Splunk for NewOps

Using Data-Driven IT Operations to Better Manage IT Systems at Scale

Andi Mann

CTA | Splunk

Endre Peterfi

Sales Engineer | Splunk

splunk> .conf19

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Turn Data Into Doing, 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.

splunk> .conf19

Agenda
Splunk for NewOps

Introduction – From 'TradOps' to 'NewOps'

Splunk for NewOps – Examples & Demos
Splunk for CloudOps
Splunk for DevOps
Splunk for SREOps
Splunk for AIOps
Splunk for ChatOps

Summary/Wrap-up

splunk> .conf19

From TradOps to NewOps

TradOps

IT Ops for a world of 'traditional' technologies, strategies, processes

Platforms

Strategies

Bare Metal Virtualized DAS/NAS/SAN Monoliths

IT Silos Ticket-Driven Runbooks I-Shaped

Dashboards Spreadsheets Thresholds Alerts

Specialized Single Platform Frameworks ITSM-Based

Insights & Process

Tools

Designed for 8x5 operations, 'bricks & mortar', monolithic applications, 'online day', overnight batch, separated teams, limited abstraction
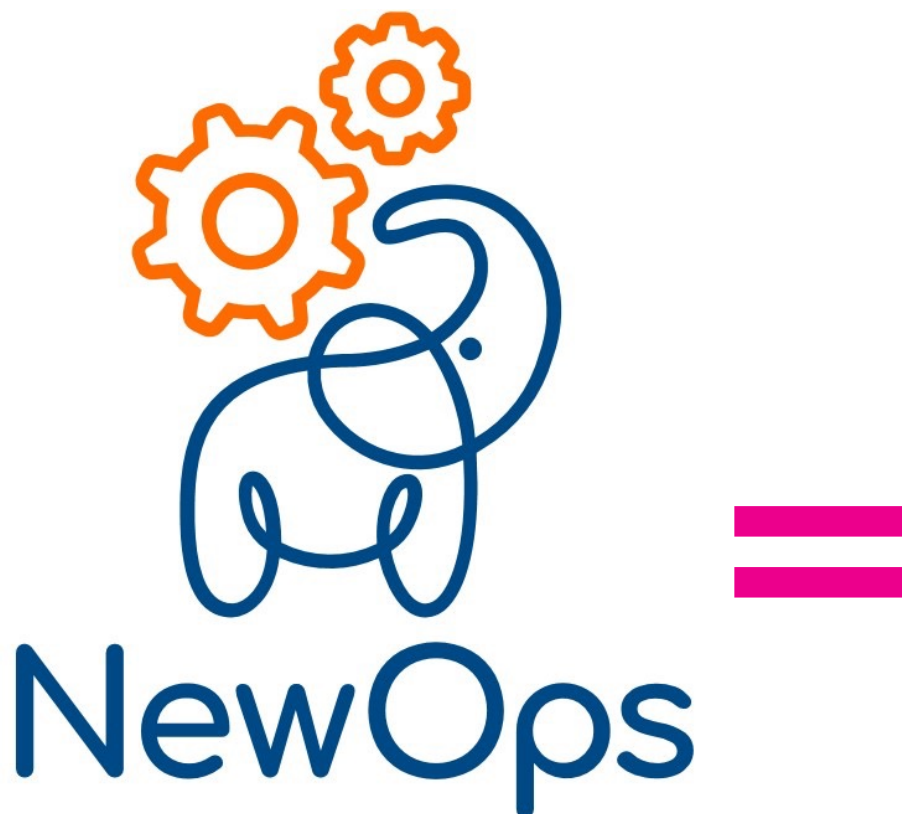
Built for 'legacy' processes and tools
- ITIL, ITSM, CoBIT, CAB, etc,
- APM, Service Desk, CMDB, etc.

Old, slow, cumbersome, stagnant
- By design!!

splunk> .conf19

© 2019 SPLUNK INC.

NewOps

A modern approach for new technologies, strategies, processes

**NOT ONLY IS THIS
HARD WORK …**

CloudOps
WebOps
MSAOps
DevOps
AgileOps
SREOps
AutoOps
DataOps
ObservableOps
MLOps
AIOps
CXUXOps
ChatOps

**… BUT TURNS OUT
THIS DIDN'T GO AWAY!**

TradOps
(incl:
Sysadmin
DCOps
APMOps
TicketOps
CMDBOps
ITSMOps
ITILOps)

splunk> .conf19

Key Characteristics of NewOps Approaches

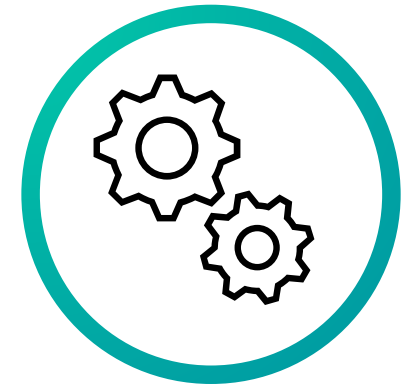Modern Problems Need Modern Solutions

Data Driven

Collaborative

Business-Aligned

Automated

splunk> .conf19

Splunk for CloudOps

New Approaches for IT Operations to support Cloud, Web, Containers, Microservices, Serverless, etc.

