EVIDEN

Beyond Monitoring - The Rise of Observability

Sameer Paradkar – Enterprise Architect – Digital
Distinguished Expert – Modern Applications

an atos business

08/06/2023

EVIDEN

Agenda – Beyond Monitoring - The Rise of Observability

Under the hood

KRA & KPI and its Impact

Open Telemetry Framework

Tool Stack & Monitoring Platform

Observability Framework

Self Healing Infrastructures

Observability: Background

System un-availability and under-performance **of applications** ***in IT landscape negatively affect user experience and customer satisfaction causing revenue losses for organizations*****.**

In a complex, multi-layered, distributed computing environment with so many interdependencies it is impossible to keep track of application full-stack, and this is where ***observability enables organizations to find needle in the haystack*****,** ***by identifying and responding to systems issues before they affect customers.***

Observability provides multiple stakeholders with actionable insights into the distributed infrastructure and is a capability of modern enterprises.
Observability enables end-to-end data visibility across multi-layered IT architecture simplifying root cause analysis.
DevOps and SRE teams can quickly identify and resolve issues no matter where they originate or at what point in the software lifecycle they emerge.
This talk will provide you with an understanding of methods, processes and tools that are part of an enterprise scale observability platform.

Observability: Under the Hood

Complex modern infrastructure involves distributed components like cloud, containers, microservices, serverless, and a lot more combinations of these technologies. As the usability and complexity of your system increases with too many moving parts, it becomes difficult to analyze the problems and predict future ones.

Observability is the ability to understand a system's internal states from external outputs such as logs, metrics, and traces.
Observability is a technical solution that uses instrumentation to gather insights, and explore patterns and properties not defined in advance.
Actionable insights **obtained by evaluating the outputs generated by software systems enable you to** ***reach meaningful conclusions into your system's health.***

Observability Vs Monitoring

Monitoring	Observability
Reactive	Proactive
Situational	Predictive
Speculative	Data-driven
What + when	What + when + why + how
Expected problems (known unknowns)	Unexpected problems (unknown unknowns)
Data silos	Data in one place
Data sampling	Instrument everything

As per Gartner's predictions about the pace of change in the software delivery world, *"By 2024, 30% of enterprises implementing distributed system architectures will have adopted observability techniques to improve digital business service performance, up from less than 10% in 2020."*

EVIDEN

Telemetry : Pillars of Observability

Telemetry Type	Pillar Description
Metrics	These are numeric values measured over an interval of time with attributes like granular, timestamped, and immutable records of application events. System metrics are easier to query and can be retained for longer periods.
Logs	**These are time-stamped text records of events that occurred at a particular time.** They come in three formats: plain text, structured, and binary. Error logs are basically the first thing you look for when something goes mayhem in a system.
Traces	**These represent the end-to-end 'journey' of a user request through the entire distributed architecture and back to the user.** Using distributed tracing, you can track the course of requests through your system and identify the cause of any breakdown.

Observability: KPI and KRAs that it impacts (NFRs)

KPIs & KRAs	Description
Customer Experience	Improves the end-to-end customer journey / experience.
MTTR	Reduces Mean Time to Repair **MTTR**
MTBF	Improves Mean Time Between Failures **MTBF**
Reliability & Availability	Improves Reliability & Availability based on business objectives and goals.
Performance	Improves System Performance
Scalability	Improves System Scalability

Observability Platform Objectives

One needs an observable system to spot problems as they arise before they disrupt the customer experience. Early recognition and pre-emptive resolution enable better decision-making and a faster feedback loop.

