SKILUP DAYS
by: DevOps Institute
ADVANCING THE HUMANS OF DEVOPS

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

Andi Mann
Chief Technology Advocate
Splunk
@AndiMann
amann@splunk.com

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

Forward-Looking Statements

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.

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

splunk> turn data into doing™

What is AIOps? (and what is it not)

splunk> turn data into doing™

“ AIOps combines **big data** and **machine learning** to **automate** IT operations processes, including event correlation, anomaly detection and causality determination.”

-Gartner

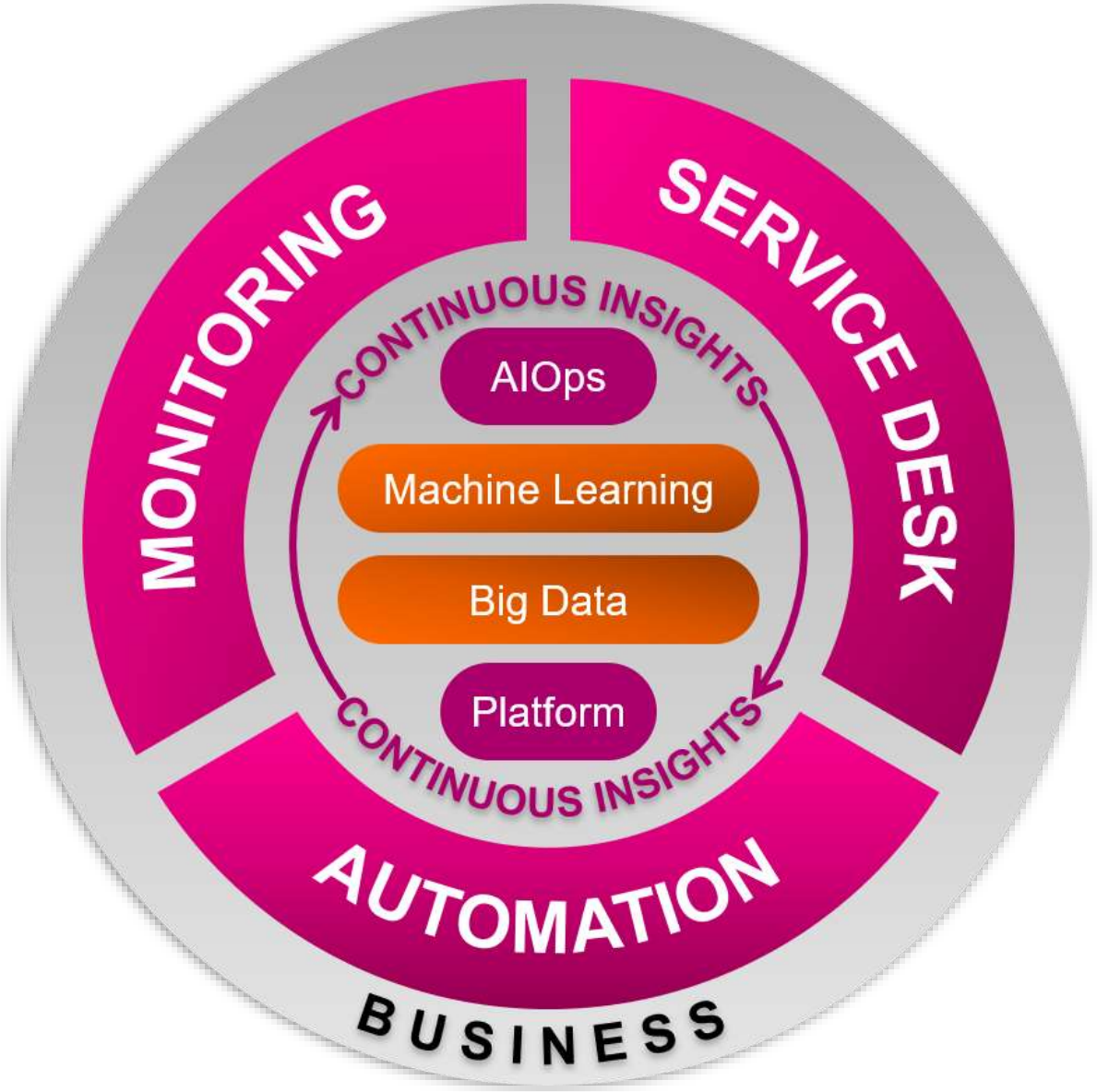
*Gartner, “Gartner Glossary” https://www.gartner.com/en/information-technology/glossary/aiops-artificial-intelligence-operations

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!

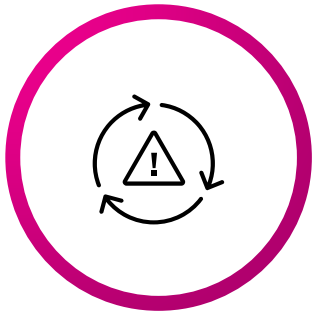


splunk> turn data into doing

AIOPs Uses Powerful Analytics Techniques

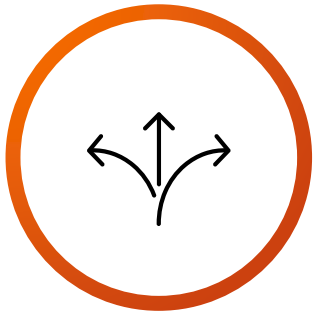
To Make IT Effective, Proactive and Predictive

Anomaly Detection



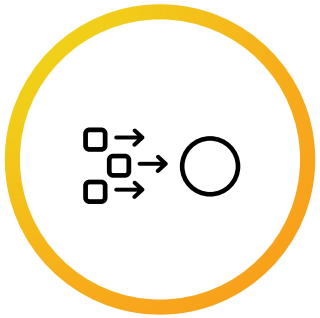
- Alerts triggered automatically by anomalous activity
- Incident responders can see across all silos to find a quicker MTTR

