AI-powered IT incident resolution application, fueled by your own data
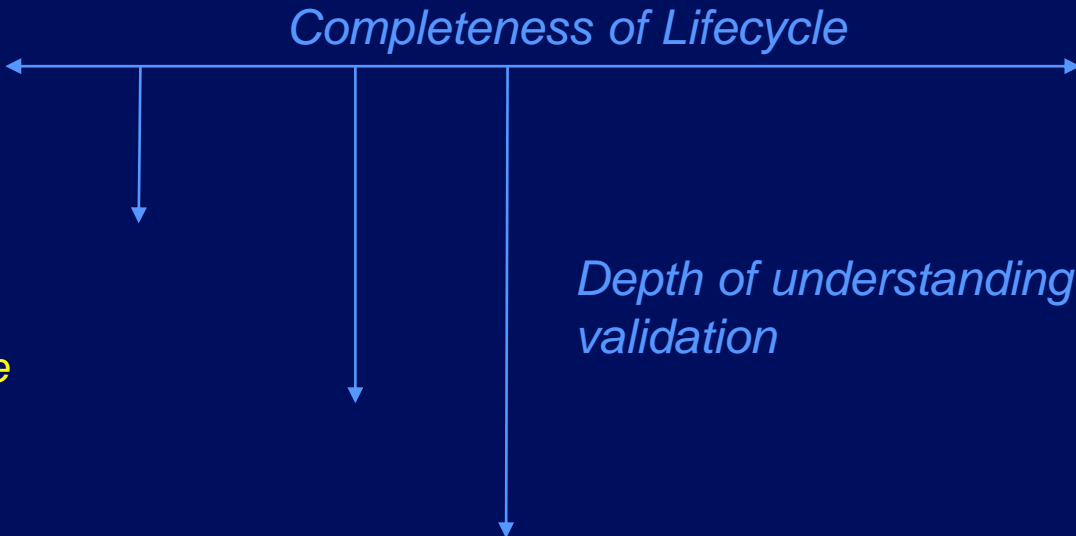# Cloud Service Management and Operations

Completeness of Lifecycle

Depth of understanding & validation

Richard Wilkins
Distinguished Engineer, IBM Garage

IT Grappling With New Challenges

IBM surveyed senior IT leaders and teams to understand the need for AI in IT.

CIOs

IT Ops Teams

Innovation v. Stability

Thousands of IT incidents per month

9 incidents will be critical, costing **$139k each** on average

Impacts compound with regulator penalties, SLA penalties, and reduced customer LTV

Negotiating Complexity & Scale

Days to detect and diagnose a complex issue

Major outages can cost up to **$420k per hour**

Overwhelmed by disparate tools

Struggling with inconsistent alerts, interruptions across sources

Flood reduction tools are **not transparent**

Workflow interrupted to swap between incomplete tools

Burnout & Skills

Only 10% percent of FTEs **have 90% of critical expertise**

Teams & CIOs struggle with talent risk

$1.2M spend per service in highly skilled FTEs to meet SLA and resiliency demands

Extend impact and value with AI for IT

Incorporate digital experiences

e.g. end-user or process KPIs, client sentiment

Automate
next-best action

via RBA, RPA, K8s operators

Incorporate DevOps

e.g. Code, Build, Deployment changes

Infuse AI into underlying toolchain & platform

e.g. Netcool Ops Manager, Cloud Pak for Multicloud Management

Digital transformation requires enterprise IT organizations to

Adopt new tools and practices to make the most of their legacy and new tool sets

Facilitate operational excellence and rapid innovation

Build a harmonious workflow between their devops, line-of-business and central operations teams.

What is Artificial Intelligence for IT Operations

AI for IT Operations (AIOps) is the infusion of AI into existing operational processes like incident and problem management, which then provides operational efficiencies such as predictive alerts and outage avoidance