splunk> .conf19

CloudOps

Web-scale disruptors adopt new cloud approaches

TradOps – Servers and VMs

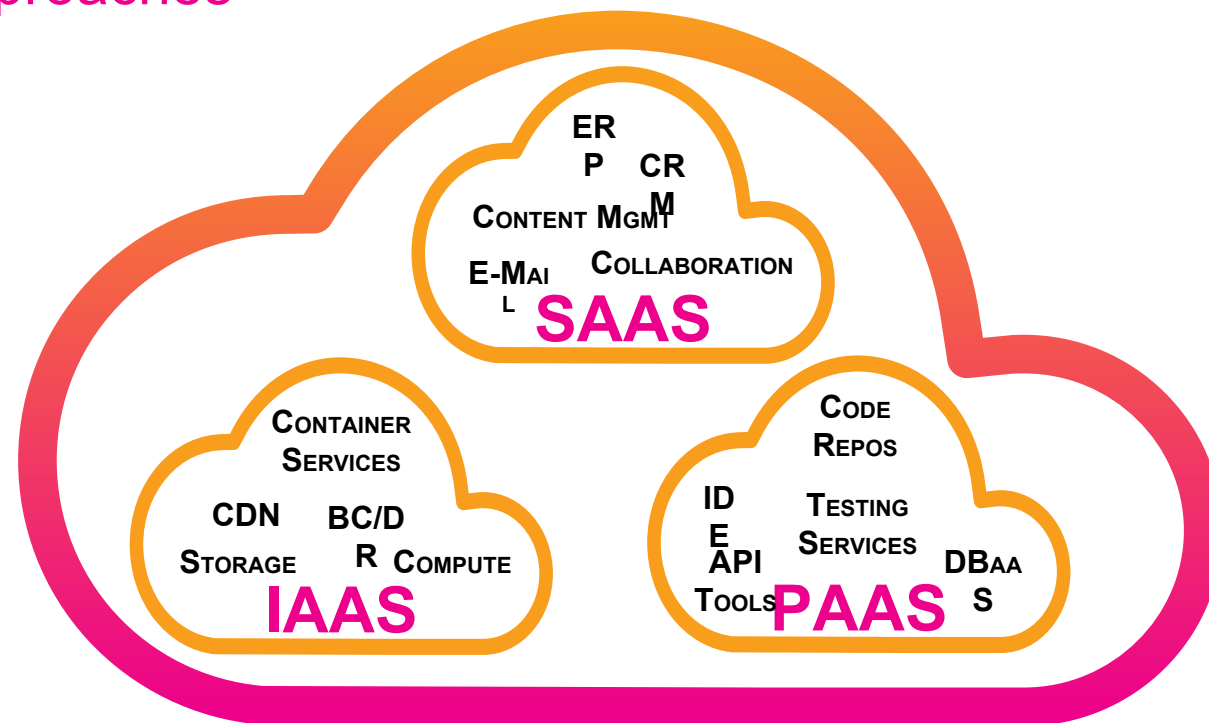NewOps – Cloud (IaaS, PaaS, SaaS)

Scale-out > scale-up
- More services across more servers/VMs
  - VS.
- More services across larger servers/VMs

More activity, more to manage/monitor

IT can see deeper into some applications; but others are even more opaque

Closer connection to customers, devs now can see deeper into business

ERP

CRM

CONTENT MGMT

E-MAIL

COLLABORATION

SAAS

CONTAINER SERVICES

CDN

BC/DR

STORAGE

COMPUTE

IAAS

CODE REPOS

IDE

TESTING SERVICES

API

DBAAS

TOOLS

PAAS

splunk> .conf19

WebOps

NewOps started in disruptive web-scale businesses – with no legacy!

TradOps – Internal users, private network

NewOps – External customers, public network

Public systems ☐ degraded performance
- Network latency, edge devices, variable n/w infra

Innovation > performance
- Gmail was beta for 5 years

Load time > stability
- No "5 nines" for movies and social

splunk> .conf19

MSAOps

Finally – maybe? – realizing the potential of SOA and WS
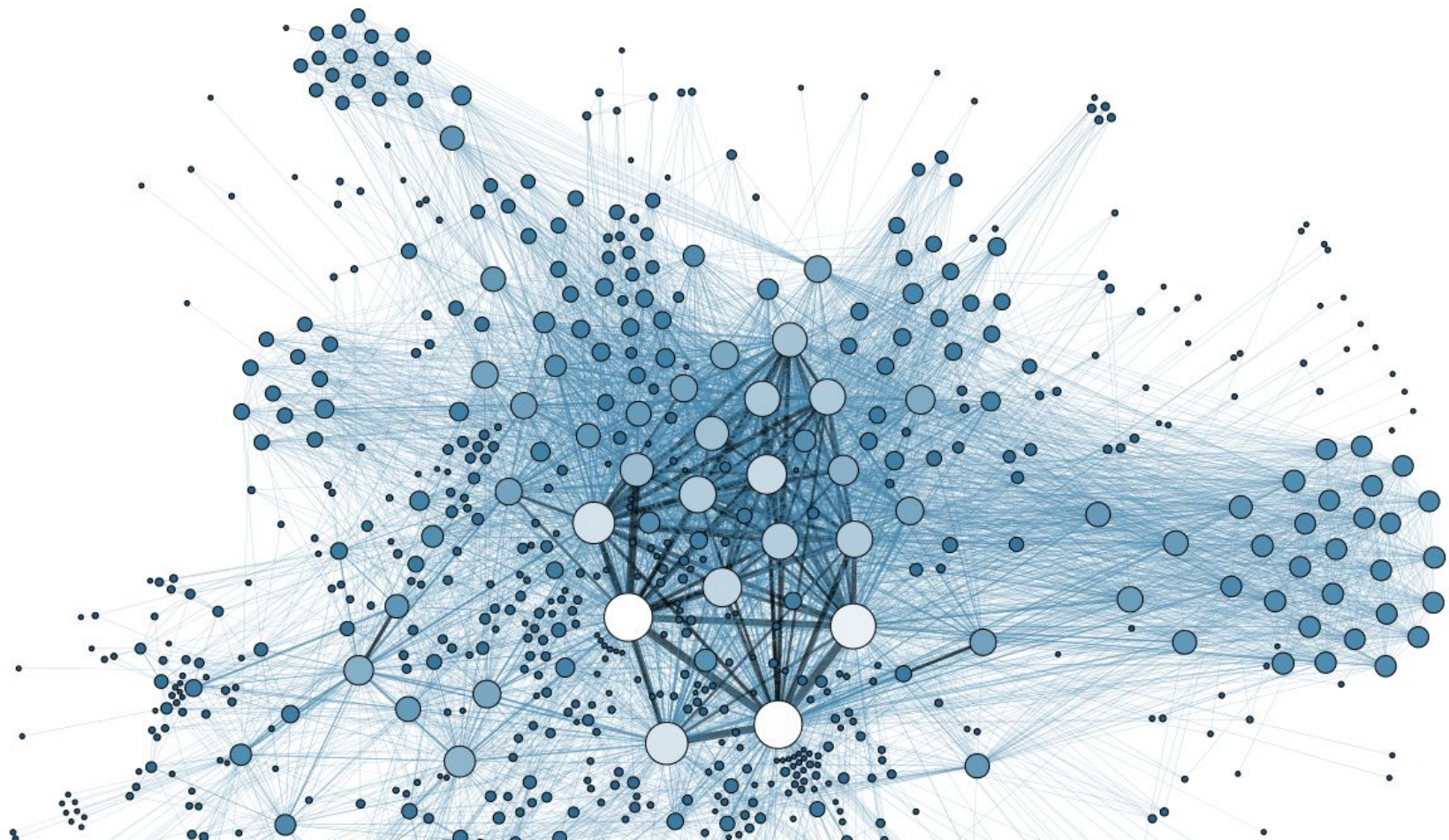
TradOps – Monoliths

NewOps – Microservice

More nodes == more tra

Even greater abstraction

'Composable' applicatio

Exponential complexity

nf19

ContainerOps

Taking system virtualization to the cloud level

TradOps – Servers

NewOps – Containers

Automated deployments

Abstracted visibility

'Cattle not pets'

Exponential complexity

splunk> .conf19

Demo

splunk> .conf19

Splunk for DevOps

New Approaches for IT Operations to support DevOps, Agile, Collaboration, etc.