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

splunk> turn data into doing

@AndiMann

AIOps vs. DataOps

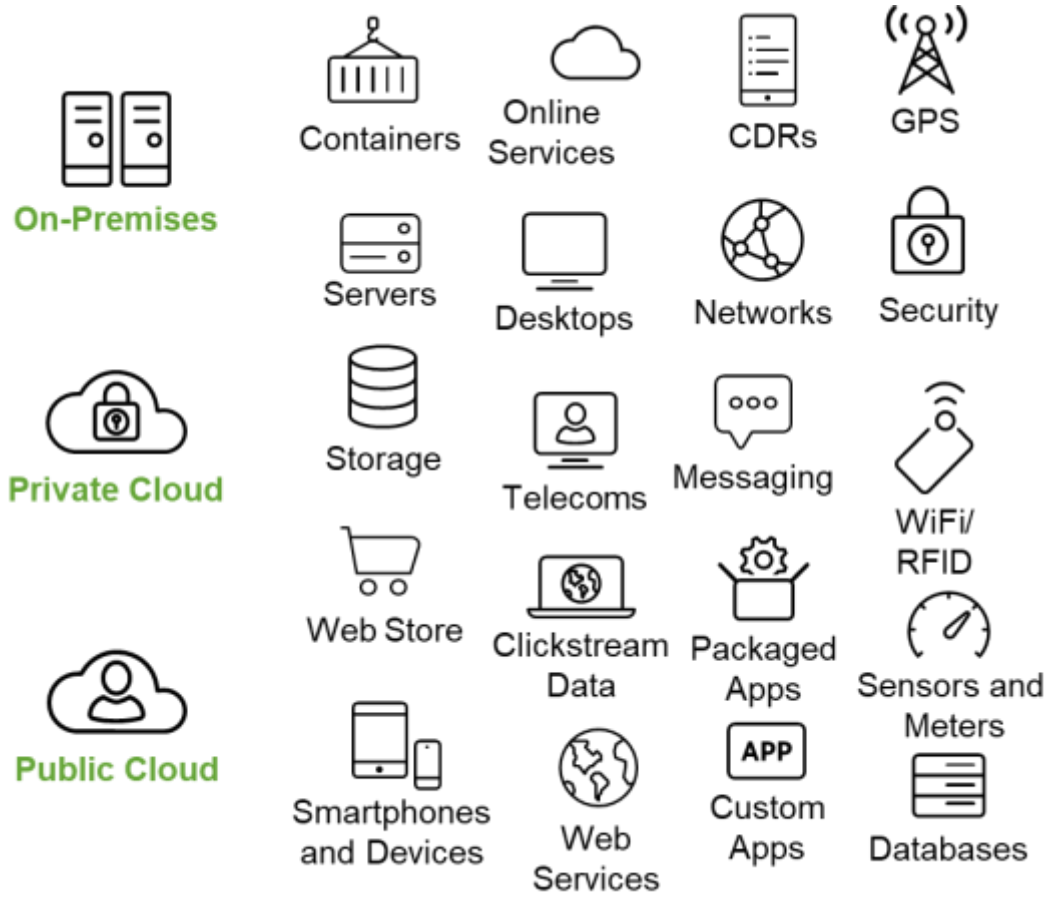
AIOps utilizes the data that is managed and stored in DataOps

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. MLOps

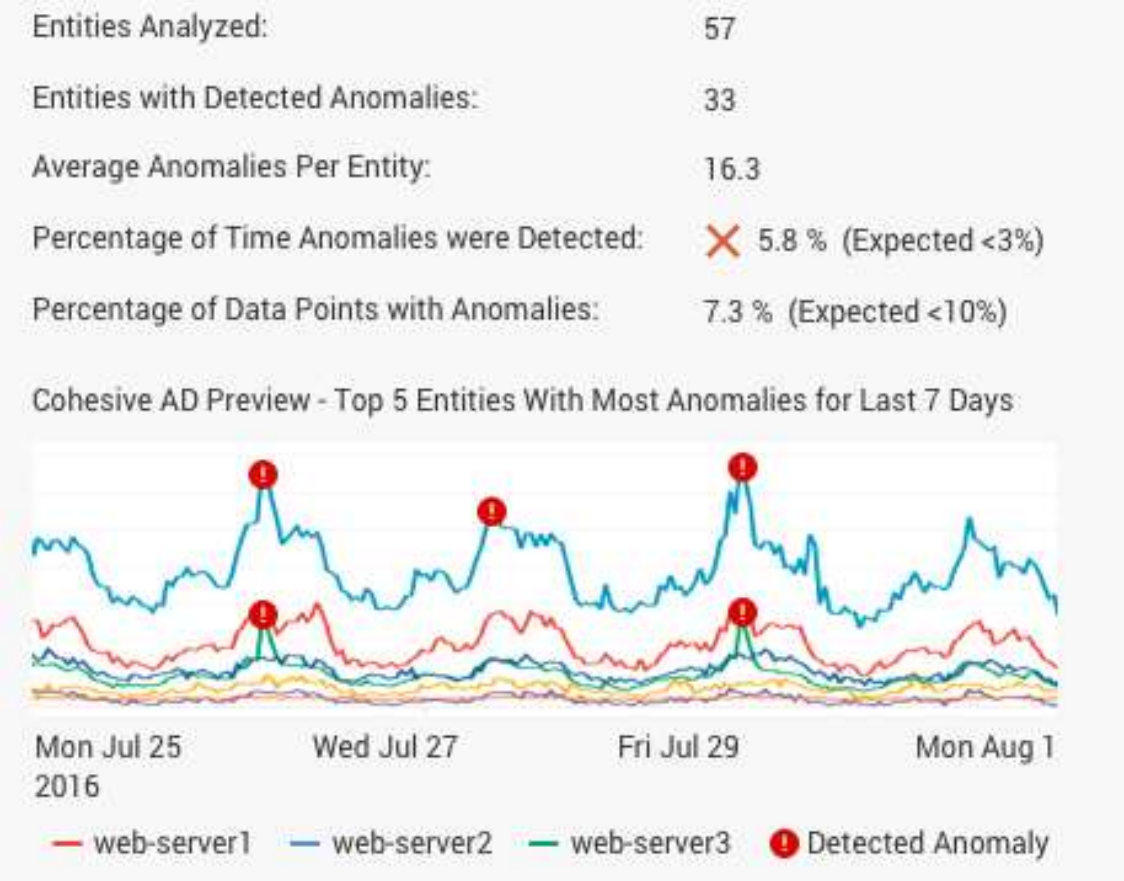
AIOps utilizes the algorithms that are produced through MLOps

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. ITOA (vs. *the other* AIOps)

AIOps was ITOA before it was *the other* AIOps before it was *today's* AIOps

ITOA

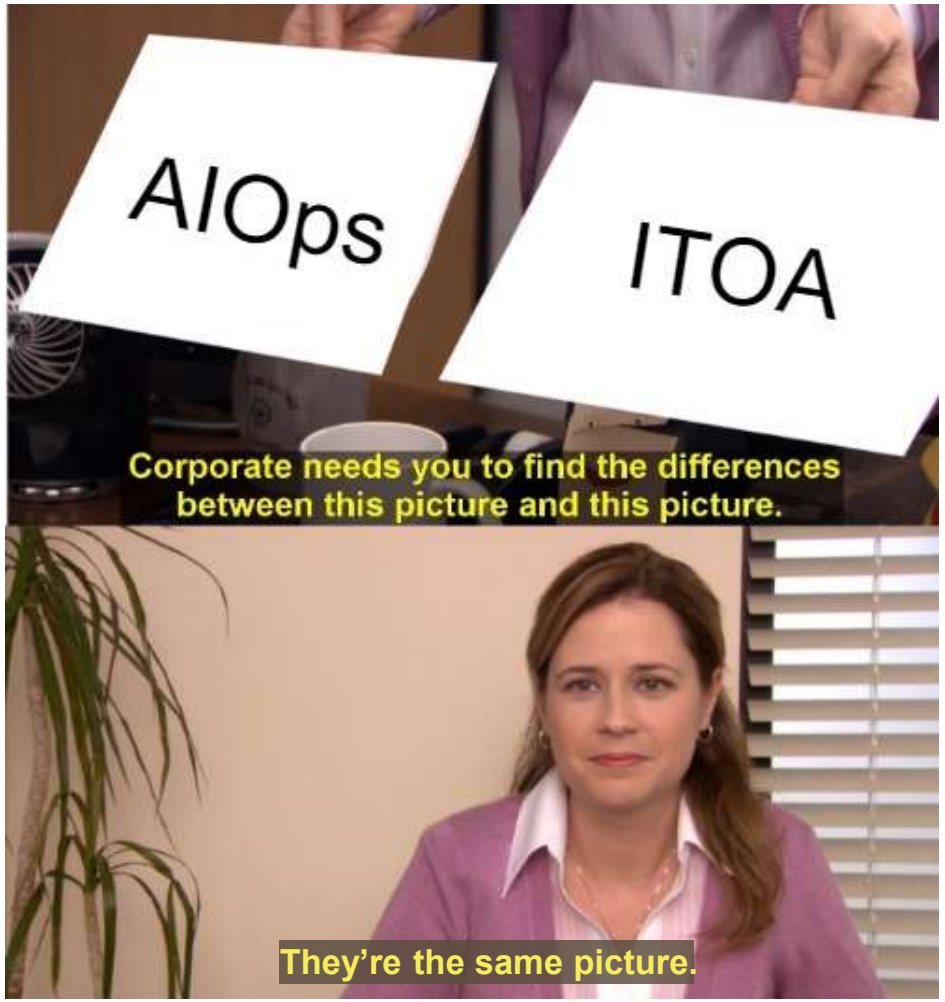
… IT Operations Analytics is the practice of monitoring systems and gathering, processing, analyzing and interpreting data from various IT operations sources to guide decisions and predict potential issues

