Service Performance Analytics

Enabling predictive and preventative management...

PCTY2012

Pulse Comes to You

Optimizing the World's Infrastructure
London

Please note:

- IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.

- Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

- The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

- Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

The Need For Proactive Management

- Few companies truly operate their infrastructure in a truly proactive manner.

- Most organization react to service outage or degradation after it occurs, even though the impact may be counted in the million of dollars per hour.

- Compound service degradation, that spans operational silos is, is one of the biggest challenges for management teams.

- IT and Operations Management teams are now being tasked with avoiding these problems and ensuring service continuity.

So Why Are So Few Operational Teams Proactive?

- **Problems are not being detected in the emerging phase, before they become service impacting.**

  - The manifestation of emerging problems in performance data may not be sufficient to trip traditional univariate thresholds

  - Problems may be complex, with a combination of faulty metrics compounding to contribute to a outage or service degradation.

- **There is too much infrastructure management noise, so even if an emerging alert is produced, it is lost in the daily noise.**

  - Too many performance threshold violations are produced.

  - Random threshold thrashing generate large volumes of events, that while valid, are a poor indication of actual problem conditions.

  - Many hundreds of threshold violations may be produced per problem, with many tens of problems existing concurrently.

An Introduction to multivariate analytics

Optimizing the
World's Infrastructure

A Comparison Of Analytic Approaches

Monitoring the heath of a regular car engine using basic metrics

Fuel

Engine Temp

Outside Temp

Oil Pressure

Engine Revs

Brake Usage

Brake Fluid

Battery

Speedometer

Monitoring engine heath with time series metrics
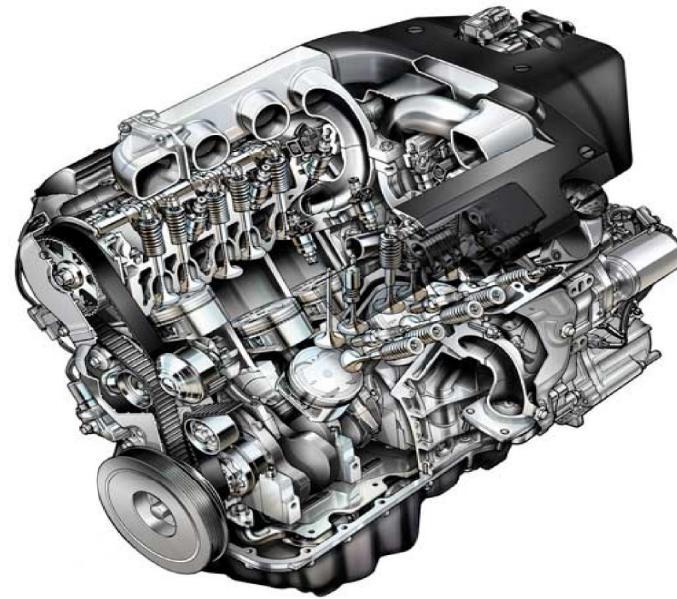
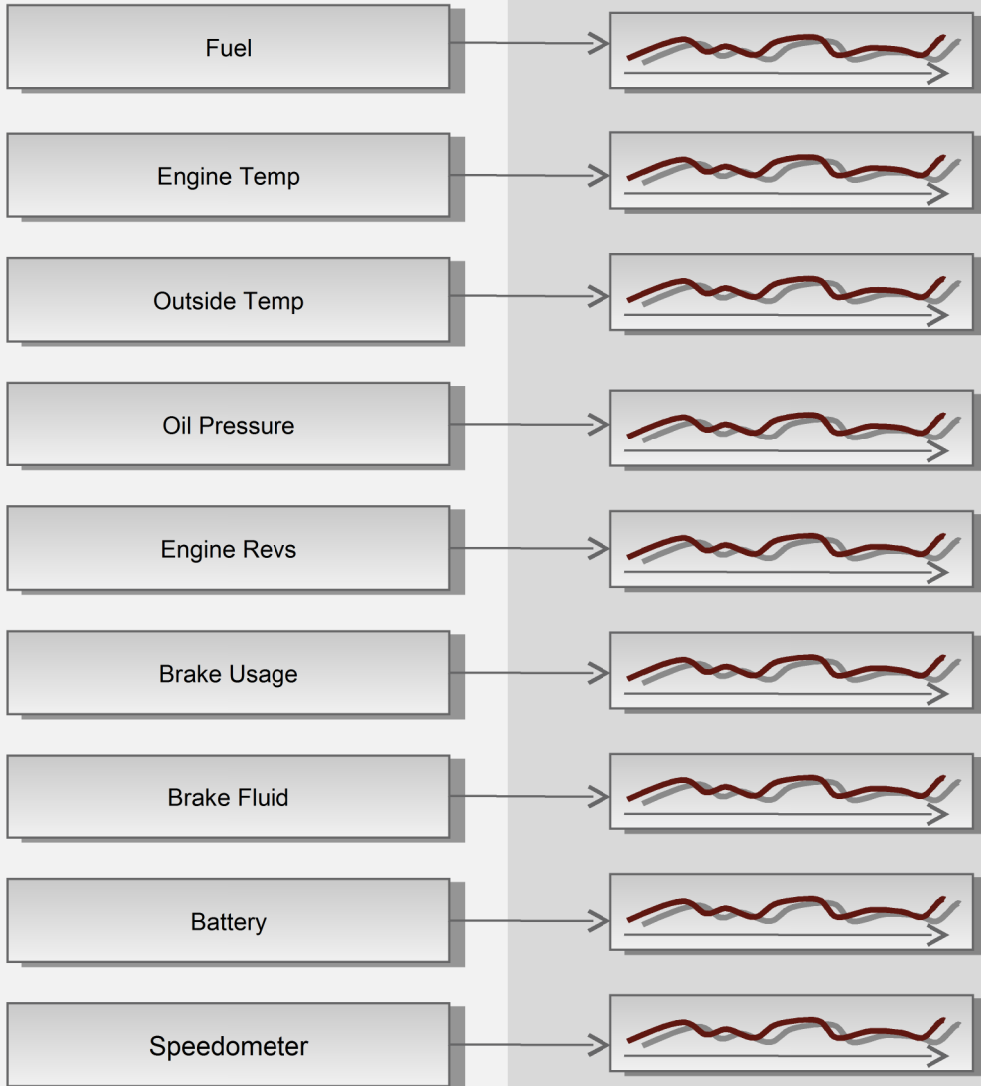# Monitoring Engine Health, A Univariate Approach