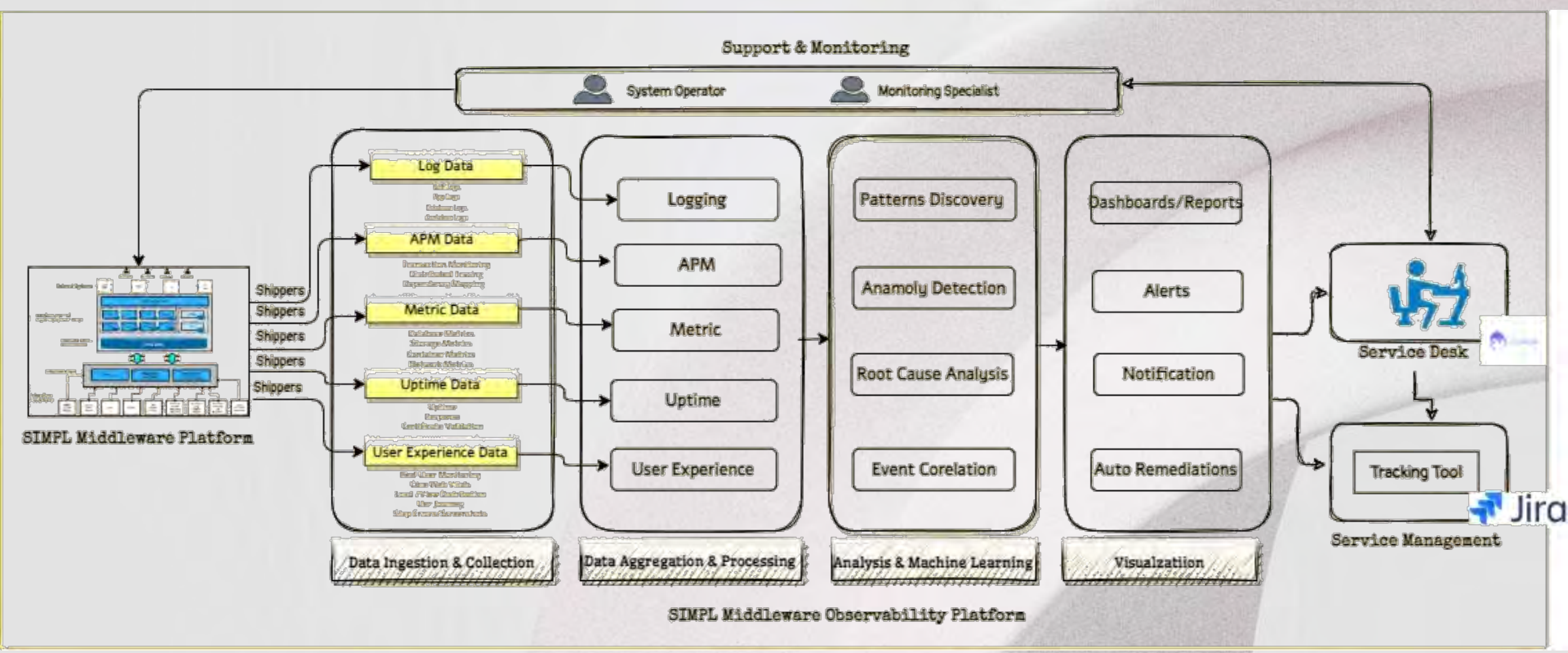
Description
Enhanced visibility of system performance and health.
Discover and address unknown issues with accurate insights.
Fewer problems and blackouts as a result of observability capabilities deployed as part of the IT Landscape.
Predict issues based on system behavior / outs by combining observability with AIOps machine learning and automation capabilities.
Catch and resolve issues in the early phases of the software development process.
Deep-dive into logs and inspect stack trace errors.

Observability Platform Framework

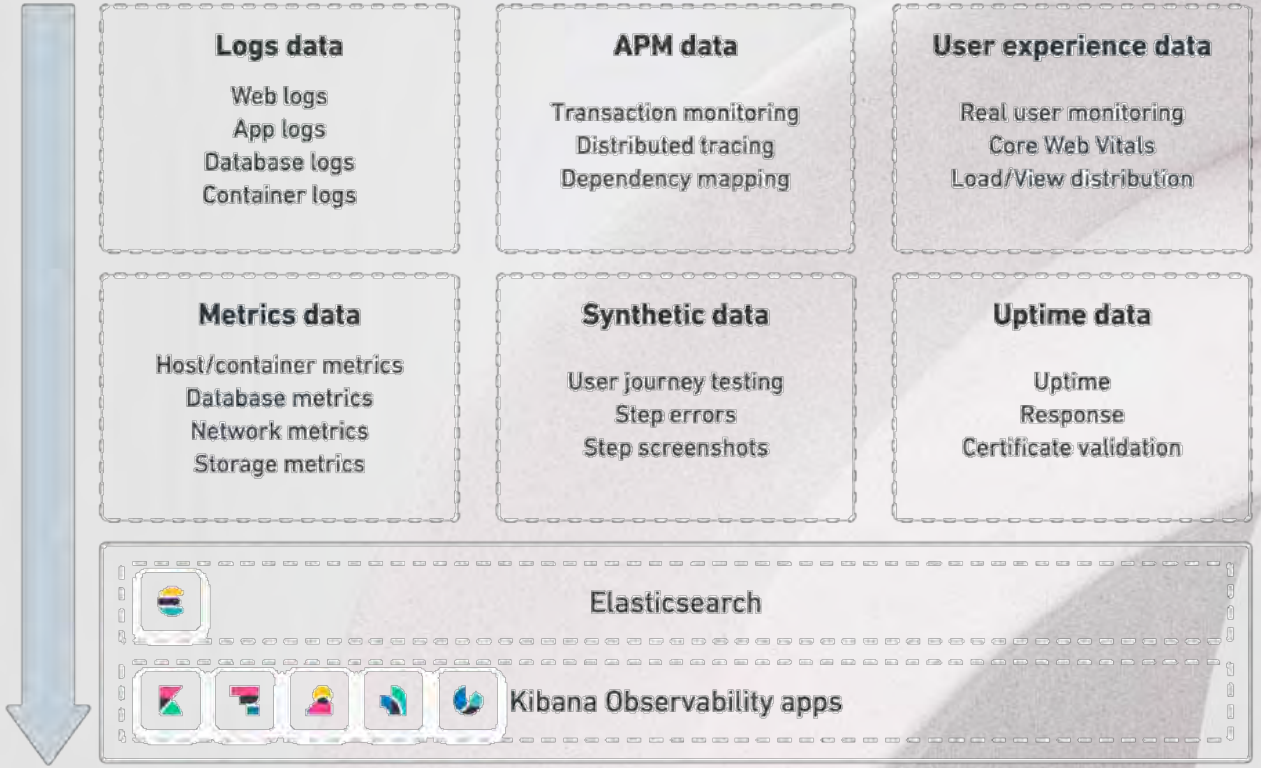
Best Practices and Guidelines for the capabilities to be built into the design of an observability solution:

