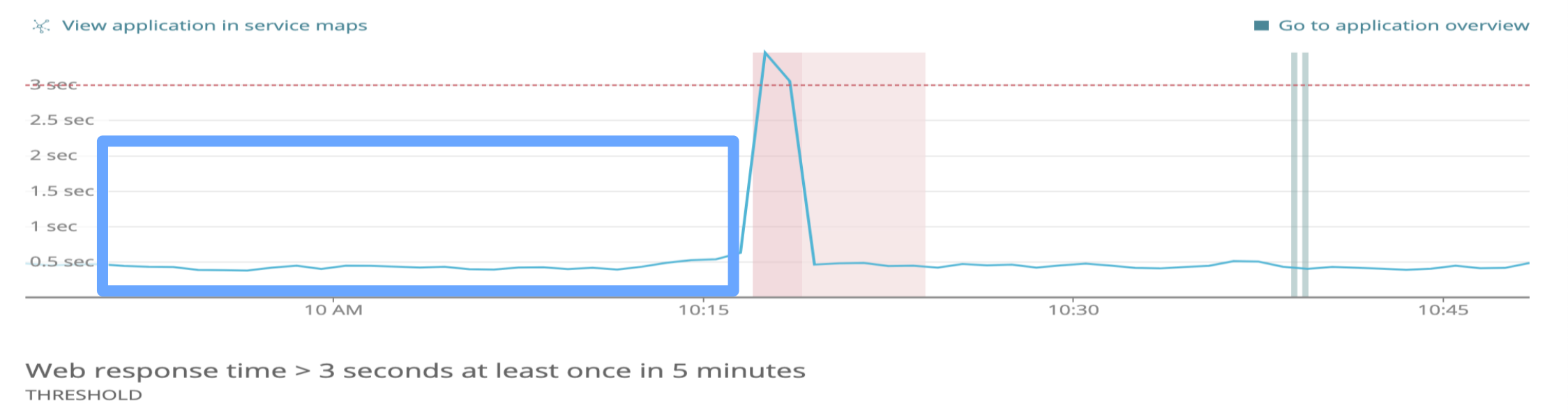
Title:

- Abnormal behavior found in component *ts-assurance-mongo*
- 4 errors found in pod *ts-assurance-mongo-54b557bfbc*

Allow SREs to drill down into log template and it messages for induvial log anomalies

