

Data Analytics for DevOps and Cloud Transformation

SCITDA Leaders' Workshop
March, 2018

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



About Your Facilitator

Andi Mann – Chief Technology Advocate, Splunk

Global experience as a strategist, technologist, innovator, and communicator with Fortune 500 corporations, software vendors, governments, and as a leading research analyst and consultant. Business and technology commentator appearing in *USA Today*, *New York Times*, *SkyTV*, *Forbes*, *CIO*, *InformationWeek*, *Wall Street Journal*, and more.

Named to many 'Top ...' lists including Business Insider's [Top Thought-Provoking Enterprise Tech Execs](#), Apollo Research's [Top Technology Specialists on Twitter](#), Heller Search's [Top Recommended Twitter Accounts for IT Execs](#), Robert Half Technology's [Top 20 People Most Mentioned by IT Leaders](#), Huffington Post's [Top 100 Cloud Computing Experts](#), Gathering Clouds [Top 5 Cloud Experts - Who's Who in Cloud](#), and SAP's [Top 50 Cloud Computing Influencers](#).

Published author of two books - '[Visible Ops – Private Cloud](#)'; and '[The Innovative CIO](#)'; blogger at '[Andi Mann – Übergeek](#)'; tweets as [@AndiMann](#)



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.

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. © 2018 Splunk Inc. All rights reserved.

Agenda

- ▶ **Cloud and DevOps** – common elements that enable cloud and DevOps as transformative approaches
- ▶ **Metrics that Matter** – measuring cloud and DevOps for visibility into shared goals and success
- ▶ **Analytics from planning to release** – data to transform CI/CD pipelines from planning to release
- ▶ **Analytics from release to support** – data to transform monitoring, troubleshooting, & post-incident reviews
- ▶ **Analytics for constituent insights** – analyzing end user/constituent interaction for agile feedback loops
- ▶ **Analytics for service intelligence** – cross-platform data for deep insight into end-to-end constituent services
- ▶ **Analytics for breach detection** – insight into exposures, data breaches, and unauthorized user behaviors
- ▶ **Measuring ‘the new stack’** – incl. Site Reliability Engineering’ semantic logging, telemetry, observability
- ▶ **Advanced analytics** – techniques incl. machine learning, anomaly detection, and predictive analytics
- ▶ **Data-driven automation** – coupling data with automation for actionable decisions and remediation
- ▶ **Q&A, Wrap-up**

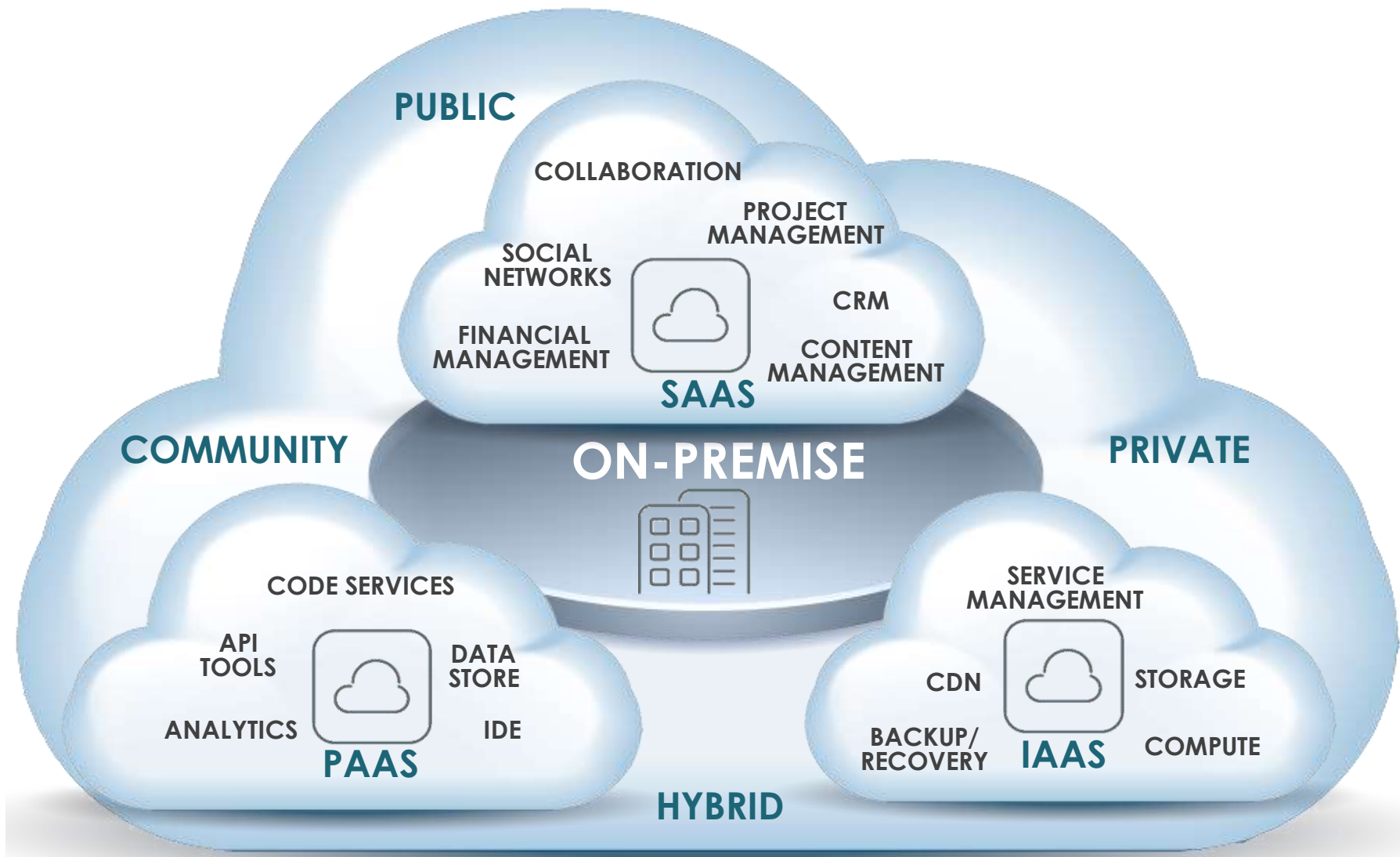
... with stories in data, analytics, and transformation from Splunk, our customers, and others in the public sector



Cloud and DevOps -

the common elements of people, process, and technology that enable cloud and DevOps as transformative approaches

Cloud Services Accelerate App Delivery Velocity



138.68.4... [07/Jan 18:10:57:153] "GET /category.screen?category_id=GLYTS&SESSIONID=5D15LAF118ADFF10 HTTP 1.1" 404 728 "http://buttercup-shopping.com/cart.do?action=view&item_id=EST-68&product_id=P1-0W-01-38&product_id=P1-0W-01-38" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:55.0) Gecko/20100826 Firefox/55.0"

Defining DevOps

METHODS FOR IMPROVING

COLLABORATION



COMMUNICATION

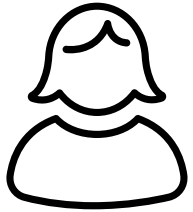


INTEGRATION

**BETWEEN DEV AND OPS
TO DELIVER BETTER SOFTWARE, FASTER**



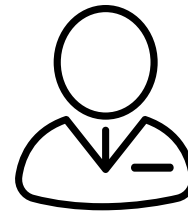
DevOps Accelerates App Delivery Velocity



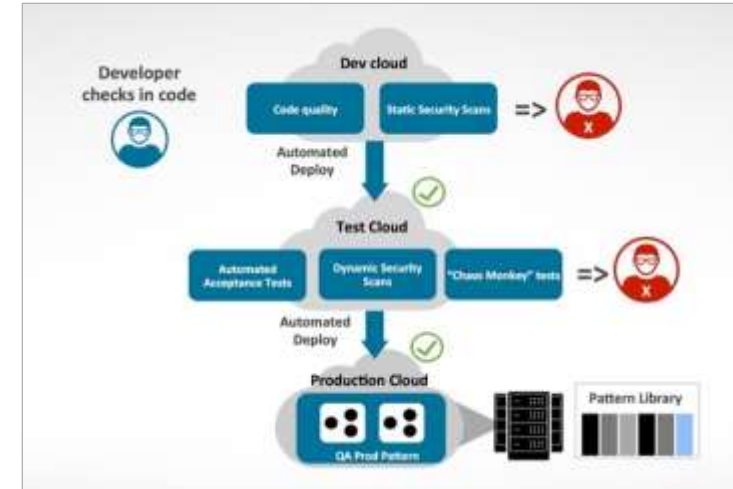
Product Managers
identify new opportunities



Code continuously delivered to market



Auditors
have visibility

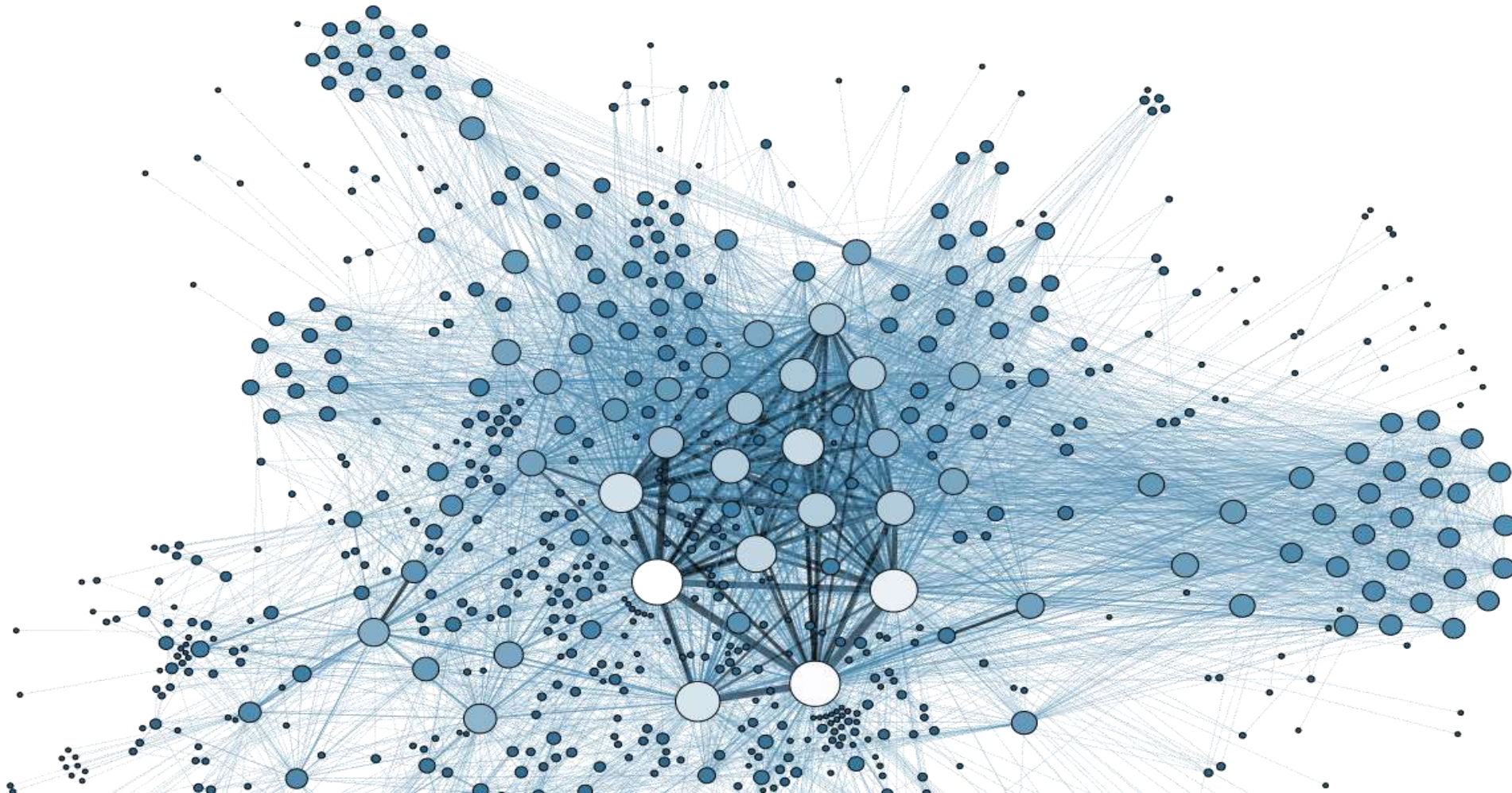


DevOps Teams iterate with **continuous insights**



Customers
are happy

Virtualization, Cloud, DevOps, Containers, MSAs, Serverless/FaaS, APIs are Disintegrating Monoliths



138.60.4 -- [07/Jan 18:10:57:153] "GET /category.screen?category_id=G1VTS&SESSIONID=SD15LAF18ADFF19 HTTP 1.1" 404 728 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI_0W_01 -> Max 1.7.8 0 1000000 20
128.241.220.82 -- [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD55L7FFGADFF9 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-2&product_id=FI_0W_01 -> Max 1.7.8 0 1000000 20
ows NY 5.1: SVI: -- [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD55L7FFGADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-2&product_id=FI_0W_01 -> Max 1.7.8 0 1000000 20
/buttercup-shopping_id=RP-LI-02" 468 125.17.14.14 "GET /oldlink?item_id=EST-268&SESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 55:387] "GET /category.screen?category_id=FLOWERS&SESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-2&product_id=FI_0W_01 -> Max 1.7.8 0 1000000 20
/buttercup-shopping_id=RP-LI-02" 468 125.17.14.14 "GET /category.screen?category_id=FLOWERS&SESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 55:387] "GET /category.screen?category_id=FLOWERS&SESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-2&product_id=FI_0W_01 -> Max 1.7.8 0 1000000 20
/buttercup-shopping_id=RP-LI-02" 468 125.17.14.14 "GET /category.screen?category_id=FLOWERS&SESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 55:387] "GET /category.screen?category_id=FLOWERS&SESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-2&product_id=FI_0W_01 -> Max 1.7.8 0 1000000 20

CAMS – as close to prescriptive as DevOps gets



Culture
Automation
Measurement
Sharing

```

... 200.0.0 - [07/Jan 18:10:57:153] "GET /category.screen?category_id=61VT5&JSESSIONID=5D15LAF1B0ADFF10 HTTP/1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-0&product_id=FI_0W_01"
itemId=EST-5V1: - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI_0W_01"
... [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI_0W_01"
... [07/Jan 18:10:56:156] "GET /oldLink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 200 125.17.14.189 "GET /cart.do?action=changequantity&itemId=EST-1&product_id=AV-CM-01&JSESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 200 300 "http://buttercup-shopping.com/oldLink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 200 125.17.14.189 "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 200 125.17.14.189 "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 200 125.17.14.189 "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 200 125.17.14.189 "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 200 125.17.14.189 "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 200 125.17.14.189
  
```

Metrics that Matter

what to measure in cloud and DevOps (across people, process, and technology) to provide shared goals and measures of success for transformation

WHAT DATA DRIVES GOOD DECISIONS?

10+ Deploys Per Day: Dev and Ops Cooperation at **flickr**

John Allspaw & Paul Hammond
Velocity 2009

Activity Data

I'm working
super hard!!

That's my
stapler!

Outcome Data

Yeah, but ...
... what are
you achieving?