- 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?

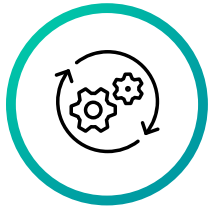
splunk> turn data into doing™

Sample AIOps Capabilities In the Real World

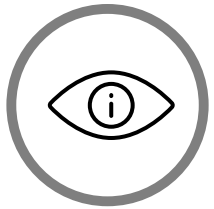
Availability & Performance Monitoring

Event Correlation & Analysis

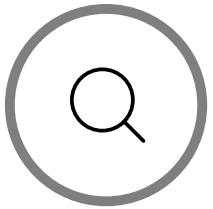
IT Service Management



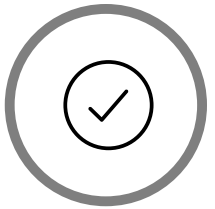
Data-Driven Automation



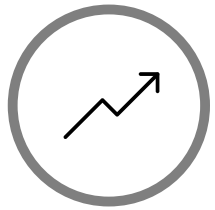
Decrease Mean Time to Detect (MTTD) through Prediction



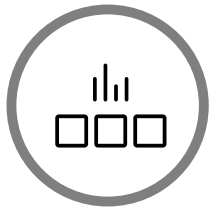
Decrease Mean Time to Investigate (MTTI)



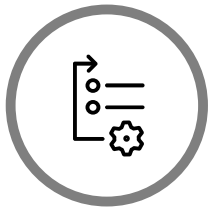
Decrease Mean Time to Resolution (MTTR)



Increase Mean Time between Failures (MTBF)