AgileOps

Cloud disruption meant speed and agility – Devs just got the message first

2009

DEVOPS AT FLICKR
10 DEPLOYS A DAY

2015

DEVOPS AT AMAZON
140,000 DEPLOYS A DAY

TradOps – Slow and Stable

NewOps – Speed and Agility

AppDev closer to business

Distributed components in constant change

Faster releases to meet new online pressures

High-performing companies deploy 30x faster with 200x shorter lead time

Sources: DevOps @ Amazon, Chris Munns, https://www.slideshare.net/TriNimbus/chris-munns-devops-amazon-microservices-2-pizza-teams-50-million-deploys-a-year
10 Deploys a Day, John Allspaw, Paul Hammond, https://www.slideshare.net/jallspaw/10-deploys-per-day-dev-and-ops-cooperation-at-flickr
Puppet Labs, *State of DevOps Report', 2018,* https://puppet.com/resources/whitepaper/state-of-devops-report

splunk> .conf19

DevOps

If only one team is agile, all you have done is shift the bottleneck
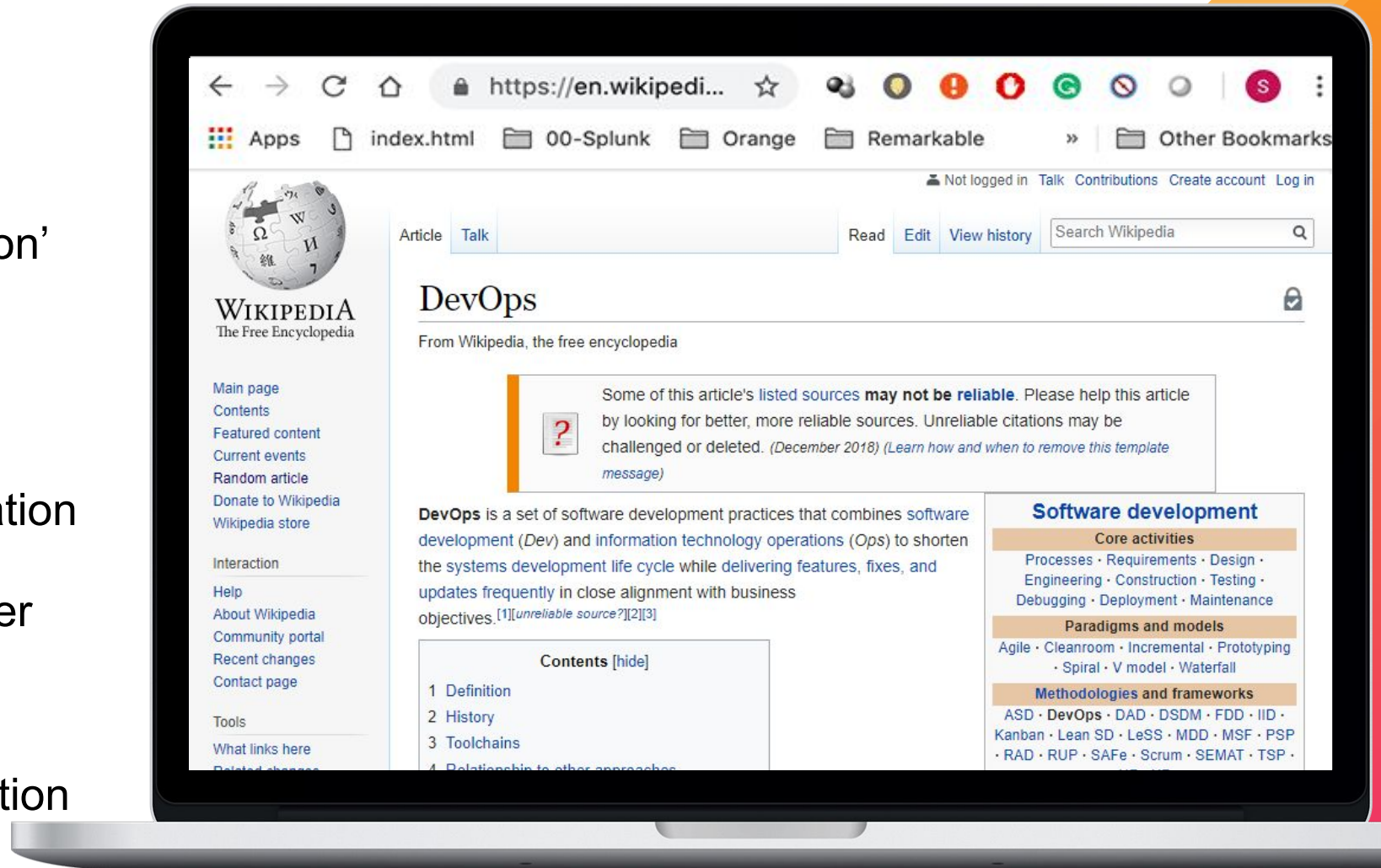
TradOps – 'Wall of Confusion'

NewOps – Collaborating Teams

DevOps - collaboration, communication, and integration between Dev and Ops to deliver better software, faster

Empowered staff, loosely-coupled toolchains, T-shaped people, collaboration across boundaries