Description
Reporting on the overall health of systems which includes systems uptime and availability. Monitoring for key business and systems metrics
Reporting on system state as experienced by customers: if the customers experience negatively impacted – Pattern Discovery
Tooling to help understand and debug systems in production. Explicitly documented Service Level Objectives with defined values indicating success or failure - Event Correlations
Access to tools and data that help trace, and diagnose infrastructure problems in the production environment, - Root Cause Analysis
Tooling to identify unanticipated problems, typically referred to in observability circles as “unknown unknowns” – Anomaly Detections

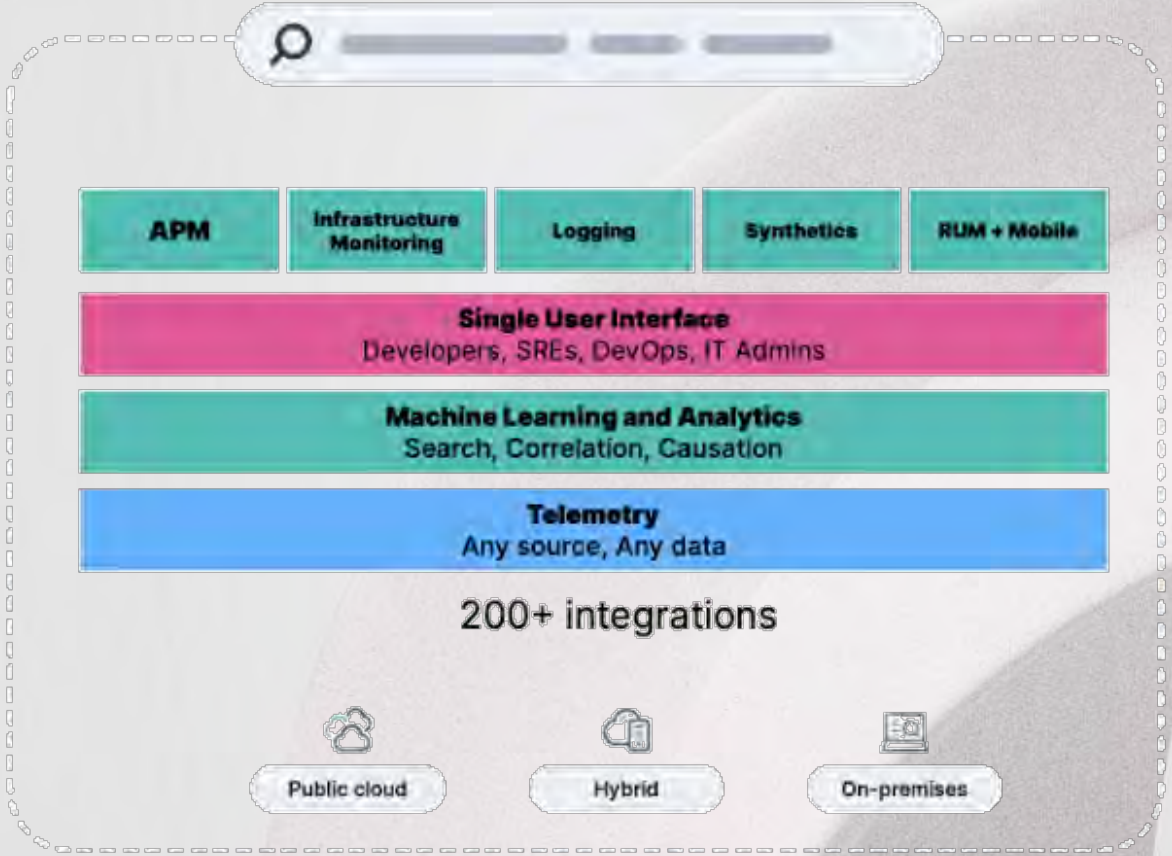
Observability Solution: Reference Architecture