Reduce Event Noise through ML



Eliminate tedious and manual tasks through Automation

splunk> turn data into doing

@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

splunk> turn data into doing

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

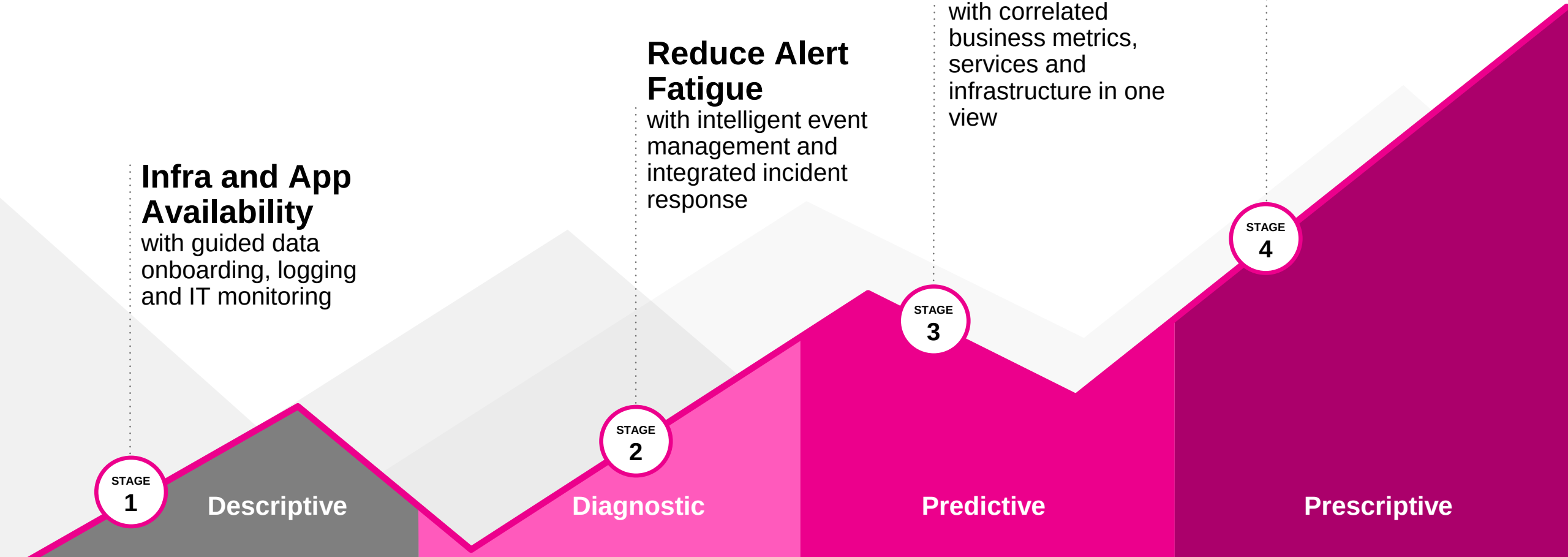
splunk> turn data into doing

Building and Maturing AIOps Practices

splunk> turn data into doing™

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

Getting started with AIOps

Identify data types and uses

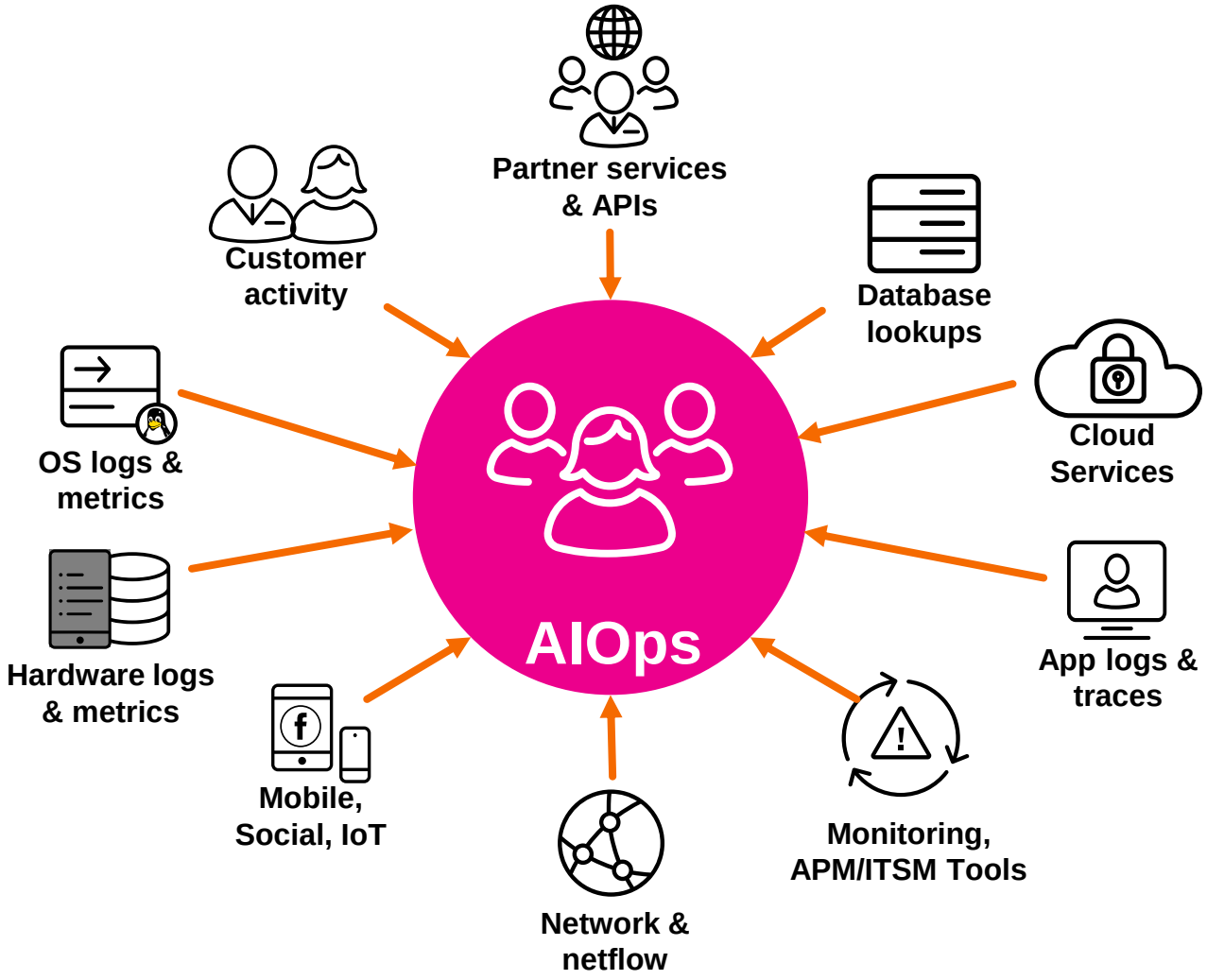
- Machine data, semantic data, tabular data
- Logs, metrics, events, traces, workflows

Establish data collection techniques

- Open source – collectd, statsd, Otel
- Proprietary – agents, drivers, APIs

Apply basic analytics

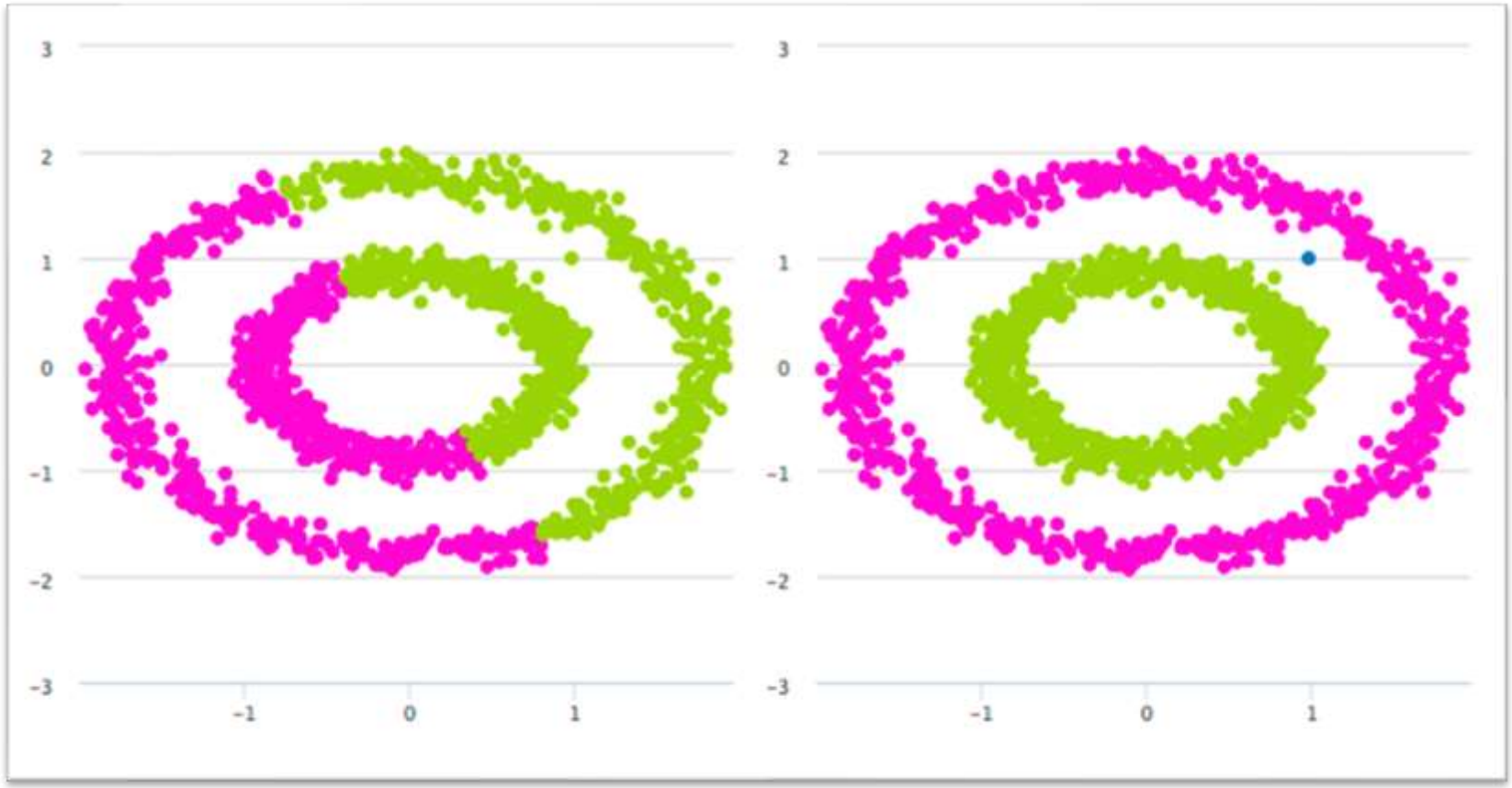
- Start with data-driven baselines
- Correlations, straight-line predictions



Apply Advanced Analytics and Algorithms

e.g.