Visibility, predictability, productivity all much harder

Source: Wikipedia

splunk> .conf'19

Demo

Splunk for SREOps

New Approaches for IT Operations to support Site Reliability Engineering, 'Relentless Automation', Observability, etc.
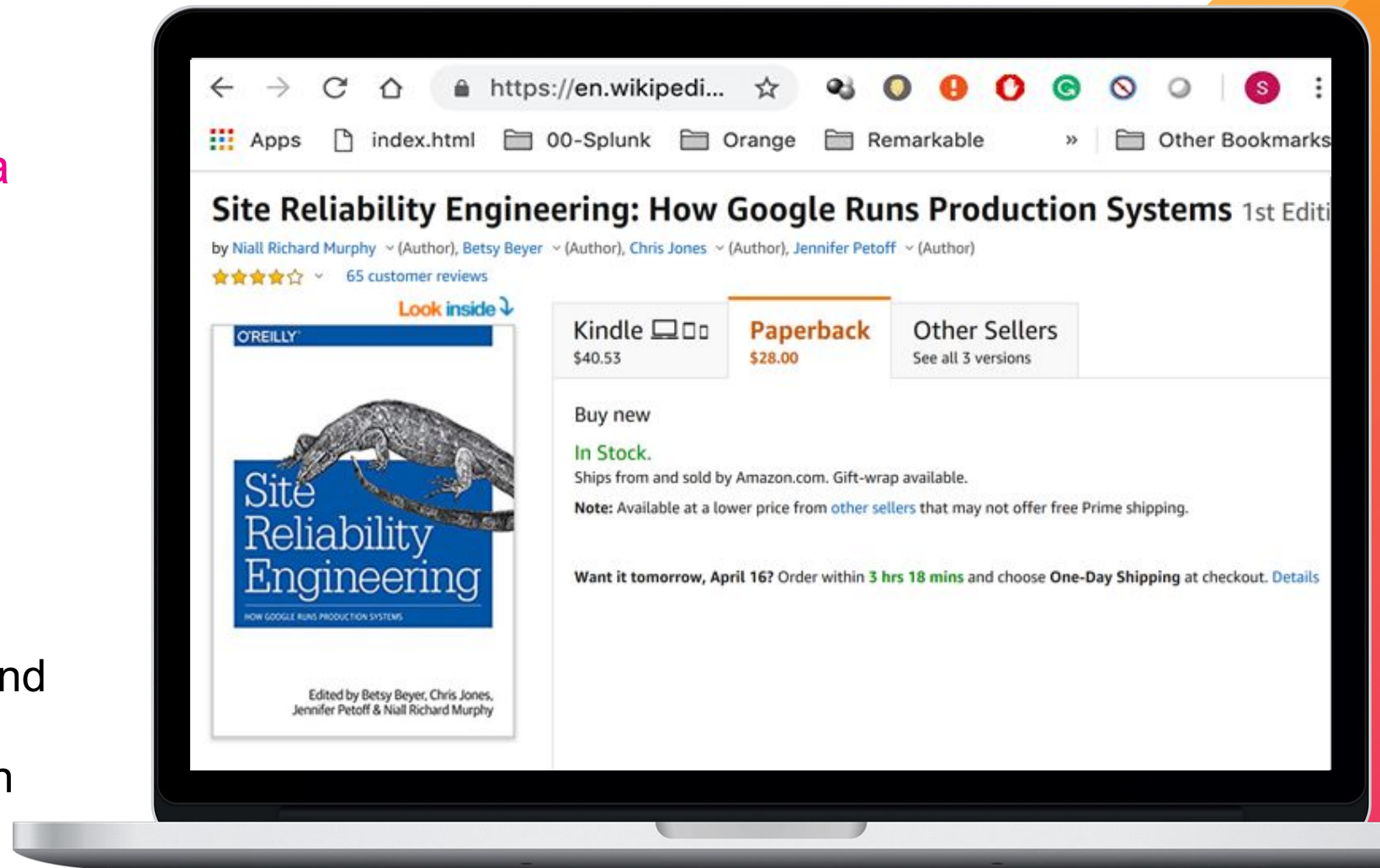
splunk> .conf19

SREOps

Collaborative cultures and technologies foster a new approach to Ops

TradOps – IT System Administration

NewOps – Site Reliability Engineering

"Apply the principles of computer science and engineering to the design and development of computing systems … [with] a focus on system reliability"

– Google/O'Reilly

Source: Site Reliability Engineering, Betsy Beyer, Chris Jones, Jennifer Petoff, Niall Richard Murphy, O'Reilly Media, Inc., 2016

splunk> .conf19

AutoOps

IT Ops always automated at least *some* work – but automation is no longer optional

TradOps – Manual toil, some automation

NewOps – 'Relentless Automation'

