A Brief History of AIOps

Andi Mann
Chief Technology Advocate, Splunk

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

For DevOps Institute

November, 2020

Virtual/Online

splunk> turn data into doing™

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.

In the beginning, there was monitoring …

…and it was good (enough)

IT Ops always included monitoring

It was 24x7, but ‘Batch’ vs ‘Online’

Monitoring data wasn’t all that different

Messages, metrics, traces, and logs

‘Engineers’ carried screwdrivers

Resources were scarce, static, costly

No DevOps – we all sat together!

Distributed systems added complexity

The first ‘shadow IT’ brought new IT Operations paradigms, controls, frameworks

All in silos, no T-shaped people

‘IT Operations Management’ (ITOM)

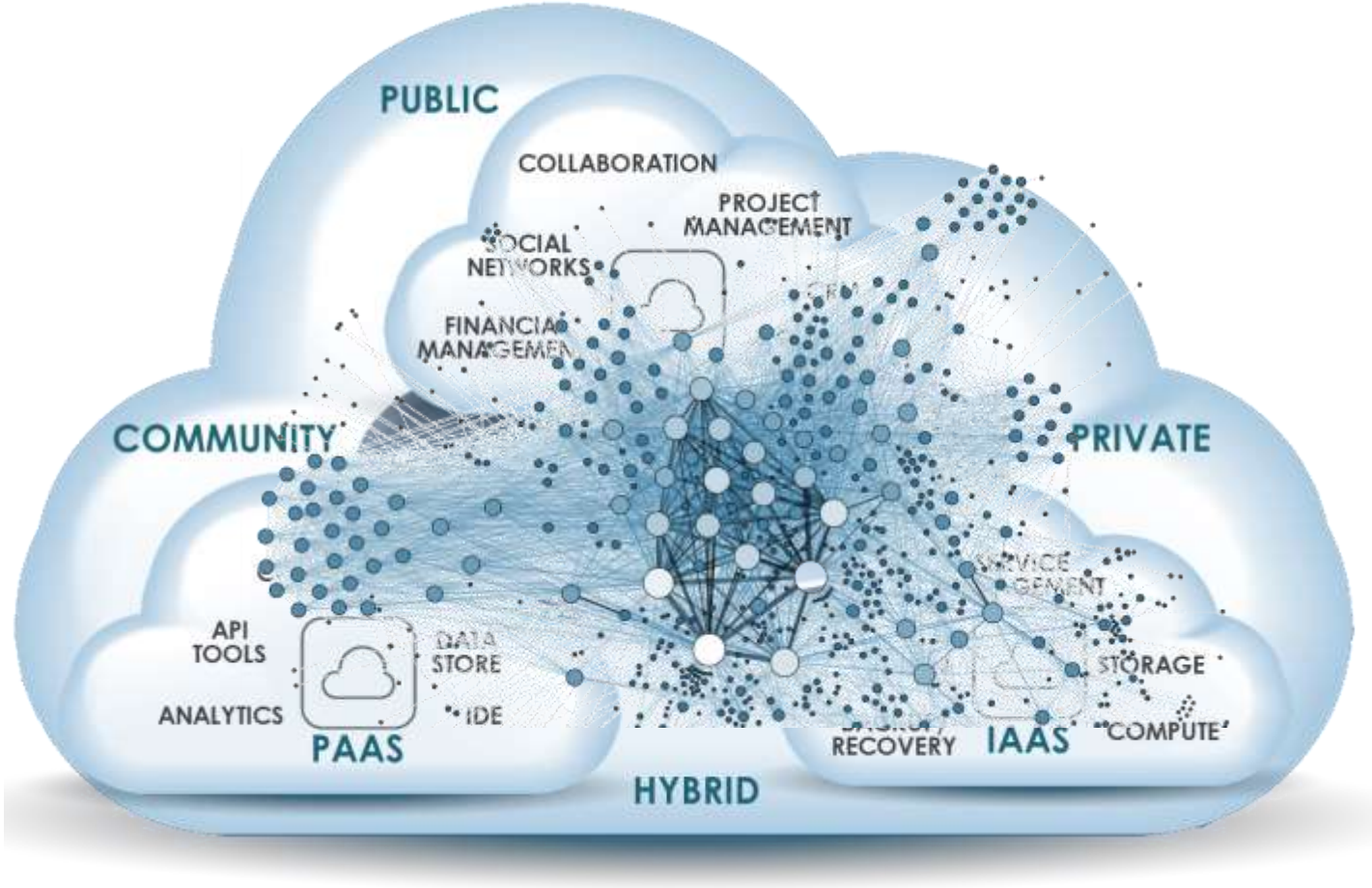
- batch scheduling, content management, resource management, capacity planning, financial planning …

IT Infrastructure Library (ITIL) and IT Service Management (ITSM)

- Problem/Incident Management, Capacity Planning, Configuration Management, Service Management …

APM – simulated ‘observability’

NPM – sniffing and inspecting traffic



splunk> turn data into doing

@AndiMann

Then, there was ITOA (and *the other* AIOps)