Metrics	Analysis	Alerts/Alarms
Fuel		With univariate, each metric is considered in isolation.
Engine Temp		
Outside Temp		**Now imagine two problem occur simultaneously!**
Oil Pressure		
Engine Revs		1. Blown oil gasket
Brake Usage		2. Battery loses charge
Brake Fluid		
Battery		
Speedometer		

Monitoring Engine Health, A Univariate Approach
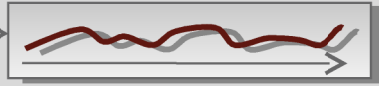
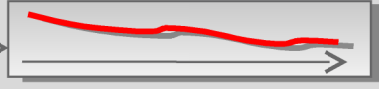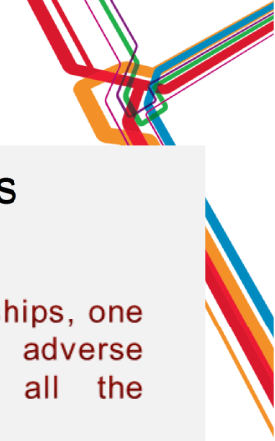| Metrics	Analysis	Alerts/Alarms
Fuel		
Engine Temp	Alert!	ID: 1 Threshold Violation: Engine Temp
Outside Temp		
Oil Pressure	Alert!	ID: 2 Threshold Violation: Oil Pressure
Engine Revs		
Brake Usage		Each metric generates an alert in isolation.
Brake Fluid		
Battery	Alert!	ID: 3 Threshold Violation: Battery
Accelerometer		
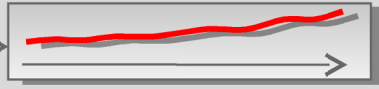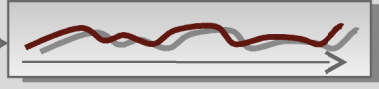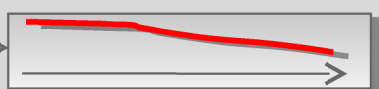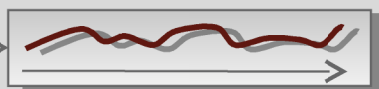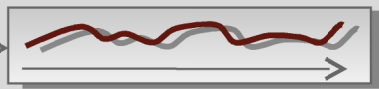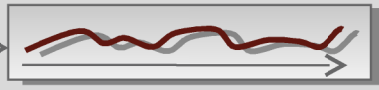
Monitoring Engine Health, A Multivariate Approach

Metrics

- Fuel
- Engine Temp
- Outside Temp
- Oil Pressure
- Engine Revs
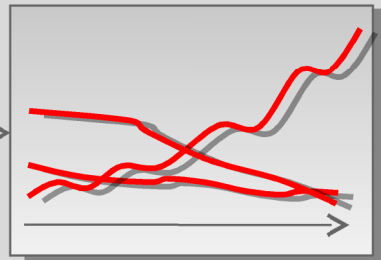- Brake Usage
- Brake Fluid
- Battery
- Accelerometer

Analysis

All metrics are considered together.

Alert!

Alert!

Relationships between metrics are discovered.

Alerts/Alarms

By learning metric relationships, one alert is generated for an adverse change, which includes all the deviating metrics involved.

ID: 1 Anomaly

Anomaly Alert. Related Metrics:
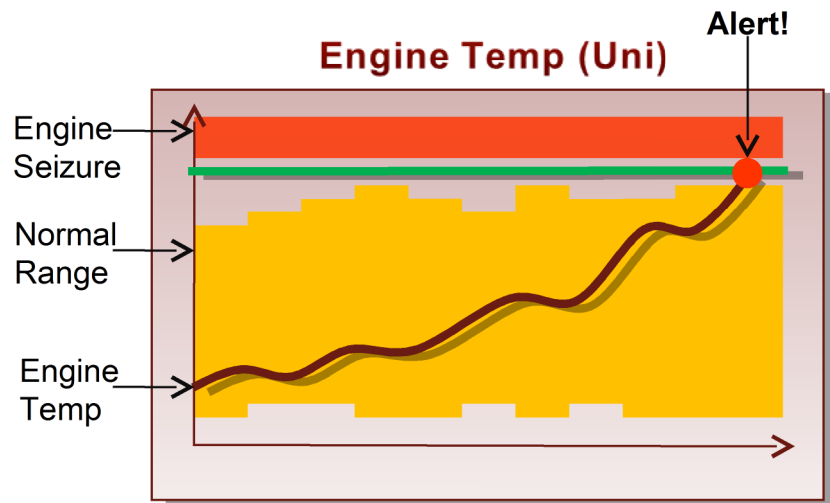- Oil Pressure Deviation: 46%
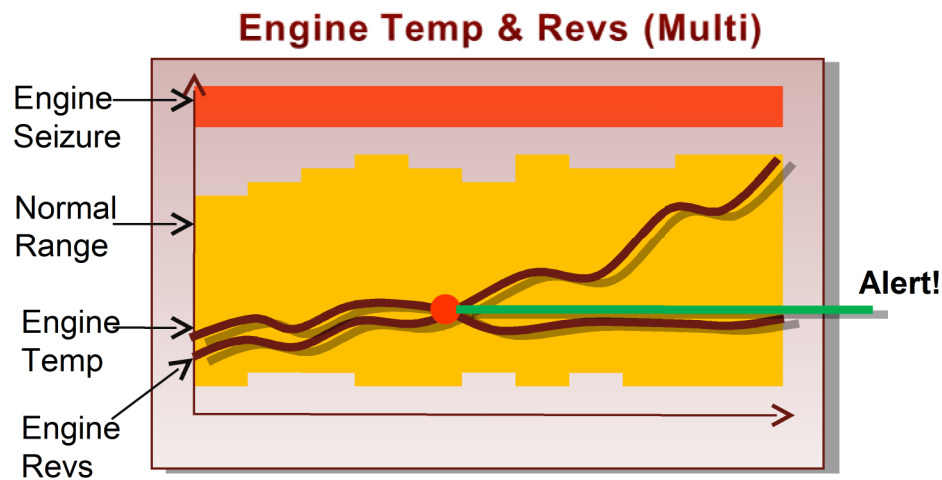- Engine Temp Deviation: 16%

ID: 2 Anomaly

Anomaly Alert. Related Metrics:
- Battery Deviation: 32%

- Correlates metrics
- Fewer more accurate alerts
- Helps with root cause analysis.
- Detects problem sooner (how?, next)

How Does Multivariate Analytics Detect Problems Sooner?