Automate the mundane

Orchestrate the Complex

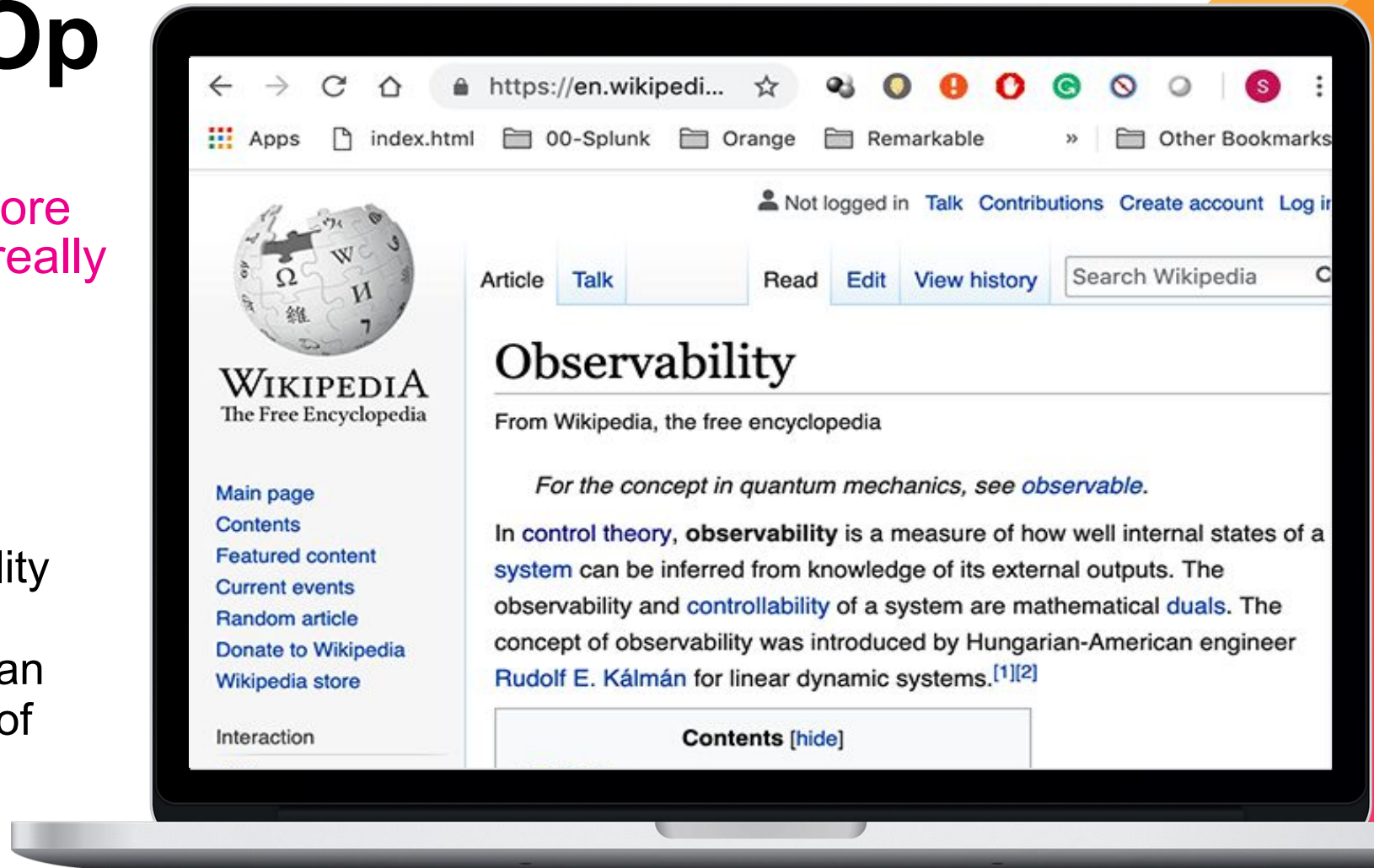Work smarter, not just faster

But also, work faster!

ObservableOps

Observability might be more than monitoring, but not really as new as it seems
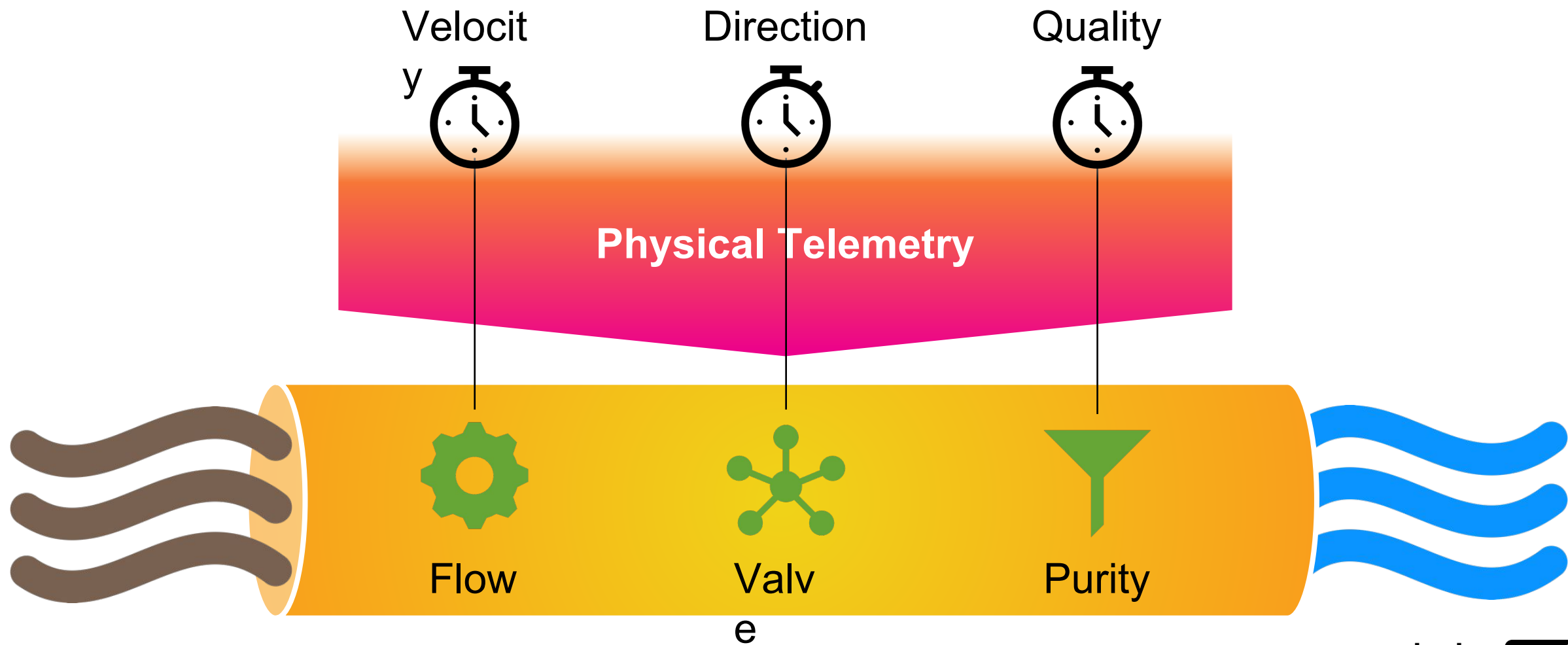
TradOps – Monitoring, exceptions, search