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

ITOA

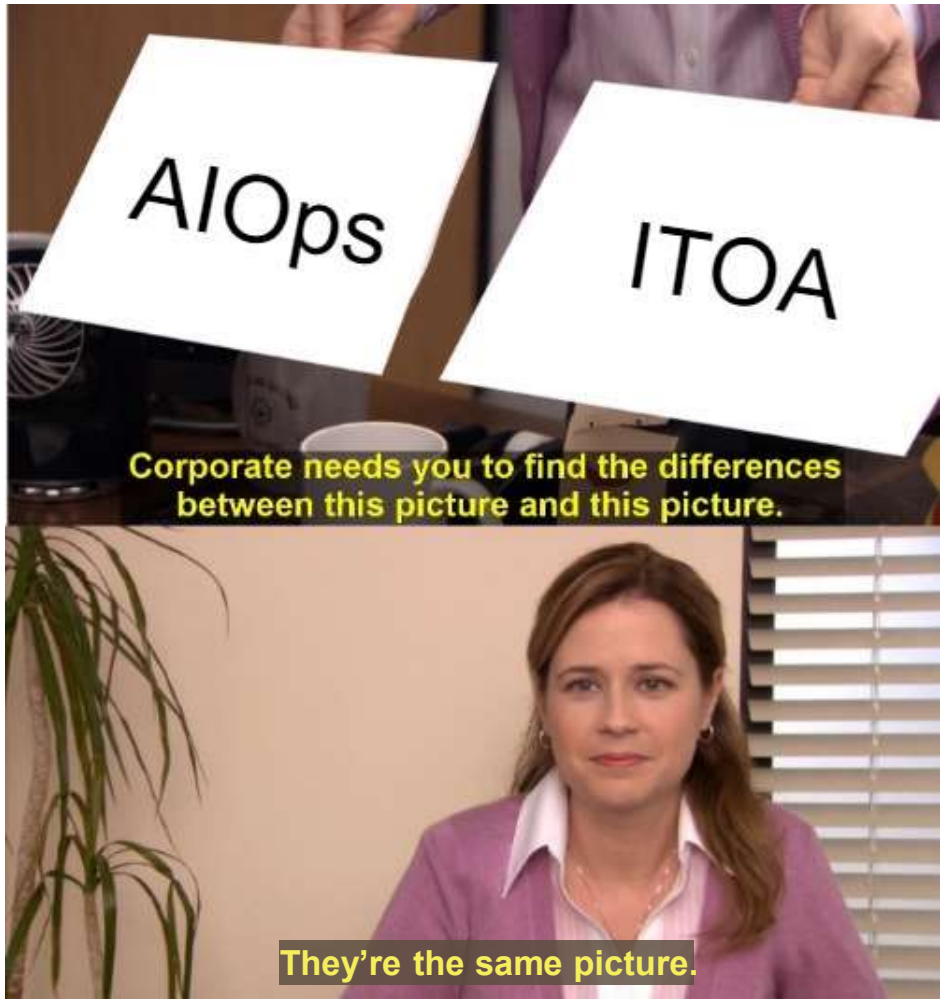
… gathering, processing, analyzing and interpreting data from various IT operations sources to guide decisions and predict potential issues