Engine Temp (Uni)

Alert!

Engine Seizure

Normal Range

Engine Temp

Static Threshold = Short Warning

Engine Temp & Revs (Multi)

Engine Seizure

Normal Range

Engine Temp

Engine Revs

Alert!

Multivariate = Alerts earlier on Deviation

Multivariate analytics detects problems sooner by detecting the deviation of metrics that normally move together.

For example:

• Engine temperature and engine revolutions normal move together. This is healthy system behaviour...

• But when engine temperature deviates from engine revolutions, as would happen with coolant leak, this indicates a problem and an alert is generated.

• The alert is generated much sooner than waiting for engine temperature to exceed normal operational ranges.

This advanced warning time helps you become proactive and mitigate damage before service is impacted.

Value of a Multivariate Analytics System
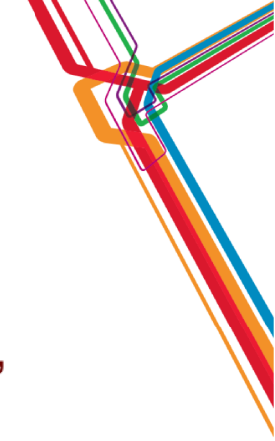
- Learns normal operational behaviour across the infrastructure, including how metrics behave together.

- Maximize Advance Warning: Identifies metric relationship changes that signal a problem long before traditional thresholds

- Identifies problems before you know to look for them

- Detects service impacts that are not identifiable by fixed thresholds alone.

- Assists with root cause analysis by indicating the most offending metrics.

- Reduces expensive and time consuming false alerts.

An Introduction to service performance analytics

Optimizing the
World's Infrastructure

Ongoing Investment In Analytics, Both Acquisitions and Organic

IBM is helping the industry by continuing on a journey of innovation. We have committed over $23 billion to acquire and develop best-of-breed tools

IBM is driving the future of integrated analytics through acquisitions and our strategic partnerships:

ACXIOM

Experian — A world of insight

Business Analytics & Optimization Solutions

Business Analytics & Optimization Platform

Trusted Information Platform

NETEZZA

SPSS

EXEROS

unica

princeton softech

ILOG — Changing the rules of business

Core metrics — An IBM Company

COGNOS

FileNet

DataMirror

solid.

dwl

Ascential

LAS

unicorn

InfoSphere software

Trigo

iphrase

SRD

PCTY2012

IBM Research

IBM holds more patents than any other U.S. based technology company and has eight research laboratories worldwide.

IBM employees have earned Five Nobel Prizes, four Turing Awards, five National Medals of Technology, and five National Medals of Science.

2009 Patent Awards

Company	Patents
IBM	4914
Microsoft	2906
Intel	1537
HP	1273
Apple	289
EMC	250
Oracle	208
Google	141
Accenture	43

70% Software and Services
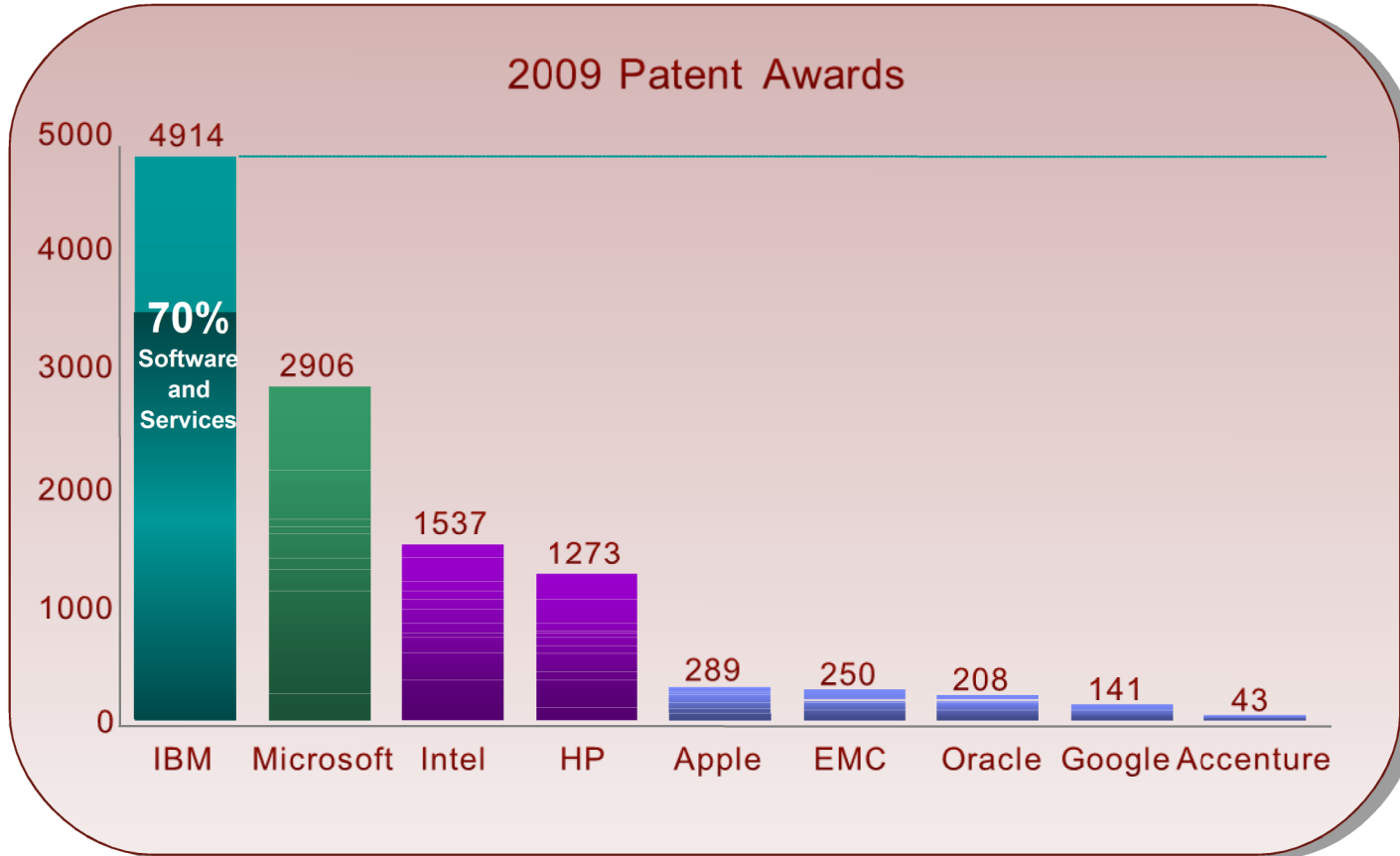
IBM Research Business Analytics and Optimisation

- **Over 200 researchers with expertise in data analytics**, operations research, mathematics, and industry applications of analytics

- **Hold 300 patents and have an additional 450 pending** on analytics and business applications

- Support IBM's "fact-based" management and processes in sales, supply chain, and services.

