# Automatización aplicada a la Observabilidad y Gestión de eventos

Saury Granados Baltodano
Software Architect
IBMchampion

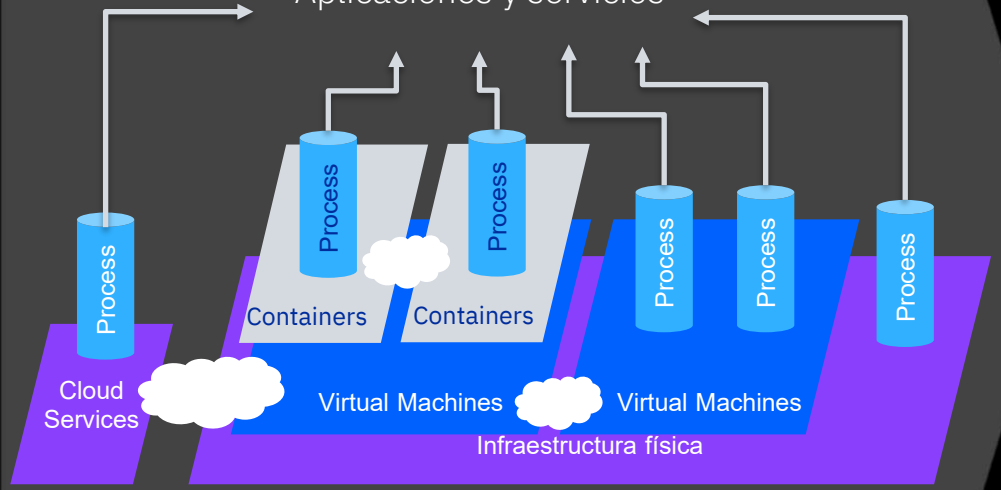
# Agenda

1. Desafio Operativo de TI
2. AIOPS – Centralizar las Operaciones de TI y Aplicaciones
3. Demo

# Desafio Operativo de TI

# Impacto en las operaciones de TI: inundación, indecisión y retrasos

*Entornos híbridos multinube cada vez más complejos*




*Aplicaciones cada vez más dinámicas con arquitecturas flexibles*

Demasiadas alertas


*El 58% de las empresas tienen entre 6 y 40 herramientas de monitoreo diferentes**

Indecisión y confusión


*El soporte de nivel 1 generalmente involucra de 3 a 4 personas por un promedio de 5 a 7 horas de persona **

Largos tiempos de resolución

*El MTTR para problemas relacionados con la aplicación suele ser de 3 a 6 horas **

* Gartner, IDC, IBM Research

# AIOps transforma los desafíos de ITOps en ventajas de ITOps

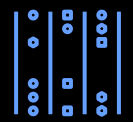
Falta de observabilidad debido a contar con equipos, herramientas y procesos aislados → Eliminar silos →

**Visualización completa y observabilidad**
El descubrimiento automatizado permite a los operadores y desarrolladores comprender el contexto, aislar y resolver problemas en tiempo real

Explosión de datos de TI: no se puede administrar utilizando los métodos actuales → Introducir soluciones inteligentes y predictivas →

**IA para obtener información de TI**
Identifica señales en el momento adecuado, lo que respalda la cultura y la automatización de DevSecOps para escalar los beneficios de TI

Enfoque centrado en la infraestructura para las operaciones de TI → Cambiar el enfoque de las aplicaciones y los propietarios de aplicaciones →