- TechTarget

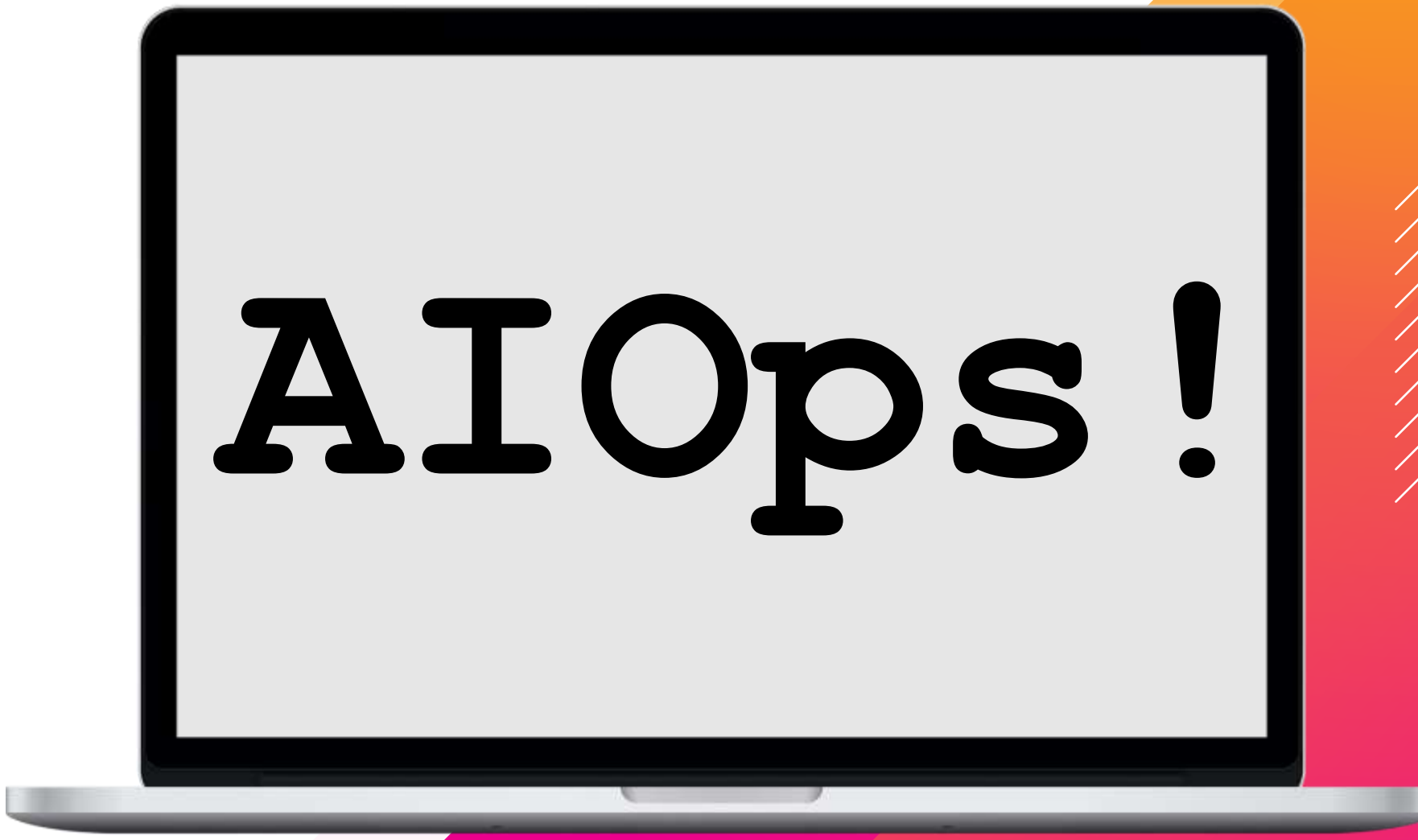
(the *other)* AIOps

… multiple layers that address data collection, storage, analytical engines and visualization.

- Gartner (2017)



Which brings us to …



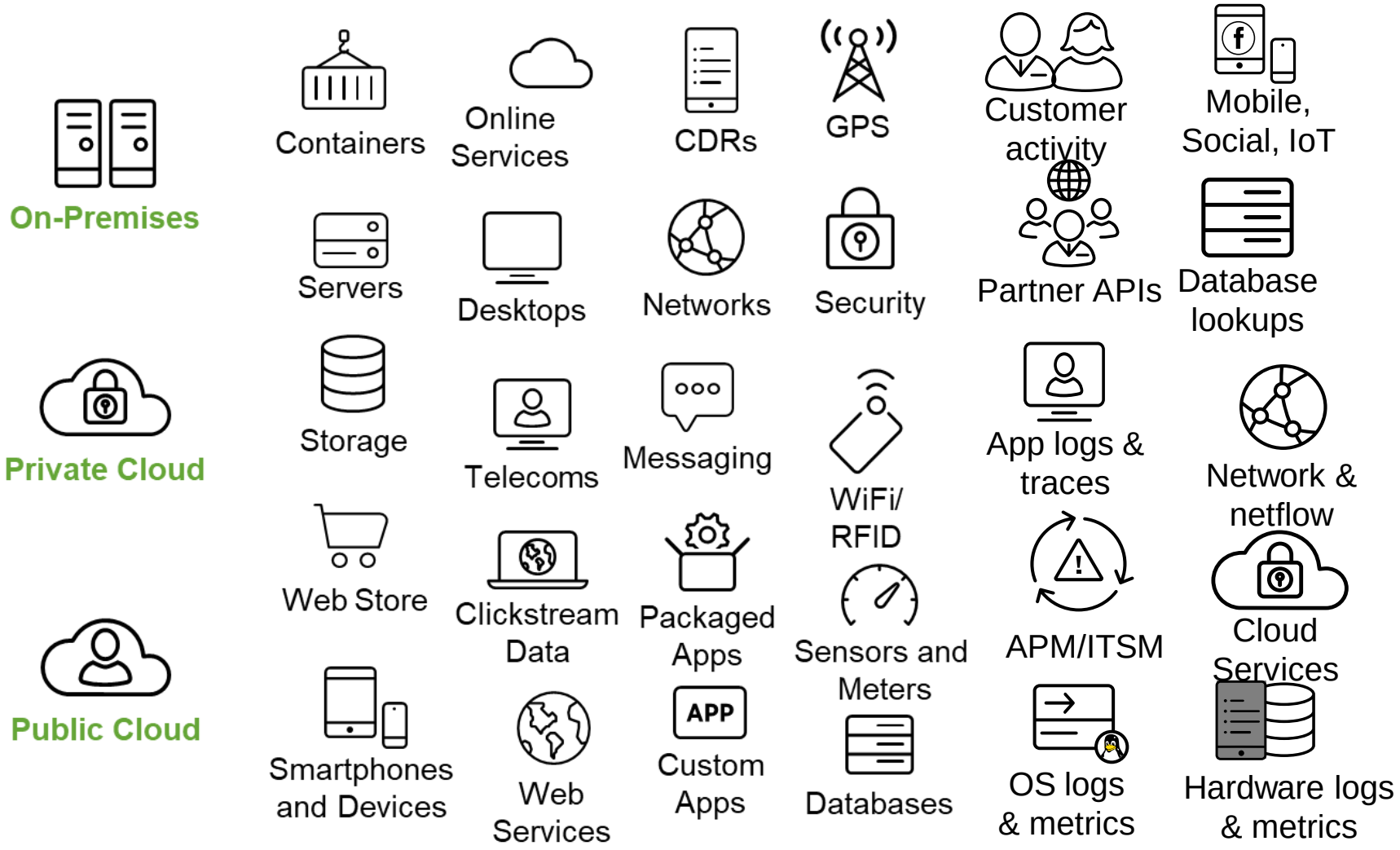
“ AIOps combines **big data** and **machine learning** to **automate** IT operations processes, including event correlation, anomaly detection and causality determination.”