I'm gonna
need you to
come in
Sunday.

Sales?

Downloads?

Installs?

Users?

What activities?
What outcomes?

Gartner's DevOps 'Metrics that Matter'



IDC's DevOps 'Metrics that Matter'

Q. What business outcomes do you expect DevOps practices to deliver?

	% of Respondents
Improved customer experience	67
Lower IT costs	61
Improved employee productivity	44
Higher profits	39
Improved IT employee satisfaction	39
Faster/increased revenue growth	33
Improved security and risk mitigation	33
Improved career development	28
Higher service availability	22
Improved EPS	11

n = 18

Note: Multiple responses were allowed.

Source: IDC's DevOps Best Practice Metrics: Fortune 1000 Survey, December 2014

Forrester's DevOps 'Metrics that Matter'

Velocity

- Business - release freq., time/cost per release, mean-time-to-change, mean-time-to-detection
- DevOps team - release/deploy automation %, mean-time-to-detection, mean-time-to-approval

Quality

- Business - MTTR, Customer experience
- DevOps team - Deployment failures, incident severities (by team, application, process, asset)

Efficiency

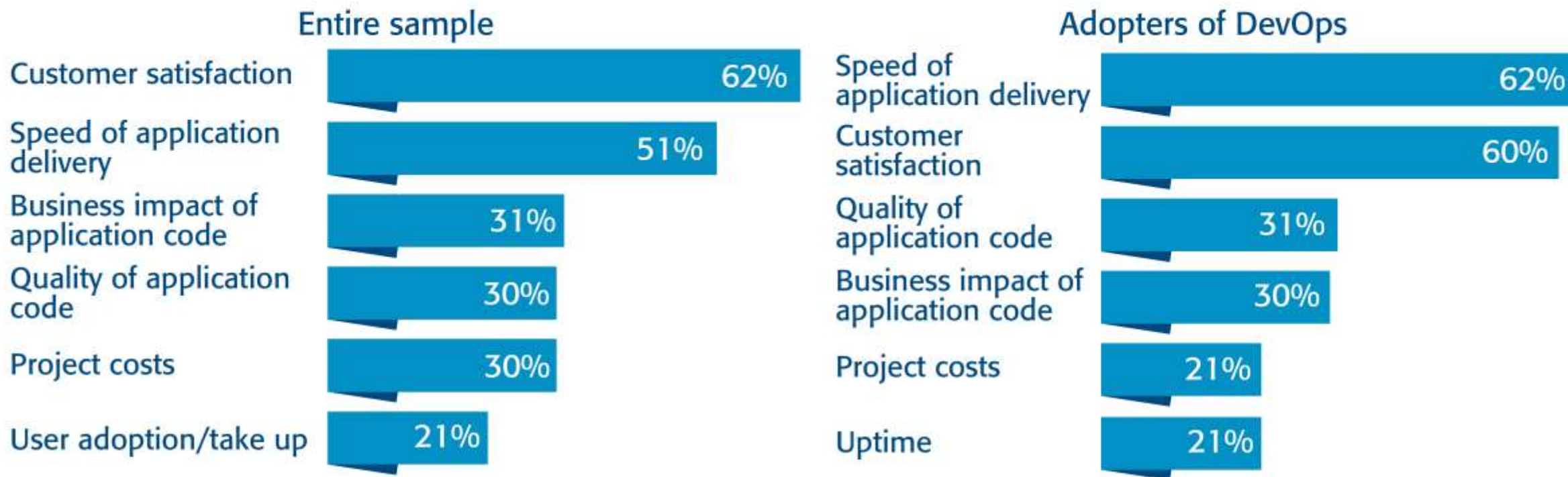
- Business - Unplanned work, happiness of CX team with technology delivery
- DevOps team - Deployment frequency/duration, Incident severity, average provisioning time

Culture

- Business - Happiness with product team, DevOps team attrition, DevOps meeting frequency
- DevOps team - Rework rate, unplanned work, satisfaction, attrition, postmortem count

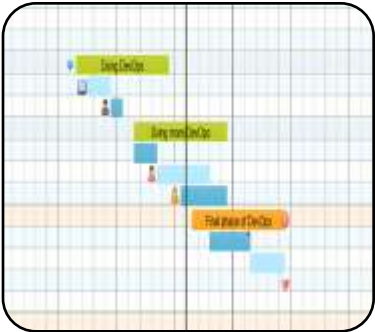
Computing UK's 'Metrics that Matter'

FIG. 5 Which metrics would be most useful in order to measure success of a DevOps implementation?



Source: Computing Research UK, *DevOps Review 2016: Accelerating Innovation*, July 2016

More Ideas for 'Metrics that Matter'



Culture
e.g.
• Retention
• Satisfaction
• Callouts

Process
e.g.
• Idea-to-cash
• MTTR
• Deliver time

Quality
e.g.
• Test pass
• Test fail
• Best/worst

Systems
e.g.
• Throughput
• Uptime
• Build times

Activity
e.g.
• Commits
• Tests run
• Releases

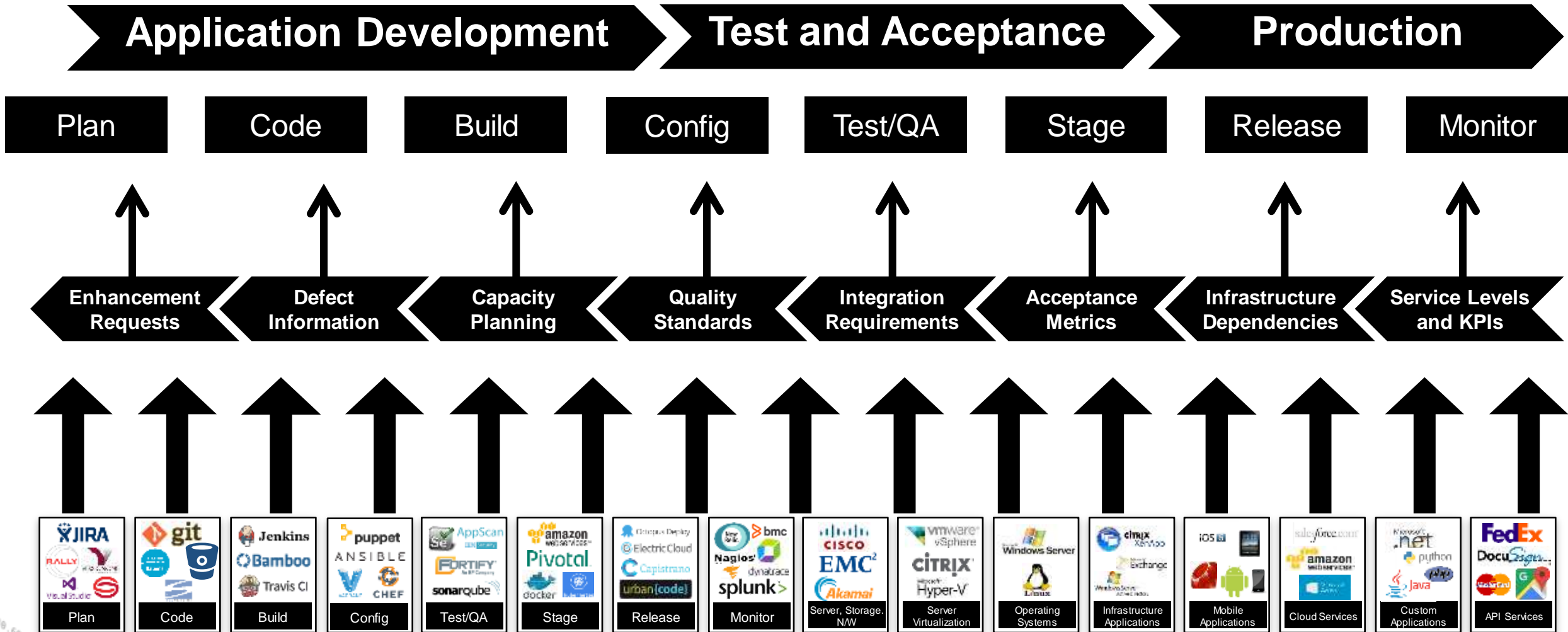
Impact
e.g.
• Signups
• Checkouts
• Turnaround

138.68.4
128.241.220.82 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=61VTS&JSESSIONID=5D15LAF18ADFF10 HTTP 1.1" 404 728 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-06&product_id=PI-06-03 -> http://buttercup-shopping.com/category.screen?category_id=61VTS" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6; rv:52.0) Gecko/20100801 Firefox/52.0
ows NY 27.168.0.0 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CN-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=registerClient&itemId=EST-26&product_id=PI-06-03" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6; rv:52.0) Gecko/20100801 Firefox/52.0
//buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" 468 125.17.14.189 "GET /cart.do?action=changequantity&itemId=EST-06&product_id=PI-06-03" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6; rv:52.0) Gecko/20100801 Firefox/52.0
//buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" 468 125.17.14.189 "GET /category.screen?category_id=61VTS&JSESSIONID=5D15LAF18ADFF10 HTTP 1.1" 404 728 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-06&product_id=PI-06-03 -> http://buttercup-shopping.com/category.screen?category_id=61VTS" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6; rv:52.0) Gecko/20100801 Firefox/52.0

Analytics from planning to release

using data to transform CI/CD pipelines from planning, to code and build, testing, configuration, and release

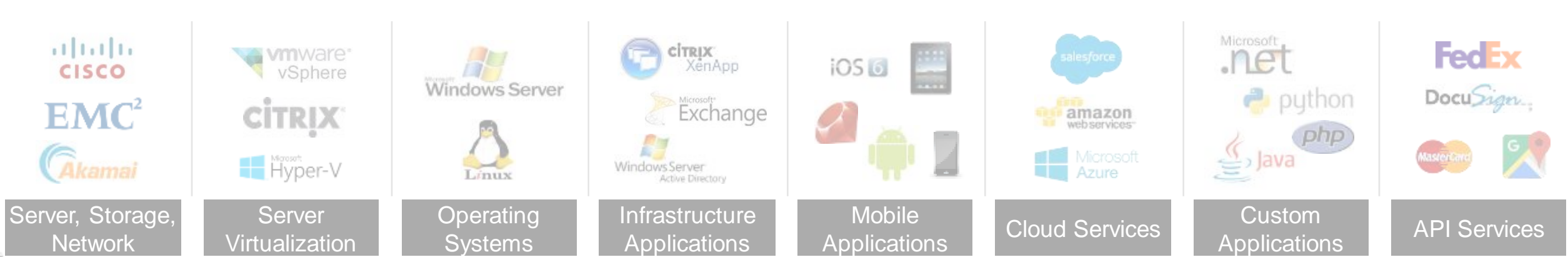
Feedback Loops Enable Continuous Improvement



Getting Visibility Across Dev and Ops



Common Data Platform – Collect, Analyze, Visualize, Share



Metrics for Resource Analytics

Insight and prediction for effective resource allocation

► Key Metrics:

- Work time vs. PTO/sick
- Hours by product/project
- Resource shortages

► Data Sources:

- Jira
- WorkDay



Metrics for Cost Analytics

Measurement and predictability for cost control

► Key Metrics:

- Productive hours
- Labor costs
- Plan vs. actual

► Data Sources:

- WorkDay
- PeopleSoft



Metrics for DevTeam Analytics

Insight to coder activity for teaming & work/life balance

▶ Key Metrics:

- Commit count
- Commits by author
- Commit days/times

▶ Data Sources:

- GitHub



Metrics for Code Analytics

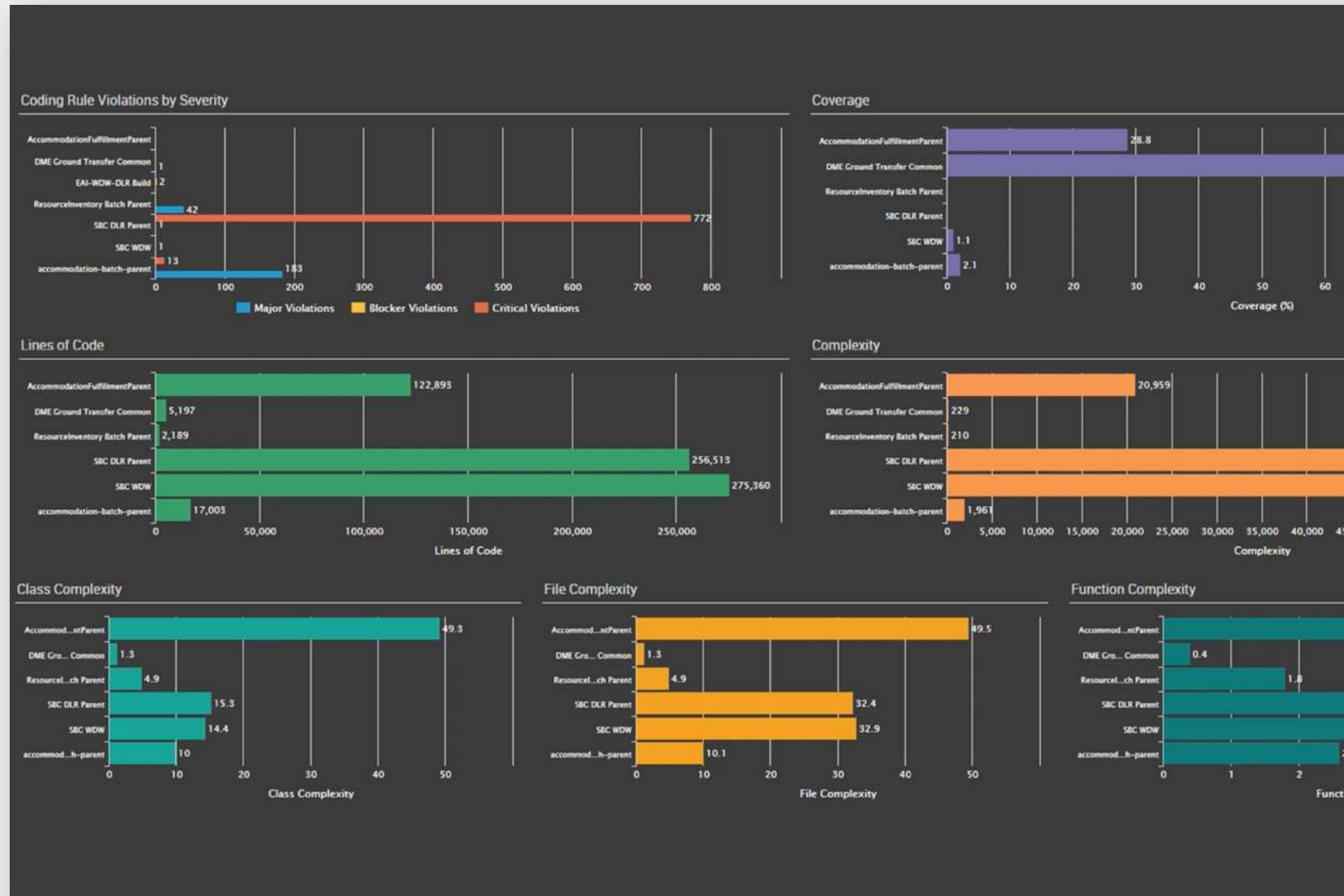
Real-time data on code quality and compliance

Key Metrics:

- Code policy compliance
- Code/file/class complexity
- Code analysis coverage

Data Sources:

- GitHub
- Sonarcube



Metrics for Build Analytics

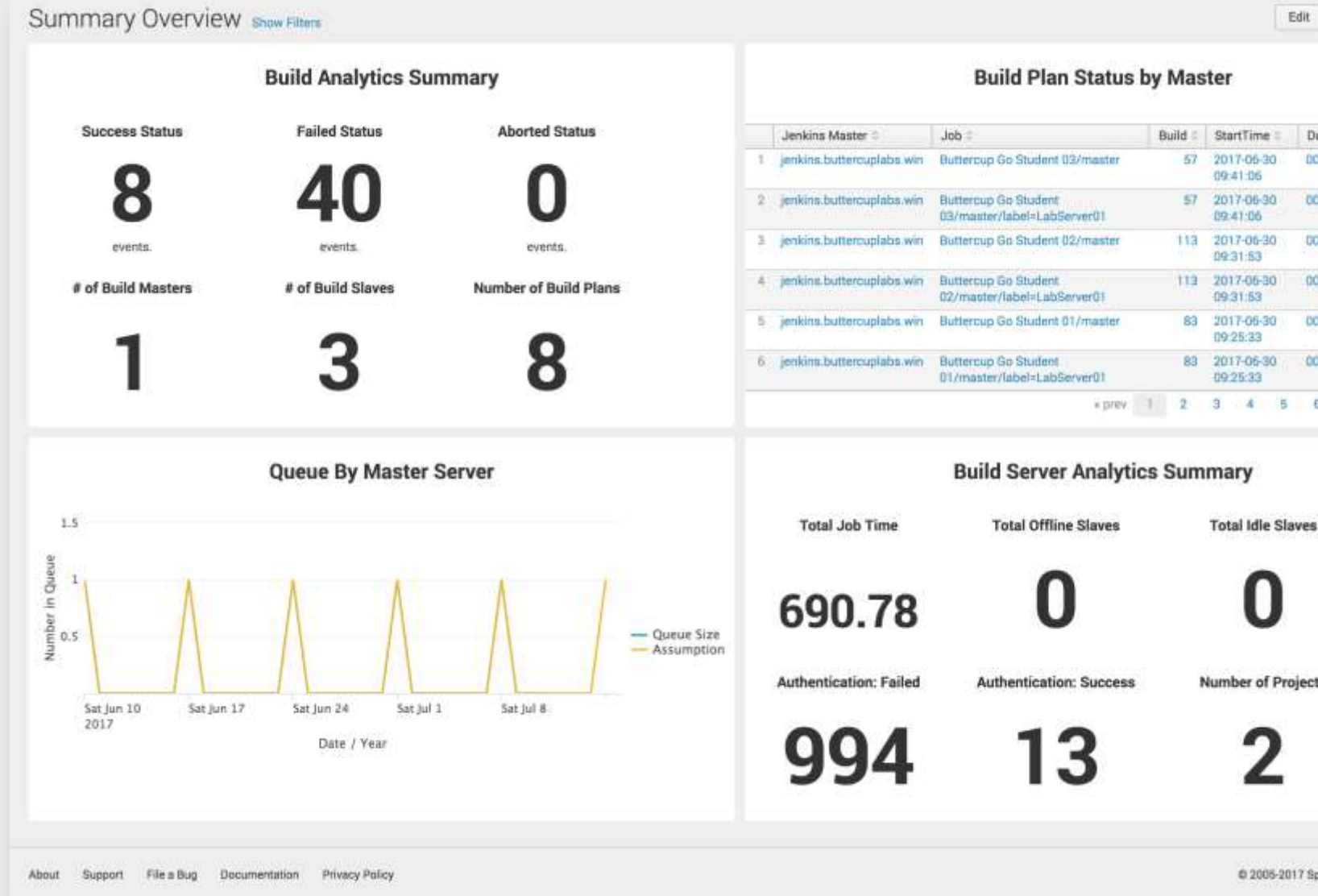
Find and fix build issues to accelerate product lifecycle

► Key Metrics:

- Build success/failure
- Build queue status
- Build process times

► Data Sources:

- Jenkins
- Sonarcube



Metrics for Quality Analytics

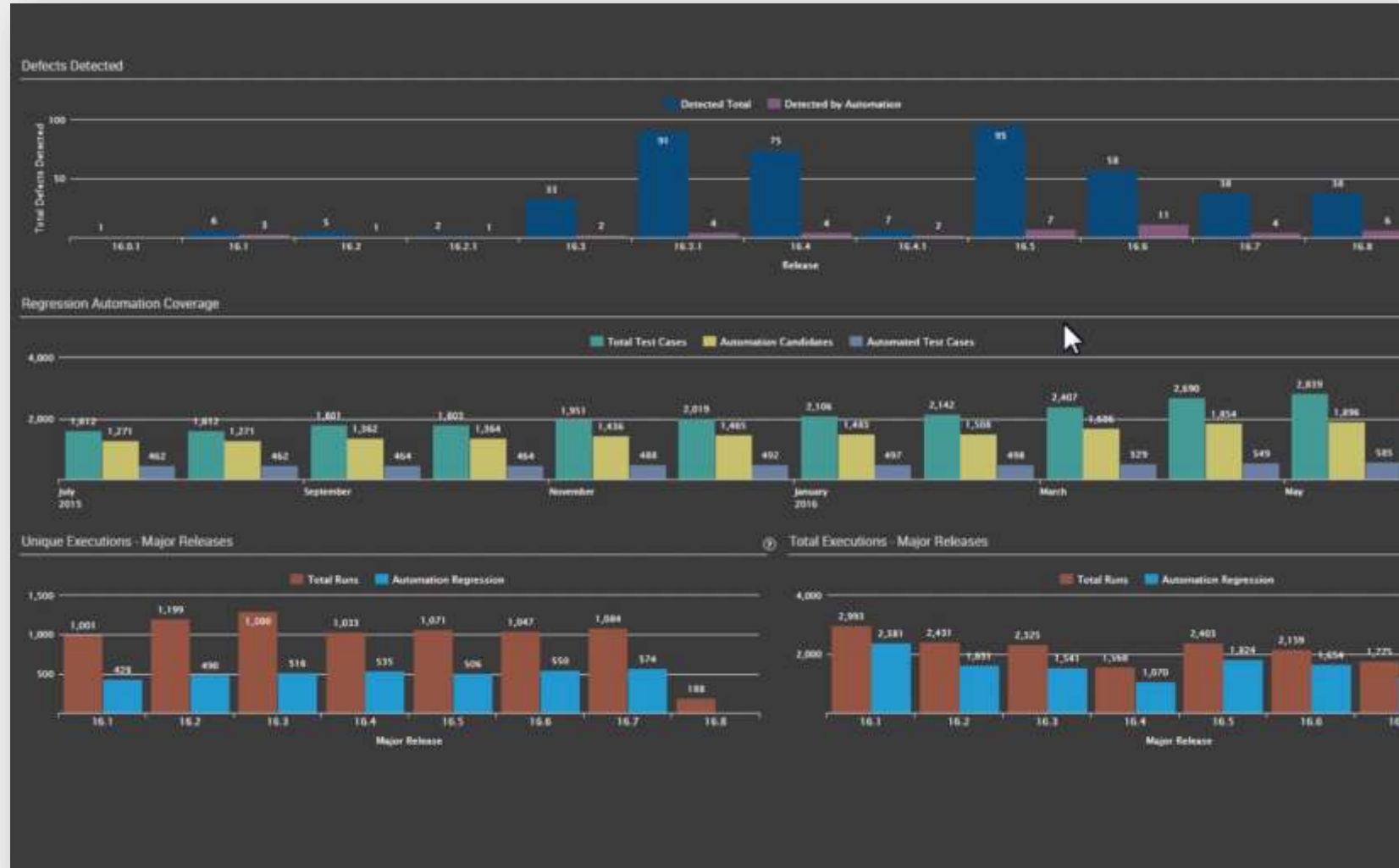
Automatically review QA results to improve quality

▶ Key Metrics:

- Defects detected
- Test coverage
- Test executions

▶ Data Sources:

- Selenium
- AppScan
- ServiceNow



Metrics for Config Analytics

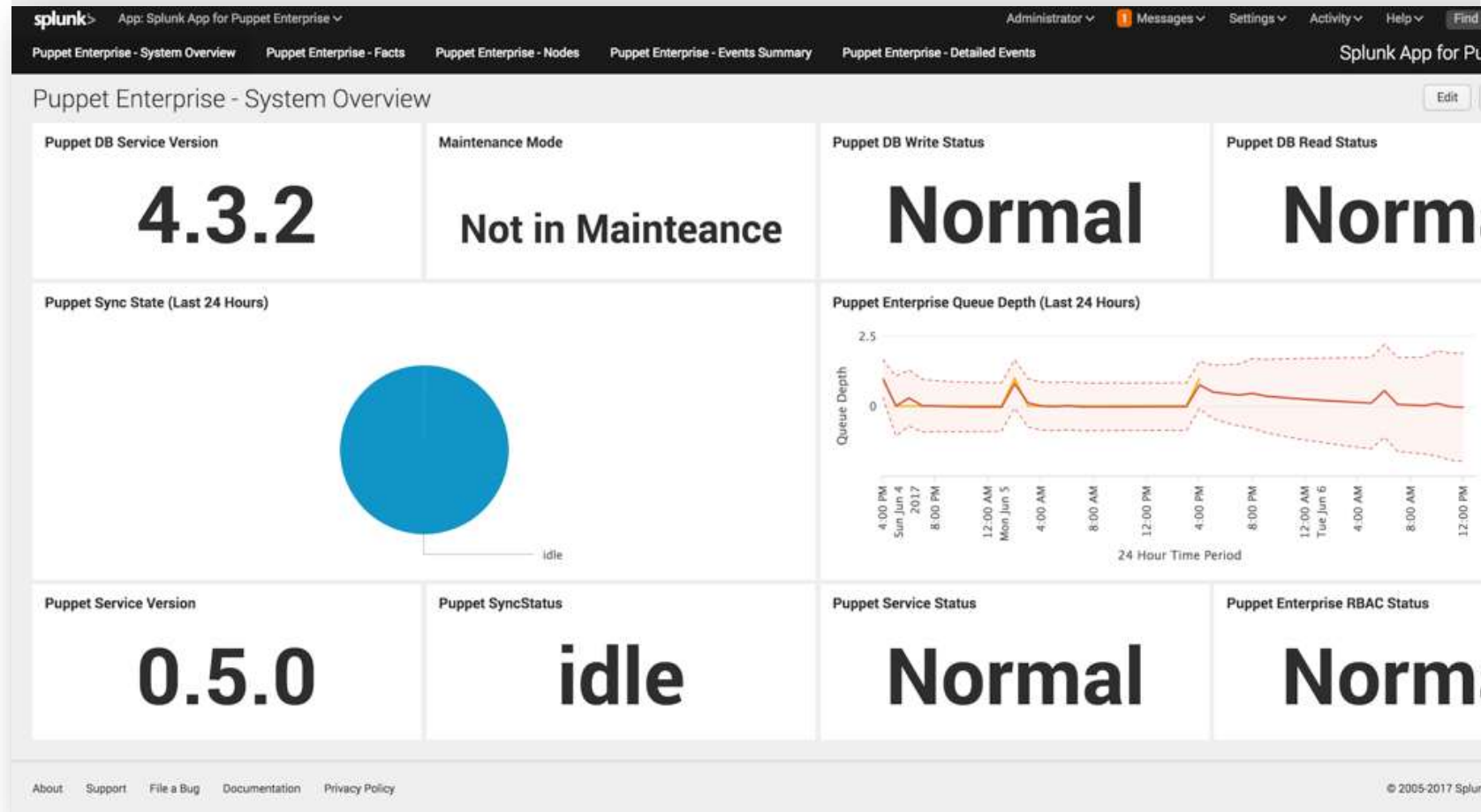
Monitor provisioning/config to accelerate time to 'done'

▶ Key Metrics:

- Provisioning success/failure
- Provisioning times
- Config drift by node

▶ Data Sources:

- Puppet



Metrics for Release Analytics

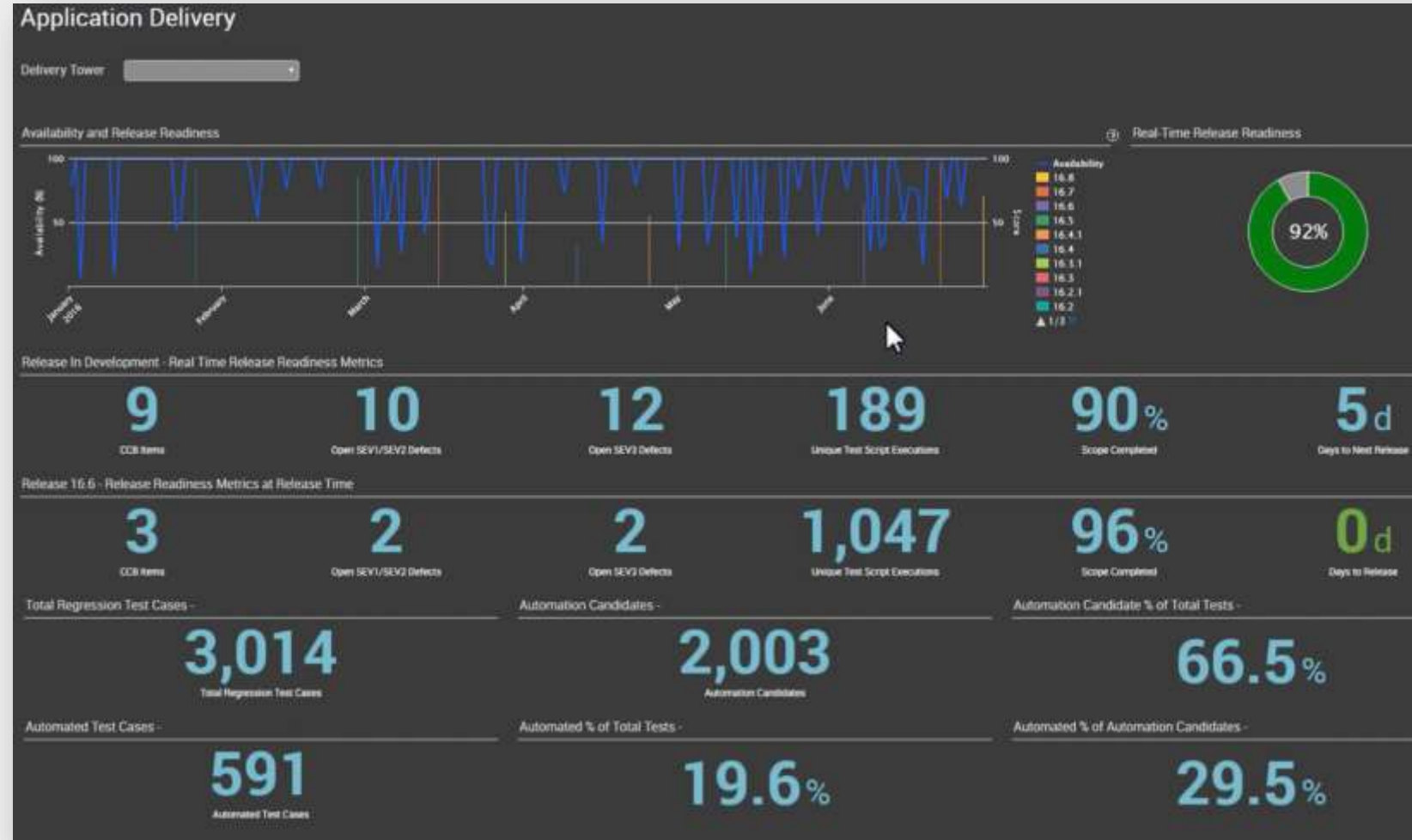
Real-time data for better, faster release decisions

