AIOps – Using Data Analytics, Machine Learning, and AI in IT Operations
Abstract

AIOps – Leveraging Big Data to Operate Complex IT Systems at Scale

AIOps – or AI for IT Operations – is a game-changing new approach to managing complex IT systems by leveraging ‘big data’ practices like data analytics, machine learning, and artificial intelligence in IT Operations.

For anyone in AppDev, DevOps, SRE, SysAdmin, ITOps, or DevOps, this session will help you achieve better IT outcomes through AIOps by learning:

- What is AIOps (and what is it not)?
- What does AIOps actually do – and how?
- Building and maturing AIOps practices
- Making AIOps practices actionable
- AIOps examples and real-world stories

Do not miss this chance to get SKIL’d Up on AIOps!
Agenda

• What is AIOps (and what is it not)?
• What does AIOps actually do – and how?
• Building and maturing AIOps practices
• Making AIOps practices actionable
• AIOps examples and real-world stories
During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.
AIOps – Using Data Analytics, Machine Learning, and AI in IT Operations

Andi Mann
Chief Technology Advocate, Splunk

@AndiMann
amann@splunk.com
www.splunk.com

For DevOps Institute SKILup Days: AIOps & MLOps
15 Oct 2020

Virtual/Online
What is AIOps? (and what is it not)
“AIOps combines big data and machine learning to automate IT operations processes, including event correlation, anomaly detection and causality determination.”

-Gartner


Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.
AIOps

Uses advanced data analytics techniques, to provide insights that improve the speed, agility, accuracy, and efficiency of:

• Monitoring and Alerting
• Service Desk Response
• Automation & Orchestration
• … and more!
AIOPs Uses Powerful Analytics Techniques

To Make IT Effective, Proactive and Predictive

**Anomaly Detection**
- Alerts triggered automatically by anomalous activity
- Incident responders can see across all silos to find a quicker MTTR

**Dynamic Thresholding**
- Thresholds adapt in real time
- Trend and alert on anomalous behavior
- Prevent service degradation

**Event Clustering**
- Detect and highlight the events that matter
- Prioritize events that need action taken

**Intelligent Alerting**
- Advanced problem detection increases alert fidelity
- Automatically identify and alert on risky service behavior

**Predictive Analytics**
- Predict outages and anomalies before they occur
- Act on predictions so services are not affected
DataOps

… is an automated, process-oriented methodology, used by analytic and data teams, to improve the quality and reduce the cycle time of data analytics.

- Wikipedia

E.g. workflow automation, governance/compliance, metadata management, benchmarking, extensibility, etc.

AIOps vs. DataOps

AIOps utilizes the data that is managed and stored in DataOps
MLOps

… is a practice for collaboration and communication between data scientists and operations professionals to help manage production ML (or deep learning) lifecycle.

- Wikipedia

e.g. model generation, test processing, tool integrations, algorithm access, version controls, compliance, etc.

AIOps vs. MLOps

AIOps utilizes the algorithms that are produced through MLOps

<table>
<thead>
<tr>
<th>Entities Analyzed:</th>
<th>57</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entities with Detected Anomalies:</td>
<td>33</td>
</tr>
<tr>
<td>Average Anomalies Per Entity:</td>
<td>16.3</td>
</tr>
<tr>
<td>Percentage of Time Anomalies were Detected:</td>
<td>5.8 % (Expected &lt;3%)</td>
</tr>
<tr>
<td>Percentage of Data Points with Anomalies:</td>
<td>7.3 % (Expected &lt;10%)</td>
</tr>
</tbody>
</table>

Cohesive AD Preview - Top 5 Entities With Most Anomalies for Last 7 Days

- Mon Jul 25 2016
- Wed Jul 27
- Fri Jul 29
- Mon Aug 1

web-server1  web-server2  web-server3  Detected Anomaly
AIOps vs. ITOA (vs. *the other* AIOps)

AIOps was ITOA before it was *the other* AIOPs before it was today’s AIOPs

**ITOA**

… IT Operations Analytics is the practice of monitoring systems and gathering, processing, analyzing and interpreting data from various IT operations sources to guide decisions and predict potential issues.

- TechTarget

**(*the other*) AIOps**

… Algorithmic IT Operations platform technologies comprise of multiple layers that address data collection, storage, analytical engines and visualization.