-Gartner

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

Take IT Ops 'Big Data' Sources

AIOps utilizes the data that is managed and stored in DataOps

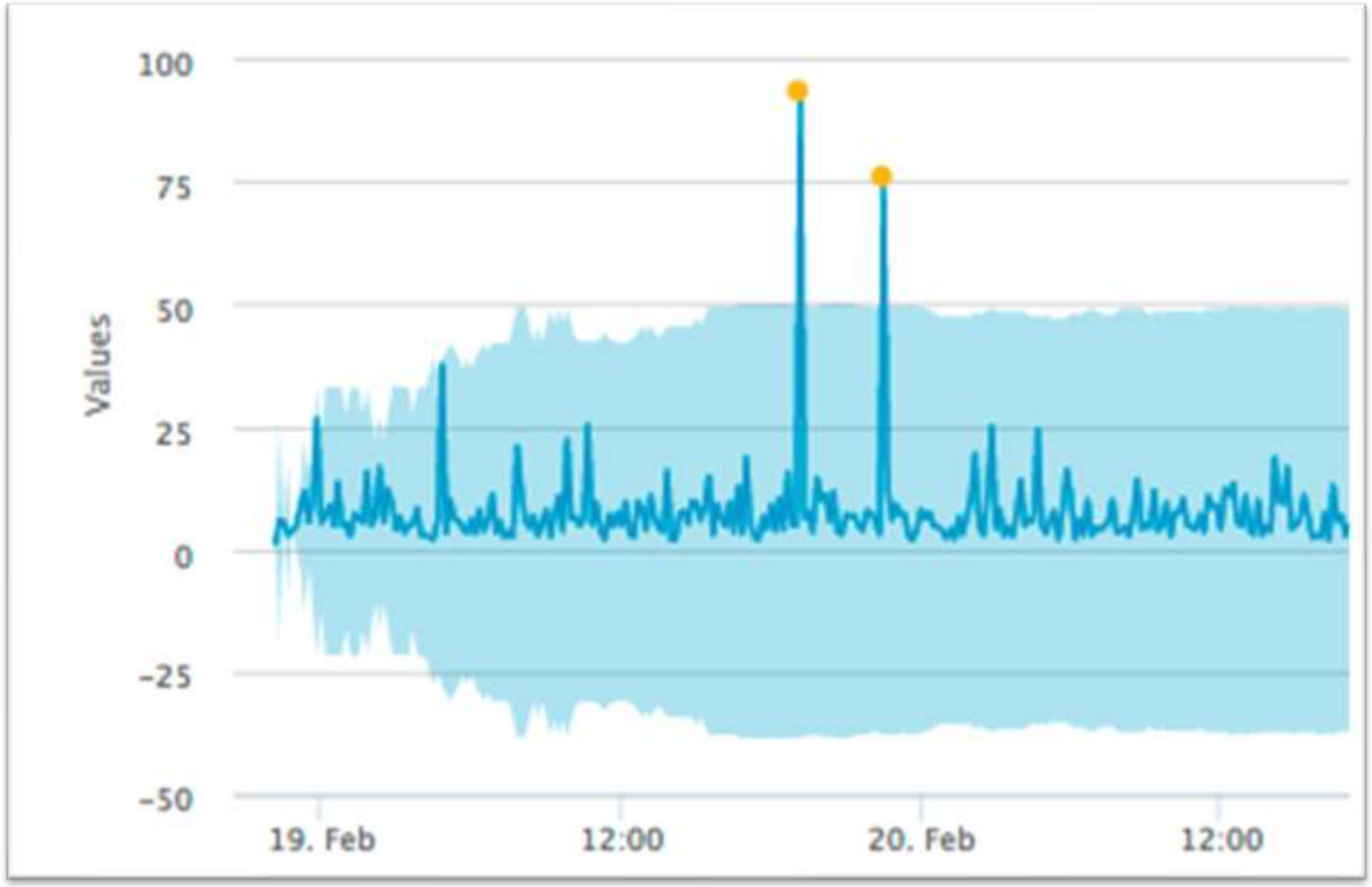


splunk> turn data into doing

Apply Machine Learning Algorithms

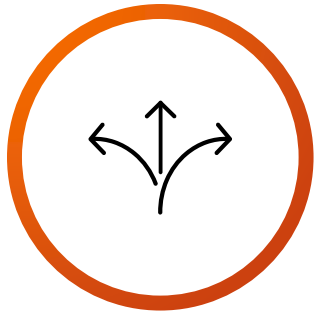