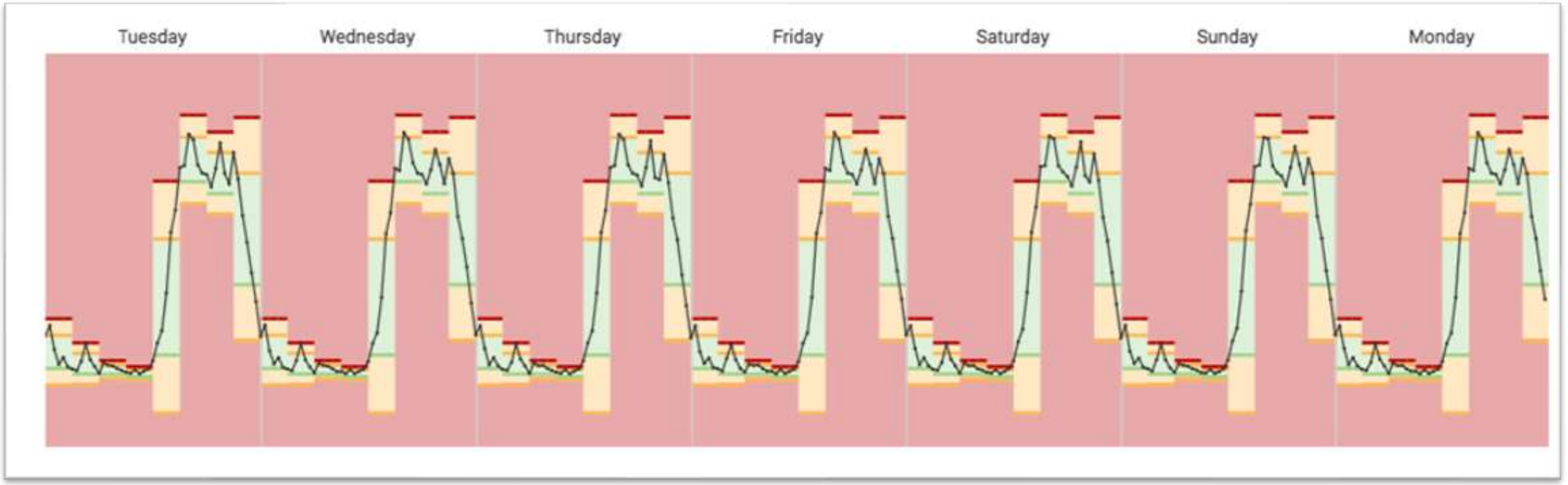
- Event clustering



Apply Advanced Analytics and Algorithms

e.g.

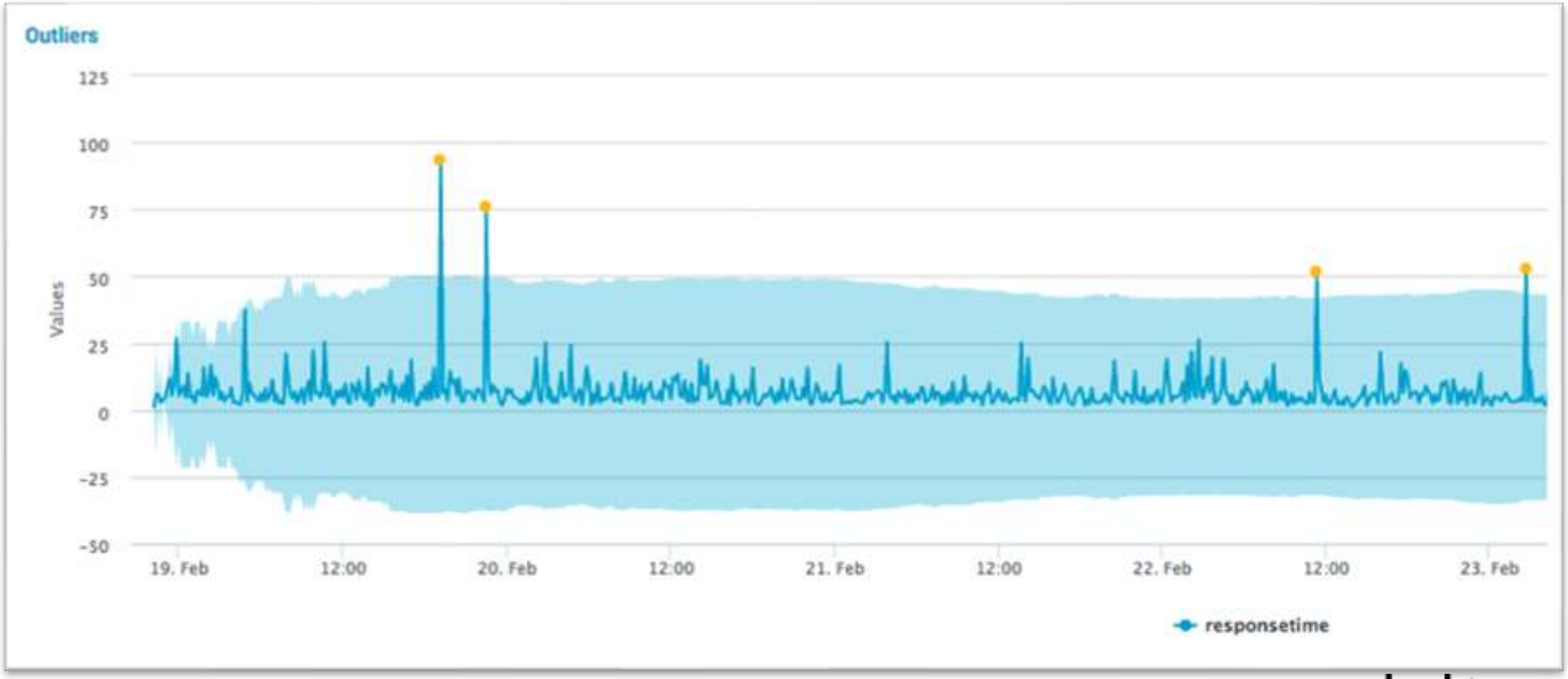
- Event clustering
- Dynamic thresholding



Apply Advanced Analytics and Algorithms

e.g.