- Lead in the global scientific community
  - Over 250 publications in leading conferences and journals in recent years
  - Fellows at several leading professional societies
  - Successive wins at KDD Cup and INFORMS Data Mining Competitions (premier competitions)
  - Leaders in Optimization Open Source
  - Major INFORMS prizes and awards
  - Adjunct faculty at leading universities

Improved profitability through analysis of customer networks for a major telecom customer by providing better customer targeting

Deployed operational planning and scheduling to run steel plants at several leading Asian steel manufacturers – improved productivity

Design optimal maintenance plan for a set of interconnected offshore oil platforms - improve availability of oil platforms

Analytics-Driven Solutions for Increased IBM sales force productivity – increased revenue and profitability

Improved wafer yield at the IBM 300mm semiconductor plant deploying data mining and machine learning

Creation of state-of-the art error correction code technology that is used in main memory systems of IBM's computers

Provide analysis of operational risk loss data for 36 leading banks from 13 countries - cross enterprise secure and anonymous data sharing

Centralized control and real-time visibility of the end-to-end supply chain for IBM supply chain – reducing inventory

Coming Soon: Analytics for Service Performance

Proactive and self-learning performance and bsm intelligence

- Real-time analytics for detecting and avoiding service disruption.

- Uses advanced multivariate analytic algorithms; providing all the advantages mentioned previously.

- Correlates metric across multiple domains and heterogeneous data sources.

- Ultra scalable; analyzing massive volumes of metrics in a single multivariate instance.

- Leverages key IBM analytic engines and mediation

- Works in non-Tivoli environments, as well as integrating tightly with Tivoli suite.

PCTY2012

Software Architecture

3rd Party Event Consoles

SNMP

TIP Visualization

Analytic Algorithm Application

Streaming Analytic Engine

Mediation
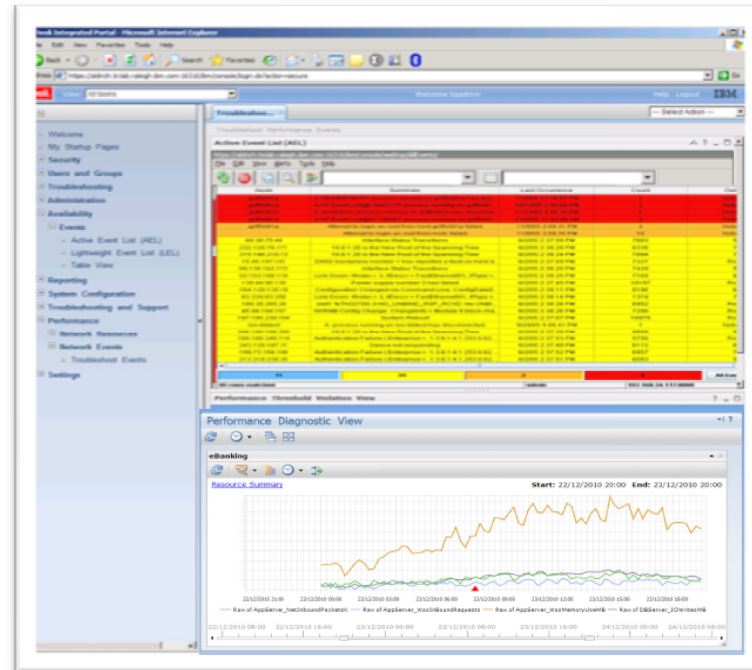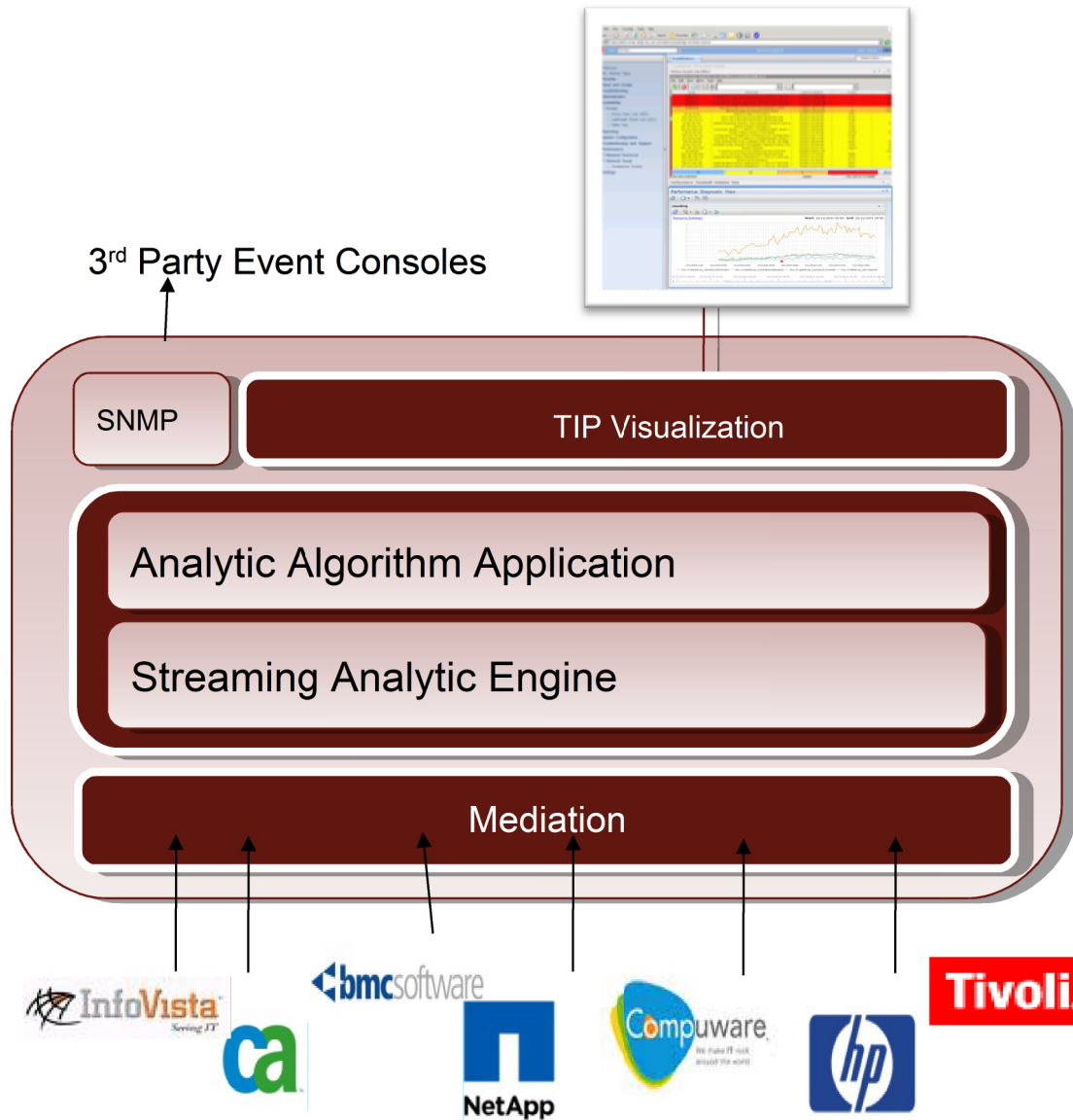
- Leverages IBM Information Management assets to fields a state-of-the-art solution:

- Highly scalable and resilient streaming analytic engine.

- Powerful analytic algorithms, combining uni & multivariate approaches, designed to leverage InfoSphere Streams engine for unlimited scalability.

- Highly scalable and flexible data mediation layer providing turn-key integrations and easily extendable capabilities.

- TIP based, native visualisation.

- SNMP and Netcool/Omnibus native predictive alerts

Embedded Analytic Visualization:
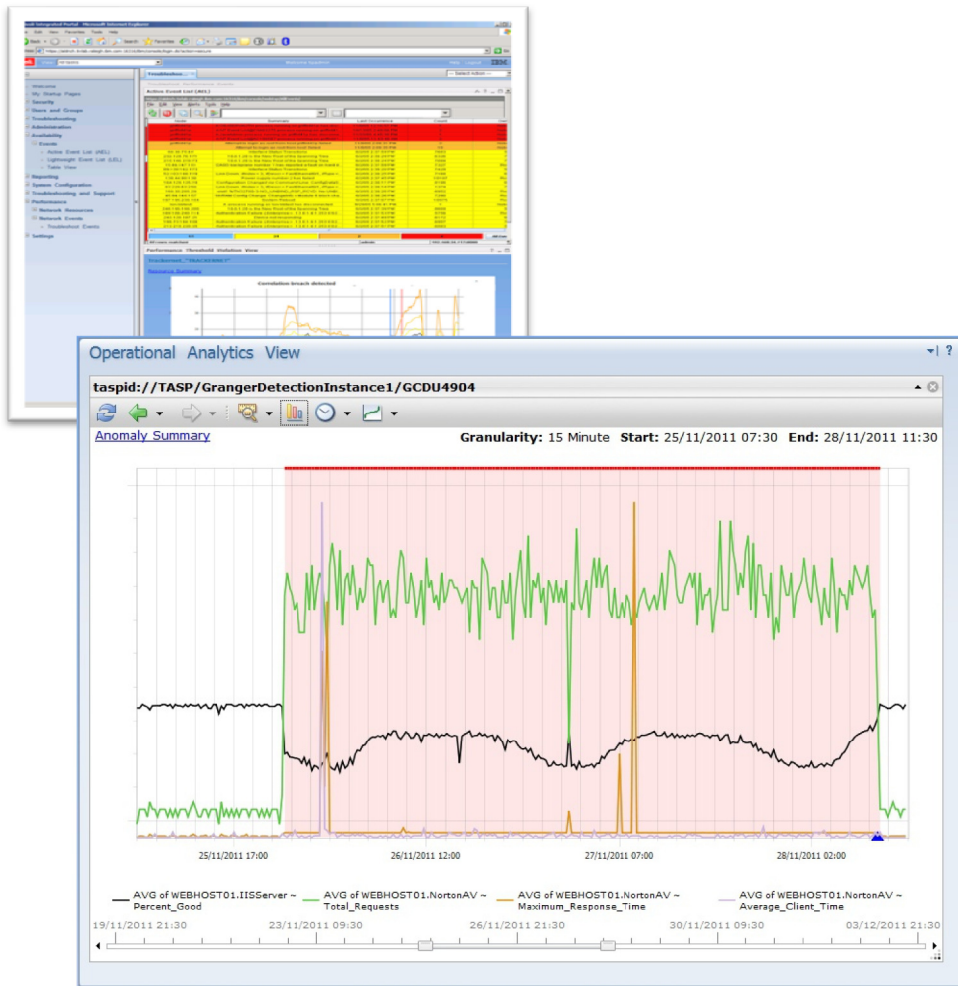
- Modular design plugs into Tivoli environment or installs independently, quickly accepting data from any source (including Tivoli products of course)

- TIP based user & security framework.

- TIP based native WEB 2.0 visualisation

- Multiple metric chart overlay.

- Toggle display of individual metrics.

- See correlated metrics and relationships.

- See deviations details.

- Out of the Box integration with Tivoli Netcool/OMNIbus event management console.

- Easily linked to any event system that receives SNMP traps and supports HTML Launch in Context

Streaming Engine Deployed in World's Fastest Options Trading Environments

High performance and scalability:

- Simplifies deployment setup (no splitting service metrics across multiple multivariate instances).

- Reduces human "guesswork" on which metrics to ignore or analyse

- By evaluating many metrics, the maximum value of multivariate analytics is gained.

- Allows for continuous learning configuration; one instance learning, one running; always adapting to dynamic environments.