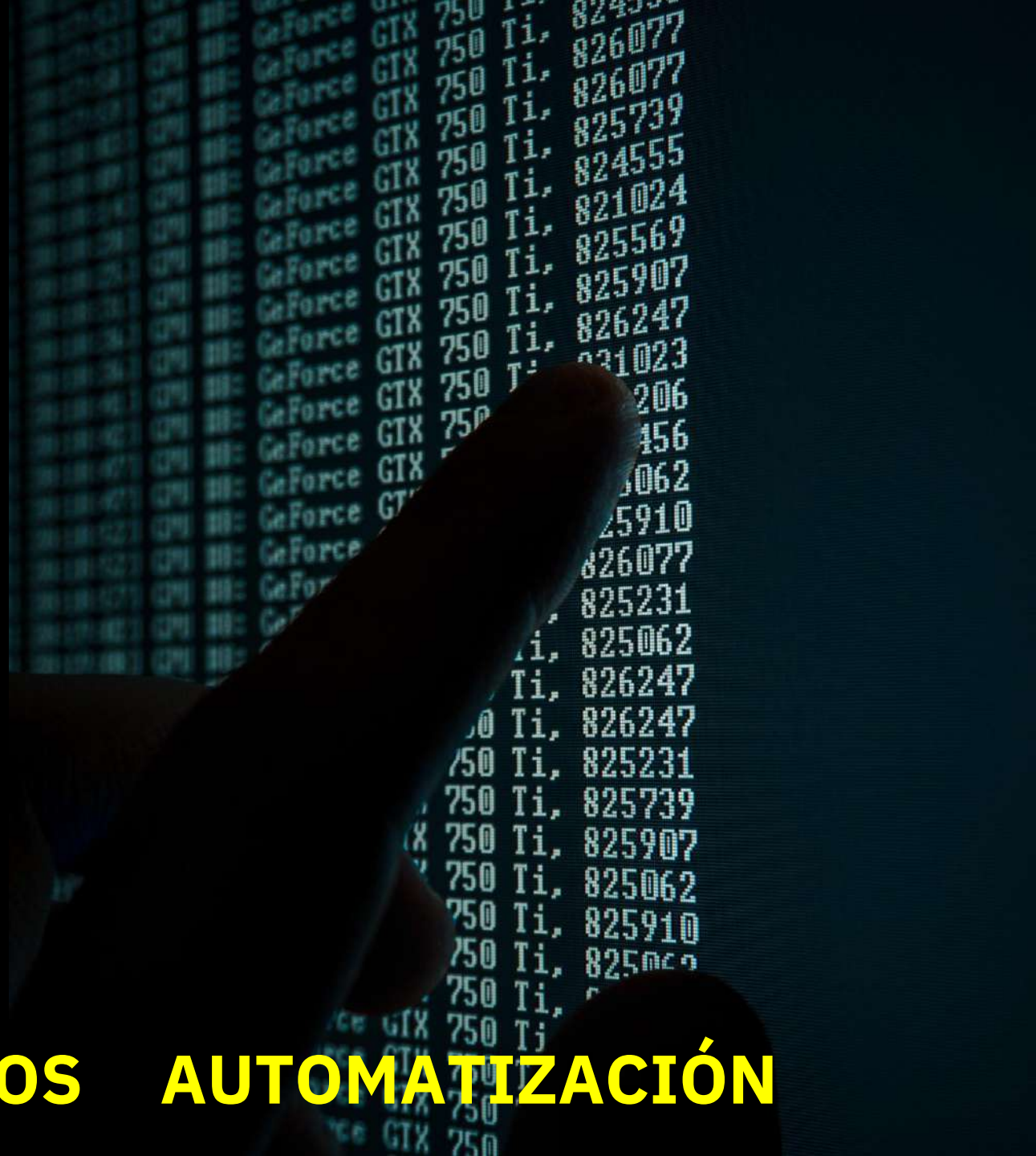


**Enfoque centrado en la aplicación**
Concéntrese en lo que más importa para TI y el rendimiento empresarial: relevante para desarrolladores, operadores y propietarios de aplicaciones

# AIOPS
# Centralizar las Operaciones de TI y Aplicaciones

# AIOps

utiliza la inteligencia artificial para simplificar la gestión de operaciones de TI, acelerar y automatizar la resolución de problemas en los complejos entornos modernos de TI.



**MTTR** **MTTD** **COSTOS** **AUTOMATIZACIÓN**

# Roadmap de Capacidades de Gestión de ITOps con el uso de IA


**Watson AIOps**

Visión Moderna

Fase 1
## Reactivo

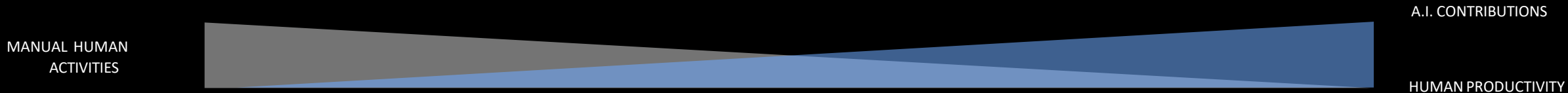
- Correlaciones manuales
- Resoluciones y diagnóstico manuales.
- Analítica basada en reportes

Fase 2
## Proactivo

- IA aplicada para automatizar análisis de las aplicaciones.
- Predictive Insights con sugerencias para la NBA (Next Best Action) y aumentar la interacción humana con la analítica.

Fase 3
## Predictivo

- IA para automatizar la identificación y resolución de problemas potenciales.
- Supervisión y autorización de Operadores humanos.
- Uso de RPA y autómatas*




# Observabilidad

- **Inputs:**
  - Métricas
  - Logs
  - Trazas
  - Indicadores de salud
- **Herramientas posibles:** Instana, Prometheus, Elastic, etc.

# Procesamiento de Eventos / Enriquecimiento

- **Procesos:**
  - Correlación
  - Agrupación
  - Enriquecimiento de datos
- **Objetivo:** Transformar datos crudos en eventos significativos.