Four stages of the AIOps Journey
Collect – Provide relevant and make it accessible
Organize – Curate, Cleanse and Govern the data
Analyze – Add additional insights with ML/DL
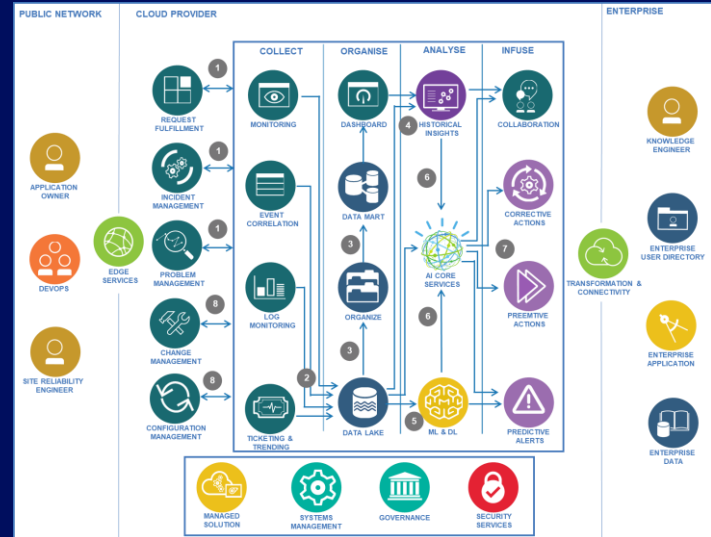**Infuse** – Include AI in Operational Processes

Maturity levels within AIOps
Simplified – Noise Reduction and de-duplication
Reactive – Real-time Insights into the data trends
Predictive – Predictive Multivariate Correlation
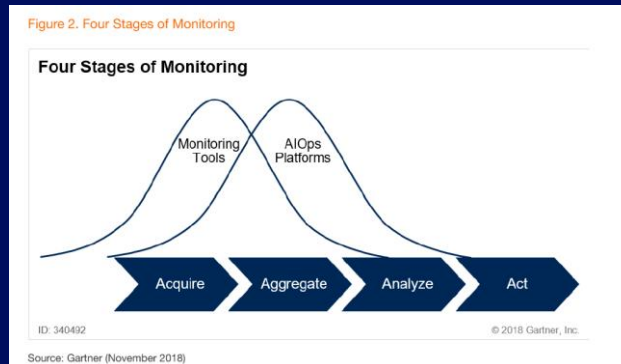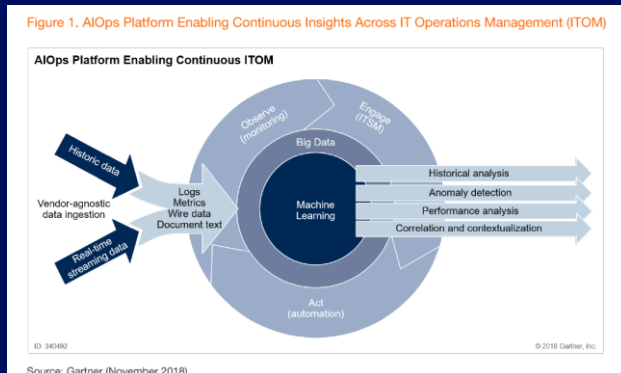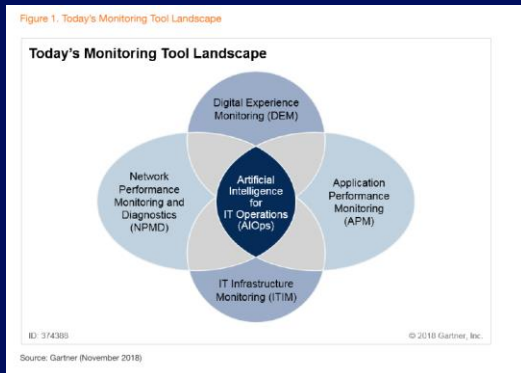**Proactive** – Smart Incident for outage avoidance