- Proven in the most unforgiving high volume low latency environments – processing 5 Million events/second with 150ms average latency

- Also deployed in finance, defence and security applications world-wide

- Core product of IBM's Smarter Planet strategy

Under the covers: Market Leading Mediation
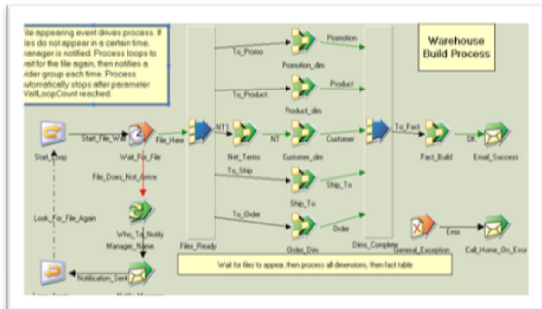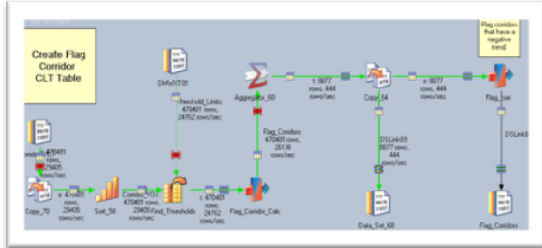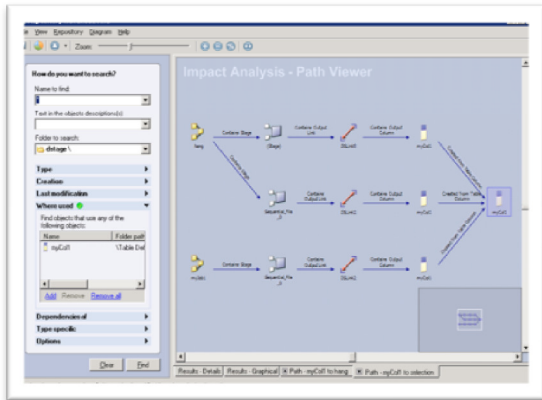
- Market leading mediation software, used in thousands of accounts

- Proven rapid integration with new data sources

- Platform Productivity & Collaboration (Tooling & Metadata, Reuse)

- Performance & Scalability (True Parallel Pipelining & Partitioning, Seamless Grid Support)

- Large framework of connectors available to make new integrations;

- Turn-key integrations to common performance monitoring suites...

Large Framework of Connectors:

RDBMS

DB2 (on Z, I, P or X series)
Oracle
Informix (IDS and XPS)
Ingres
Netezza
Progress
RDB
RedBrick
SQL/DS
SQL Server
Sybase (ASE & IQ)
Teradata
Universe
UniData
NonStop SQL
InfoSphere Federation Server
InfoSphere Classic Federation
And more…..

General Access

Sequential File
Complex Flat File
File Set
Data Set
Named Pipe
iWay
FTP
SFTP
Compressed / Encoded Data
External Command Call
Parallel/wrapped 3rd party apps
EMC InfoMover
Web logs
Email

Enterprise Applications
JDE/PeopleSoft OneWorld
Oracle Applications
PeopleSoft
SAS
SAP BW
SAP R/3
Siebel
Ariba
Manugistics
I2
Etc…

Standards & Real Time
WebSphere MQ
Java Messaging Services (JMS)
Java
XML & XSL-T
EBXML
Web Services (SOAP)
Enterprise Java Beans (EJB)
EDI
FIX
SWIFT
HIPAA

CDC
DB2 (on Z, I, P, X series)
Oracle
SQL Server
Sybase
Informix
IMS
VSAM
ADABAS
IDMS
Datacom

Legacy
Allbase/SQL
C-ISAM
D-ISAM
Datacom/DB
DS Mumps
Enscribe
Essbase
FOCUS
IDMS/SQL
ImageSQL
Infoman
KSAM
M204
MS Analysis
Nomad
Nucleus
RMS S2000
Supra
TOTAL
TurboImage
Unify
And many more….

Optimizing the
World's Infrastructure

Presenting Anomalies in Context

Integrated Analytics Dashboard

Analytics User Interface

BSM helping further drive IT Operations by aligning Correlated Actual and Predictive States into Business Reprioritized actions

IT Operations now managing from the Predictive and Actual states of Services. Proactive Management

Visualize Results (TBSM)

Add Service and Operations Context (Impact)

Insert anomaly events and their associated KPI relationships

Learn normal behaviour and alert on anomalies (TASP)

Historical Data

Real-time Data

Topology, Configuration, Fault, Maintenance

Data

Tivoli's solutions allows you see anomalous conditions priortized for business impact associated with other environmental data, such as faults, configurations changes, maintenance activities, etc...