# Automatización

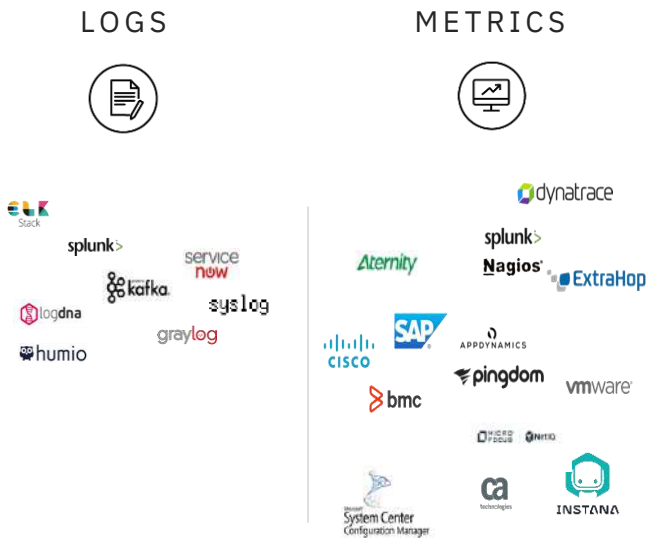
- **Flujos de trabajo automáticos:**
  - Notificación (ej. correo, Teams, Slack)
  - Escalamiento
  - Ejecución de scripts
  - Apertura de tickets (ej. ServiceNow)
- **Herramientas posibles:** IBM AIOps, Ansible, Runbook Automation, etc.