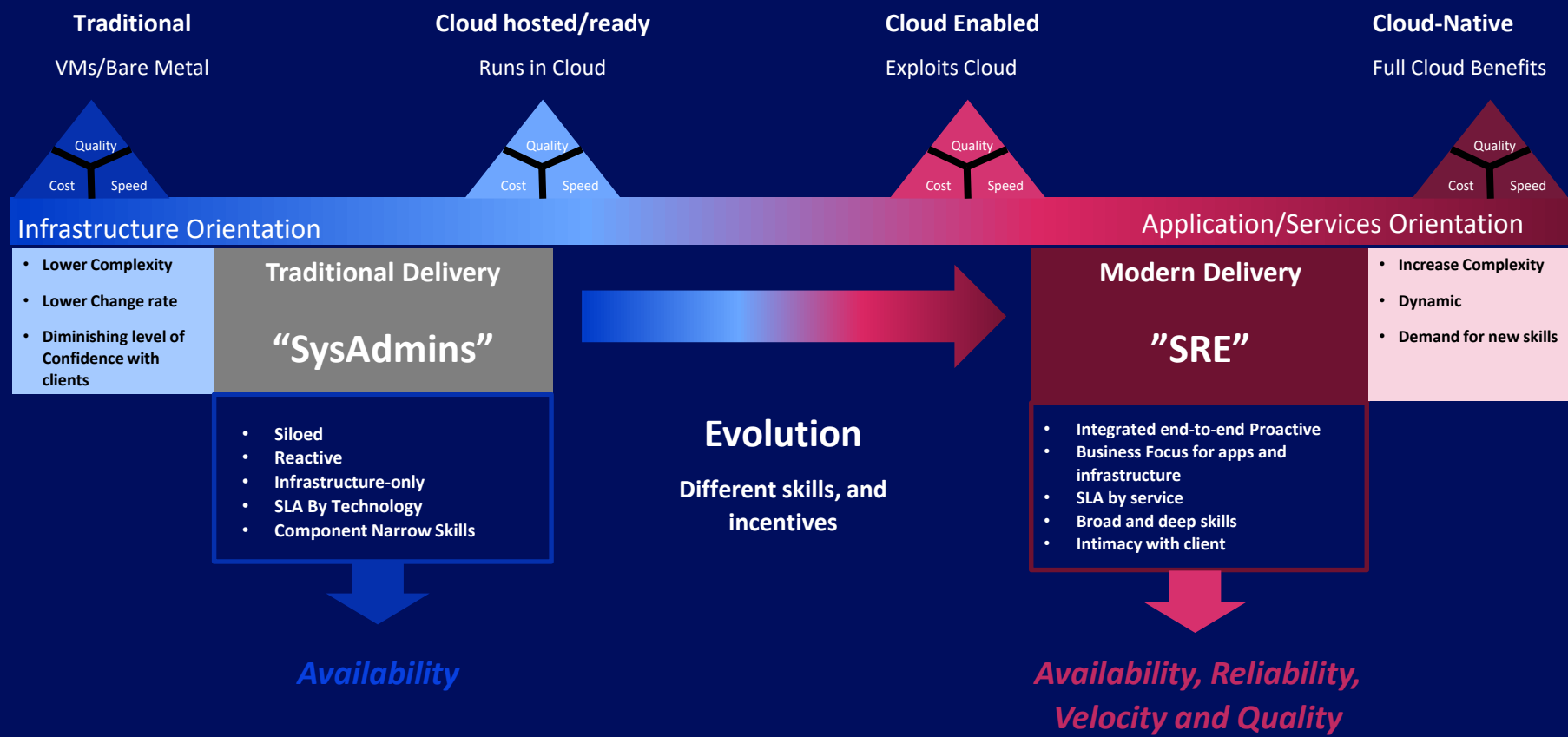
Reference Architecture

What is AIOps

Defined by Gartner

AIOps is the application of machine learning (ML) and data science to IT operations problems. AIOps platforms combine big data and ML functionality to enhance and partially replace all primary IT operations functions, including availability and performance monitoring, event correlation and analysis, and IT service management and automation.

AIOps adoption is projected to grow to 30%, by 2023, for large enterprise

Figure 1. Today's Monitoring Tool Landscape

Today's Monitoring Tool Landscape

ID: 374388
© 2018 Gartner, Inc.
Source: Gartner (November 2018)

Figure 1. AIOps Platform Enabling Continuous Insights Across IT Operations Management (ITOM)

AIOps Platform Enabling Continuous ITOM

ID: 340492
© 2018 Gartner, Inc.
Source: Gartner (November 2018)

Figure 2. Four Stages of Monitoring

Four Stages of Monitoring

ID: 340492
© 2018 Gartner, Inc.
Source: Gartner (November 2018)

Source: https://www.gartner.com/smarterwithgartner/how-to-get-started-with-aiops/

Source: Gartner Research
ID:G00374388

Gartner, Inc. | G00365738

Evolution of the Delivery model

Delivery evolution from infrastructure to full-stack application DevOps pipeline focus