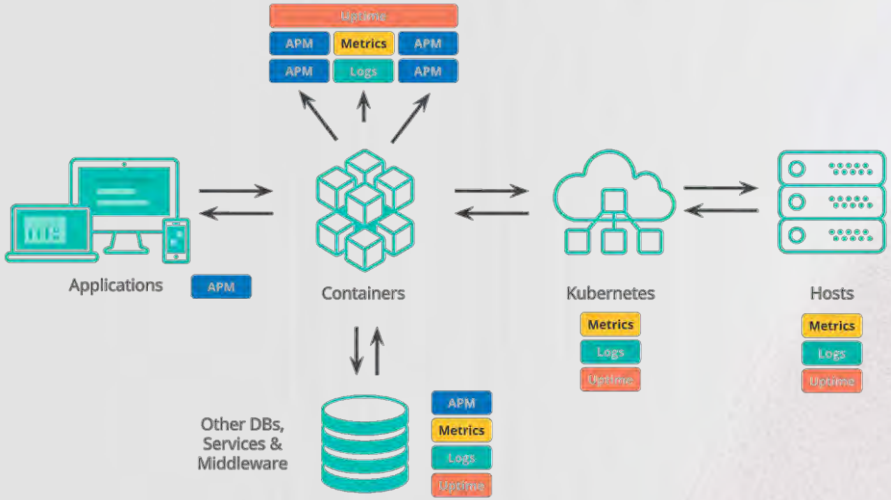
Observability – Logical Architecture

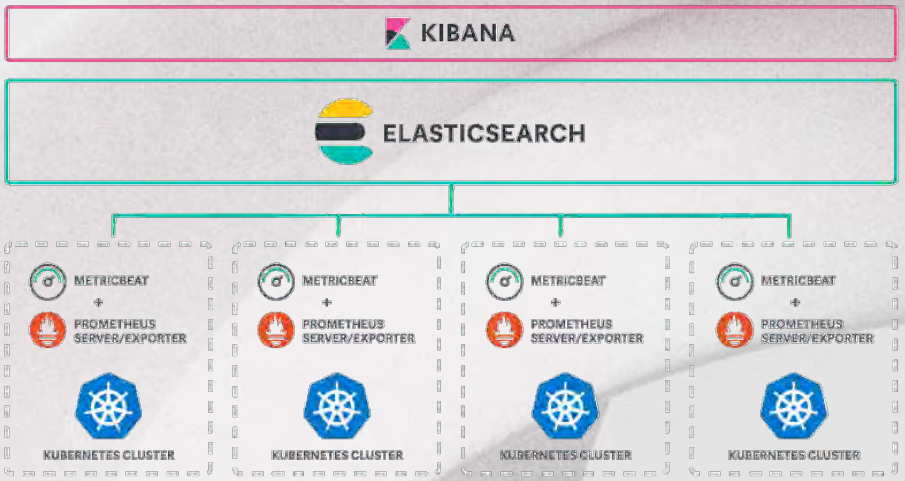


Elastic Observability – Functional Architecture



Observability – Telemetry Parameters





Observability Tooling Stack Comparison – ISV, Open Source & Hyper Scalers

Observability Stages	Open-Source	Azure Native	ISV
Logging	Logstash	Azure Monitor	Dynatrace, AppDynamics, NewRelic
Application Monitoring	Prometheus	Application Insights, Service Health, Service Map	
Distributed Tracing	Jaeger	Application Insights	
Infrastructure Monitoring	Nagios	Azure Monitor, Network Monitor	
User Experience Monitoring	JavaMelody, Apache SkyWalking		
Analyze	Elasticsearch	Azure Advisor, Azure Log Analytics, Azure Metrics Analytics	
Visualize & Respond	Kibana	Alerts, Dashboards, Power BI	

Observability Tooling Stack Comparison – Open Source

Observability Stages	Open-Source - Hybrid	Open Source - ELK
Logging	Logstash	Logstash. Filebeat, Metricbeat
Application Monitoring	Prometheus	Logstash. Filebeat, Metricbeat
Infrastructure Monitoring	Nagios	Logstash. Filebeat, Metricbeat
Distributed Tracing	Jaeger	Logstash. Filebeat, Metricbeat
User Experience Monitoring	JavaMelody (Apache SkyWalking)	Logstash. Filebeat, Metricbeat
Analyze	Elasticsearch	Elasticsearch
Visualize & Respond	Kibana	Kibana

Observability: KPIs & KRAs that it monitors

- ITSI v2.6 ships with nine (9) modules each with prebuilt KPI's
  - Application Servers – 17 KPI's
  - Cloud Services – 7 KPI's
  - Database Systems – 7 KPI's
  - End Use Experience – 8 KPI's
  - Load Balancers – 7 KPI's
  - Operating Systems – 12 KPI's
  - Storage Arrays – 10 KPI's
  - Virtualization – 10 KPI's
  - Web Servers - 8 KPI's
- 86+ available today!