NewOps – Observability, correlation, analytics

"In control theory, observability is a measure of how well internal states of a system can be inferred from knowledge of its external outputs"
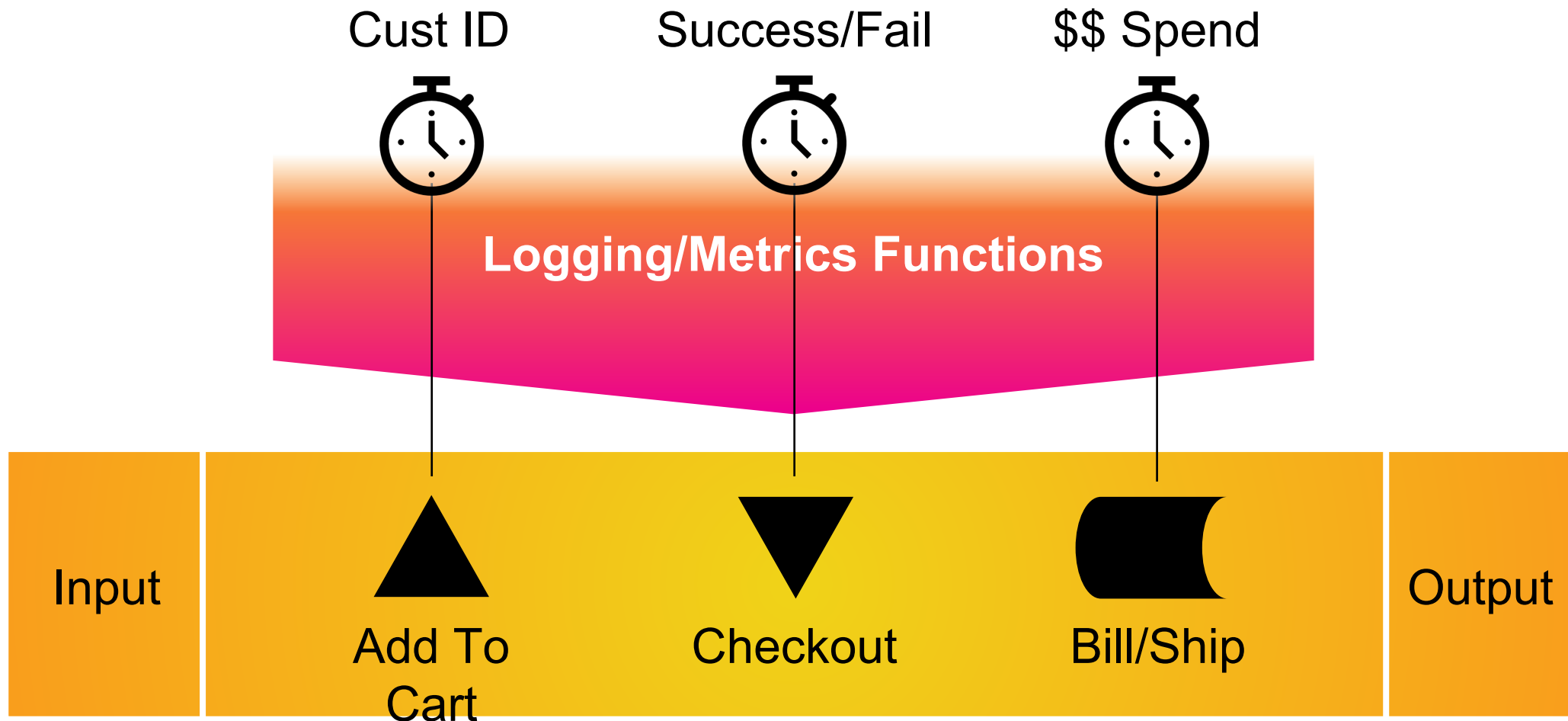

Source Wikipedia

splunk> .conf'19

Observability in Industrial Systems

Velocity

Direction

Quality

Physical Telemetry

Flow

Valve

Purity

splunk> .conf19

SREs 'Observe' With Logs, Metrics, Traces

NewOps look at aggregated events for meaning at massive scale

Sample Metric

1481050800	os.cpu.user	42.12345	hq:us-west-1
Timestamp	**Metric Name**	**Value**	**Dimensions**

Sample Log

Equivalent to 1 metric value

[29/Aug/2018 ... 3] "POST
/cart.do?u... 9&action=remove&&product_id=BS-2&JSESSIONID=SD6SA
L4FF1ADF ... 69 "http://www.buttercupenterprises.com/product.screen?
product_i ... (Intel Mac OS X 10_12_2) AppleWebKit/537.36 (KHTML, like
Gecko) Ch ... afari/537.36" 98

2569

splunk> .conf19

Demo

Splunk for AIOps

New Approaches to IT Operations using Data, Machine Learning, Predictive Analytics, Artificial Intelligence, etc.

splunk> .conf19

DataOps

With distributed, atomized, composable services, the only constant is data
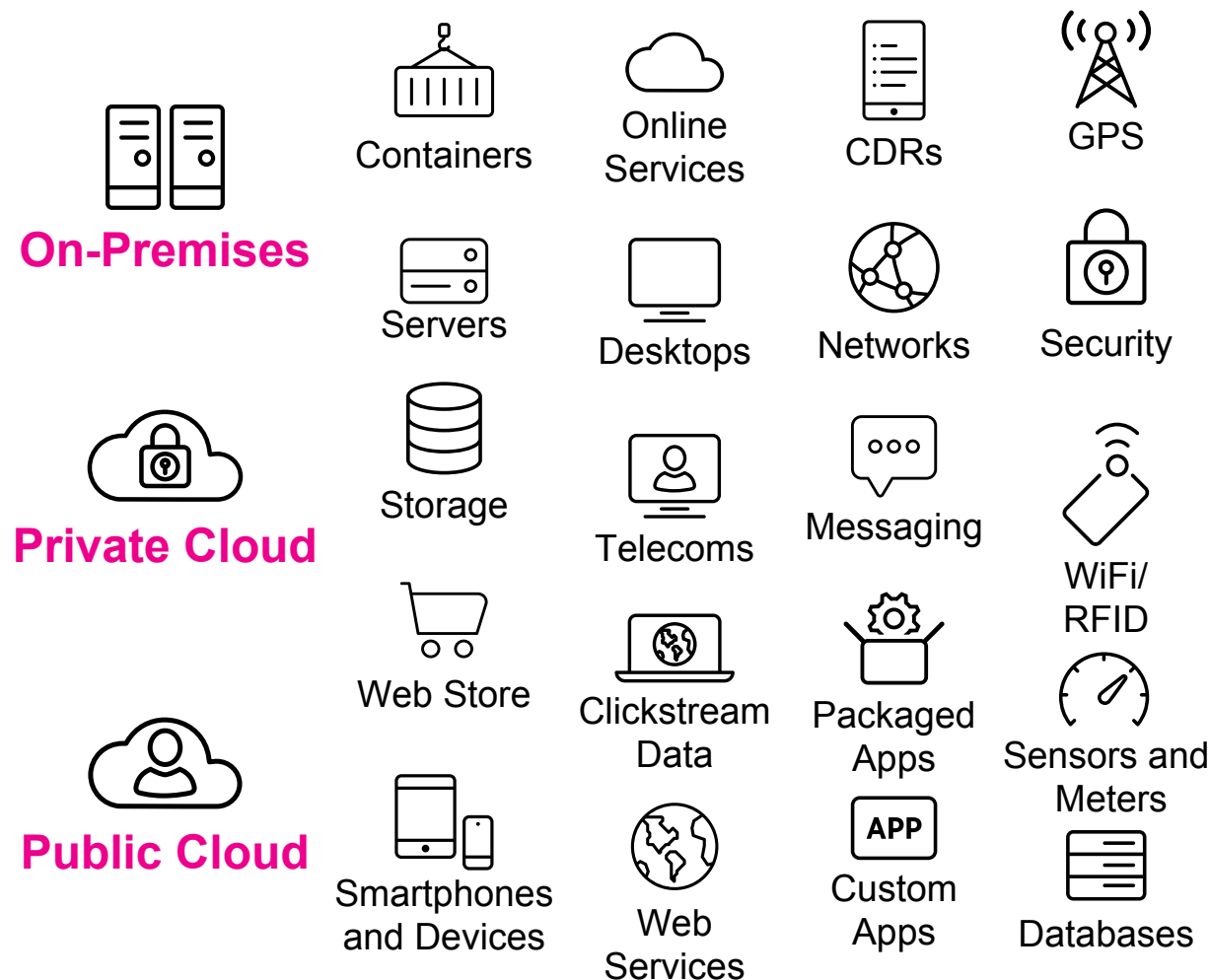
TradOps – Exception management