# Presenting Anomalies in Context

Detected Problem 2 Days Ahead of Outage
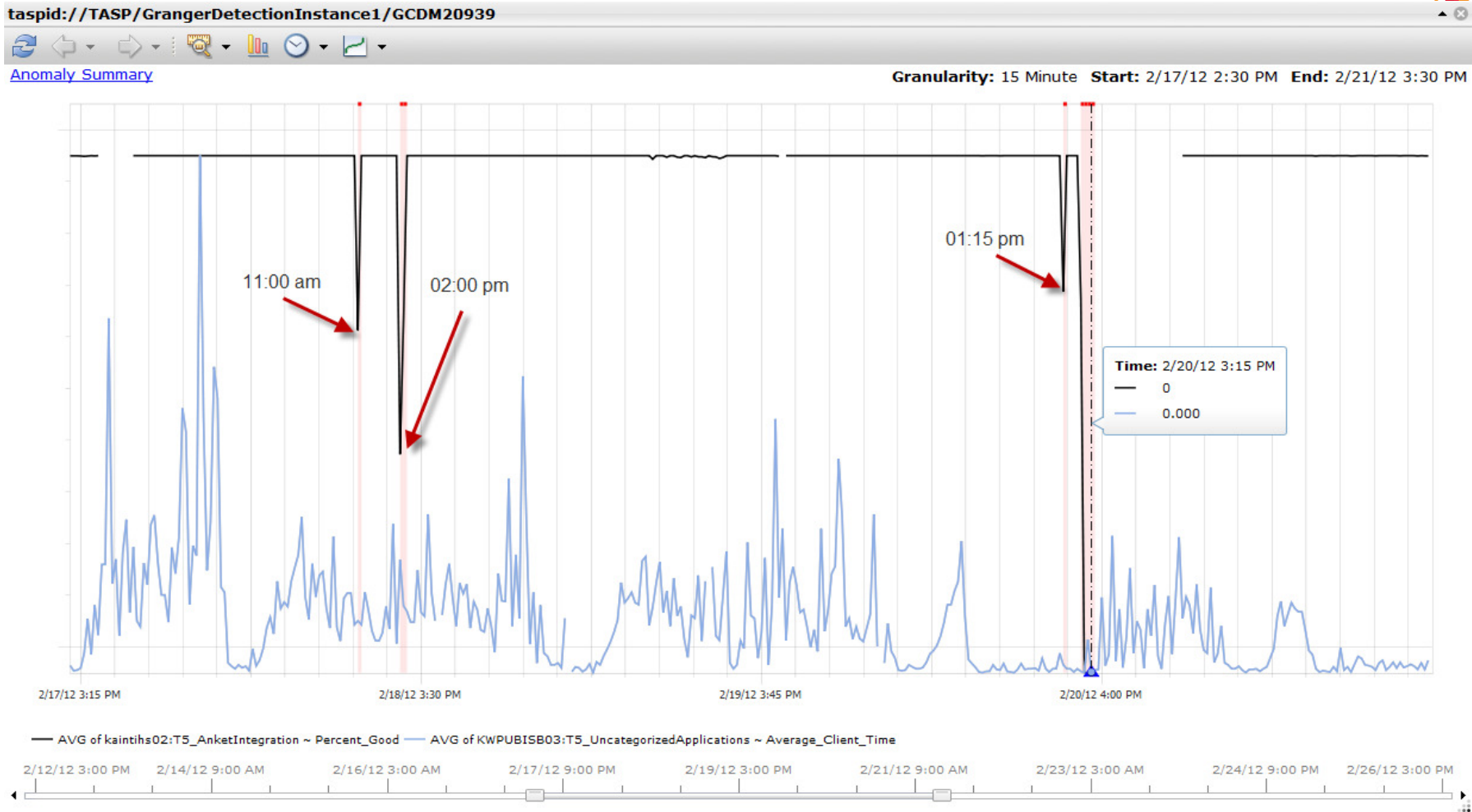
Customer comment: If they had seen the first couple of anomalies and investigated the root-cause, they might have averted the outage.

Optimizing the World's Infrastructure

Confirmed Server Problem

taspid://TASP/GrangerDetectionInstance1/GCDU10189

Anomaly Summary

Granularity: 15 Minute **Start:** 2/26/12 7:00 AM **End:** 3/1/12 8:30 AM

Time: 2/29/12 4:45 AM
— 1,691,559

— AVG of Primary:KWPUBISB02:NT_SYSTEM ~ System_Calls/Sec
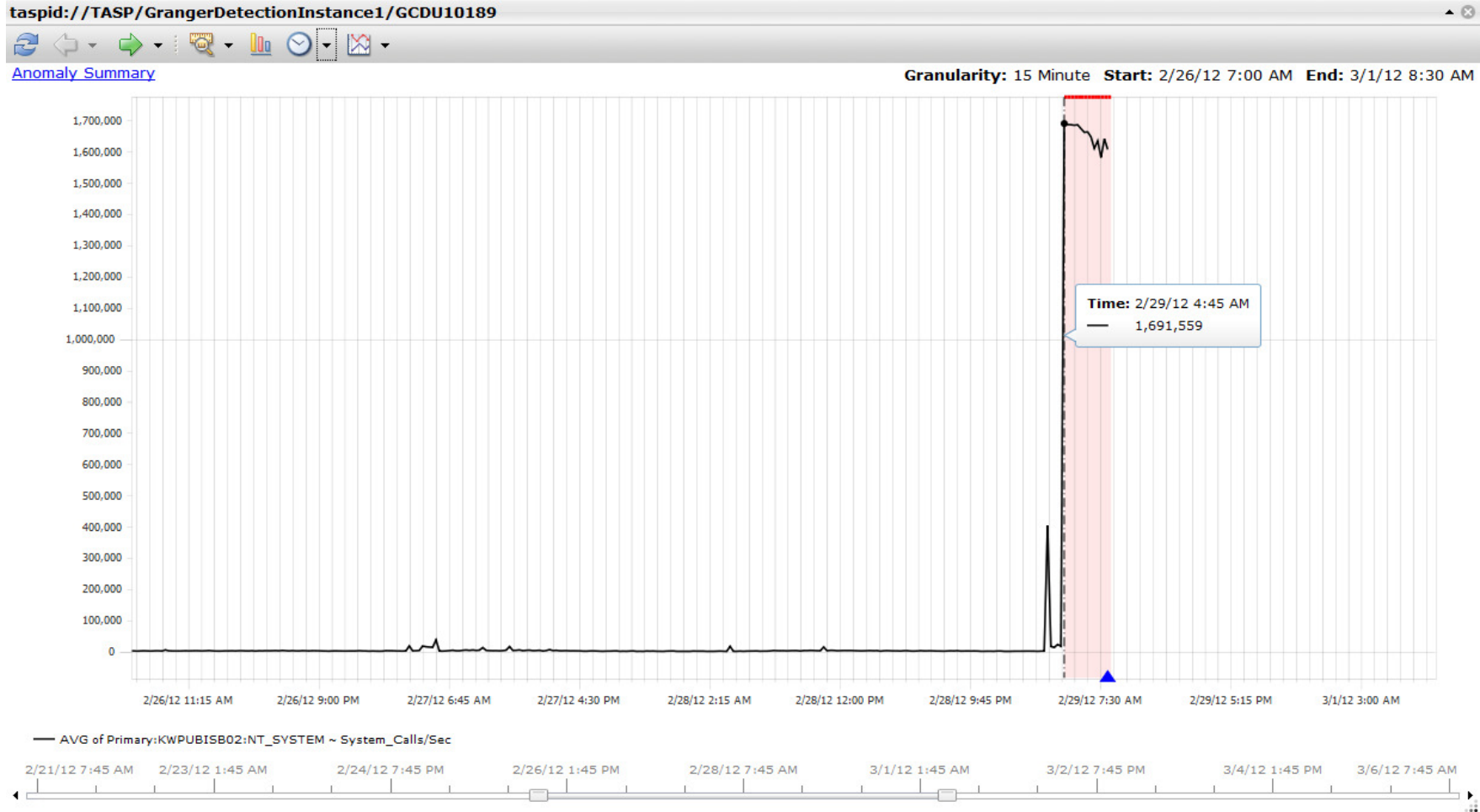
Customer suspected a problem in server that was causing application problems, but Microsoft had returned 'no fault found' when a case was opened. IBM information helped confirm suspicions and the workload was moved to an alternative.