KPIs & KRAs: Application Server Module

KPI and Threshold Reference Table

KPI Name	Description	Unit Type	Threshold Values
4xx Errors Count	Total transaction errors for the analyzed time window	Count	Normal: 0-5, Medium: 5-50, High: >50
5xx Errors Count	Total transaction errors for the analyzed time window	Count	Normal: 0, Medium: 1-25, High: >25
Active Threads Count	Total count of active threads.	Count	No predefined threshold values
Available Thread Count %	Amount of threads that are currently available.	Percentage	Normal: >20, Medium: 5-20, High: <5
Average Transaction Response Time	Average response time (ms) for successful transactions	ms	2-hour blocks every day (adaptive/quantile adaptive thresholding enabled)
Active Sessions Count	Currently active sessions on the application server.	Count	2-hour blocks every day (adaptive/quantile adaptive thresholding enabled)
CPU Utilization %	Amount of CPU utilized by the application server process instance	Percentage	Normal: <70, Medium: 70-90, High: >90
Garbage Collection Time (ms)	Processing time of garbage collection.	ms	No predefined threshold values
Garbage Collections Count	Total count of collected unused heap memory.	Count	No predefined threshold values
Hung Threads Count	Total count of hung threads.	Count	No predefined threshold values
Memory Heap Free %	Amount of Memory Heap available.	Percentage	Normal: <70, Medium: 70-90, High: >90
Memory Heap Size (MB)	Total size of Memory Heap	MB	No predefined threshold values
Memory Heap Used (MB)	Amount of Memory Heap currently used by all applications.	MB	No predefined threshold values
Memory Pool Size	Total size of allocated memory blocks	MB	No predefined threshold values
Memory Used (MB)	Count of total memory in use	MB	No predefined threshold values
Perm Gen Usage (MB)	Total PermGen space currently in use	MB	No predefined threshold values

EVIDEN

KPIs & KRAs: Database Module

Database Module KPI Availability

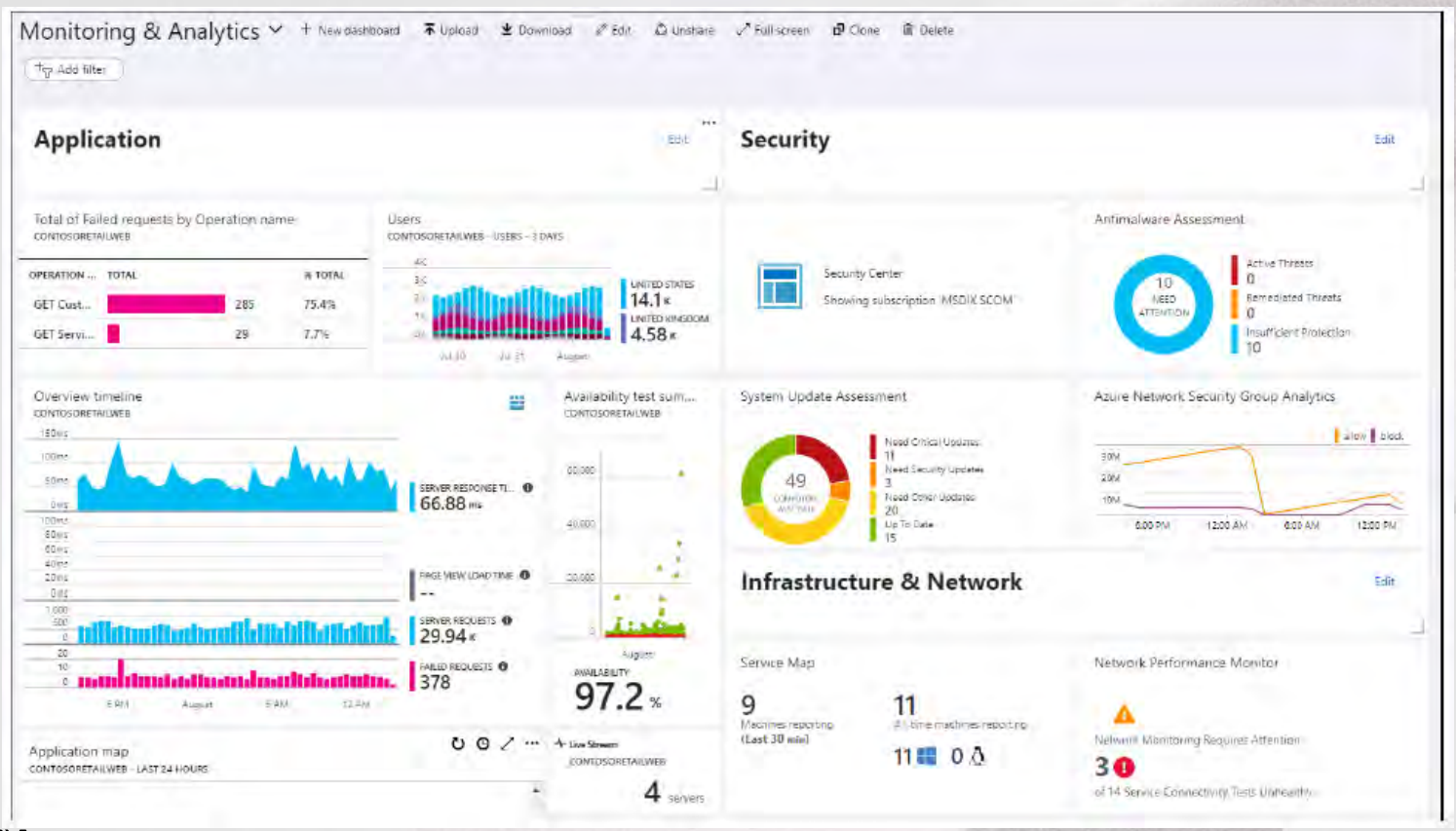
The table below displays KPI availability based on the add-on that is used to collect data, and will display in its corresponding ITSI KPI swim lane.