e.g. Anomaly Detection

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

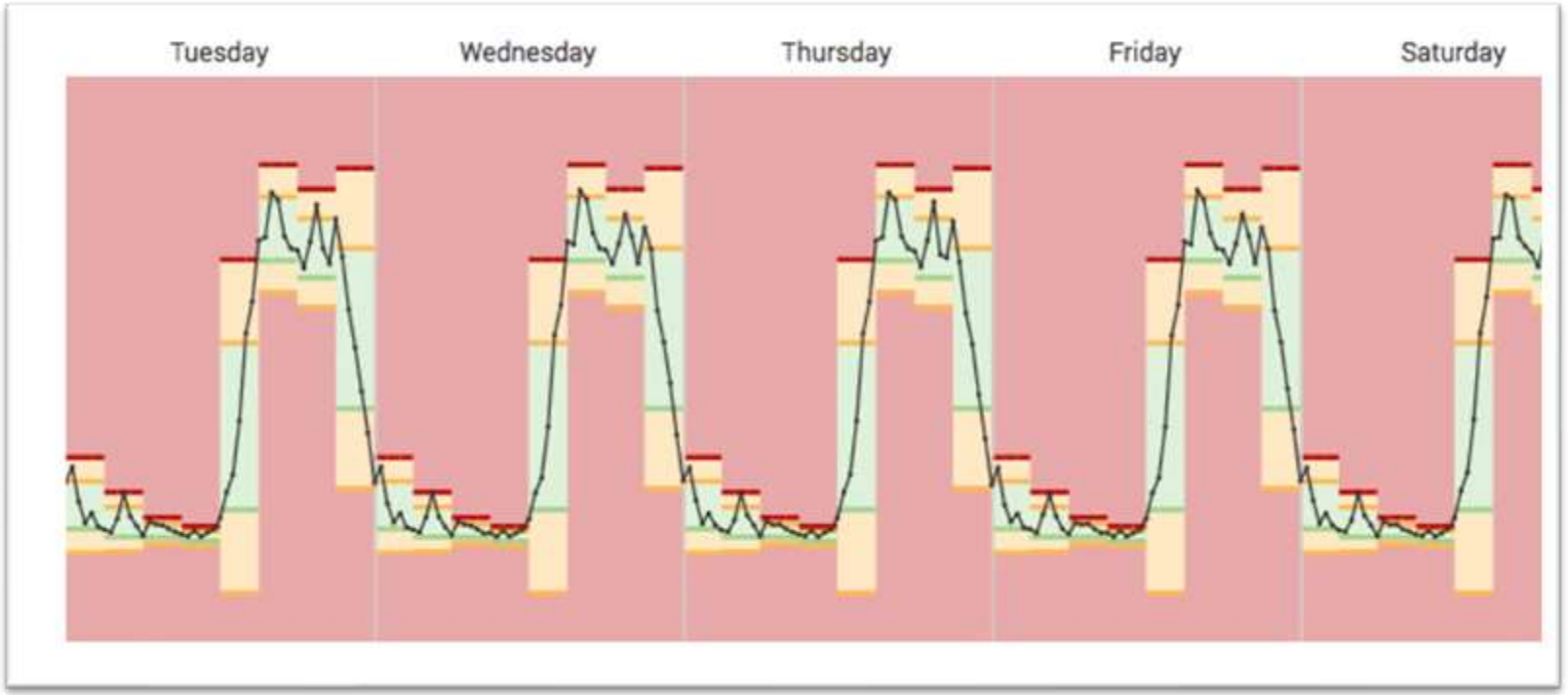


Apply Machine Learning Algorithms

e.g. Dynamic Thresholding

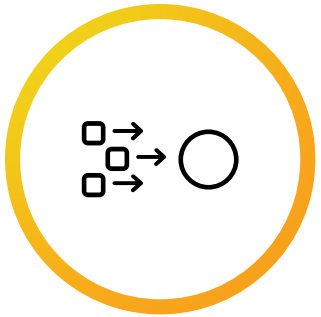


- Thresholds adapt in real time
- Trend and alert on anomalous behavior
- Prevent service degradation