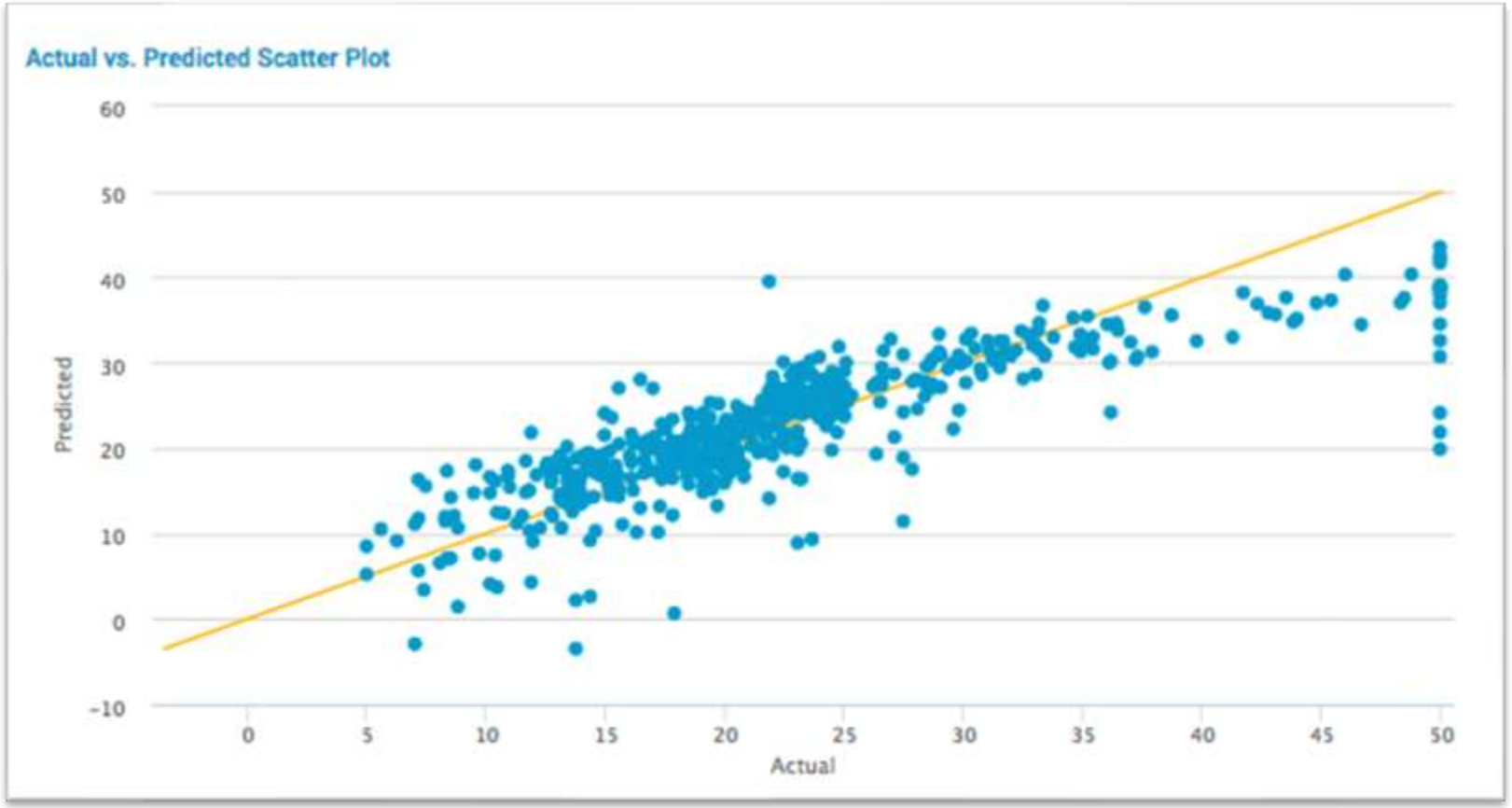
- Event clustering
- Dynamic thresholding
- Anomaly detection



Apply Advanced Analytics and Algorithms

e.g.

- Event clustering
- Dynamic thresholding
- Anomaly detection
- Predictive analysis



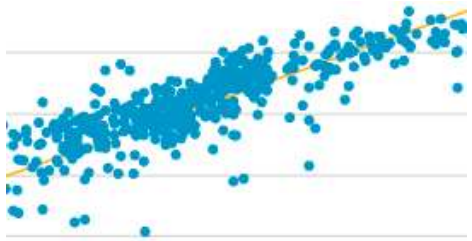
Train and Apply Machine Learning Models

Acquire data to test an algorithm

Train algorithms to create a model

Apply real data to validate model

Surface model to solve problems



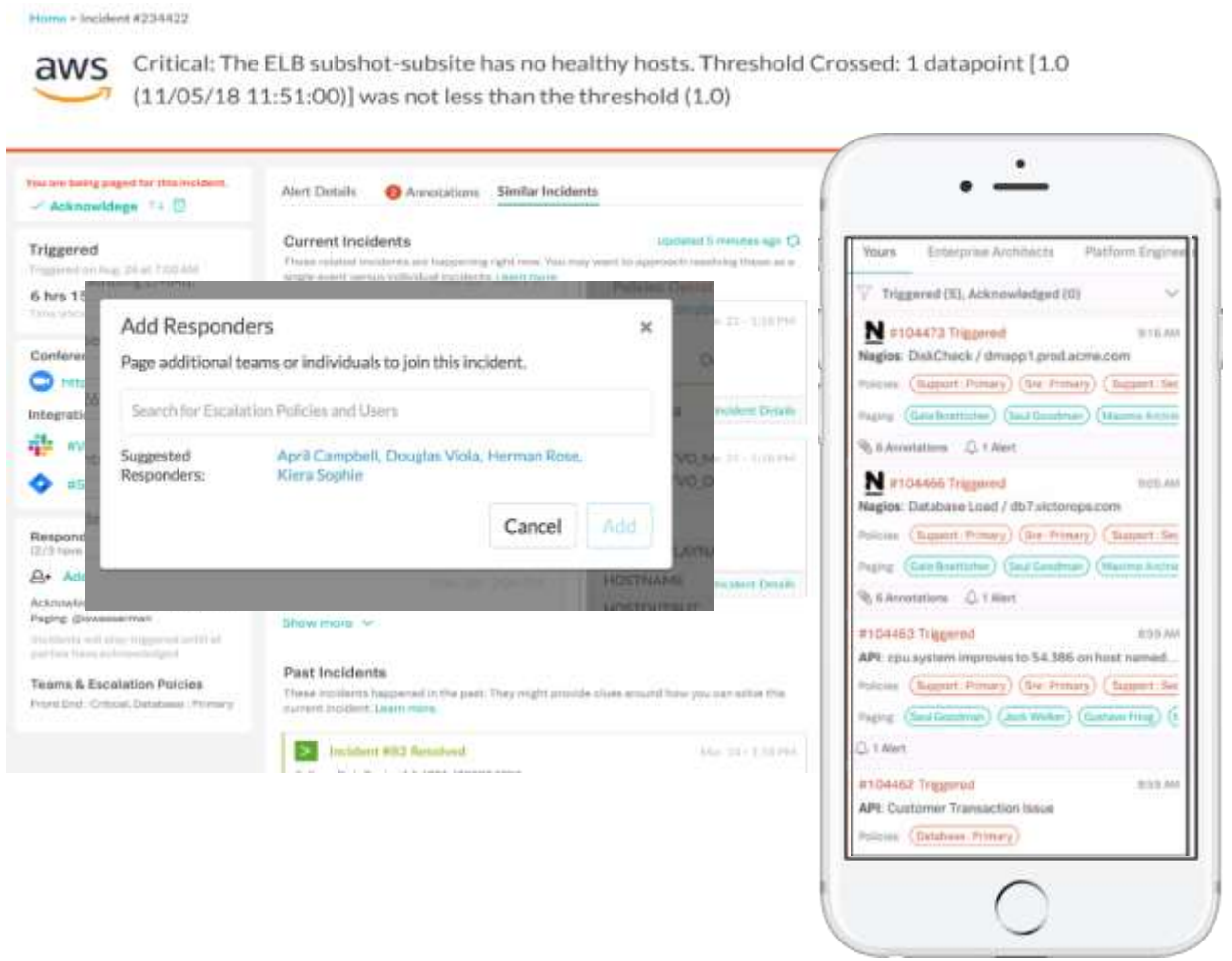
Operationalize your model

splunk> turn data into doing

Make Your AIOps Practices Actionable

Integrate and Activate Other Tools and Processes e.g.