# Incident management without AIOps

# Incident management without AIOps

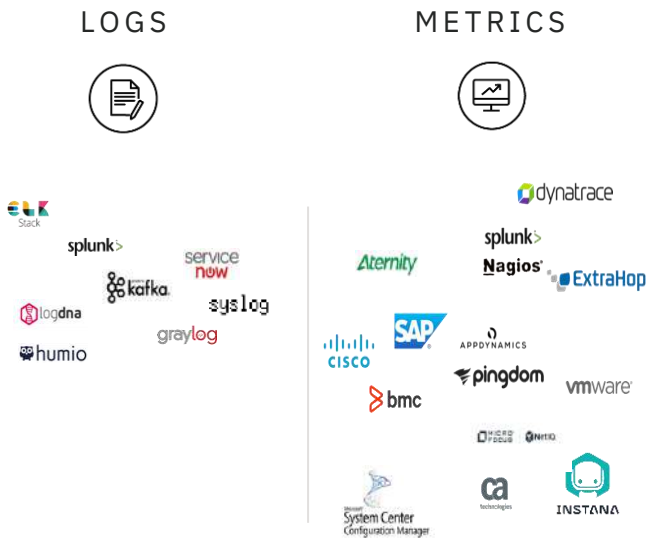
LOGS

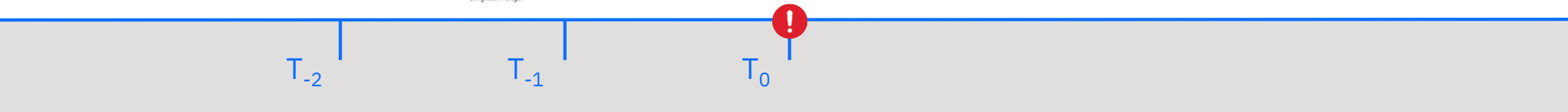
# Incident management without AIOps



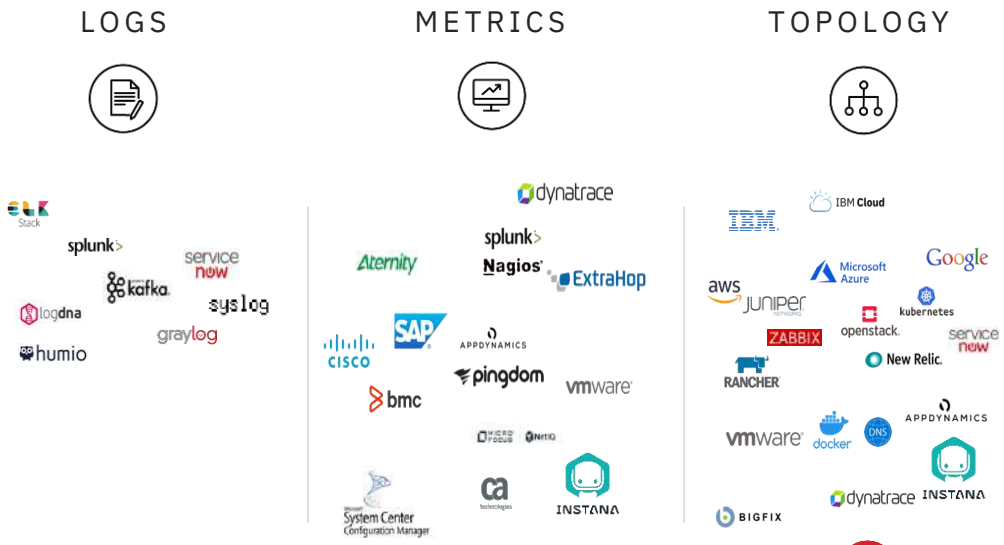

$T_{-2}$ $T_{-1}$

# Incident management without AIOps



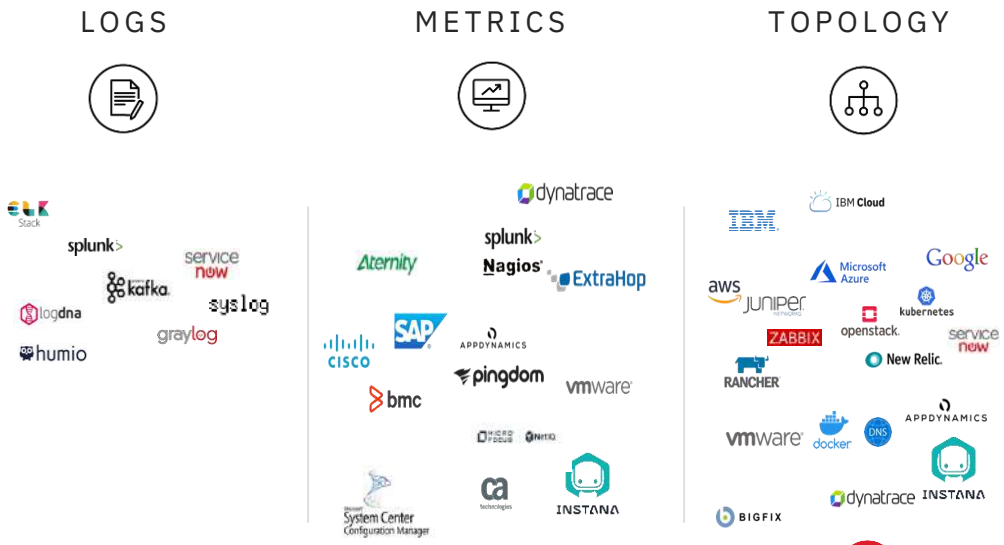



# Incident management without AIOps




$T_{-2}$ $T_{-1}$ $T_{0}$

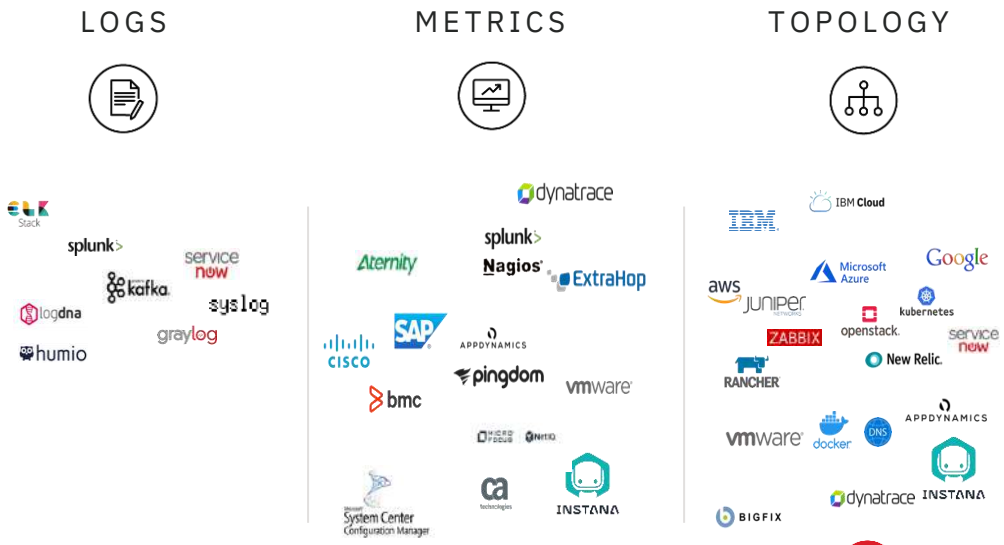
# Incident management without AIOps




$T_{-2}$ $T_{-1}$ $T_0$

OBSERVABILITY

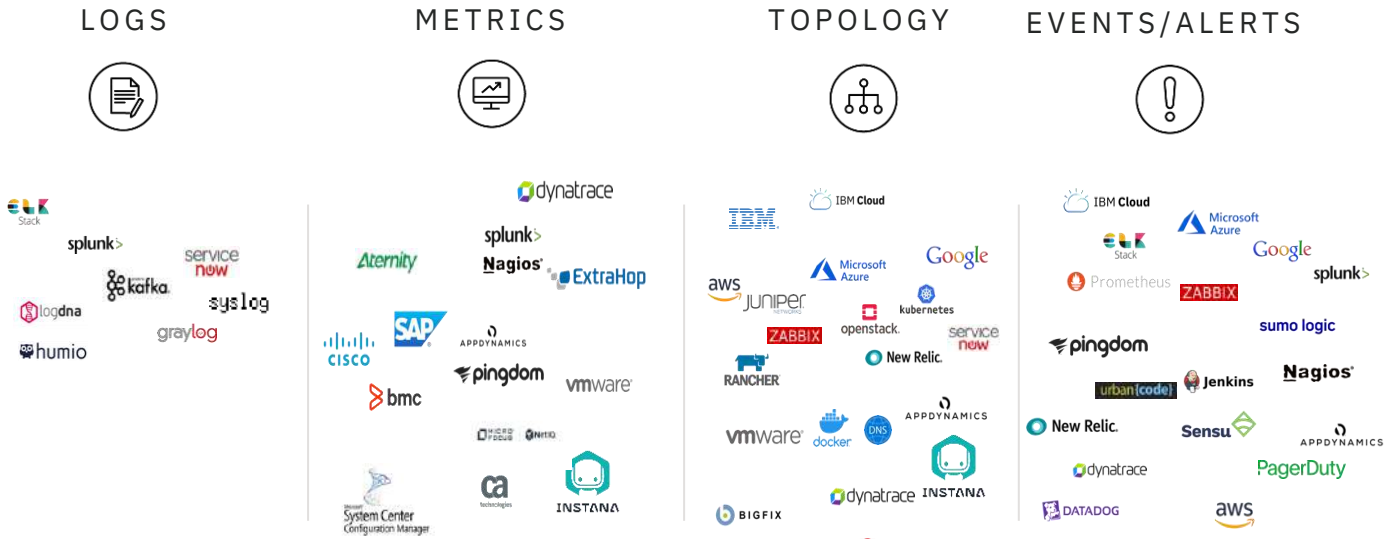
# Incident management without AIOps




$T_{-2}$ $T_{-1}$ $T_0$

OBSERVABILITY AVAILABILITY

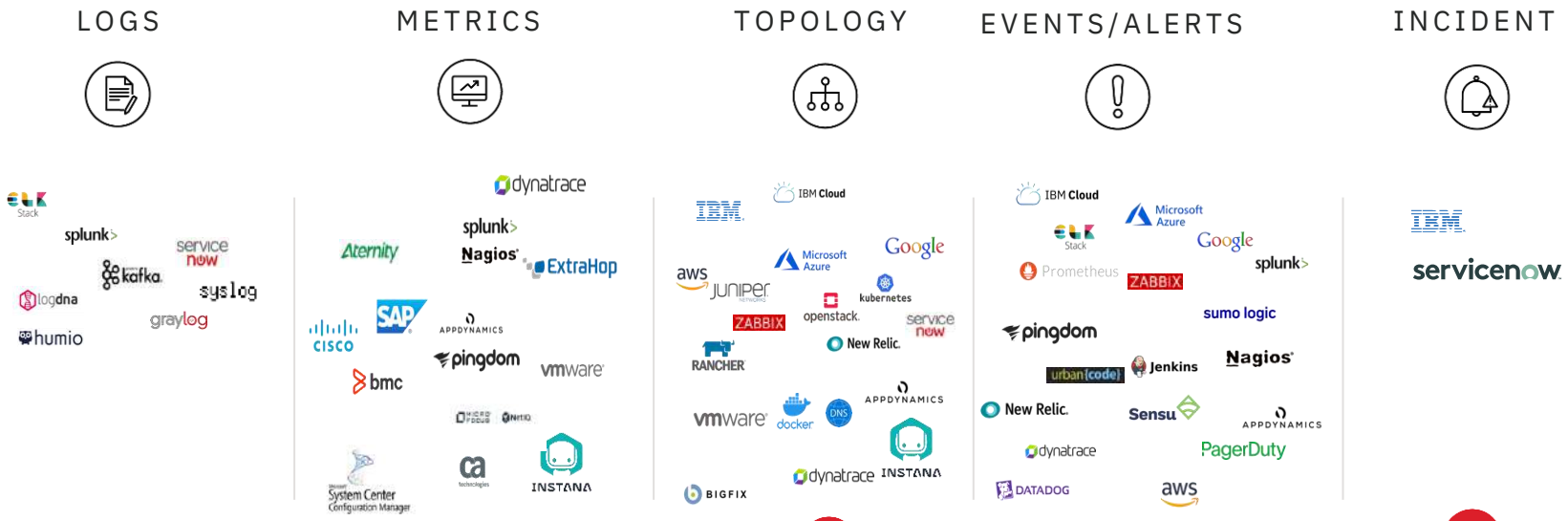
# Incident management without AIOps




$T_{-2}$ $T_{-1}$ $T_0$ $T_1$