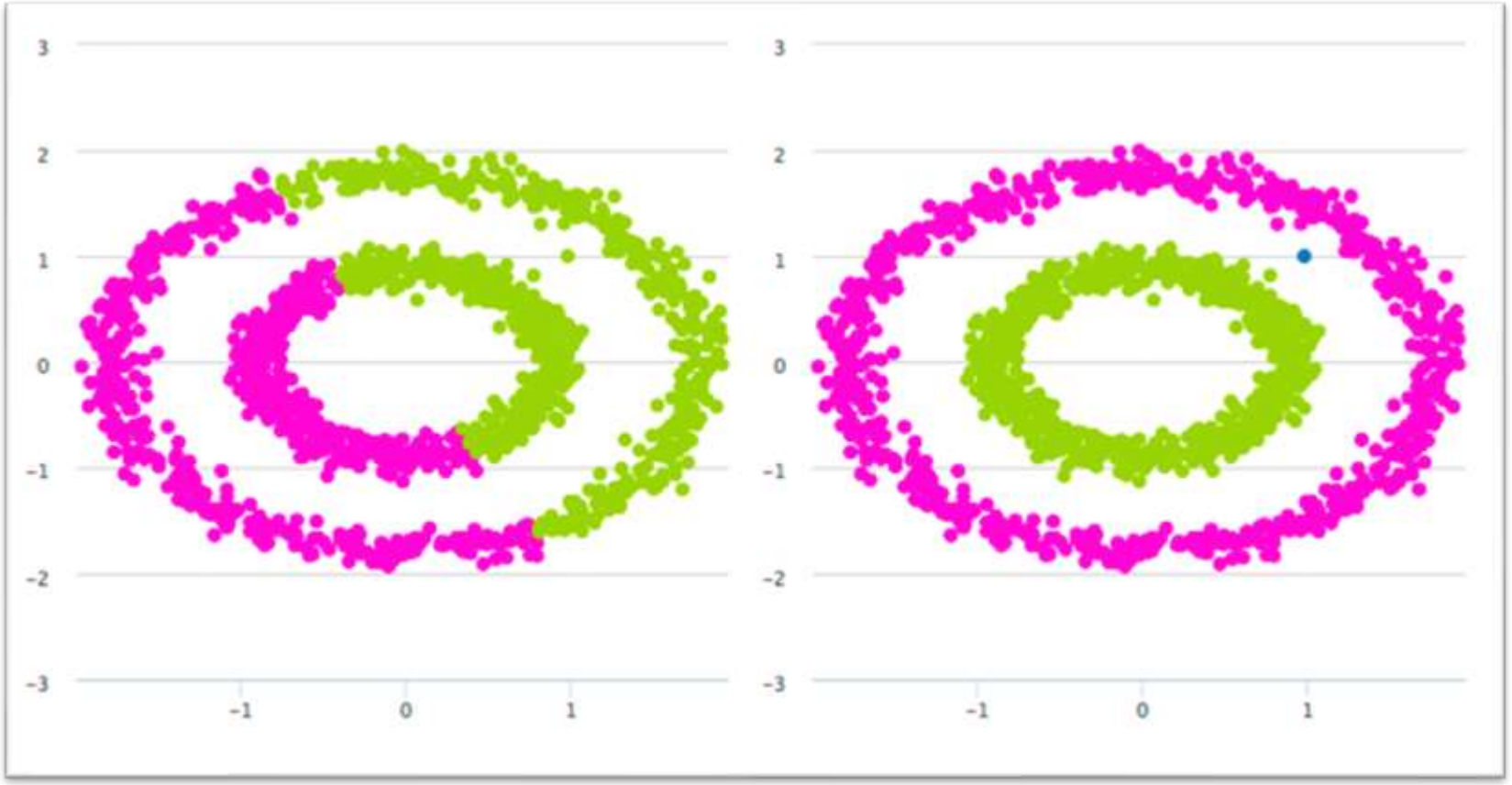


Apply Machine Learning Algorithms

e.g. Event Clustering



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



Apply Machine Learning Algorithms

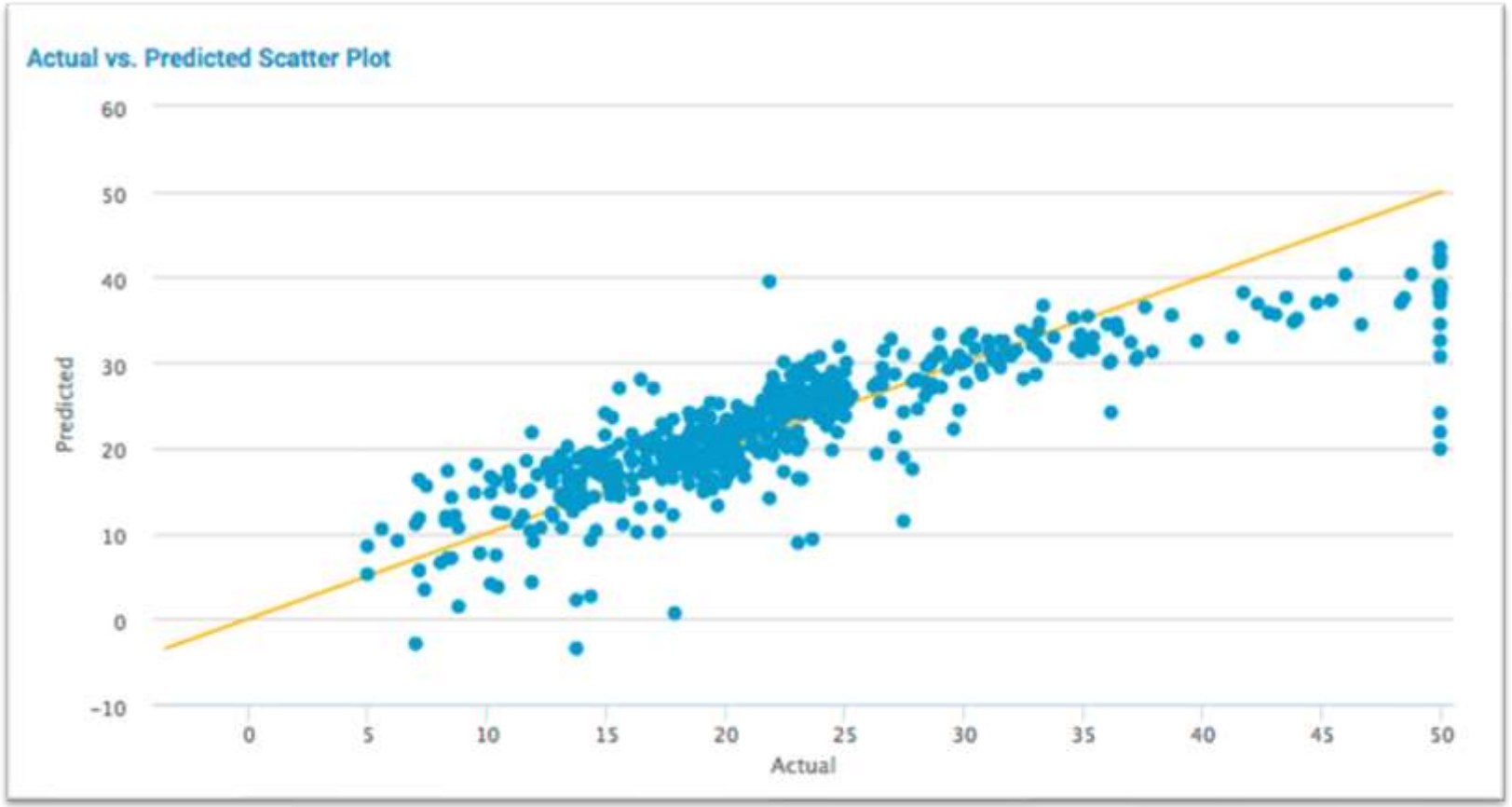
e.g. Intelligent Alerting

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

Apply Machine Learning Algorithms

e.g. Predictive Analytics

- Predict outages and anomalies before they occur
- Predict demand for new products and features