NewOps – Data-driven operations

Every microservice, every API, every component, every entity spewing data
- Stats, Metrics, Logs, Traces, Semantics

SO MUCH DATA!!!
- Ops are overwhelmed.

On-Premises

Private Cloud

Public Cloud

Containers

Online Services

CDRs

GPS

Servers

Desktops

Networks

Security

Storage

Telecoms

Messaging

WiFi/ RFID

Web Store

Clickstream Data

Packaged Apps

Sensors and Meters

Smartphones and Devices
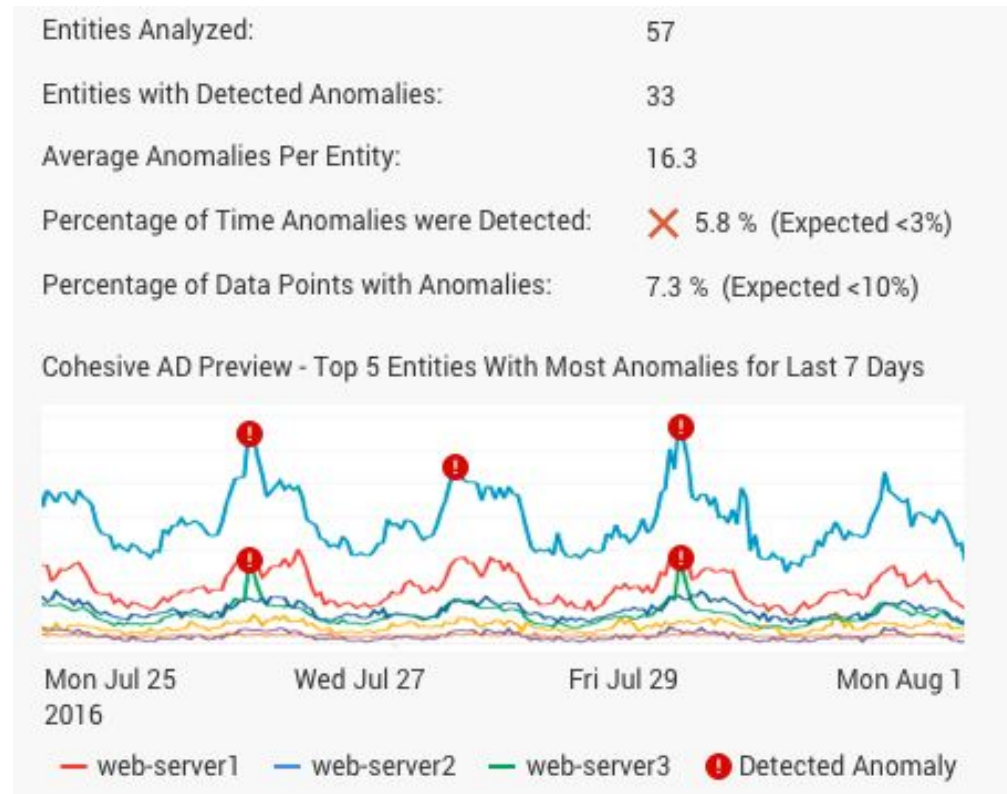
Web Services

Custom Apps

Databases

MLOps
Ops are overwhelmed with data, need machine speed to process it all

TradOps – Dashboards and Excel

NewOps – Analytics and ML

Make the machines do the number crunching, let humans be creative

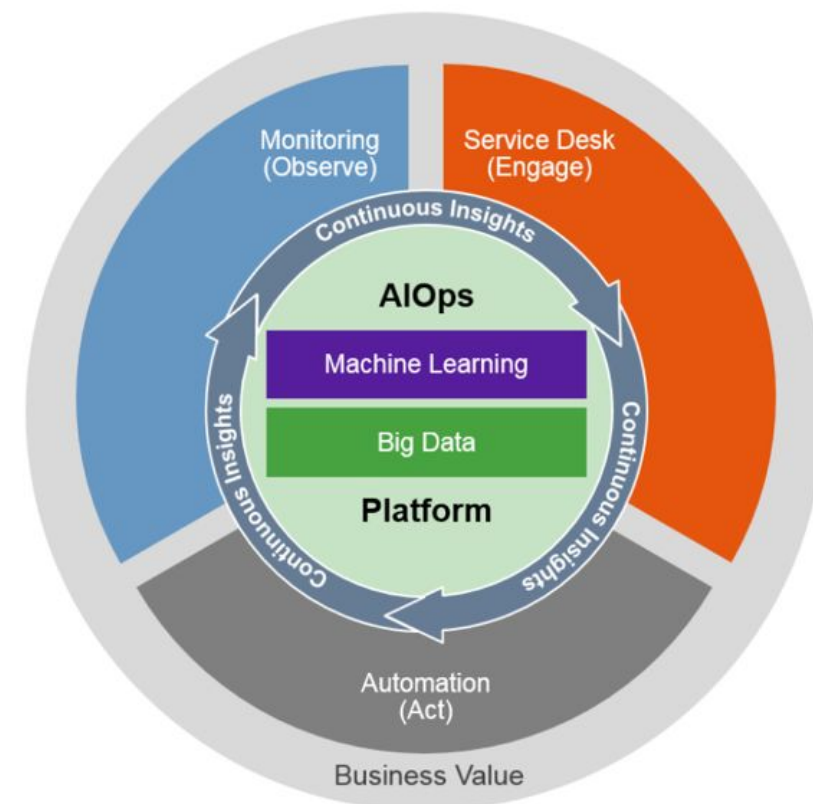Free up NewOps to architect and engineer to advance the business