OBSERVABILITY AVAILABILITY

# Incident management without AIOps

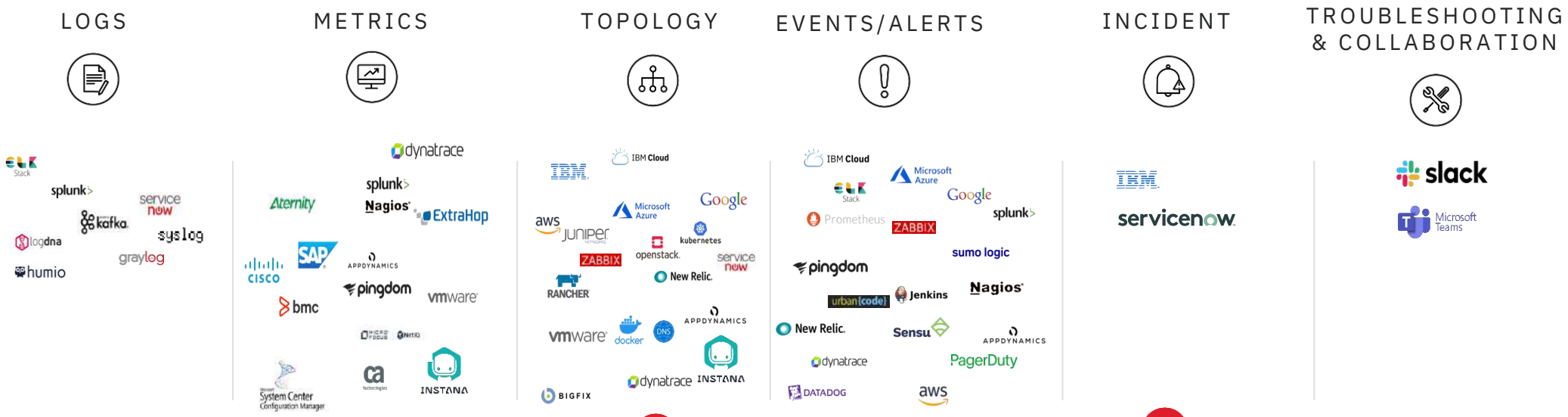



$T_{-2}$ $T_{-1}$ $T_0$ $T_1$ $T_2$

OBSERVABILITY

AVAILABILITY

# Incident management without AIOps



# Populating a virtual war-room / Building a Watson AIOps Story

STORY

LOGS


METRICS


TOPOLOGY


EVENTS/ALERTS


INCIDENT


TROUBLESHOOTING & COLLABORATION


$T_{-2}$ $T_{-1}$ $T_0$ $T_1$ $T_2$ $T_3$

OBSERVABILITY

AVAILABILITY

# Incident management without AIOps

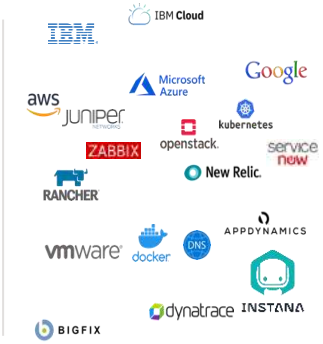
STORY

METRICS


LOGS


METRICS


TOPOLOGY




EVENTS/ALERTS


INCIDENT


TROUBLESHOOTING & COLLABORATION


T-3 T-2 T-1 T0 T1 T2 T3

OBSERVABILITY

AVAILABILITY

# Populating a virtual war-room / Building a Watson AIOps Story

STORY

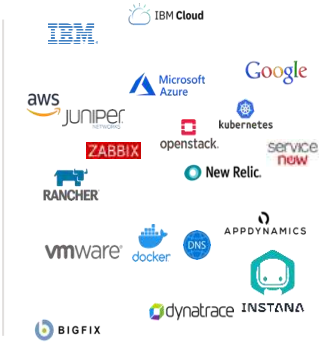