KPI Name	Microsoft SQL Server Add-on	Oracle Add-on
Database Active Connection	X	X
Database Connection Pool Usage	X	X
Database Deadlock Rate	X	X
Database Query Response Time	X	X
Database Storage Read IOPS	X	X
Database Storage Write IOPS	X	X
Database Transaction Rate	X	X

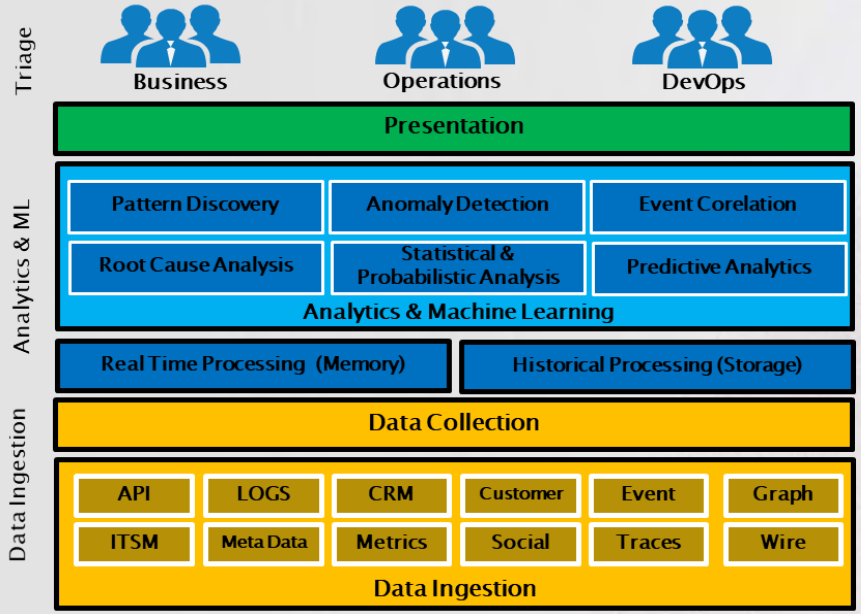
KPI and Threshold Reference Table

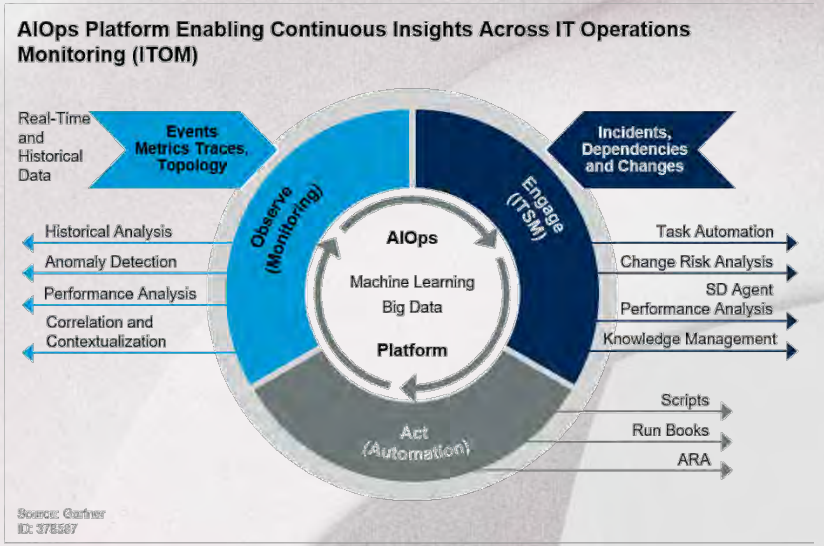
KPI Name	Description	Unit Type	Threshold Values
Database Active Connection	The number of connections currently active per database instance.	Count/Numeral	Adaptive Thresholding Enabled
Database Connection Pool Usage	The percentage of the connection pool being used per database instance.	Percentage	Adaptive Thresholding Enabled
Database Deadlock Rate	The number of deadlocks per second per database instance.	Deadlocks per second	Adaptive Thresholding Enabled
Database Query Response Time	The average amount of time it takes for a query request to return a response per database instance.	Milliseconds	Adaptive Thresholding Enabled
Database Server Storage Read IOPS	The number of reads per second to storage per database instance.	Reads per second	Adaptive Thresholding Enabled
Database Server Storage Write IOPS	The number of writes per second to storage per database instance.	Writes per second	Adaptive Thresholding Enabled
Database Transaction Rate	The number of transactions per second per database instance.	Transactions per second	Adaptive Thresholding Enabled
Database Transaction Rate	The number of transactions per second per database instance.	Transactions per second	Adaptive Thresholding Enabled