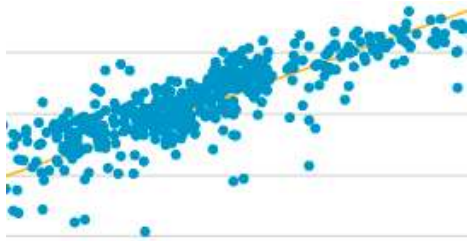
Train Machine Learning Models

Acquire data to test an algorithm

Train algorithms to create a model

Apply real data to validate model

Surface model to solve problems



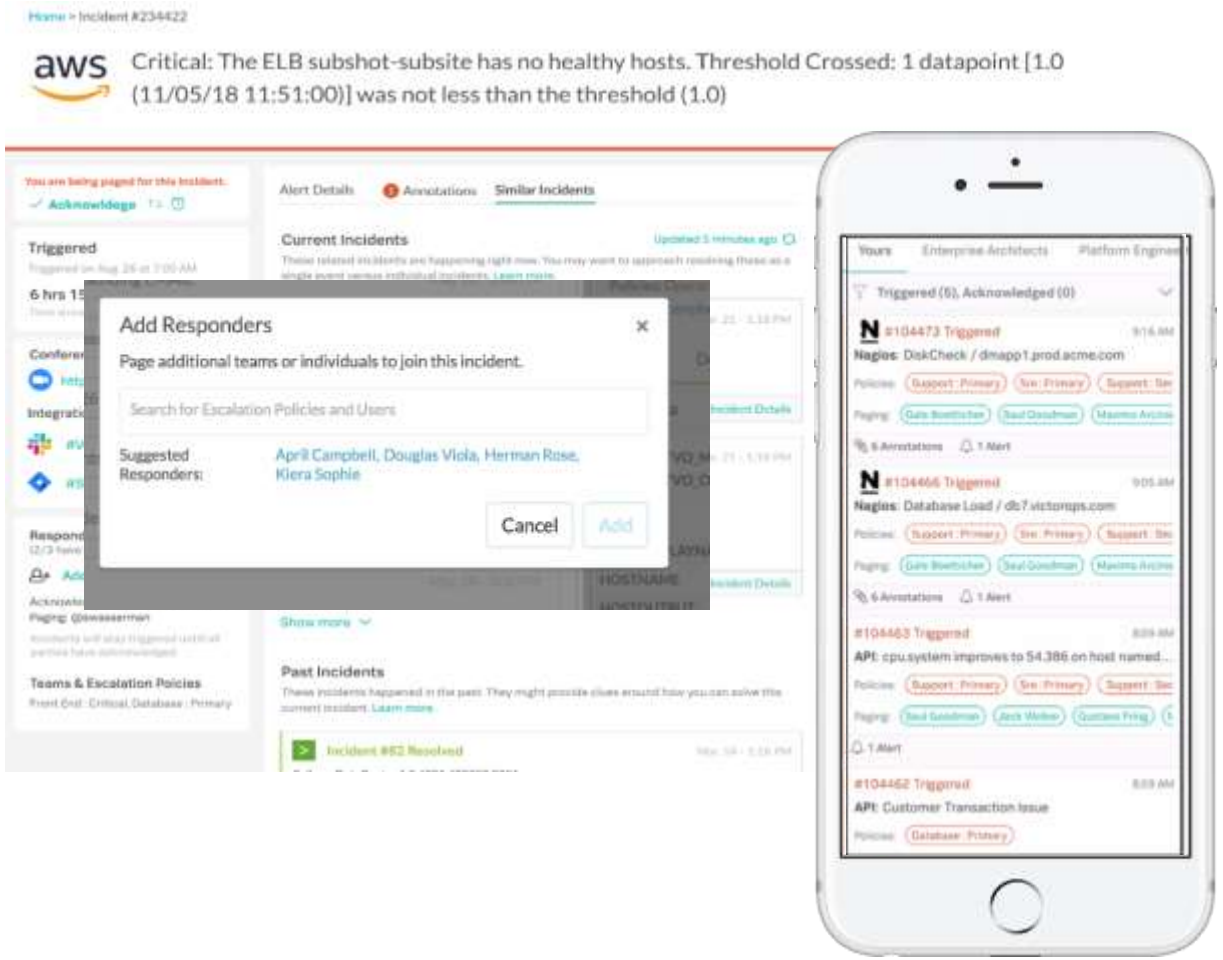
Operationalize your model

splunk> turn data into doing

Turning AIOps Data Into Doing

Integrate and Activate Other Tools and Processes e.g.