- Gartner (2017)
What does AIOps actually do – and how?
Sample AIOps Capabilities In the Real World

- **Availability & Performance Monitoring**
  - Decrease Mean Time to Detect (MTTD) through Prediction
  - Decrease Mean Time to Investigate (MTTI)
  - Decrease Mean Time to Resolution (MTTR)

- **Event Correlation & Analysis**
  - Reduce Event Noise through ML

- **IT Service Management**
  - Increase Mean Time between Failures (MTBF)
  - Decrease Mean Time to Investigate (MTTI)

- **Data-Driven Automation**
  - Eliminate tedious and manual tasks through Automation

© 2019 SPLUNK INC. 
@AndiMann
Example AIOps Capabilities

**Event Analytics**

- Event analytics and alert workflow to automate managing events
- Machine learning to reduce noise and find alerts on root causes of issues
- Initiate incident and remediation responses
- Operators and engineers access business service data for triage and investigation

**Service Insights**

- Service health scores calculated from KPIs
- Baseline KPI trends to identify abnormal conditions for meaningful alerts
- Organized view of KPIs and trends for fast triage and analysis
- Deep insights into technology domains to speed investigation
What This Means for IT Operations
Faster Time to Business Outcomes and Unified Toolsets Across Every Team

- **Speed Up Investigations**
  Spot trends and pinpoint root causes leveraging metrics and logs

- **Streamline Monitoring**
  Visibility to services, apps, physical, virtual, and cloud infrastructure

- **Analyze System Health**
  Service Insights & Event Analytics to focus on what’s important, not just what’s noisy

- **Act & Increase Productivity**
  Smart collaboration, orchestration and automation
Building and Maturing AIOps Practices
AIOps for Every Stage of Modernization Journey
Splunk meets you wherever you are

Infra and App Availability
with guided data onboarding, logging and IT monitoring

Reduce Alert Fatigue
with intelligent event management and integrated incident response

360° Visibility
with correlated business metrics, services and infrastructure in one view

Prevent Incidents
with predictive alerting, actionable insights and auto-remediation

STAGE 1: Descriptive
STAGE 2: Diagnostic
STAGE 3: Predictive
STAGE 4: Prescriptive
Getting started with AIOps

Identify data types and uses
- Machine data, semantic data, tabular data
- Logs, metrics, events, traces, workflows

Establish data collection techniques
- Open source – collectd, statsd, Otel
- Proprietary – agents, drivers, APIs

Apply basic analytics
- Start with data-driven baselines
- Correlations, straight-line predictions
Apply Advanced Analytics and Algorithms

e.g.
- Event clustering
Apply Advanced Analytics and Algorithms

e.g.
- Event clustering
- Dynamic thresholding
Apply Advanced Analytics and Algorithms

e.g.

- Event clustering
- Dynamic thresholding
- Anomaly detection
Apply Advanced Analytics and Algorithms

e.g.
• Event clustering
• Dynamic thresholding
• Anomaly detection
• Predictive analysis
Train and Apply Machine Learning Models

- **Acquire**
  - data to test an algorithm

- **Train**
  - algorithms to create a model

- **Apply**
  - real data to validate model

- **Surface**
  - model to solve problems

---

Operationalize your model
Make Your AIOps Practices Actionable

Integrate and Activate Other Tools and Processes e.g.

- **ITSM tool integration**
  - Automatically open, update, close Service Desk tickets
  - Interrogate CMDB/CMS for diagnostics, ‘known knowns’

- **Automation integration**
  - Execute discrete tasks to aid investigation
  - Collect additional data, execute diagnostic scripts

- **Orchestration integration**
  - Identify and execute complex remediation
  - Trigger ITPA, RPA, CM, or SOAR processes

- **Collaborative Incident Response**
  - Correlate and analyze data across tools
  - Identify responders and share diagnostics
AIOps Maturity Example – Achieving Negative MTTR

Traditional
Descriptive
Diagnostic
Predictive
Prescriptive

Incident Occurs!