► Key Metrics:

- Availability by release
- Tickets by release
- Release readiness

► Data Sources:

- ServiceNow
- SonarCube
- HP OpenView



MEDIA & ENTERTAINMENT – APPLICATION DELIVERY

Improved DevOps Agility



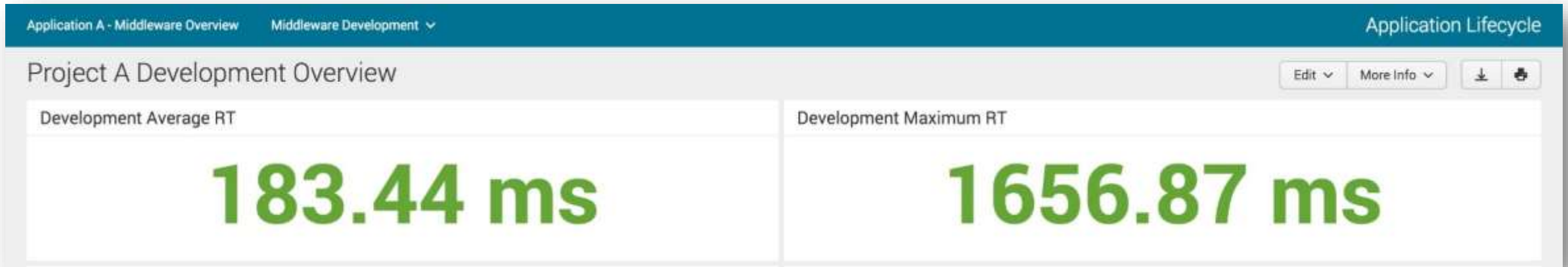
“It’s like we were working without peripheral vision before and now we have it.”
– Robert Gonsalves, Web Operations

► Key Customer Benefits

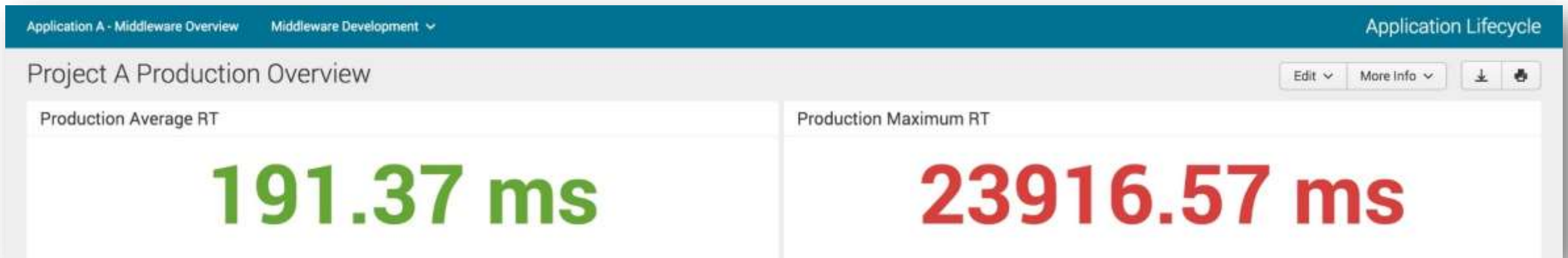
- Increased success rate of deployments
- Ability to detect issues before they affect broad production
- Monitoring deployment process several times per day

Use Live Data to Better Prepare For Release

Compare the release in dev, staging, pre-prod ...



With the release currently in production



Analytics Across the End-to-End Software Pipeline



Don't Forget to Measure Cultural Change

- ▶ e.g.
 - Absenteeism
 - 'Work from home'
 - Staff attrition and retention
 - eNPS
 - Employee 'happiness'



Image source: [@danslimmon](https://twitter.com/danslimmon/status/806156237926780928) - <https://twitter.com/danslimmon/status/806156237926780928>

FamilySearch Moves to Continuous Delivery and Gains Real-Time Visibility



“Splunk Cloud has been more stable than our internal implementation and has freed up two resources to work on software development instead of managing infrastructure. It has clearly proven to be cost-effective compared to managing infrastructure ourselves.”

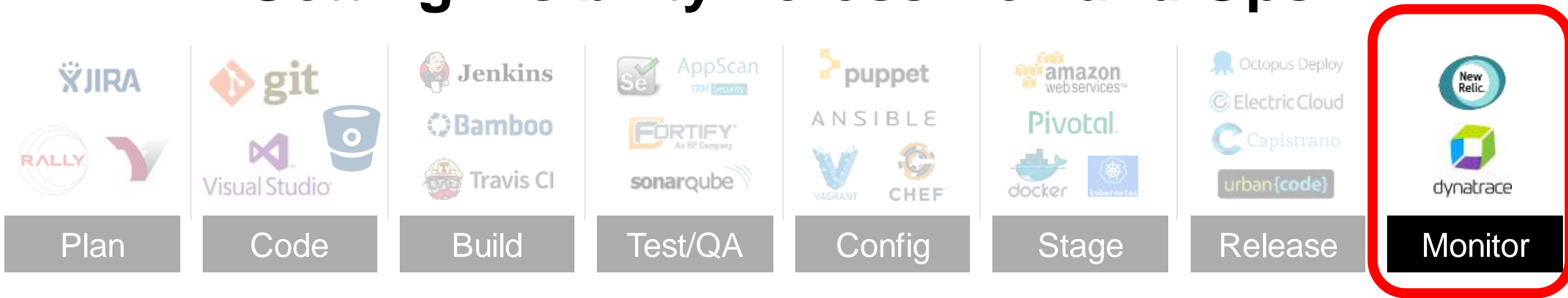
– *Director of Engineering, FamilySearch*

- ▶ Successful migration from monthly releases to over 900 deploys per day
- ▶ Ability to re-allocate 12 developers to more value-added tasks
- ▶ Visibility into the AWS environment to support AWS migration strategy

Analytics from release to post-mortem

using data to transform event management, problem analysis, troubleshooting, and post-incident reviews

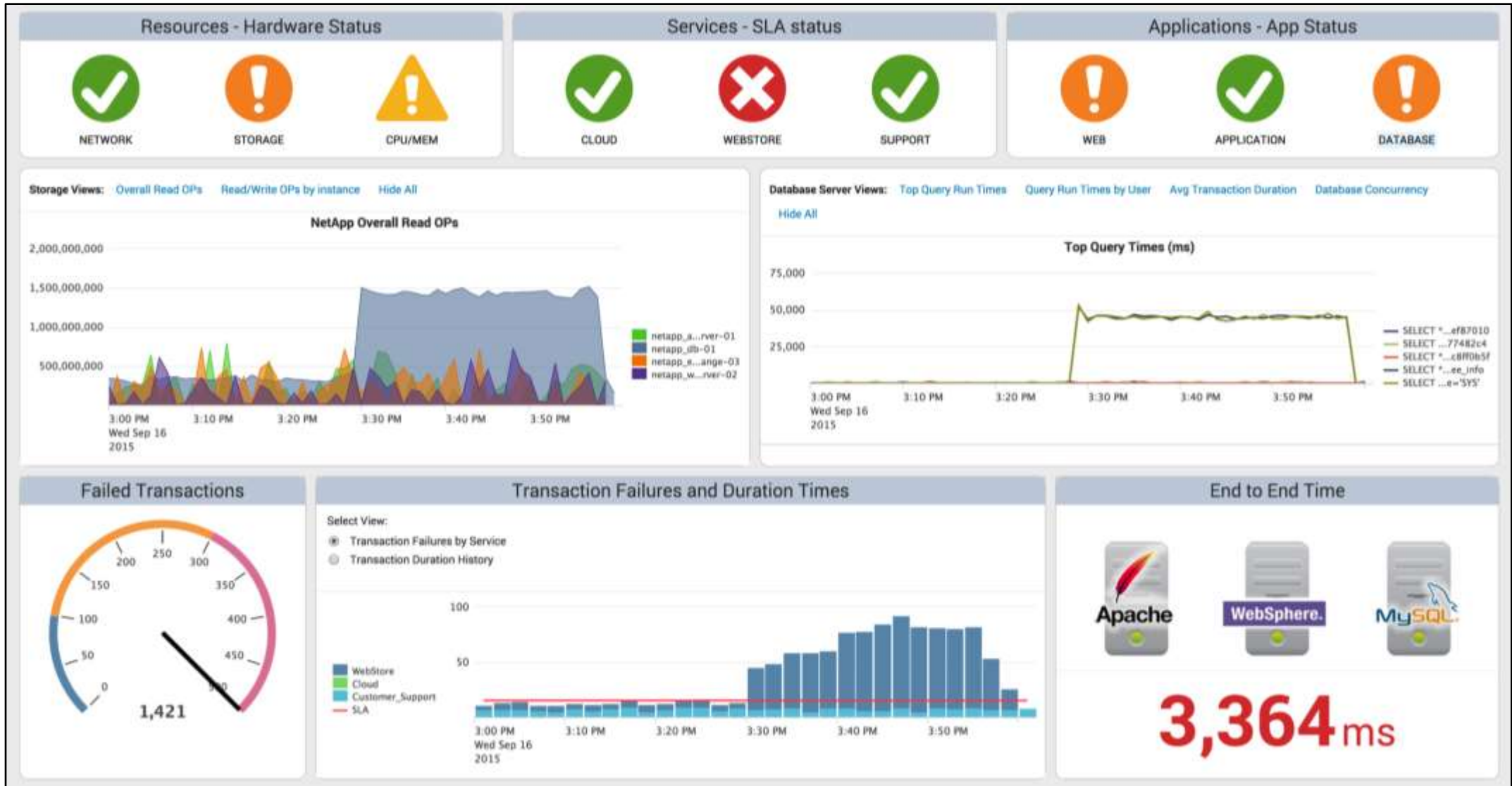
Getting Visibility Across Dev and Ops



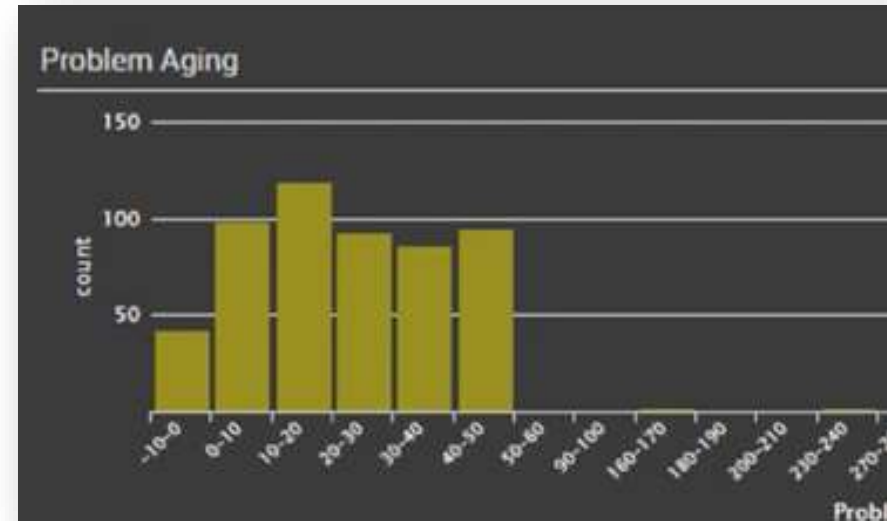
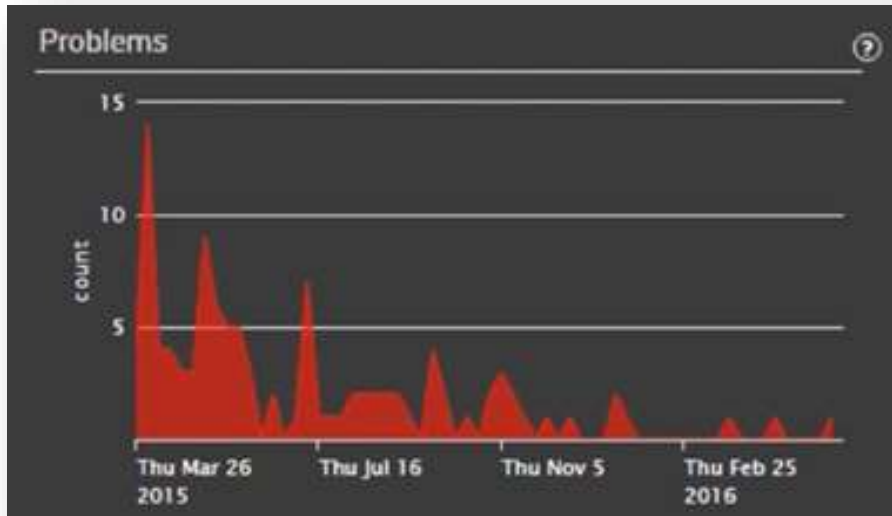
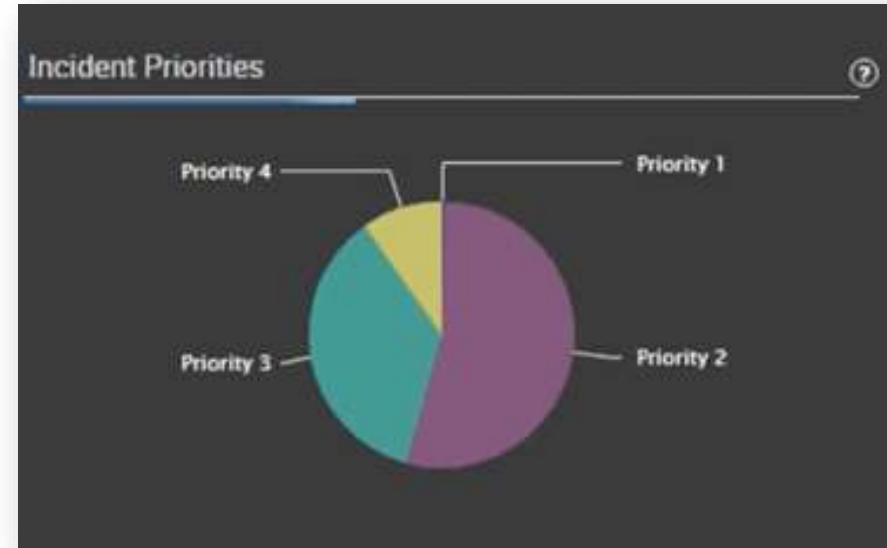
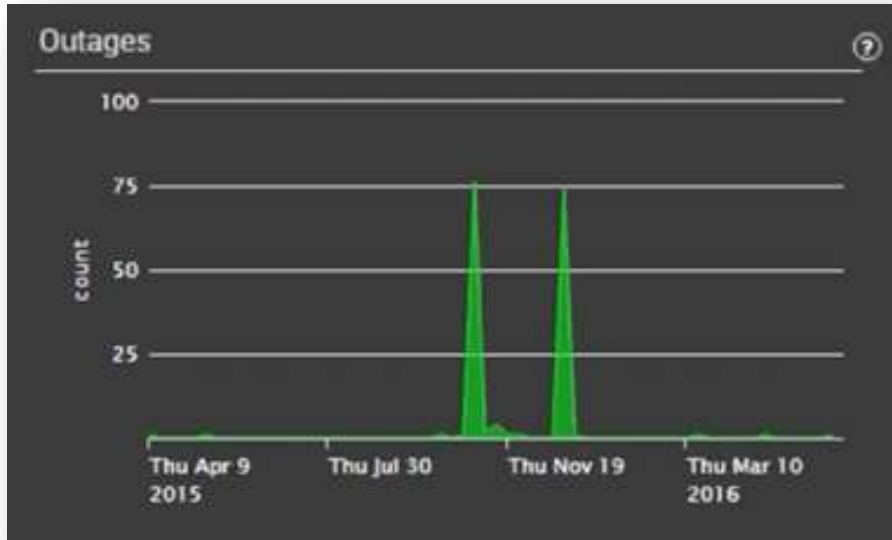
Common Data Platform – Collect, Analyze, Visualize, Share