Traditional

VMs/Bare Metal

Quality

Cost   Speed

Cloud hosted/ready

Runs in Cloud

Quality

Cost   Speed

Cloud Enabled

Exploits Cloud

Quality

Cost   Speed

Cloud-Native

Full Cloud Benefits

Quality

Cost   Speed

Infrastructure Orientation

Application/Services Orientation

- **Lower Complexity**
- **Lower Change rate**
- **Diminishing level of Confidence with clients**

Traditional Delivery

"SysAdmins"

- **Siloed**
- **Reactive**
- **Infrastructure-only**
- **SLA By Technology**
- **Component Narrow Skills**

Evolution

Different skills, and incentives

Modern Delivery

"SRE"

- **Integrated end-to-end Proactive**
- **Business Focus for apps and infrastructure**
- **SLA by service**
- **Broad and deep skills**
- **Intimacy with client**

- **Increase Complexity**
- **Dynamic**
- **Demand for new skills**

Availability

Availability, Reliability, Velocity and Quality

6

Modernize your ITOps with a single Solutions that lets you

Connect, Observe & Ingest

Manage virtually any source across local, hybrid and multi cloud environments

Reduce noise and incidents

AI driven automatic consolidation and grouping of events into smarter and actionable incidents

Get Relevant Context

Quickly understand what is happening or what happened with enriched and relevant context to speed up probable cause determination
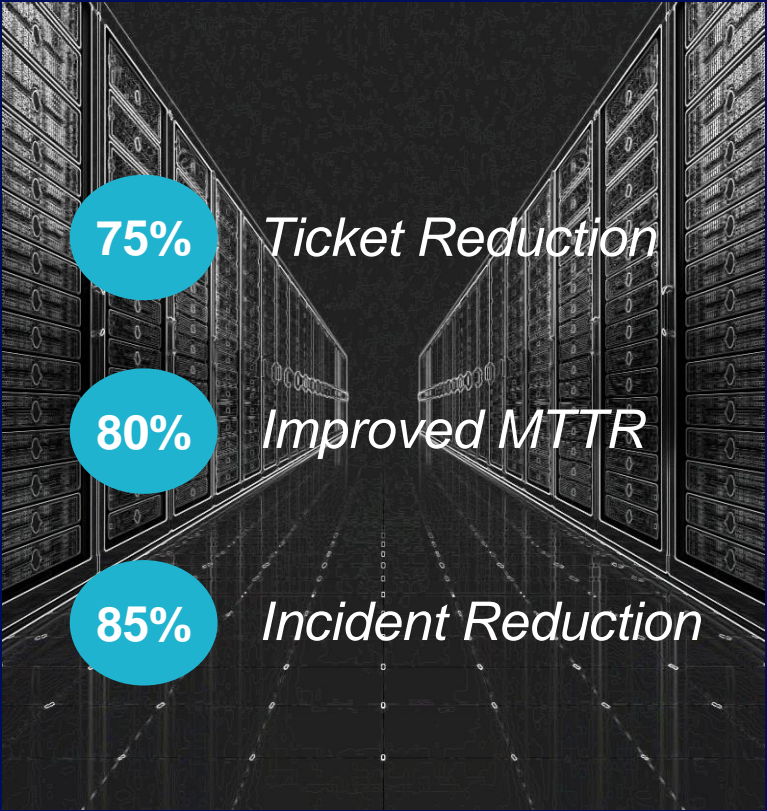
Automate Response

Create, manage and execute guided or fully automated response for rapid incident resolution

Collaborate

Work smarter with AI enriched tickets and stay connected with relevant stakeholders for effective collaboration

75% *Ticket Reduction*

80% *Improved MTTR*

85% *Incident Reduction*

IT Operations without AI
CIO Challenges in incident management & resolution

| Mean time to detect MTTD | Mean time to identify MTTI | Mean time to know MTTK | Mean time to repair MTTR | Mean time to resolve MTTR |