- ITSM tool integration
  - Automatically open, update, close tickets
  - Interrogate CMDB for diags, ‘known knowns’
- Automation integration
  - Execute discrete tasks to aid investigation
  - Collect more data, execute diagnostics
- 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



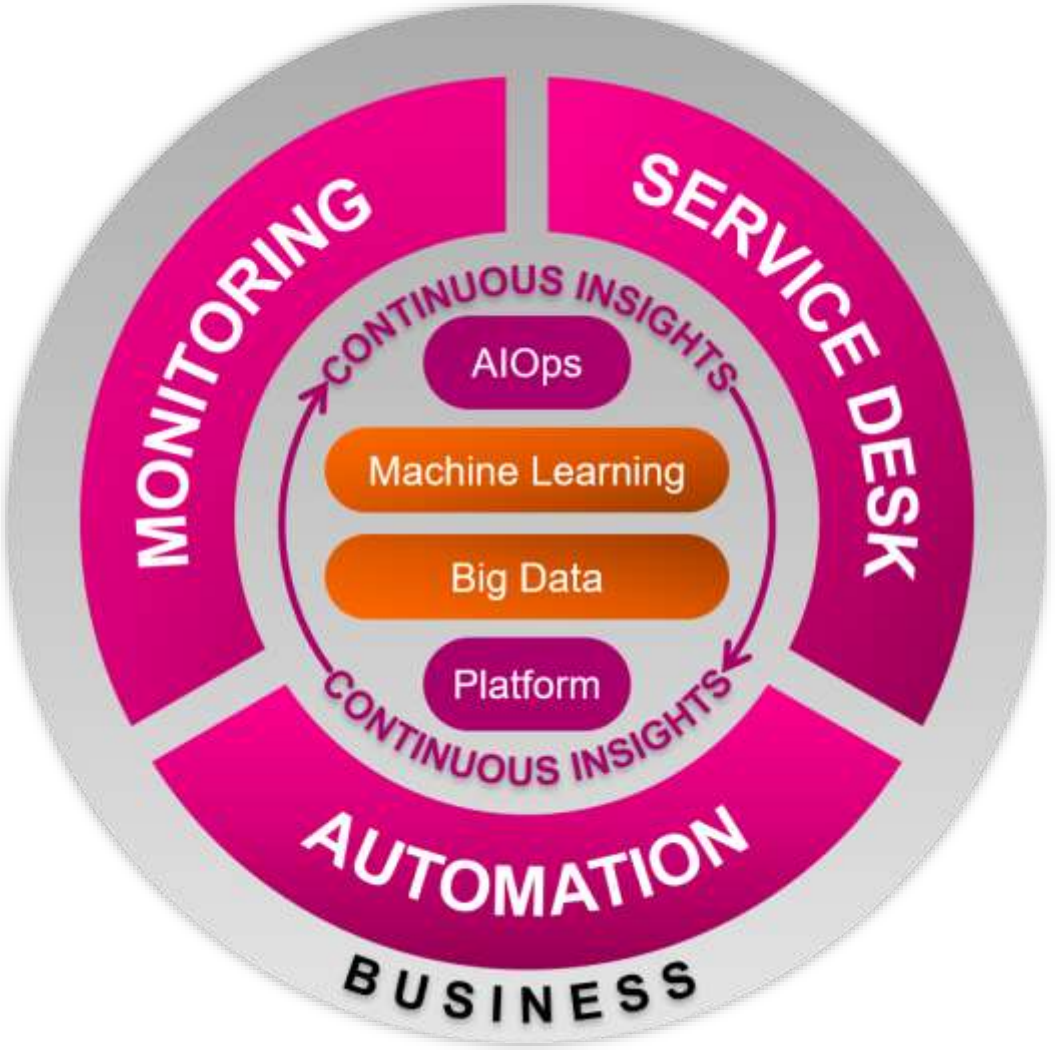
splunk> turn data into doing

And that's AIOps!

Using big data and machine learning to provide continuous insights that improve the speed, agility, accuracy, and efficiency of IT Operations processes, including:

- Monitoring and Alerting
- ITSM and Service Desk
- Automation & Orchestration

… and more!



More Learning Resources for Your AIOps Journey

2019 Gartner Market Guide for AIOps Platforms

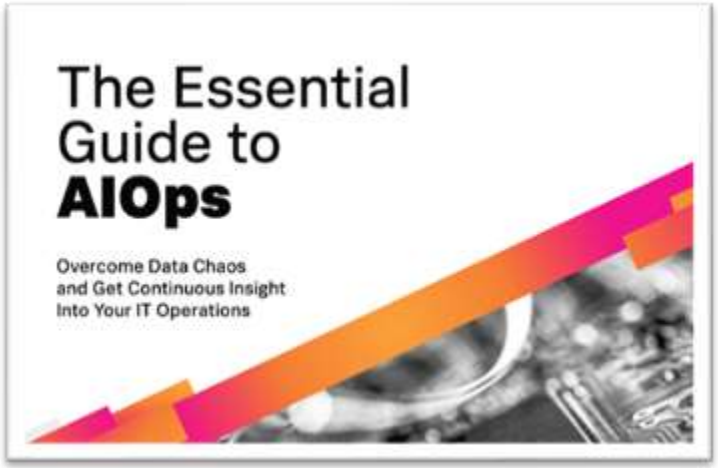
Find this report on our website, and you'll be able to compare different AIOps platform

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!

@AndiMann
amann@splunk.com

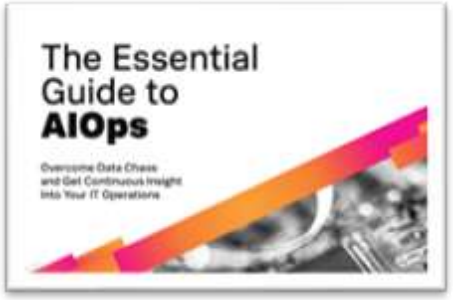
GLOBAL SKILUP FESTIVAL SM
by DevOps Institute

[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.