Adjust Severity Level and Grouping based on Causality Scores

Client Engagement

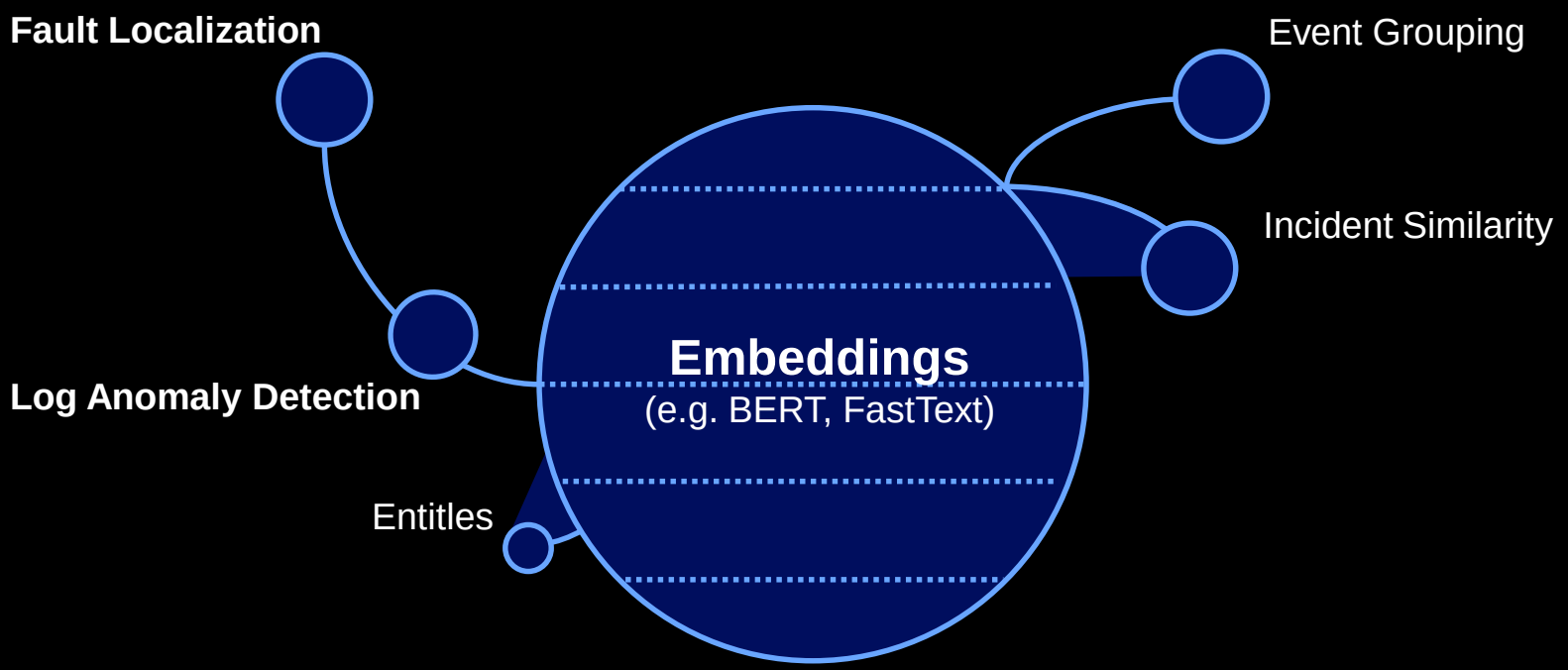


Telcom Company: "*The results (log anomaly results) from my perspective were absolutely amazing, … (log anomaly results)* ***have provided from near realtime reactive + 6.5hrs predictive. I do not think the client could ask for anything better than these***."

Marketing Company: "*… using when Watson AIOps,* ***we were able to find and localize new anomalies within our data sets which helped our teams address potential long-standing issues*** *and has improved our overall service levels and incident responses*."

Next Step - Uses Language Models to Optimize IT Operations Management

One-stop solution to encode text for IT Operations Management Tasks

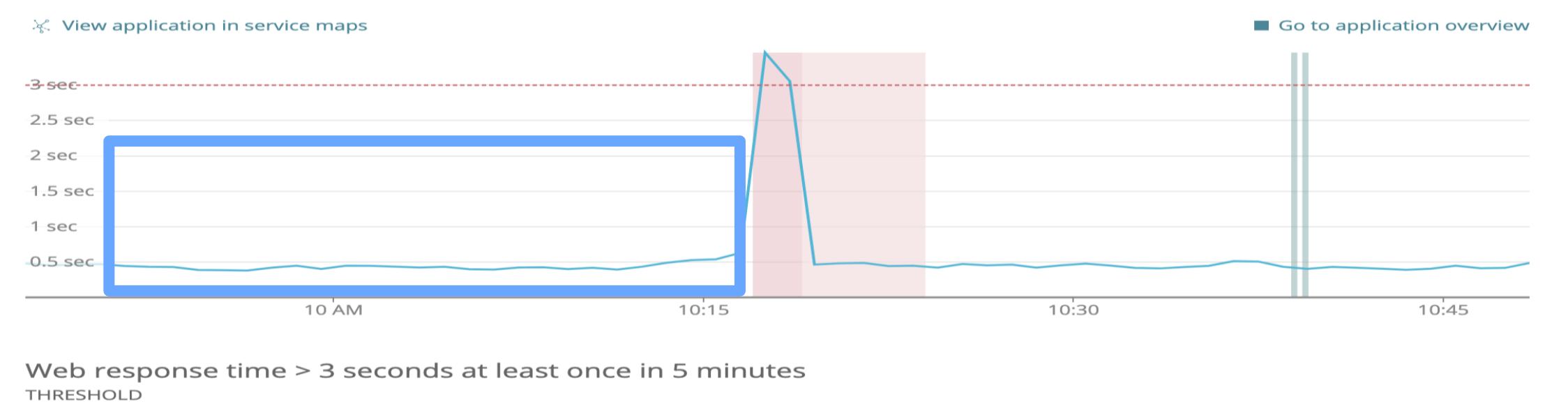


Generalizability across Data Types
Multi-lingual learning
Multi-task learning

Continuous Improvement
Model customization without labeled data
Automatically improve models with payload

X. Liu, Y. Bei, A. Xu, R. Akkiraju. Using Language Models to Pre-train Features for Optimizing Information Technology Operations Management Tasks*. International Workshop on Artificial Intelligence for IT Operations (AIOPs) 2020.*

Next Step – Golden Signal Driven Log Anomaly Detection & Fault Localization



Model for multiple components (Detection & Fault Localization)

- Consider golden signals (e.g. Latency).
- Consider trace logs based on discriminatory entities such as "transaction_id ".

Out-of-the-box models

- Provide Content Pack, so AIOps can benefit clients on Day 0.

Quality Evaluation

Dataset		Per-class Accuracy	
Data Source	Env.	Normal	Abnormal
Chatbot Service	Cloud	93.3%	66.7%
HDFS	Cloud	99.99%	54.8%
Trian Ticket App	Cloud	95.1%	55.1%
Financial Service	Traditional	99.99%	100%
<XXX> Bank	Traditional	91%	60%
<YYY> Bank	Traditional	96%	100%
Marketing Company	Cloud	Was able to detect the client's incident from logs	
Telecom Company	Traditional	Was able to detect the client's incident from logs	

IBM Watson AIOps
Log Anomaly Detection

Leverage Watson AIOps to better predict IT outages from logs.

Anbang Xu, anbangxu@us.ibm.com
Rama Akkiraju, akkiraju@us.ibm.com