Realtime

Realtime

2 hours

6 hours

Focus work on lasting fixes

Detect — Isolate — Diagnose — Fix — Verify

Incident management workflow

*Potential impact

8
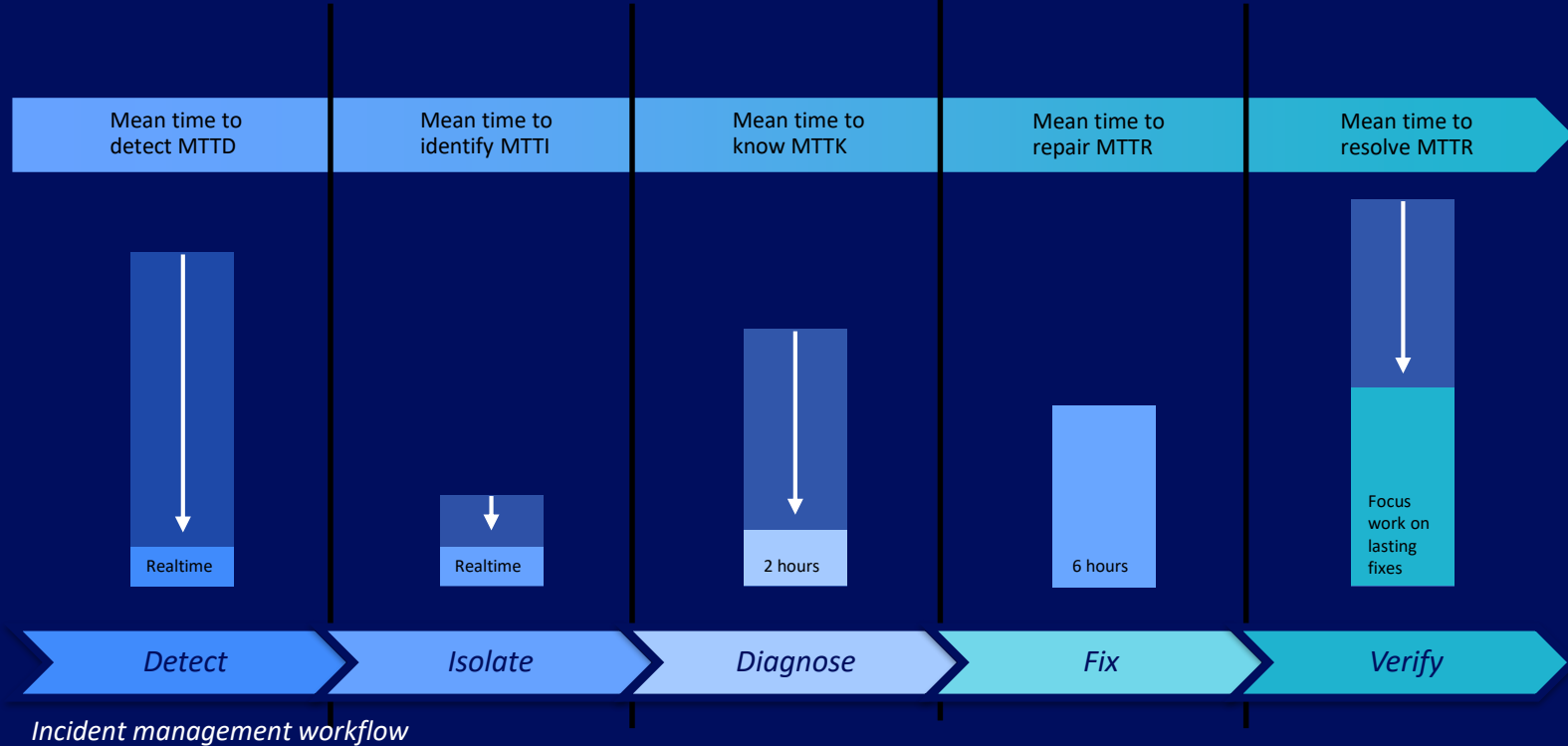
Collect

The mindset toward the way that traditional monitoring is done is changing. Teams can no longer rely on administrators to define a set of monitors and associated thresholds that might or might not detect an issue as it occurs. This lack of insight into a system means that significant events can occur with almost no foresight or warning.

Monitoring products must support the collection of large amounts of data that is streamed into a common centralized data lake. The data lake allows AI models to create a baseline of the way that a system is performing.

This same concept must be applied to any data that is produced either by the application this data includes structured data from logs, events, and even collaboration tools, and unstructured data from the internet in the form of customer feedback or even social media.