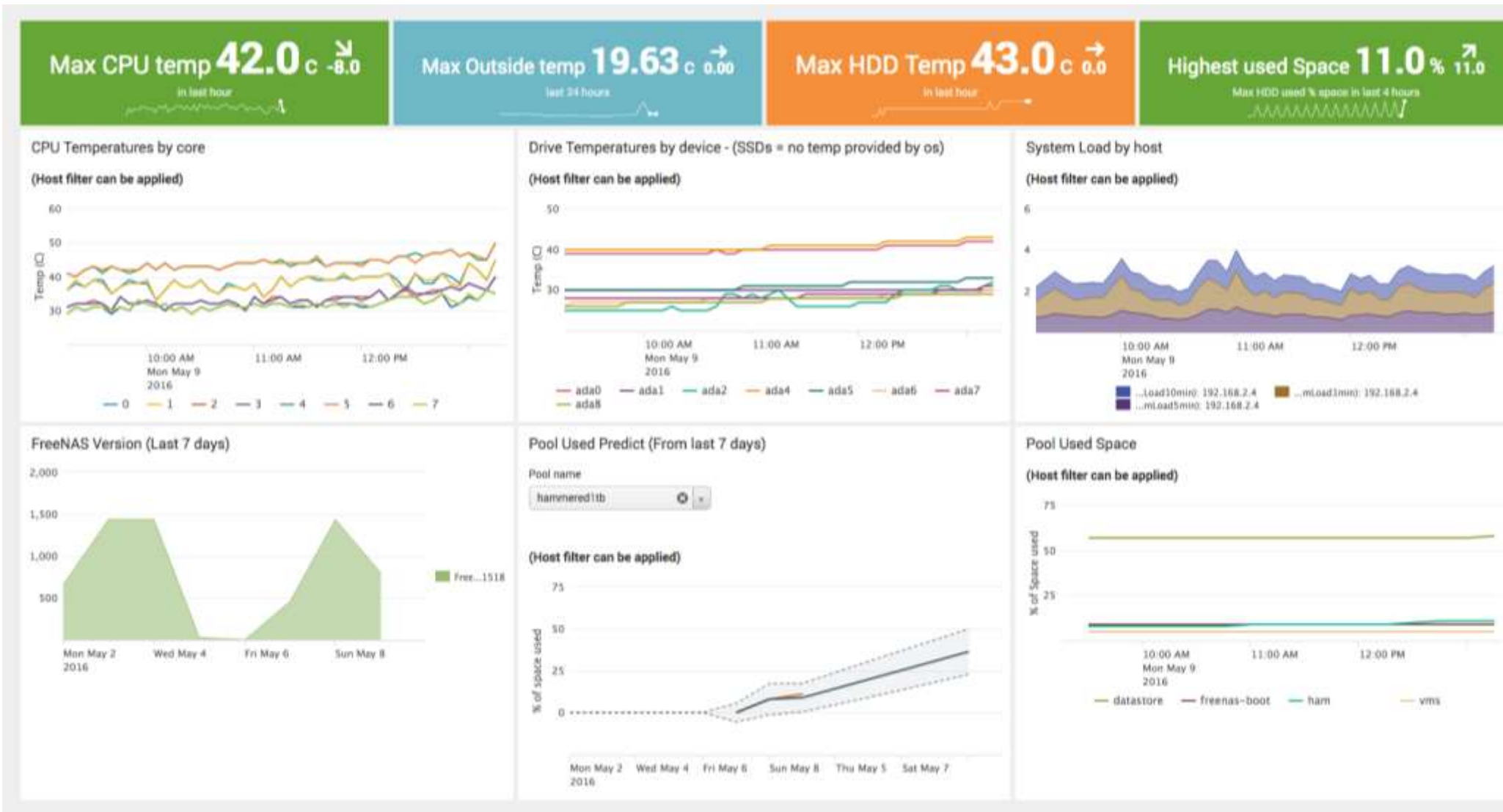
Data-driven Feedback Drives Continuous Improvement



Get Visibility into Ops Status and Incidents



Analytics to Ensure Infrastructure Health



Analytics for Visibility into Storage and Capacity



VMAX Virtual Free Capacity

26.85 TB

VMAX Virtual Used Capacity

3.90 TB

VMAX Virtual Total Capacity

30.75 TB

Storage Group Compliance: Stable

26

Storage Group Compliance: Marginal

0

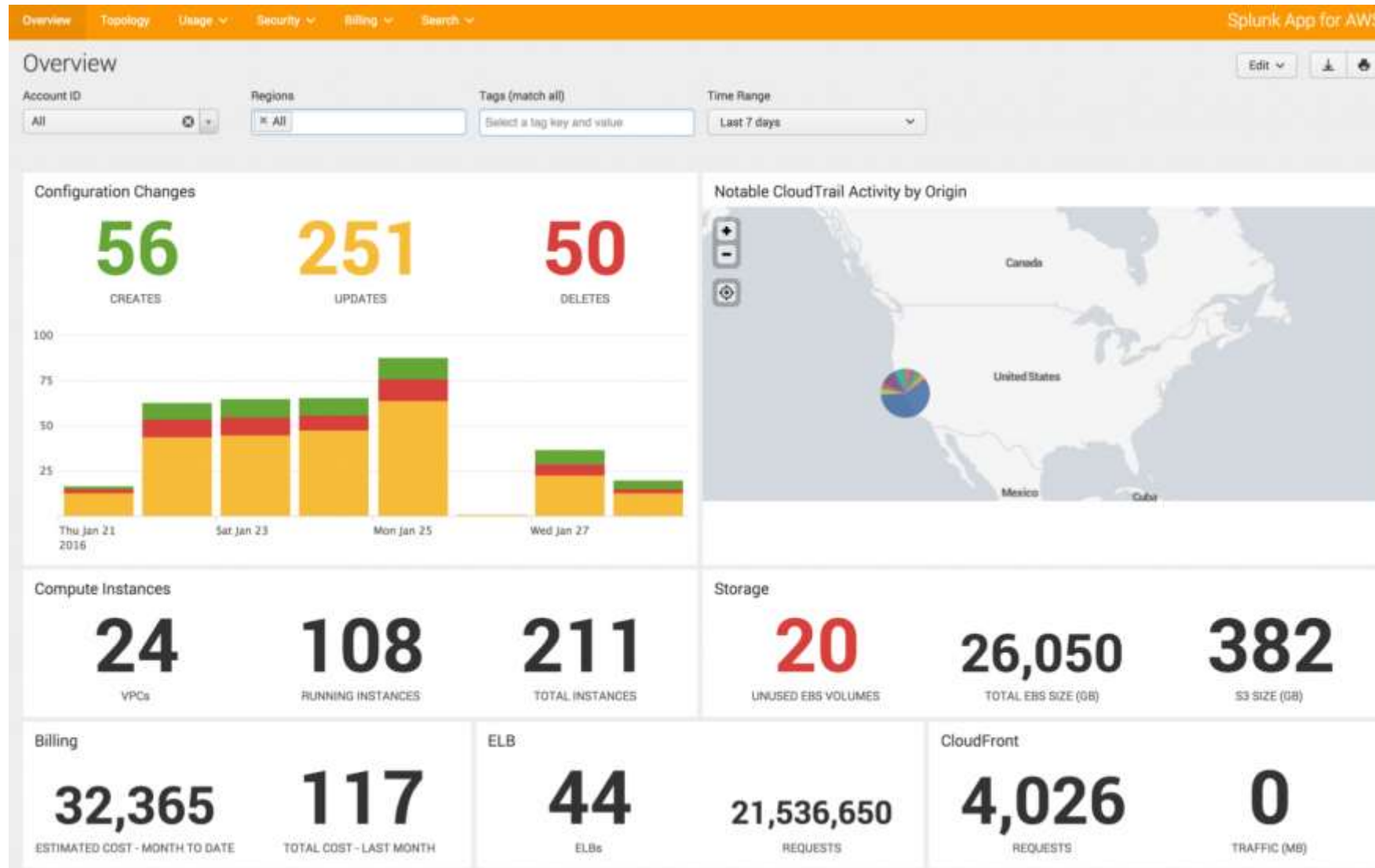
Storage Group Compliance: Critical

0

VMAX Storage Arrays

VMAX	Model	uCode	# Devices	Free Capacity (TB)	Used Capacity (TB)	Total Capacity (TB)	Overall Compression Ratio	Overall Efficiency Ratio
000207900050	VMAX250E	5077 025 002	000	5.44	25.30	30.74	1.0	1.0

Analytics to Manage Cloud Resources



Source Data for Containers and MSAs

Data Type	Where to Find It	What It Can Tell You
Container and microservices logs	Logs can be ingested via any native Docker logging driver such as syslog, Splunk, JournalD and via Cloud integrations (e.g., Amazon CloudWatch, Google Cloud Platform Logging Export)	Container and application errors. Monitor any performance counters that can be calculated on top of logs (e.g., web and application server logs)
Container metrics and events	Docker APIs (e.g., Docker inspect, Docker top, Docker stats, Docker events), cloud APIs (e.g., AWS CloudWatch, Google Stackdriver)	Health, performance, availability and events generated by all monitored containers
Container clusters, nodes and applications	Docker UCP APIs and logs from containers	Application health, nodes, clusters and containers associated with an application, change history of containers and configuration
Application logs	Custom logs set by application developers	Application errors and other valuable machine data logged by developers
Wire data	Wire data probes (software based)	Communication between an app component, application response times and payload of applications as they traverse your network (even when you may not have direct visibility to some app components)



Maryland's Prince George's County Mission-Ready With Splunk

“Splunk is a platform for Operational Intelligence for Prince George's County. With Splunk, we're able to have greater visibility across functional teams, to identify trends and potential problems in advance and to resolve issues more quickly by seeing a broader view of the problem.”

— *Enterprise Architect, Prince George's County OIT*

- ▶ Improved government efficiency and transparency to better serve constituents
- ▶ Helped small IT team reduce time to identify and resolve IT issues from days or weeks to hours
- ▶ Transformed county operations by replacing data silos with a platform for IT operations, application monitoring and security

Analytics for constituent insights

collecting and analyzing end user activity and constituent interaction data to establish agile feedback loops to IT

Data Tells a Story

Sources

Order Processing



Middleware Error



Care IVR



Twitter



ORDER,2014-05-21T14:04:12.484,10098213,569281734,67.17.10.12,43CD1A7B8322,SA-2100

May 21 14:04:12.996 wl-01.acme.com Order 569281734 failed for customer 10098213. Exception follows: weblog.jdbc.extensions.ConnectionDeadSQLException: weblog.common.resourcepool.ResourceDeadException: Could not create pool connection. The DBMS driver exception was: [BEA][Oracle JDBC Driver]Error establishing socket to host and port: ACMEDB-01:1521. Reason: Connection refused

05/21 16:33:11.238 [CONNEVENT] Ext 1207130 (0192033): Event 20111, CTI Num:ServID:Type 0:19:9, App 0, ANI T7998#1, DNIS 5555685981, SerID 40489a07-7f6e-4251-801a-13ae51a6d092, Trunk T451.16
05/21 16:33:11.242 [SCREENPOPEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092 CUSTID 10098213
05/21 16:37:49.732 [DISCEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092

{actor:{displayName:"Go Boys!!",followersCount:1366,friendsCount:789,link:"http://dallascowboys.com/",location:{displayName:"Dallas, TX",objectType:"place"},objectType:"person",preferredUsername:"B0ysF@n80",statusesCount:6072},body:"Can't buy this device from @ACME. Site doesn't work! Called, gave up on waiting for them to answer! RT if you hate @ACME!!",objectType:"activity",postedTime:"2014-05-21T16:39:40.647-0600"}

Data Tells a Story

Sources

Order Processing



Middleware Error



Care IVR



Twitter



```

ORDER,2014-05-21T14:04:12.484, Customer ID 10098213, Order ID 569281734, 67.17.10.12,43CD1A7B8322, Product ID SA-2100
May 21 14:04:12.996 wl-01.acme.com Order Order ID 569281734 failed for customer Customer ID 10098213.
Exception follows: weblogic.jdbc.extensions.ConnectionDeadSQLException:
weblogic.common.resourcepool.ResourceDeadException: Order ID Could not create pool Customer ID The
DBMS driver exception was: [BEA][Oracle JDBC Driver]Error establishing socket to host and port:
ACMEDB-01:1521. Reason: Connection refused

05/21 16:33:11.238 [CONNEVENT] Ext 1207130 (0192033): Event 20111, CTI Num:ServID:Type
Time Waiting On Hold 98#1, DNIS 5555685981, SerID 40489a07-7f6e-4251-801a-
13ae51a6d092, trunk 451.16
05/21 16:33:11.242 [SCREENPOPEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092
Customer ID CUSTID 10098213
05/21 16:37:49.732 [DISCEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092

{actor:{displayName:"Go Boys!!",followersCount:1366,friendsCount:789,link:
"http://dallascowboys.com/",location:{display:"Twitter ID Dallas, TX",objectType "Customer's Tweet
objectType:"person",preferredUsername:"B0ysF@n80",statusesCount:6072},body:"Can't buy
this device from @ACME. Site doesn't work! Called, gave up on waiting for them to answer! RT if
you hate @ACME!!",objectType:"activity",postedTime:"2014-05-21T16:39:40.647-0600"}
Company's Twitter ID

```

Metrics for Impact Analytics

Realtime business insight to drive impactful development

► Key Metrics:

- Revenue per min
- Checkout rate
- Cart fulfillment/abandon

► Data Sources:

- Web logs
- HTTP events
- SFA/CRM

Business Status (Medium)

Standard View ▾ 5



Store Status

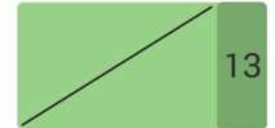
87.69

Health score

780.1

USD

Revenue per minute



Checkouts per minute
(Last 1 hour)



Website Component

409.4

USD

Revenue per minute



Checkouts per minute
(Last 1 hour)