Azure Monitoring - Dashboard



AIOps Architecture



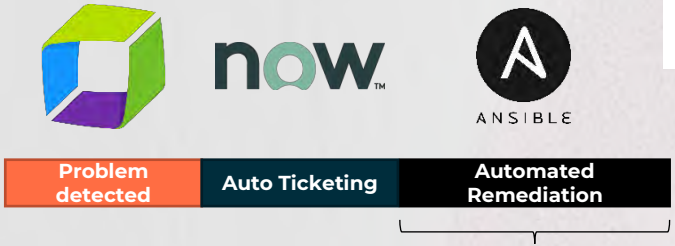


Observability: Automated Cloud Remediation

dynatrace + now + ANSIBLE

Before ACE

After ACE

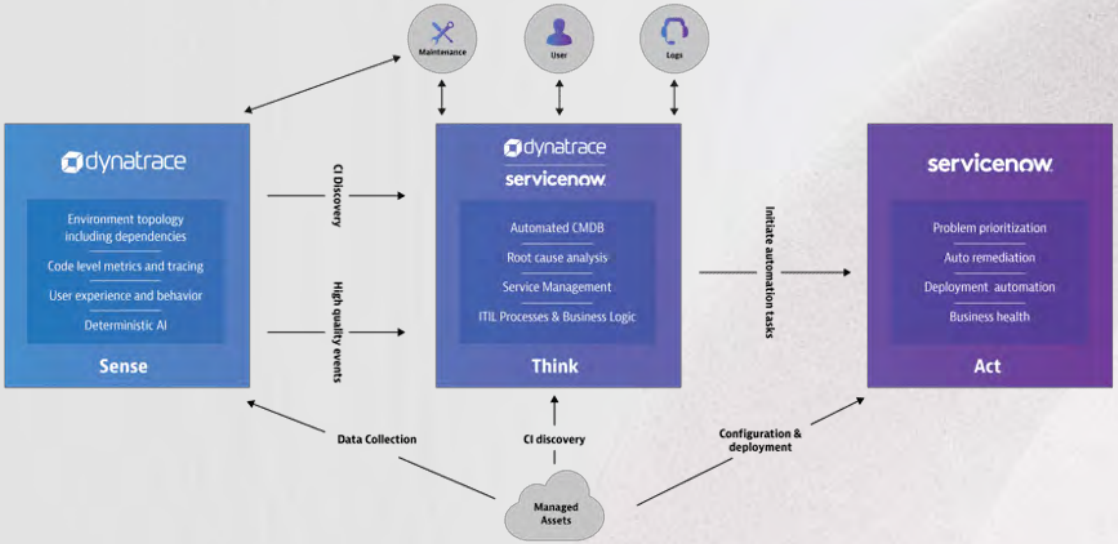


Results Show up to 99% reduction in incident response time

"With Cloud Automation Enablement, we've improved outage resolution time from 1hr to 9 seconds"

Automated Cloud Enablement

Integrate with both ServiceNow & Ansible for automated remediation



- Correlate events in Event Management
- Generate ticket in ITSM
- Notify impacted users in CSM
- Notify IT or DevOps teams via Major incident
- Kick-off automated remediation workflow via Orchestration or Integration hub

Information on problem resolution can be tracked across both systems; bi-directional data flow also helps refine ML models for both systems

Infrastructure as a Code - IaaC

Automate the deployment and management of your entire IT footprint.