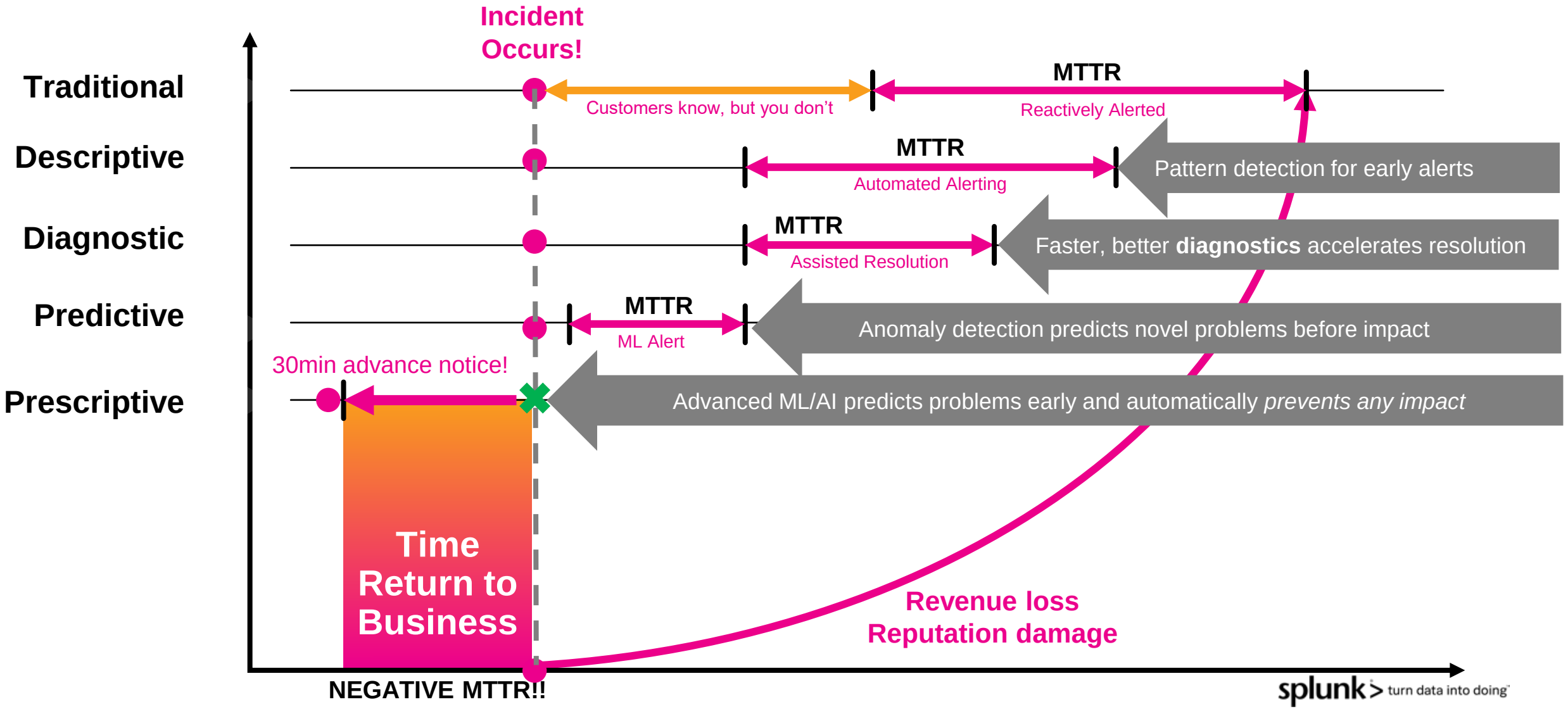
- ITSM tool integration
  - Automatically open, update, close Service Desk tickets
  - Interrogate CMDB/CMS for diagnostics, ‘known knowns’
- Automation integration
  - Execute discrete tasks to aid investigation
  - Collect additional data, execute diagnostic scripts
- Orchestration integration
  - 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



splunk> turn data into doing

@AndiMann

AIOps Maturity Example – Achieving Negative MTTR



AIOps in the Real World: Case Studies & Examples

splunk> turn data into doing™

AIOps is a catalyst for transformation!