Mobile Component

370.7

USD

Revenue per minute



Checkouts per minute
(Last 1 hour)



Going Deeper with Business Analytics



DIGITAL
MARKETING

insight across the complete web-based business process



CUSTOMER
EXPERIENCE

insight into end user experience, engagement, and behavior



PRODUCT
ANALYTICS

insight into product, service, or feature adoption, usage, and effectiveness



BUSINESS PROCESS
ANALYTICS

insights across the complete end-to-end business process

Constituent Experience Analytics – Data Sources

Data Type	Where to Find It	What It Can Tell You
Application Logs	Local log files, log4j, log4net, Weblogic, WebSphere, JBoss, .NET, PHP	User activity, fraud detection, application performance
Business Process Logs	Business process management logs	Customer activity across channels, purchases, account changes, process bottlenecks
Call Detail Records	Call detail records (CDRs), charging data records, event data records logged by telecoms and network switches	Billing, revenue assurance, customer assurance, partner settlements, bandwidth use
Clickstream Records	Web server, routers, proxy servers, ad servers	Usability analysis, digital marketing and customer journey
Mobile Application Data	SDKs embedded in mobile apps, application and server application logs	Mobile app usage, mobile app crashes, performance, latency, troubleshooting (stack trace) intelligence
Web Access Logs	Web access logs report every request processed by a web server	Web analytics reports for marketing
Web Proxy Logs	Web proxies log every web request made by users through the proxy	Terms of service and data leakage incidents
Wire Data	DNS lookups and records, protocol level information including headers, content and flow records	Performance and availability of applications, end user experiences, incident investigations, networks, threat detection, monitoring, compliance



Optimize Multi-Channel Marketing Campaigns

- ▶ Multi-channel analytics for web, mobile and 10,000+ store locations
- ▶ Real-time revenue insights, product mix and promotion effectiveness
- ▶ Marketing campaign optimization

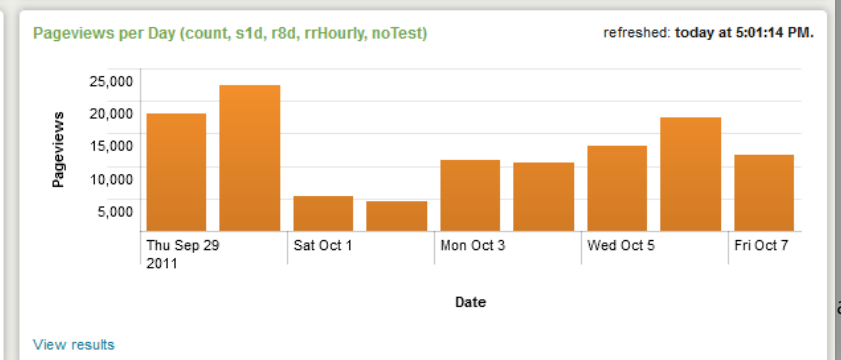
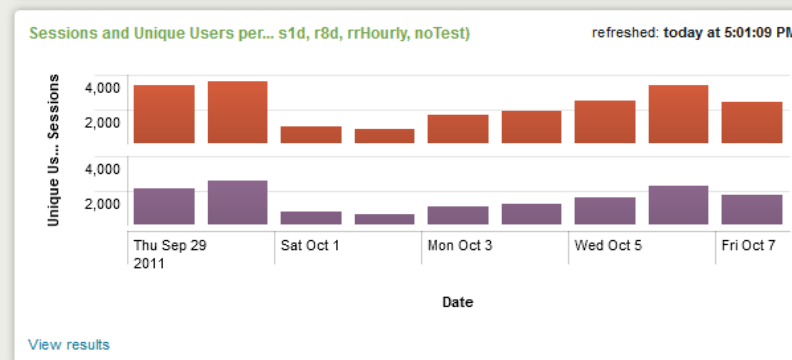
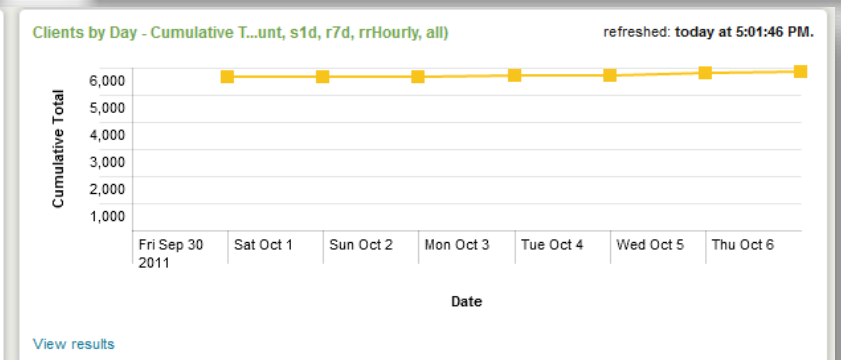
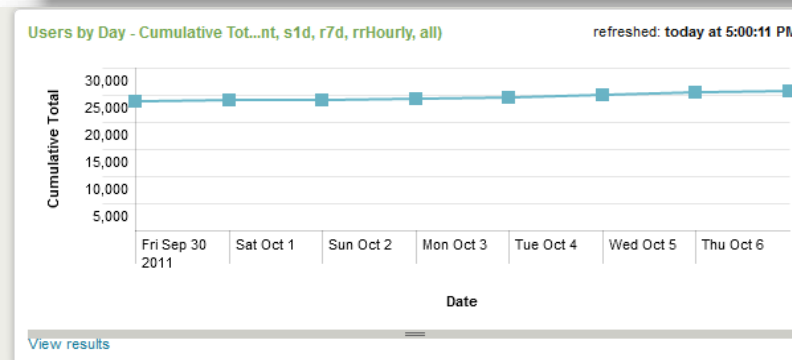
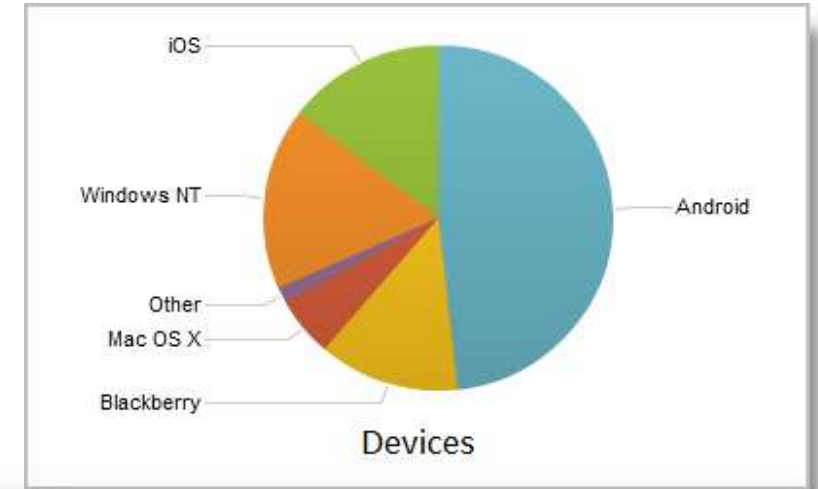
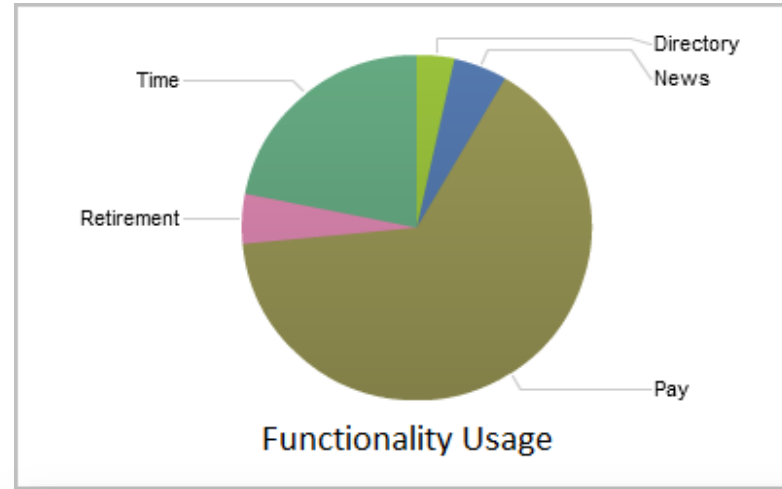
Engagement Analytics

- Better understanding of customer interactions
- Real-time end-to-end tracking of transactions
- Improved customer satisfaction and experience
- Business visibility and performance awareness
- Tracking and understanding the root cause for website errors



Mobile Device Analytics

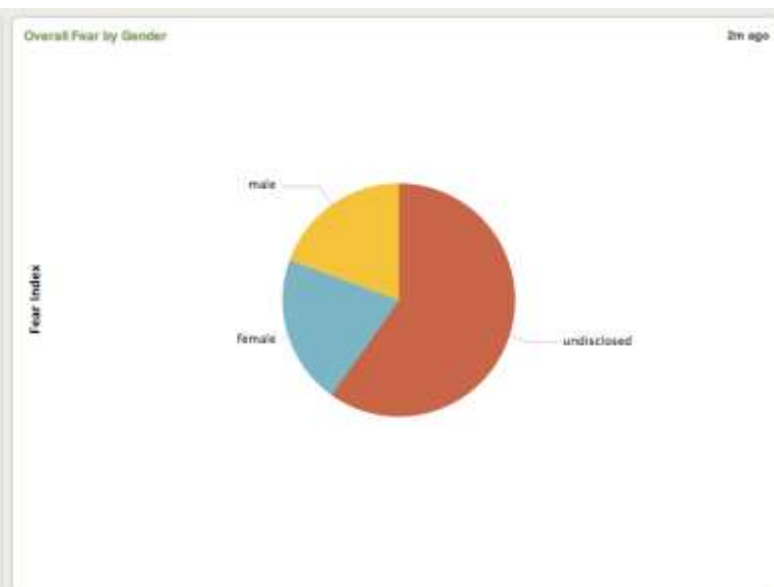
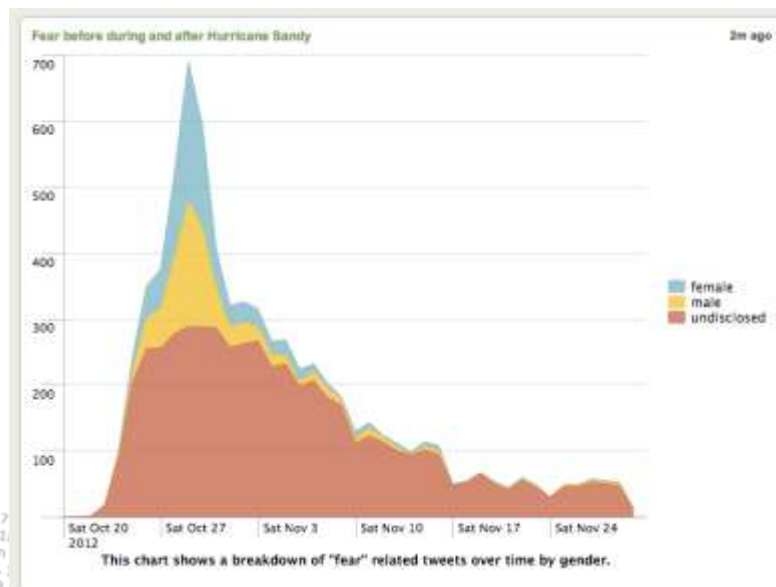
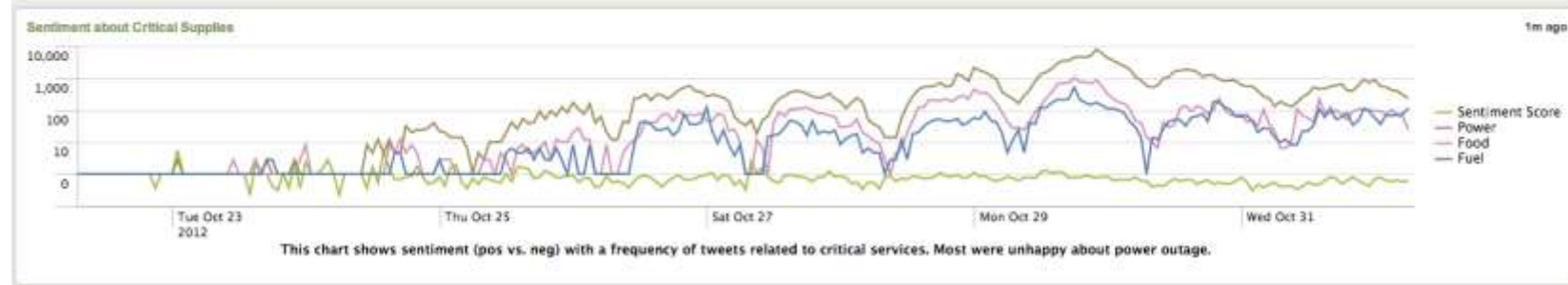
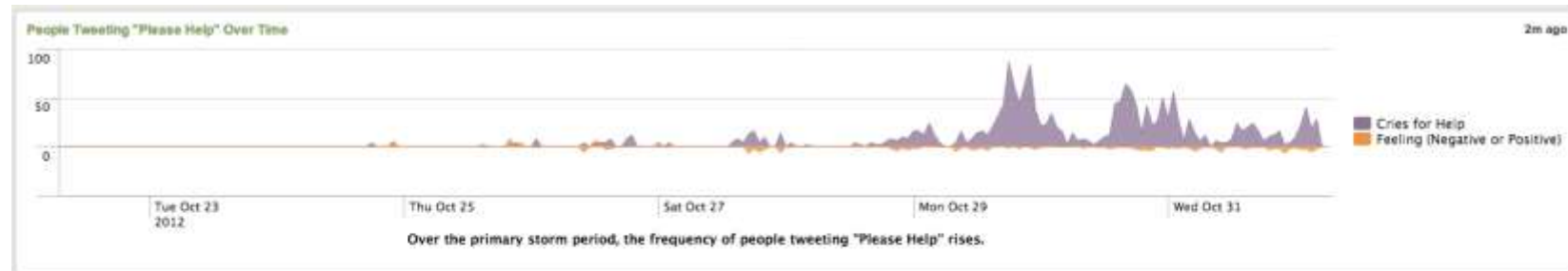
- ▶ Product adoption
- ▶ Users and clients
- ▶ Feature adoption
- ▶ User engagement
- ▶ Usage patterns
- ▶ Mobile devices
- ▶ Client dashboard