Predictive anomaly detection

METRICS

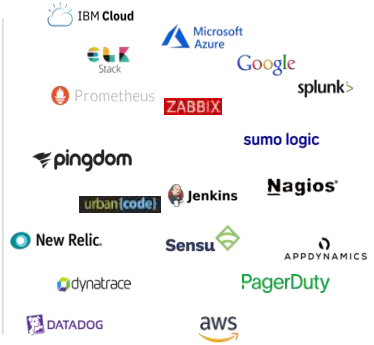

LOGS


METRICS


TOPOLOGY




EVENTS/ALERTS




INCIDENT


TROUBLESHOOTING & COLLABORATION


T-3 T-2 T-1 T0 T1 T2 T3

OBSERVABILITY

AVAILABILITY

# Populating a virtual war-room / Building a Watson AIOps Story

STORY

Notification

Runbook

Next best action

Predictive anomaly detection

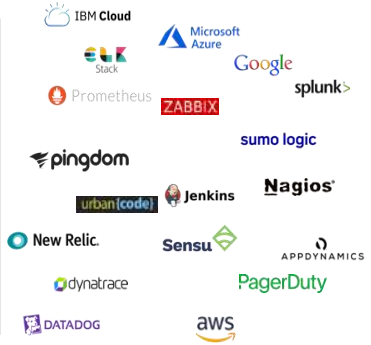
METRICS


LOGS


METRICS


TOPOLOGY


EVENTS/ALERTS




INCIDENT


TROUBLESHOOTING & COLLABORATION


T-3 T-2 T-1 T0 T1 T2 T3

OBSERVABILITY

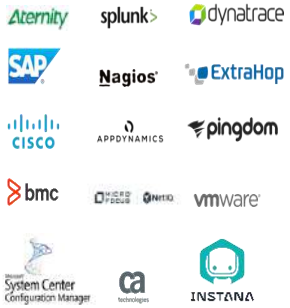
AVAILABILITY

# Populating a virtual war-room / Building a Watson AIOps Story

**STORY**

- Grouping
- Predictive anomaly detection
- AI Models
- Notification
- Runbook
- Next best action