Customers know, but you don’t
MTTR
Reactively Alerted

Pattern detection for early alerts
MTTR
Automated Alerting

Faster, better diagnostics accelerates resolution
MTTR
Assisted Resolution

Anomaly detection predicts novel problems before impact
MTTR
ML Alert

Advanced ML/AI predicts problems early and automatically prevents any impact

30min advance notice!

Time Return to Business

Revenue loss
Reputation damage

NEGATIVE MTTR!!
AIOps is a catalyst for transformation!

Nearly every function in IT Operations benefits from AIOps

- Customer Experience: up
- MTTD / MTTR: down 70%
  - from Hours to Minutes
- Incidents: down 5x
  - & reduced MTTR by 63%
- Events: down 98%
  - & event storm noise
- KPI Predictions: up
  - Incidents: down 90%
90% Reduction in Auction Incidents

We have been able to reduce the number of incidents at our auctions by 90%. We have proactive infrastructure monitoring to ensure a consistent level of customer service. -VP Technology Application Development & Operations, Cox Automotive

- Reduced time-to-investigate and resolution with real-time insights
- Reduced incidents across global auctions by 90%
- Improved end-user experience and service reliability
98% Reduction in Event Noise

“I've been in IT management for over 20 years… this is the first time I've been able to do heterogeneous, up-and-down-the-stack monitoring of my IT environment…”

~ Director of Performance Management, Leidos

- Reduced 5000 events to 200 actionable events after replacing legacy systems
- Real-time enterprise-wide infrastructure monitoring
- Dashboards for different audiences, from problem-solving techs to big-picture managers
AIOps in the Real World: Deep Dive: 3M Case Study
AIOPS Benefits

**Goal attainment:**
Reduced unplanned downtime by **64%**

Unplanned Downtime Incidents

**Achieved Benefits**
- Automatic Critical Notifications
- Reduced MTTD ~ 80-90% for critical focus areas
- Reduced MTTR ~ 70-80%
- Reduced RCA Costs
- Reduced War Room Costs
  - 65% less War Room Activity

**Anticipated Benefits**
- Automated Resolutions
- Predictive Operations
- Reduced War Room Costs
  - 90% less war room activity
- Reduced TCO
3M required integrated incident management to reduce costly hourly outages

- Replaced outdated event management console with integrated operations across monitoring, service management, orchestration/automation

- Track outbound delivery business process with health scores

- Reduced unplanned downtime and war room activity by 64%

Reduced MTTR by 70% with AIOps
3M Reduced Unplanned Downtime by 64%

Splunk helped understand complex SAP data and create alerts that matter

- Hourly outages were costing $100k+ loss in revenue
- Leveraged PowerConnect to get data out of SAP and Splunk to orchestrate event management and AIOps
  - ITSI for views into application, infrastructure and business process layers
  - Phantom for automating critical notifications and resolutions
- Tracked business process for outbound delivery - each step generated a health score
- Impactful ROI:
  - Went from 4-6 hour performance impact to no impact
  - Reduced
    - MTTD 80-90%
    - MTTR 70-80%
    - RCA Costs
    - War Room Costs - 65% less war room activity

Technology, Manufacturing

$32.8 billion in global sales
Four business groups
90,000 employees
117,000 patents
One of 30 companies on Dow Jones Industrial Index

Splunk helped understand complex SAP data and create alerts that matter
Wrap-Up

... and Next Steps
More Learning Resources for Your AIOps Journey

2019 Gartner Market Guide for AIOps Platforms
Find this report on our website, and you’ll be able to compare different AIOps platform
www.splunk.com/marketguide aiops

Independent analysis and unique strengths of seventeen AIOps vendors

The Essential Guide to AIOps
Authored by experts at Splunk, everything you need to know to begin your AIOps journey
www.splunk.com/aiopsguide

Modern IT Management With AIOps
A practical guide to using Splunk for AIOps, for current and new Splunk users.
THANK YOU!
Meet me in the Network Chat Lounge for questions

@AndiMann
amann@splunk.com

2019 Gartner Market Guide for AIOps Platforms
Find this report on our website, and you'll be able to compare different AIOps platforms

Independent analysis and unique strengths of seventeen AIOps vendors

The Essential Guide to AIOps
Authored by experts at Splunk, everything you need to know to begin your AIOps journey

Modern IT Management With AIOps
A practical guide to using Splunk for AIOps, for current and new Splunk users.