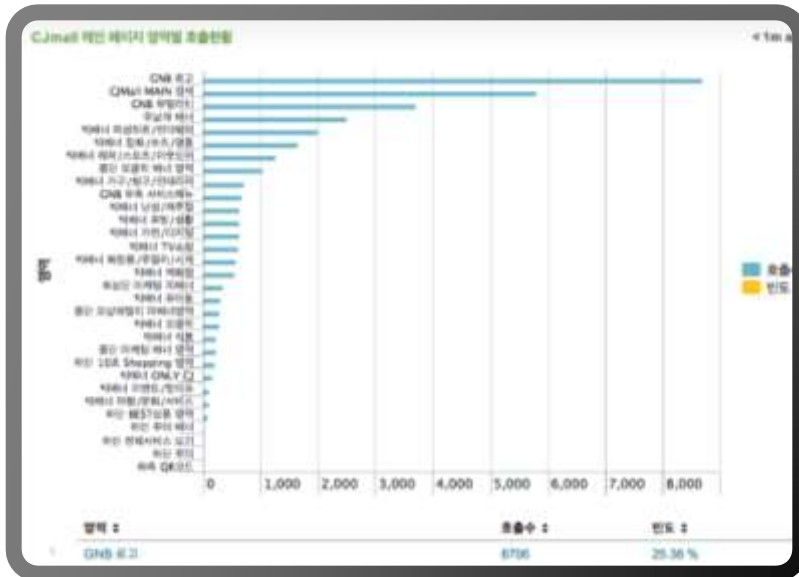
138.60.4
128.241.220.82
317.27.168.0.0
itemid=EST-16apro
//buttercup-shop
ofaction=purchas
pping.com/cas
//buttercup-shop

id=GLYTS&JSESSIONID=5D15L41
duc_id=FL-DSH-01&JSESSION
EST-26&JSESSIONID=5D55L9FF

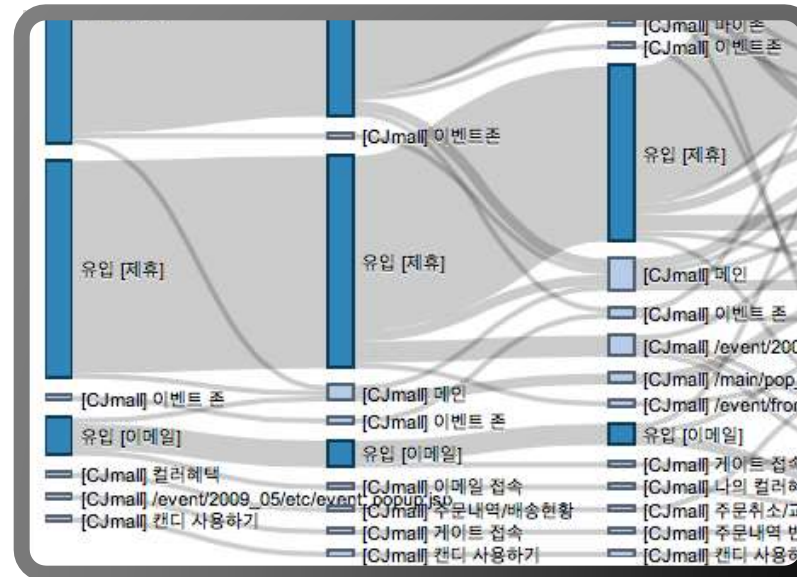
Social Sentiment Analytics



Online Service Engagement Analytics



Measure customer attention to specific areas of content



Analyze click trough's and how they navigate to CJ mall



Track and analyze mobile shopping customers in real time



Understand Digital Media Usage & Engagement



Business Analytics Use Case

- Analyze audio and podcast usage
- Accurately report royalty payments
- Faster identification of errors and abandonment
- Correlate weblogs with application performance data

Data sources: weblogs, audio/podcast logs, Akamai logs

PUBLIC SECTOR – BUSINESS ANALYTICS

Sacramento County Sheriff's Department: Intelligence-Led Policing



“The Splunk platform is critical to our Intelligence-Led Policing strategy. Our command group is now able to more clearly see trends in our crime statistics and take proactive action to address areas of concern and provide the best possible service to the public.”

– *Senior IT Analyst and Application Team Lead Technical Services Division,
Sacramento County Sheriff's Department*

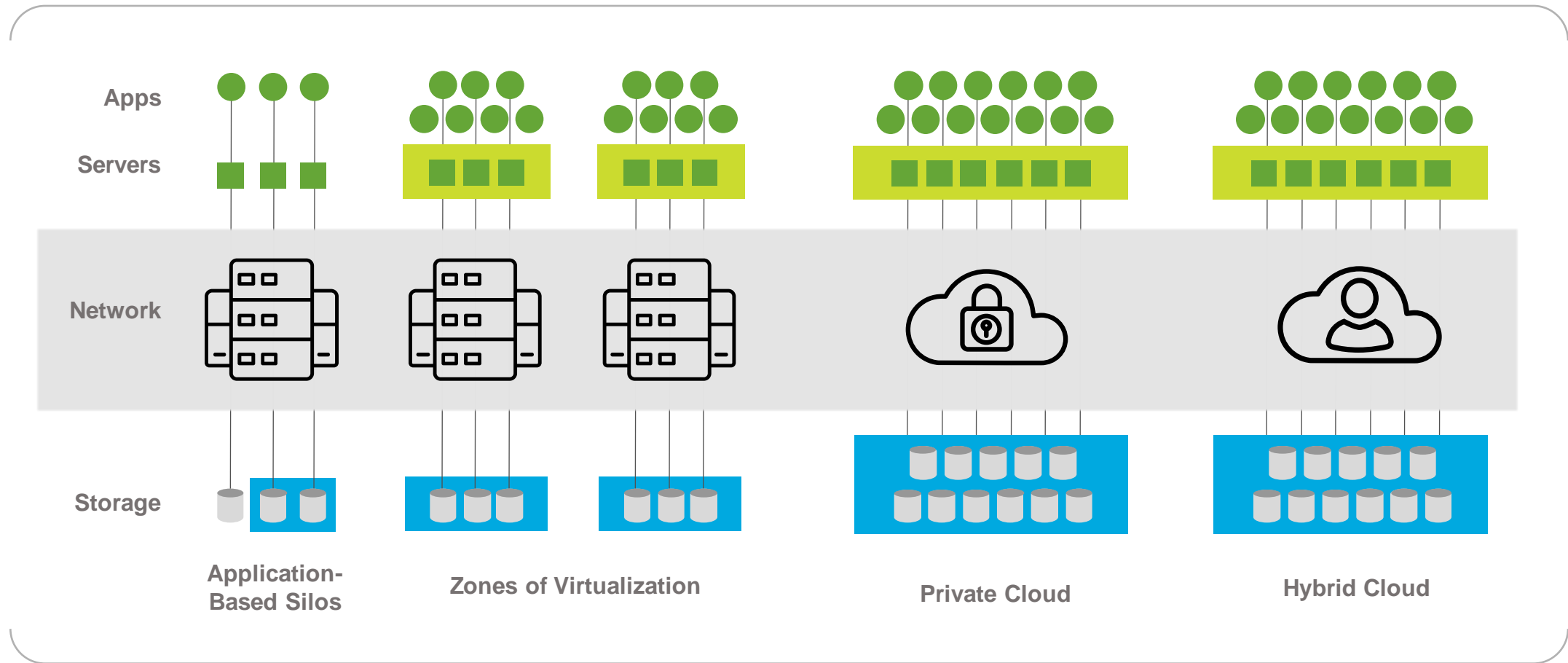
- ▶ Integrated and visualized crime, management and corrections data
- ▶ Enhanced accountability, helping to reduce crime report backlog
- ▶ Supported proactive policing based on big data analytics

Analytics for service intelligence

applying multi-channel and cross-platform data to gain insight into the quality and impact of end-to-end constituent services

Visibility Across All Dimensions

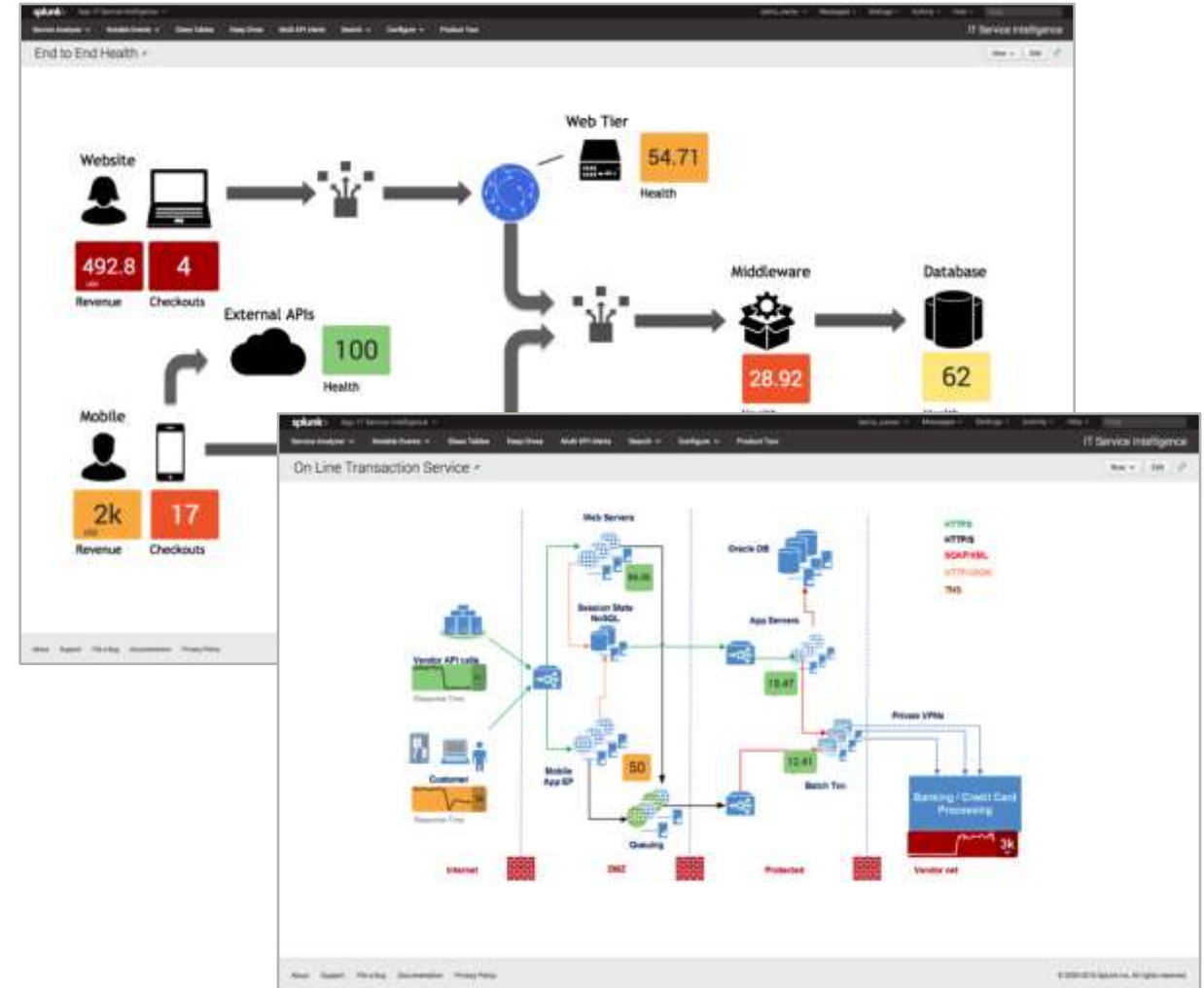
of your application and technology stack



138.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GLVTS&JSESSIONID=5D15LAF18ADFF10 HTTP/1.1" 404 728 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-06&product_id=PI_06_01" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0" [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FFADFF0 HTTP/1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=PI_26_01" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0" [07/Jan 18:10:57:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FFADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/changequantity&itemId=EST-58&product_id=PI_58_01" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0" [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 200 300 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3" [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L7FFADFF0 HTTP/1.1" 200 300 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L7FFADFF0" [07/Jan 18:10:55:188] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L7FFADFF0 HTTP/1.1" 200 300 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L7FFADFF0"

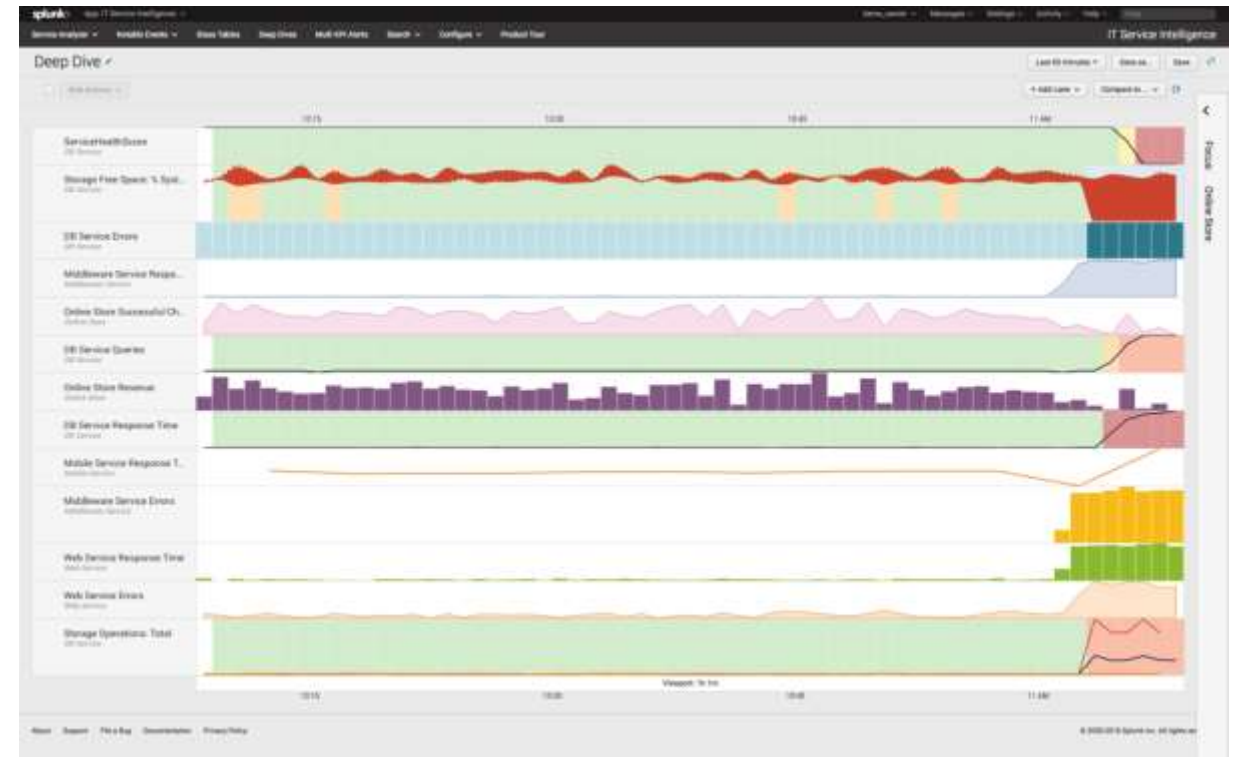
Contextual Service Visualizations

- ▶ Visualize contextual inter-relationships across service delivery components
- ▶ Illustrate business and service activity using indicators aligned with strategic goals
- ▶ Drive decisions by monitoring service health against performance indicators



Organized View of Key Performance Indicators

- ▶ Organize and correlate KPIs to speed up investigations and diagnosis
- ▶ Compare performance over time and in real time to understand trends and identify systemic issues
- ▶ Enable broad and deep investigation with contextual drill-downs