Nearly every function in IT Operations benefits from AIOps

Carnival | 3M | MOLINA HEALTHCARE | leidos | COX AUTOMOTIVE

Customer Experience

⬇70%
MTTD / MTTR
from Hours to Minutes

⬇5x
Incidents
& reduced MTTR by 63%

⬇98%
Events
& event storm noise

+KPI
Predictions

⬇90%
Incidents

COX AUTOMOTIVE™

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

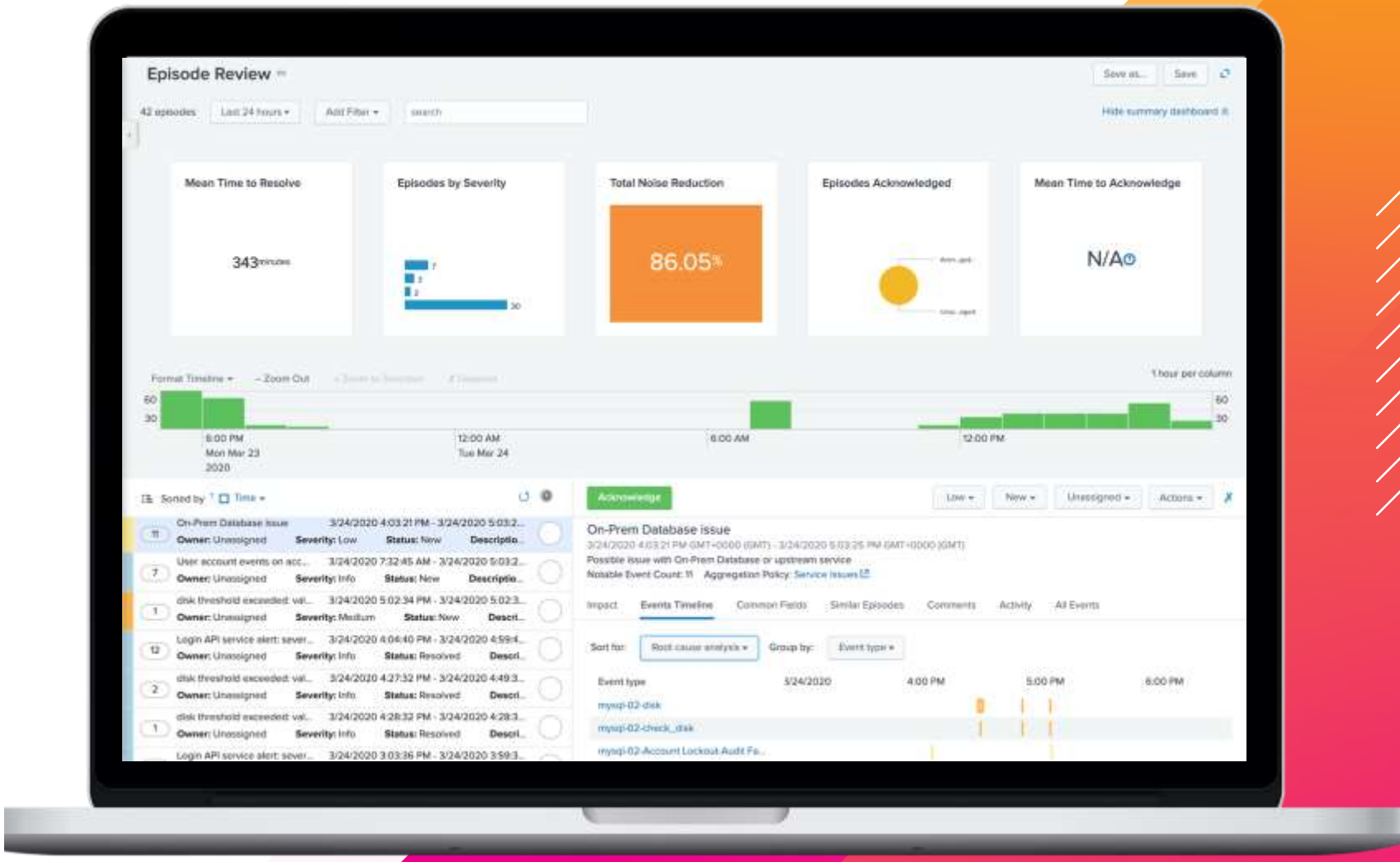
splunk> turn data into doing

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



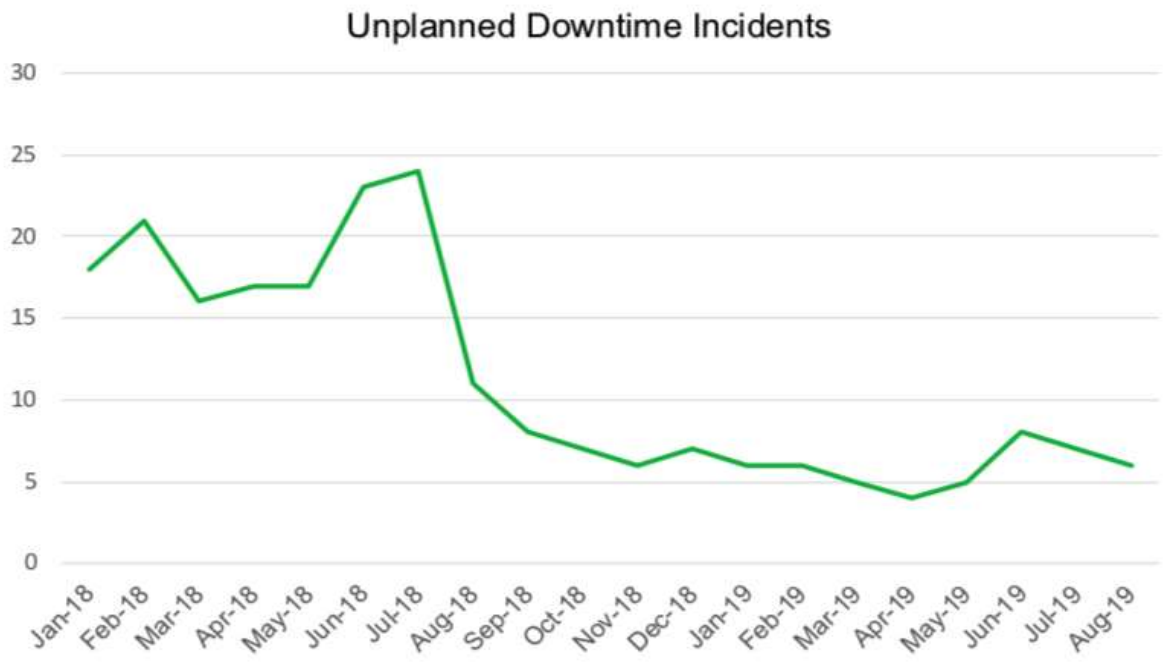
AIOps in the Real World: Deep Dive: 3M Case Study

splunk> turn data into doing™

Public Case Study

AIOPS Benefits

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



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

Reduced MTTR by 70% with AIOps

- 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%

splunk> turn data into doing

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> turn data into doing

@AndiMann

Wrap-Up

… and Next Steps

splunk> turn data into doing™

More Learning Resources for Your AIOps Journey

2019 Gartner Market Guide for AIOps Platforms

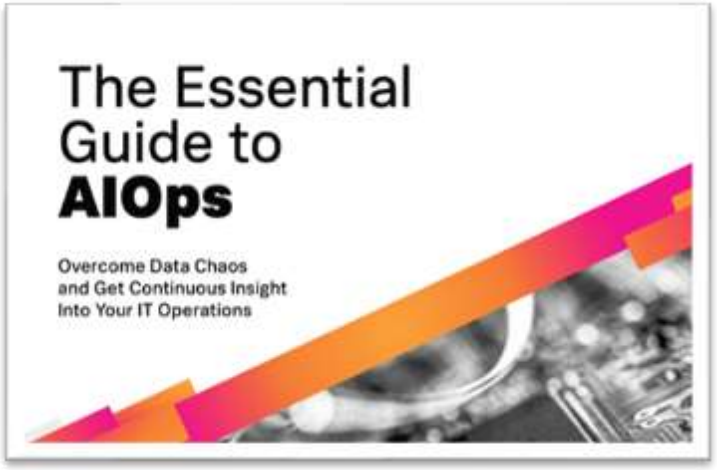
Find this report on our website, and you'll be able to compare different AIOps platform

www.splunk.com/marketguide aiops

2020 EMA Radar Report: AIOps, A Guide for Investing in Innovation

Independent analysis and unique strengths of seventeen AIOps vendors

https://www.splunk.com/en_us/form/ema-radar-report.html



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.

https://www.splunk.com/en_us/form/modern-it-management-with-aiops.html

splunk> turn data into doing

THANK YOU!

Meet me in the Network Chat Lounge for questions

@AndiMann
amann@splunk.com

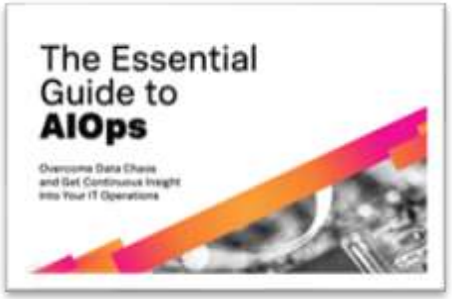
SKILUP DAYS by: DevOps Institute ADVANCING THE HUMANS OF DEVOPS

[2019 Gartner Market Guide for AIOps Platforms]

Find this report on our website, and you'll be able to compare different AIOps platform

[2020 EMA Radar Report: AIOps, A Guide for Investing in Innovation]

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.