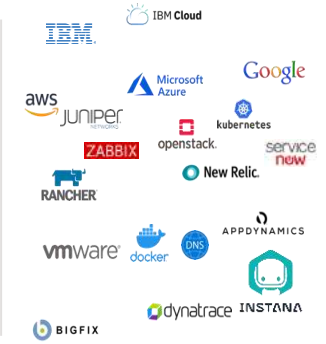
## METRICS



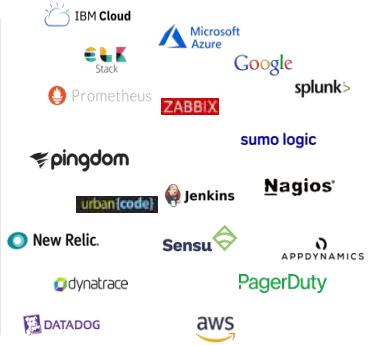

## LOGS


## METRICS


## TOPOLOGY




## EVENTS/ALERTS




## INCIDENT


## TROUBLESHOOTING & COLLABORATION


$T_{-3}$ $T_{-2}$ $T_{-1}$ $T_0$ $T_1$ $T_2$ $T_3$

OBSERVABILITY

AVAILABILITY

# Populating a virtual war-room / Building a Watson AIOps Story

**STORY**

- Grouping
- Multi variant analysis
- Trending/forecasting
- Predictive anomaly detection
- AI Models
- Dynamic thresholding
- Notification
- Runbook
- Next best action

## METRICS

Aternity, splunk>, dynatrace, SAP, Nagios, ExtraHop, Cisco, AppDynamics, pingdom, bmc, Microfocus, Netiq, vmware, System Center Configuration Manager, ca technologies, INSTANA

## LOGS

Elk Stack, splunk>, syslog, logdna, kafka, service now, humio, graylog

## METRICS

Aternity, splunk>, dynatrace, SAP, Nagios, ExtraHop, Cisco, AppDynamics, pingdom, bmc, Microfocus, Netiq, vmware, System Center Configuration Manager, ca technologies, INSTANA

## TOPOLOGY

IBM, IBM Cloud, aws, Juniper, Microsoft Azure, Google, kubernetes, openstack, ZABBIX, service now, New Relic, RANCHER, vmware, docker, DNS, AppDynamics, dynatrace, INSTANA, BIGFIX

## EVENTS/ALERTS

IBM Cloud, Elk Stack, Microsoft Azure, Google, Prometheus, ZABBIX, splunk>, pingdom, sumo logic, urban[code], Jenkins, Nagios, New Relic, Sensu, AppDynamics, dynatrace, PagerDuty, DATADOG, aws

## INCIDENT

IBM, servicenow

## TROUBLESHOOTING & COLLABORATION

slack, Microsoft Teams

$T_{-3}$ $T_{-2}$ $T_{-1}$ $T_0$ $T_1$ $T_2$ $T_3$

OBSERVABILITY | AVAILABILITY

# Populating a virtual war-room / Building a Watson AIOps Story

**STORY**

- Grouping
- Multi variant analysis
- Weighted analysis
- Trending/forecasting
- Event Clusters
- Predictive anomaly detection
- AI Models
- Dynamic thresholding
- Blast radius
- Notification
- Runbook
- Next best action

## METRICS

Aternity, splunk>, dynatrace, SAP, Nagios, ExtraHop, Cisco, AppDynamics, pingdom, bmc, Microfocus, Netiq, vmware, System Center Configuration Manager, ca technologies, INSTANA

## LOGS

Elk Stack, splunk>, syslog, logdna, kafka, service now, humio, graylog

## METRICS

Aternity, splunk>, dynatrace, SAP, Nagios, ExtraHop, Cisco, AppDynamics, pingdom, bmc, Microfocus, Netiq, vmware, System Center Configuration Manager, ca technologies, INSTANA

## TOPOLOGY

IBM, IBM Cloud, Google, aws, Microsoft Azure, kubernetes, Juniper, openstack, service now, Rancher, ZABBIX, New Relic, vmware, docker, DNS, AppDynamics, BIGFIX, dynatrace, INSTANA

## EVENTS/ALERTS

IBM Cloud, Elk Stack, Microsoft Azure, Google, Prometheus, ZABBIX, splunk>, pingdom, sumo logic, urban[code], Jenkins, Nagios, New Relic, Sensu, AppDynamics, dynatrace, PagerDuty, DATADOG, aws

## INCIDENT

IBM, servicenow

## TROUBLESHOOTING & COLLABORATION

slack, Microsoft Teams

$T_{-3}$ $T_{-2}$ $T_{-1}$ $T_0$ $T_1$ $T_2$ $T_3$

OBSERVABILITY | AVAILABILITY

# Populating a virtual war-room / Building a Watson AIOps Story

**STORY**

- Grouping
- Multi variant analysis
- Weighted analysis
- Probable cause
- Trending/forecasting
- Event Clusters
- Recurring events
- Predictive anomaly detection
- AI Models
- Dynamic thresholding
- Blast radius
- Notification
- Runbook
- Next best action

## METRICS

Aternity, splunk>, dynatrace, SAP, Nagios, ExtraHop, Cisco, AppDynamics, pingdom, bmc, Microfocus, Netiq, vmware, System Center Configuration Manager, ca technologies, INSTANA