Level 1
Resource
Monitoring,
ad-hoc

Level 2
End it End
Monitoring
Response
time

Level 3
Monitoring
of golden
Signals

Level 4
Automatic
definition of
Thresholds

Level 5
Continuous
improvement
and AI
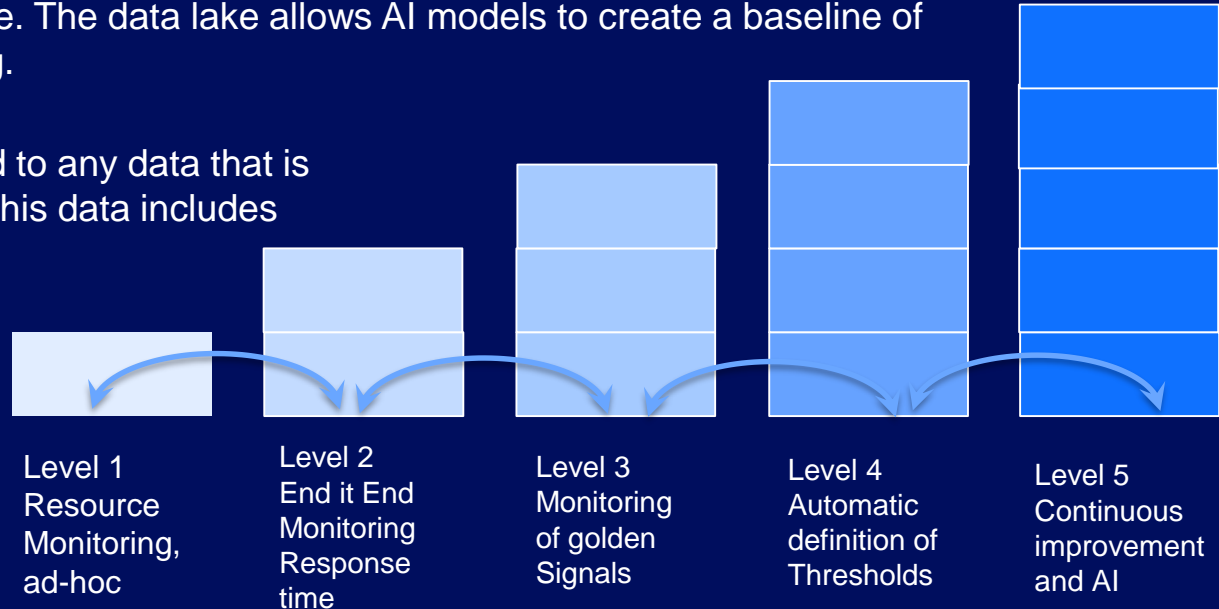
IBM Watson AIOps Fuels your AIOps Journey

Deepen your understanding. Operate proactively. Improve via automation.

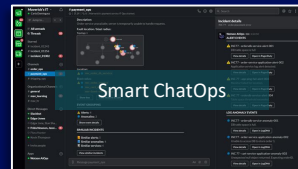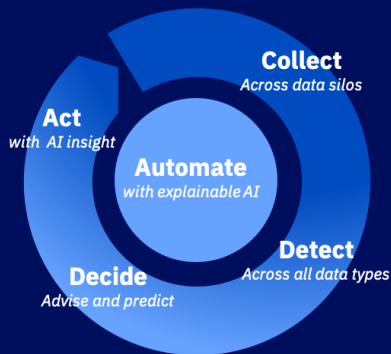*Un-structured data (Logs and Tickets)*

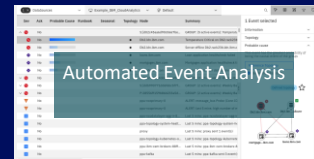*Structured data from Monitoring*

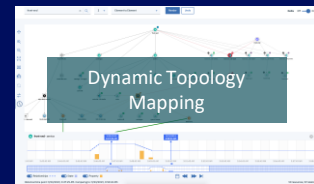*Events and Alerts*

Topology Information

Collect all relevant data

Collect
Across data silos

Act
with AI insight

Automate
with explainable AI

Decide
Advise and predict

Detect
Across all data types

Smart ChatOps

Automated Event Analysis

Dynamic Topology Mapping

Accelerate data awareness to near-real time into existing workflows or ChatOps

Correlate, curate and highlight most relevant data across tools without manual "deep-dive" investigations

Focus your efforts via automated event grouping, analytics and probable cause

Watson AIOps – one cohesive solution

Real-time data feeds

Un-structured data

Logs

Tickets

Structured data

Events / Alerts

Metrics

Topology

Watson AIOps

AI Manager
- Log anomaly detection
- Triage and correlation
- Ticket similarity analysis
- Story service