PCTY2012

Optimizing the World's Infrastructure

Earlier Detection Of Known Problem
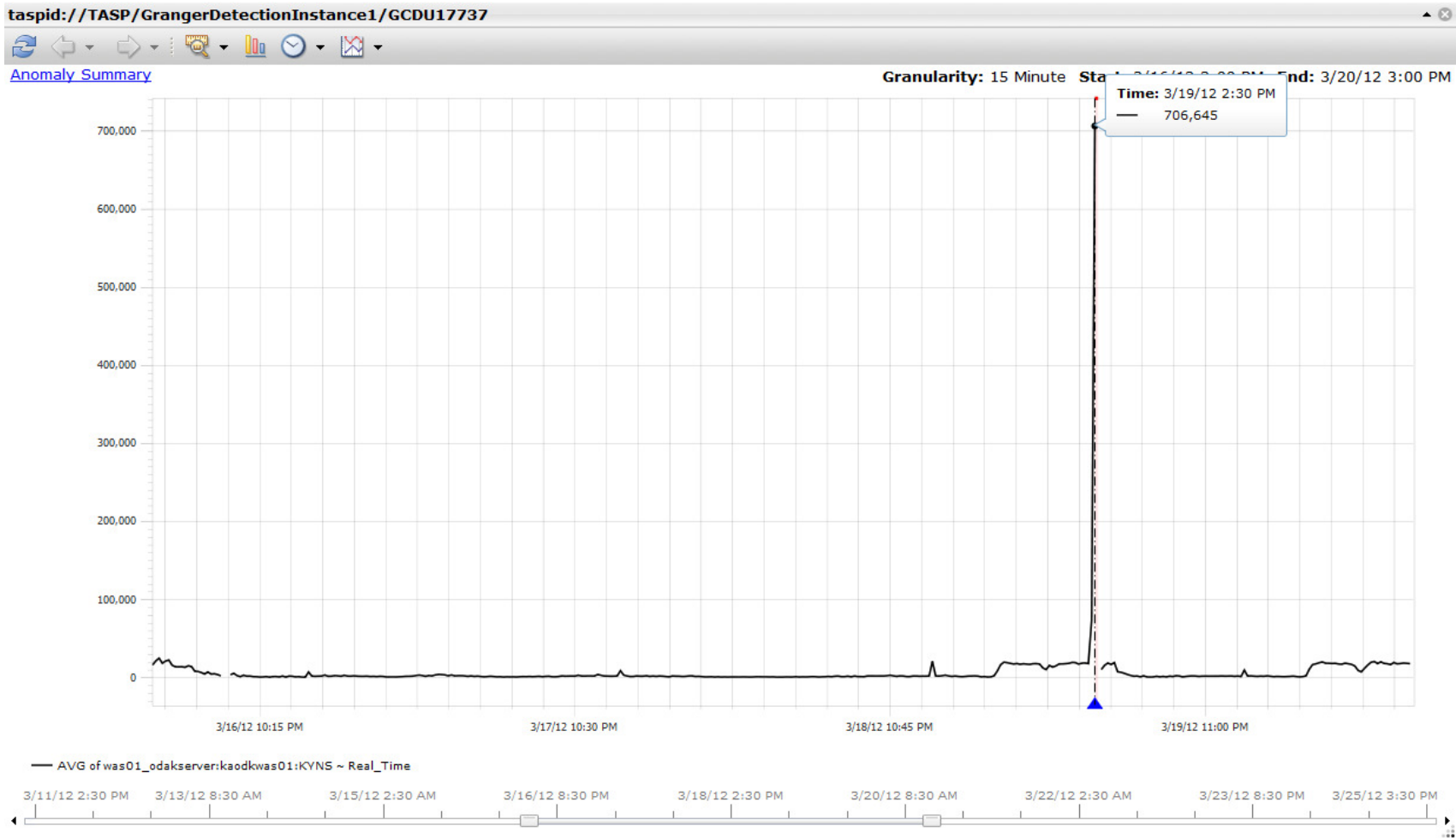
Customer comment: IBM anomaly correlated with known incident where the application gets stuck and has to be restarted (which happens every so often in reaction to services hanging). IBM detection occurs earlier so application reset can be triggered before service quality is impacted.

Optimizing the
World's Infrastructure

Detecting Unknown Problems

taspid://TASP/GrangerDetectionInstance1/GCDM1147

Anomaly Summary

Granularity: 15 Minute   Start: 4/5/12 3:00 AM   End: 4/9/12 4:30 AM

Algorithim Name:	GCDM 1.1
Summary:	Anomaly detected on 4 metrics
Quantifier:	0.9999998574057942
Severity:	5
First Occurrence:	4/8/12 2:45 AM
Anomaly Timestamp:	4/8/12 3:30 AM

4/5/12 12:15 PM   4/5/12 10:00 PM   4/6/12 7:45 AM   4/6/12 5:30 PM   4/7/12 3:15 AM   4/7/12 1:00 PM   4/7/12 10:45 PM   4/8/12 8:30 AM   4/8/12 6:15 PM   4/9/12 4:00 AM

_____ AVG of KWPUBISB07:T5_SanalPos ~
Percent_Good

_____ AVG of KWPUBIIS06:T5_CepHavaleService ~
Percent_Good

_____ AVG of KWPUBISB08:T5_CRMSurveyService ~
Average_Client_Time

_____ AVG of was01_odakserver:kaodkwas01:KYNS ~
Average_Usage_Time

3/31/12 3:45 AM   4/1/12 9:45 PM   4/3/12 3:45 PM   4/5/12 9:45 AM   4/7/12 3:45 AM   4/8/12 9:45 PM   4/10/12 3:45 PM   4/12/12 9:45 AM   4/14/12 3:45 AM

Customer comment: IBM detected an outage on an important service (virtual 'point of sale' system for customers to shop and pay with credit cards etc), it had gone unnoticed with the customer operators had failed to complain.

PCTY2012

Optimizing the
World's Infrastructure

Acknowledgements, disclaimers and trademarks

PCTY2012

Optimizing the
World's Infrastructure

PCTY2012

Pulse Comes to You