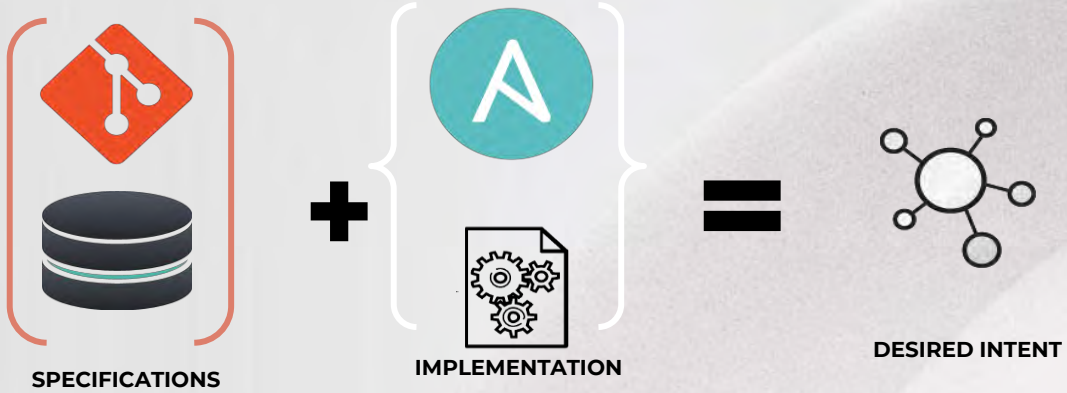
Do this...

Orchestration	Configuration Management	Application Deployment	Provisioning	Continuous Delivery	Security and Compliance

On these...

Firewalls	Load Balancers	Applications	Containers	Clouds
Servers	Infrastructure	Storage	Network Devices	And more...

Infrastructure as a Code - IaaC



The IaC approach promotes formalized, standardized, and automated operational processes—and dictates that these operational processes are documented as configuration files or programming code.

By treating infrastructure as code, IT organizations can automate management tasks while using the best practices of software development, including code review and version control.

This approach mitigates management complexity by breaking down a task into smaller, more manageable processes, controlling the execution of code, and effortlessly maintaining up-to-date documentation.

AIOps: Dynatrace + Azure

Automatically discover all containers running on Azure with a real-time view of all the connections between your containerized processes, hosts, and cloud instances

Easily trace transactions across multi-cloud instances.

Real-time auto discovery and OneAgent injection of Docker and AKS containers without code or image changes.

Leverage Dynatrace OneAgent to deploy the OneAgent onto Kubernetes nodes automatically.

Azure Solution advantages

Monitor applications, clusters, and underlying cloud infrastructure health in Azure environments, in conjunction with and in context to your broader on-premises and hybrid cloud environments.

- Dynatrace OneAgent automates deployment, configuration, and updates to remove all manual effort
- Single view across your entire Azure environment and extended hybrid, multi-cloud ecosystem
- AI-powered problem identification and root cause analytics, including container-based applications
- Scales across 100's or 1,000's of nodes and apps with ease

EVIDEN

Observability : KPIs/KRAs

Adobe Acrobat
Document

Observability : Case Study

Stripe: Another much talked-about example is payment provider Stripe's use of distributed tracing to find the causes of failures and latency within networked services—of which as many as 10 could be involved in the processing of a single one of the millions of payments the company manages daily. With its payments platform a natural target for payments fraud and cybercrime, Stripe has also developed early fraud detection capabilities, which use machine learning models based on similarity information to identify potential bad actors.

Uber and Facebook: Like Stripe, Uber and Facebook also make use of large-scale distributed tracing systems. While Uber's system, Jaeger, serves mainly to provide engineers with insights into failures in their microservices architecture by automating root cause analysis, Facebook uses distributed tracing to gain detailed information about its web and mobile apps. Datasets are aggregated in Facebook's Canopy system, which also includes a built-in trace-processing system.

Observability: Solutions Differentiators

Observability systems enable developers to understand the internal state of a system at any point in time. Let us take a look at what good observability solutions offer:

- User-friendly: Good observability platforms will provide an at-a-glance overview of multiple areas of the business, which makes even the most complex data easy to read and interpret.
- Total visibility of your system: You'll know exactly what's going on in your business at all times with insights in easily digestible formats, such as dashboards for example, that you can comprehend quickly. This way, your business is better positioned to adapt to changing market conditions.
- Delivers Business Value: When you can collect data and analyze key metrics important to your business quickly and meticulously, you get to know where to focus your time to increase results.
- Real-time, Actionable Data: With real-time insights about an issue, its impact on customers, and how it can be resolved, you have a good chance of achieving higher retention rates and increased revenue.
- Support Modern Techniques: Effective tools collect observability data from across your operating environments, stacks, and technologies, and offer the required context for teams to respond.

Closing Notes and Q & A..

@sameersparadkar

sameer.paradkar@eviden.net

https://www.linkedin.com/in/sameerparadkar/

EVIDEN

EVIDEN

Thank you!

sameer.paradkar@eviden.net