Entities Analyzed:	57
Entities with Detected Anomalies:	33
Average Anomalies Per Entity:	16.3
Percentage of Time Anomalies were Detected:	✗ 5.8 % (Expected <3%)
Percentage of Data Points with Anomalies:	7.3 % (Expected <10%)

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

Analyst branding for advanced application of ML/AI to IT Ops

TradOps – Human Intelligence

NewOps – Artificial Intelligence

"Software systems that combine big data and artificial intelligence (AI), or machine learning functionality to replace a broad range of IT Operations processes and tasks"

Gartner [Market Guide for AIOps Platform], [Will Cappelli, Colin Fletcher, Pankaj Prasad], [03 August 2017]

splunk> .conf19

Demo

Splunk for HumanOps

New Approaches to IT Operations using Swarming, Collaboration, Blameless Reviews, Group Chat, etc.
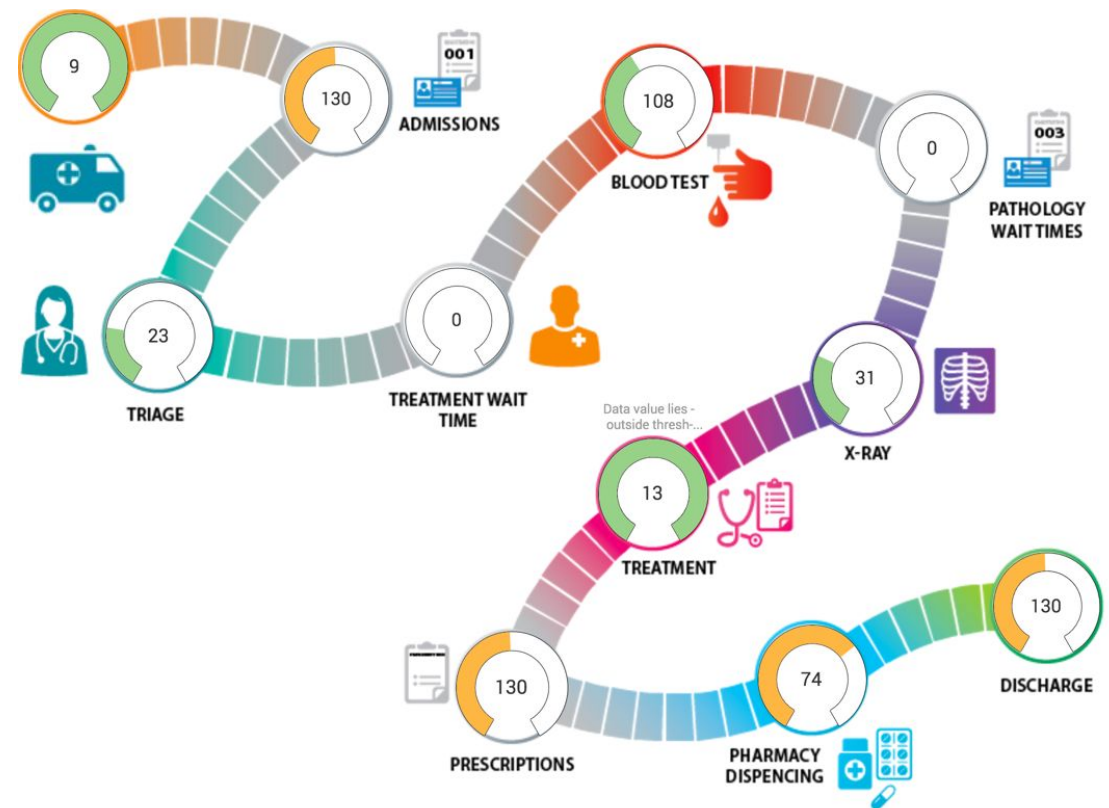
splunk> .conf'19

CX/UXOps

Because NewOps is people, not just systems

TradOps – Feeds and Speeds

NewOps – Customer Service

Customer and User Experience

- Multi-channel data
- Performance data
- Experience data
- Payload data
- Business data

splunk> .conf19

ChatOps

People communicate better if they actually talk to each other – who knew!?

TradOps – War rooms

NewOps – Swarming

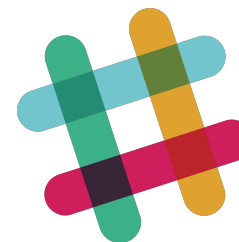Incidents managed in real-time, not by ticket

Chat room with bots to record and automate

Fix the problem, then blameless
post-mortem

Add requirements to technical backlog

Collaboration!

- Also see: CoffeeOps, BeerOps, HugOps

Demo

splunk> .conf19

What about NoOps?

A budget-fueled pider-dream a crazed accountant? a frustrated developer?

"The concept that an IT environment can become so automated and abstracted from the underlying infrastructure that there is no need for a dedicated team to manage software in-house." TechTarget

The goal of completely automating the deployment, monitoring and management of applications and the infrastructure on which they run." - Forrester

Source
https://searchcloudapplications.techtarget.com/definition/noops

splunk> .conf19

Summary

Wrap-up

NewOps: Final Thoughts

NewOps = IT Ops for modern systems

- CloudOps, WebOps, MSAOps, AgileOps, DevOps, SREOps, AutoOps, DataOps, ObservableOps, MLOps, AIOps, CXUXOps, ChatOps, CoffeeOps, BeerOps, HugOps … is that all???

- *AND* TradOps – legacy does not magically go away!

Key Takeaway: 4 core aspects of NewOps

- **Data-driven** insight into every service and issue

- **Collaborative** culture using integrated platforms

- **Business-Aligned** across full end-to-end service

- **Automated workflows** for mundane and complex

splunk> .conf19

Q&A

Andi Mann | Chief Technology Advocate
Endre Peterfi | Sales Engineer

splunk> .conf19