Event Manager
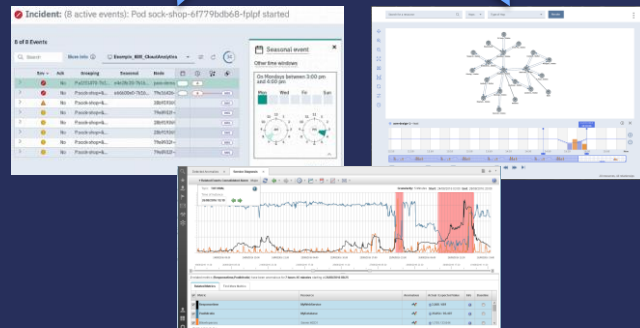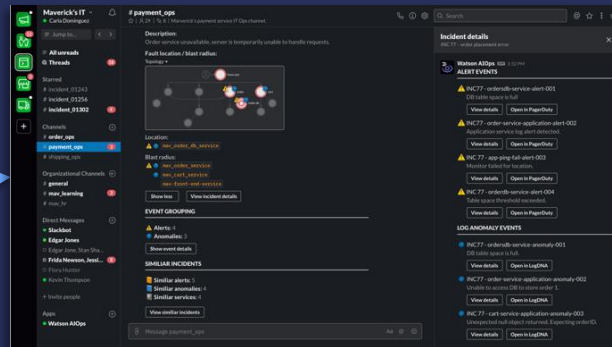- Event grouping & Analytics
- Alerting

Metric Manager
- Performance metric analysis
  Anomaly detection & prediction

Topology
- Dynamic, history
- Cloud native, VMs, bare-metal

ChatOps UX to bring insights to SRE

Dashboard UX to drill down / explain

IBM Watson AIOps key functionality differentiation

|	**Log Anomaly Detection**	**Entity Linking**	**Fault Localization & Blast Radius**	**Issue Similarity**
What	Detect anomalies from logs, and alert on issues	Grouping of events, alerts, and anomalies	Derive root fault component and blast radius of affected components	For a given problem description, find top ranked similar incidents
Value	• Reduces mean time to diagnose (MTTD) incident, detects anomalies earlier than rule-based alerts • No static thresholds • no manual rules to define & manage	• Reduces event flood • Accelerates incident diagnosis	• Reduces mean-time to isolate a problem • Fast and accurate identification of faulty component leads to fast incident resolution	• Relevant similar incidents lead to fast incident resolution
Technology Highlights	Automatic log parsing of any arbitrary log format, semantic understanding, Unsupervised learning, continuous learning	Entity linking, holistic problem context creation, real-time incident context graph, explanations	Node-weighted graph	Next best action summary Advanced language models, Deep NLP via semantic parse for action-entity extraction & incident summarization

Recap of Inferencing

- Used System logs only for training and inferencing
  - Reduced time to detection from 2 hours 24 minutes to 34 minutes
 - Detected the anomaly 34 minutes after incident due to gap in logs
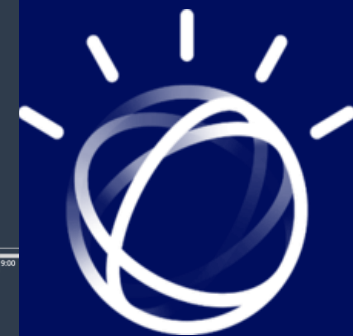
POC for Large Telco in South Africa

Goal: Demonstrate AIOps capabilities. Detect Workflow Queue error using various logs from the Sterling File Gateway Application.

Train: 4 days of noapp log representing normal log behavior.

Inference: Aggregated system, filegateway, and noapp logs on the day of incident. (Filegateway and system logs only contain errors.)

Result: Reduced detection time and resolve time down by 2 hours 24 minutes. Detected the same error in two log files at the same time.