## LOGS

Elk Stack, splunk>, syslog, logdna, kafka, service now, humio, graylog

## METRICS

Aternity, splunk>, dynatrace, SAP, Nagios, ExtraHop, Cisco, AppDynamics, pingdom, bmc, Microfocus, Netiq, vmware, System Center Configuration Manager, ca technologies, INSTANA

## TOPOLOGY

IBM, IBM Cloud, Google, aws, Microsoft Azure, kubernetes, Juniper Networks, openstack, service now, Rancher, ZABBIX, New Relic, vmware, docker, DNS, AppDynamics, BIGFIX, dynatrace, INSTANA

## EVENTS/ALERTS

IBM Cloud, Microsoft Azure, Google, Prometheus, ZABBIX, splunk>, pingdom, Elk Stack, sumo logic, urban{code}, Jenkins, Nagios, New Relic, Sensu, AppDynamics, dynatrace, aws, PagerDuty, DATADOG

## INCIDENT

IBM, servicenow

## TROUBLESHOOTING & COLLABORATION

slack, Microsoft Teams

$T_{-3}$ $T_{-2}$ $T_{-1}$ $T_0$ $T_1$ $T_2$ $T_3$

OBSERVABILITY | AVAILABILITY

# Populating a virtual war-room / Building a Watson AIOps Story

**STORY**

- Grouping
- Multi variant analysis
- Weighted analysis
- Probable cause
- Historical Analysis
- Trending/forecasting
- Event Clusters
- Recurring events
- Runbook
- Notification
- Predictive anomaly detection
- AI Models
- Dynamic thresholding
- Blast radius
- Next best action

## METRICS

Aternity, splunk>, dynatrace, SAP, Nagios, ExtraHop, Cisco, AppDynamics, pingdom, bmc, Microfocus, NetIQ, vmware, System Center Configuration Manager, ca technologies, INSTANA

## LOGS

ELK Stack, splunk>, syslog, logdna, kafka, service now, humio, graylog

## METRICS

Aternity, splunk>, dynatrace, SAP, Nagios, ExtraHop, Cisco, AppDynamics, pingdom, bmc, Microfocus, NetIQ, vmware, System Center Configuration Manager, ca technologies, INSTANA

## TOPOLOGY

IBM, IBM Cloud, Google, aws, Microsoft Azure, kubernetes, Juniper Networks, openstack, service now, Rancher, ZABBIX, New Relic, vmware, docker, DNS, AppDynamics, BIGFIX, dynatrace, INSTANA

## EVENTS/ALERTS

IBM Cloud, Microsoft Azure, Google, Prometheus, ZABBIX, splunk>, pingdom, ELK Stack, sumo logic, urbancode, Jenkins, Nagios, New Relic, Sensu, AppDynamics, dynatrace, aws, PagerDuty, DATADOG

## INCIDENT

IBM, servicenow

## TROUBLESHOOTING & COLLABORATION

slack, Microsoft Teams

T-3 | T-2 | T-1 | T0 | T1 | T2 | T3

OBSERVABILITY | AVAILABILITY

# Populating a virtual war-room / Building a Watson AIOps Story

**STORY**

Grouping

Multi variant analysis

Weighted analysis

Probable cause

Historical Analysis

Trending/forecasting

Event Clusters

Recurring events

Runbook

Optimization

Notification

Predictive anomaly detection

AI Models

Dynamic thresholding

Blast radius

Next best action

## METRICS

Aternity, splunk>, dynatrace, SAP, Nagios, ExtraHop, Cisco, AppDynamics, pingdom, bmc, Microfocus, Netiq, vmware, System Center Configuration Manager, ca technologies, INSTANA

## LOGS

Elk Stack, splunk>, syslog, logdna, kafka, service now, humio, graylog

## METRICS

Aternity, splunk>, dynatrace, SAP, Nagios, ExtraHop, Cisco, AppDynamics, pingdom, bmc, Microfocus, Netiq, vmware, System Center Configuration Manager, ca technologies, INSTANA

## TOPOLOGY

IBM, IBM Cloud, Google, aws, Microsoft Azure, kubernetes, Juniper Networks, openstack, service now, Rancher, ZABBIX, New Relic, vmware, docker, DNS, AppDynamics, BIGFIX, dynatrace, INSTANA

## EVENTS/ALERTS

IBM Cloud, Microsoft Azure, Google, Prometheus, ZABBIX, splunk>, pingdom, Elk Stack, sumo logic, urbancode, Jenkins, Nagios, New Relic, Sensu, AppDynamics, dynatrace, aws, PagerDuty, DATADOG

## INCIDENT

IBM, servicenow

## TROUBLESHOOTING & COLLABORATION

slack, Microsoft Teams

T-3 | T-2 | T-1 | T0 | T1 | T2 | T3

OBSERVABILITY | AVAILABILITY

- DEMOSTRACIÓN

## Resultado final:

Mayor eficiencia operativa al reducir ruido, detectar eventos relevantes rápidamente y automatizar la respuesta.

¿Te gustaría que lo convierta en una presentación o una versión ilustrada/rediseñada del diagrama?