Mean time to detect   Mean time to resolve

2 hours 24 mins   2 hours 31 mins

0 mins   7 mins
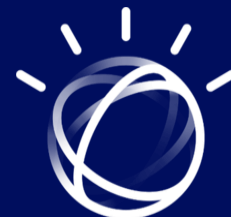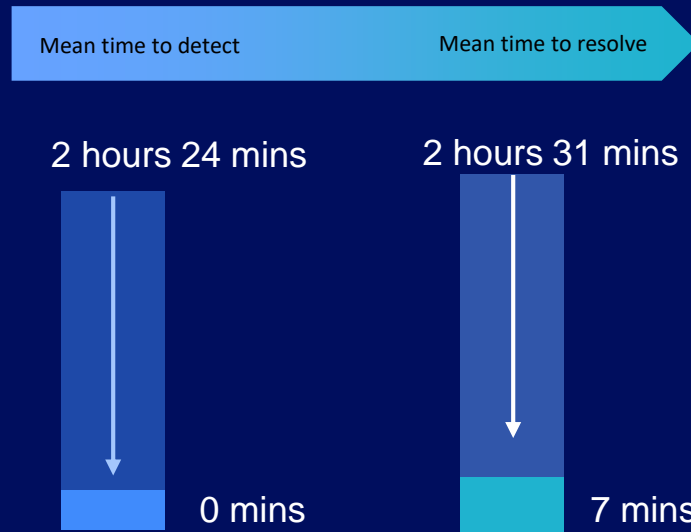
Why IBM Cloud Integration Expert Labs?

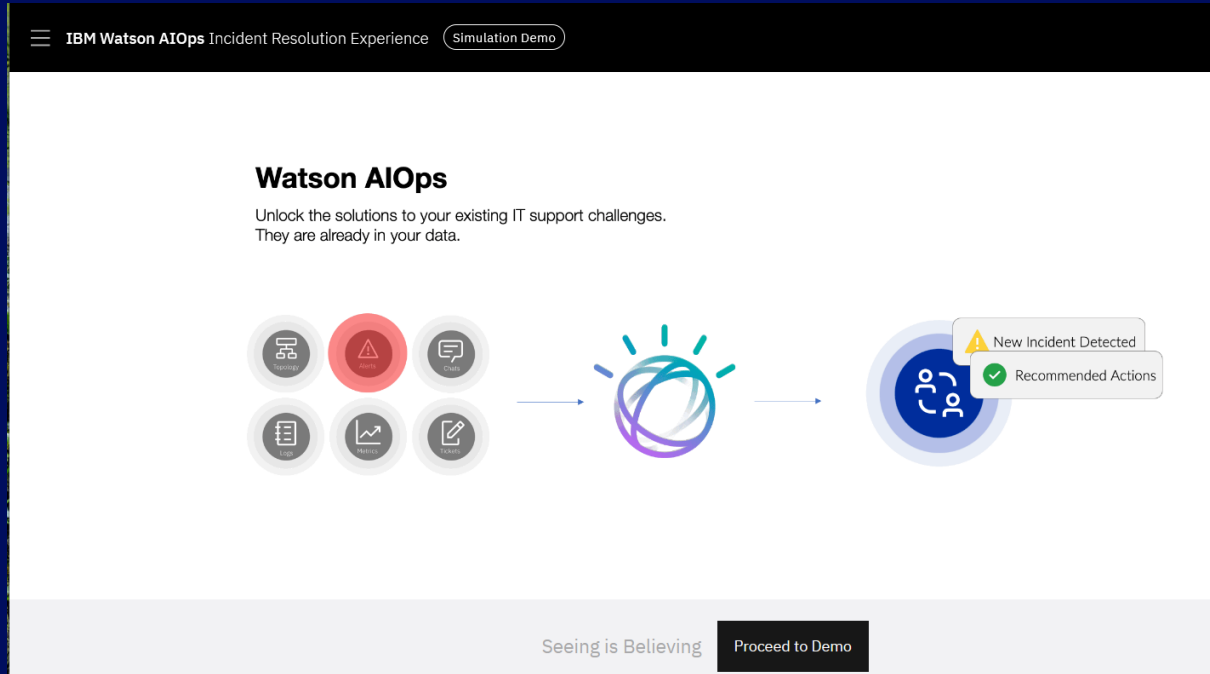| Our purpose	How we drive success	How you benefit
Expedite the successful deployment of IBM's Cloud Integration Solutions	Through our deep technical expertise, methodology, repeatable patterns, learning services and mentoring	Faster time to value from your IBM Cloud Integration Solutions

Contact us through email: **labs@us.ibm.com**

START DEMO // PAUSE DECK

https://www.ibm.com/demos/live/gated/watson-aiops-experience/simulationDemo/sales