Real-Time View of Service and KPI Health Scores

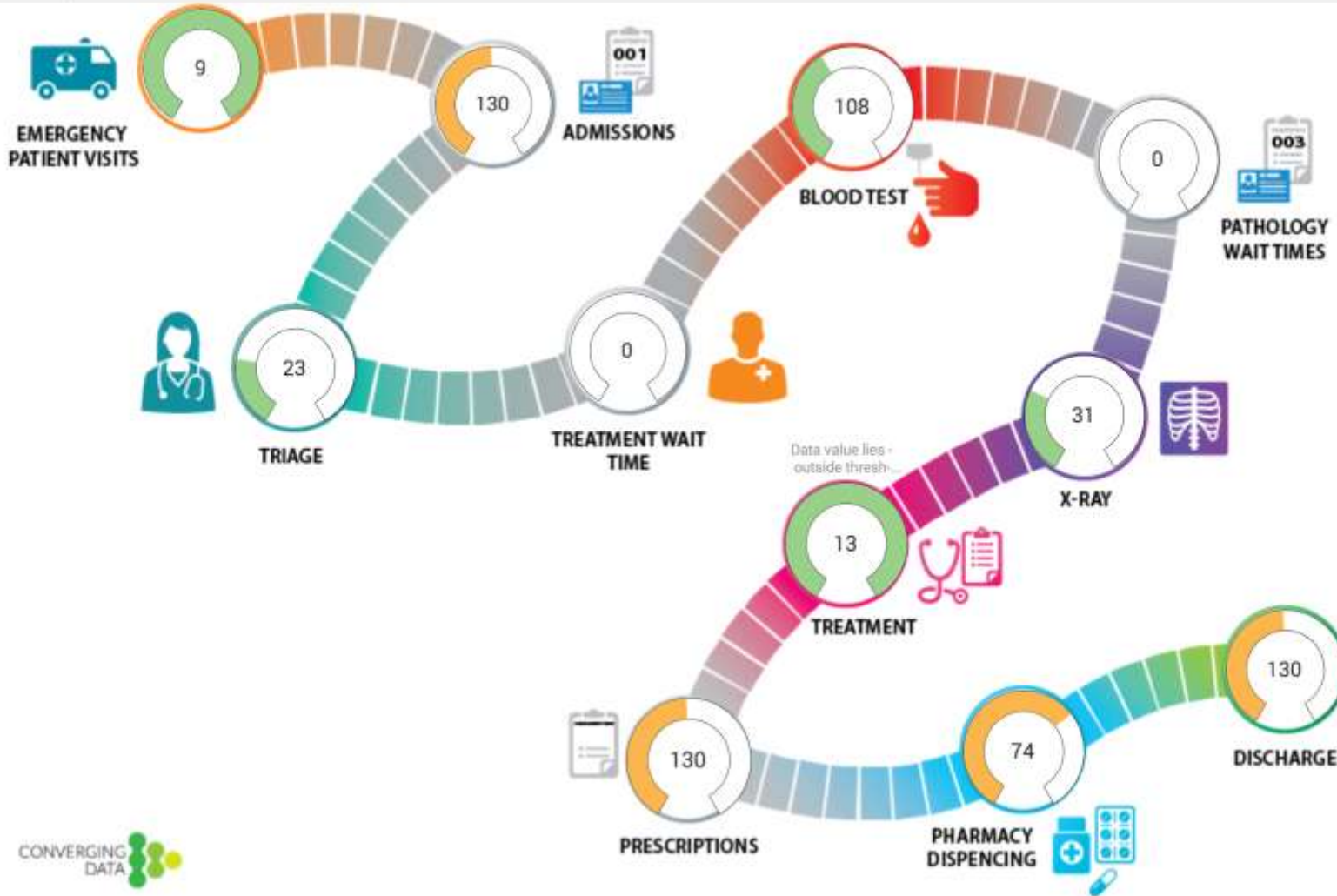
- ▶ Get early warning of emerging incidents with a heat map of service health and KPI scores, metrics, sparklines and alerts
- ▶ Drill down into service and entity details for in-depth triage



Applying Analytics for Service Intelligence

ER Patient Journey

Full Screen View Now Edit



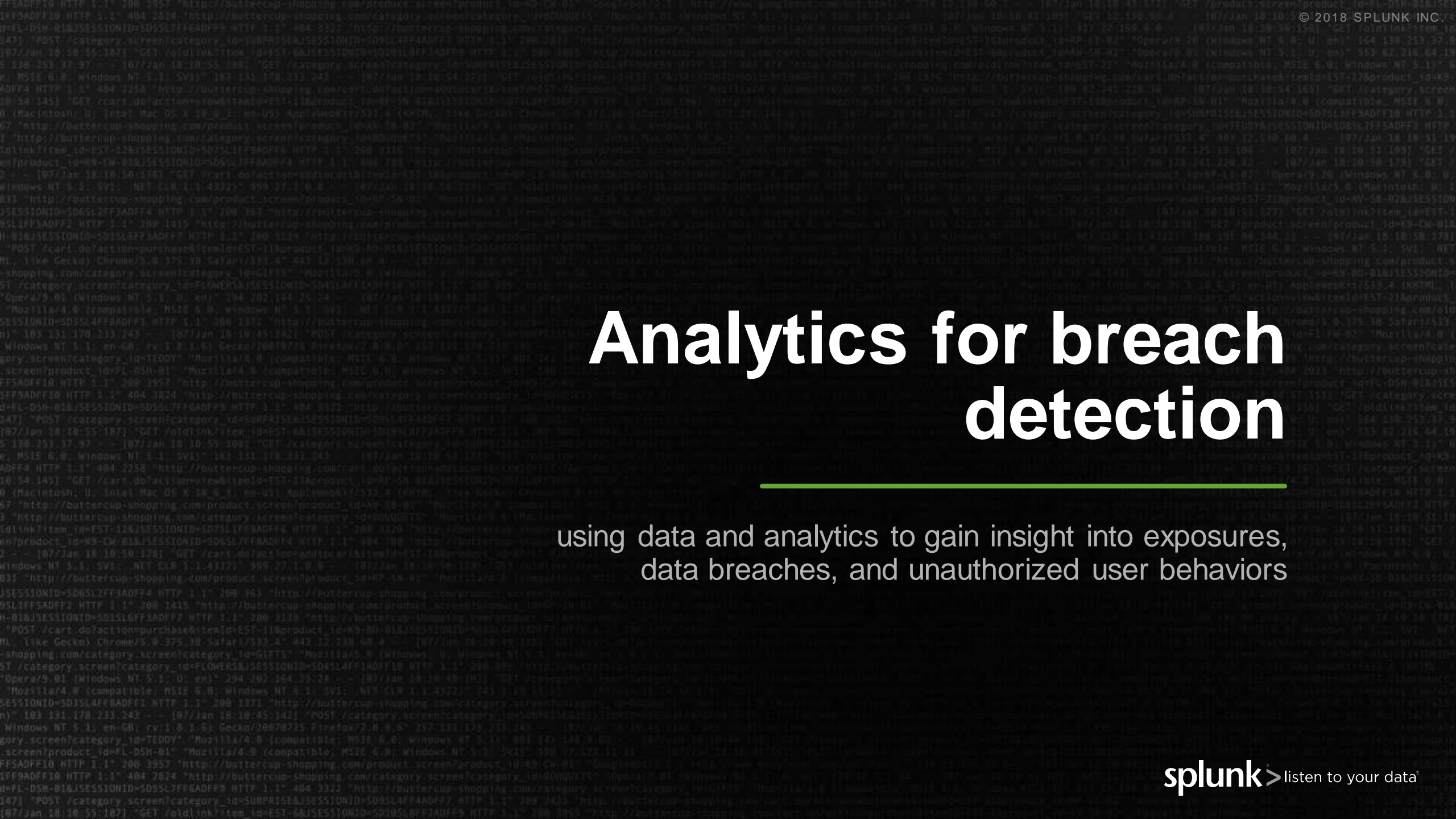


Chandler, AZ Police Dept.: Proactively Manages Vital Public Safety Systems

“We connect the dots and see patterns once hidden in all the statistics. We’re improving services, operating smarter and giving the public greater returns on its tax dollars.”

– *Sysadmin / Police Officer, Chandler AZ Police Dept.*

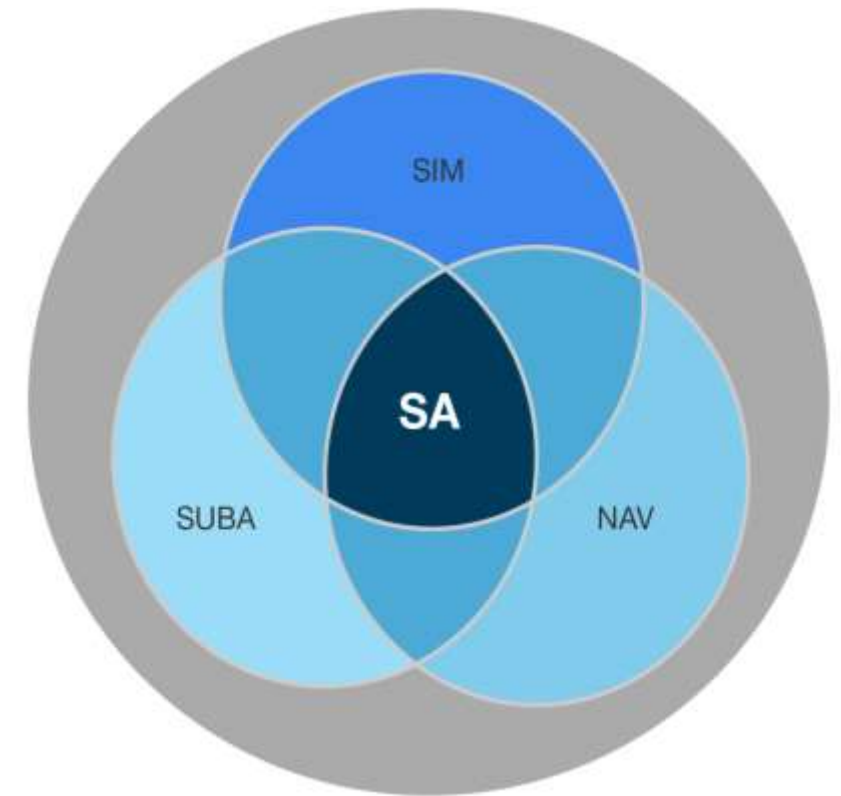
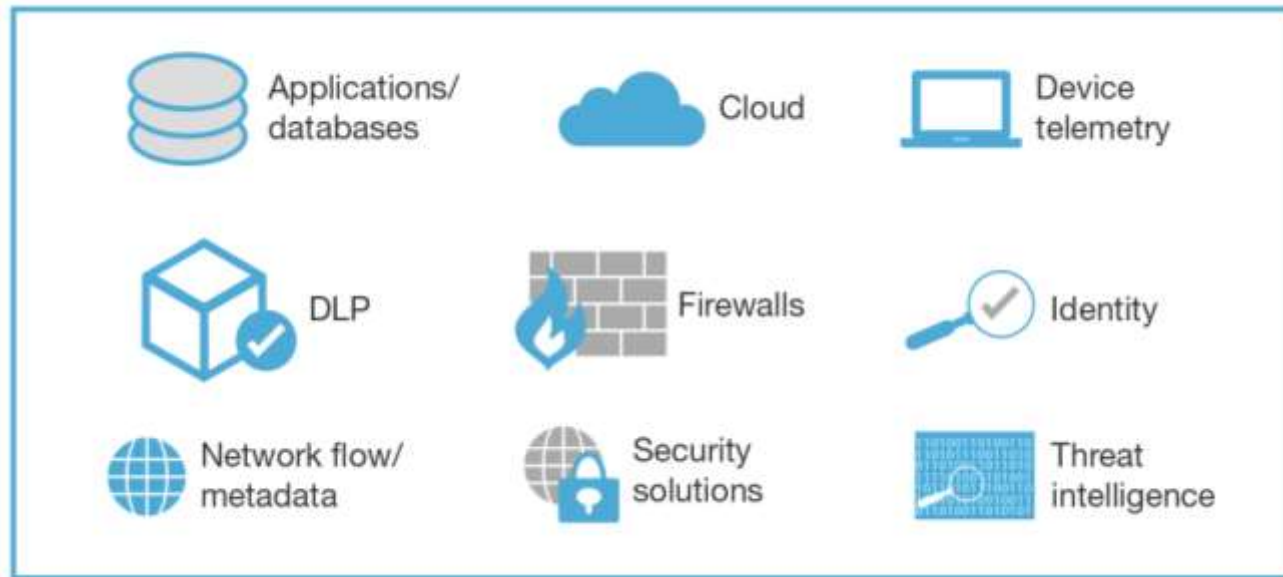
- ▶ Granular visibility and insights into all law enforcement activities
- ▶ Maximize system uptime with predictive analytics
- ▶ More effective resource allocation and faster officer response



Analytics for breach detection

using data and analytics to gain insight into exposures, data breaches, and unauthorized user behaviors

Security Analytics Enables Better Detection



▶ Source: Forrester's Vendor Landscape: Security Analytics (SA)

Security Analytics Enables SOC Processes

- ▶ Monitoring and alerting
- ▶ Event correlation
- ▶ Alert triage
- ▶ Incident response
- ▶ Threat hunting



Image: By UMD-Eskin (Own work) [Public domain], via Wikimedia Commons

Security Analytics Accelerates Detection, Investigation & Response

- ▶ Use correlation and analytics to automate notable event detection
- ▶ Execute ad-hoc queries to find root causes and malicious actors
- ▶ Use automation to take actions and review their results

+ Add New Response Action ▾

Category: Information Conveyance ▾

- Notable**
Creates notable events
Category: Information Conveyance | Task: create | Subject: splunk.event | Vendor: Splunk
- Send To UBA**
Forwards search results from Splunk Enterprise to UBA
Category: Information Conveyance | Task: create | Subject: uba.anomaly | Vendor: Splunk
- Test Builder**
Category: Information Conveyance | Task: block | Subject: endpoint.smart-meter | Vendor: Splunk

Adaptive Response Action Center

Action Status: All | Action Name: All | User: All | Search: All | Last 24 hours | Refresh | Help

Metric	Value	Trend
ACTION INVOCATIONS	80.6k	+66.9k
ACTION NAMES	7	0
ACTION SEARCH NAMES	32	+8
ACTION USERS	4	0
ACTION SEARCHES	789	+255
ACTION DURATION	260	-5.9

Action Invocations Over Time By Name

Action Name	Count
Notable	~1000
Send To UBA	~500
Test Builder	~200
Other Actions	~100

Top Actions By Name

Action Name	Search Count	Result Count	Avg. Duration (ms)
Notable	~1000	~1000	~100
Send To UBA	~500	~500	~200
Test Builder	~200	~200	~150

e.g. Phishing Search

- ▶ Detect typos, like company.com → campany.com
- ▶ Find misspelled subdomains for typo detection
- ▶ Detect suspicious subdomains, like company.com → company.yourithelpdesk.com

```

Detect New Values
Enter a search
| inputlookup Anonymized_Email_Logs.csv
| stats count by Sender
| rex field=Sender "\@(?(?<domain_detected>.*))"
| stats sum(count) as count by domain_detected
| eval domain_detected=mvfilter(domain_detected!="mycompany.com" AND domain_detected!="company.com" AND domain_detected!="mycompanylovestheenvironment.com")
| eval list="mozilla"
| 'ut_parse_extended(domain_detected, list)'
| foreach ut_subdomain_level* [eval orig_domain=domain_detected, domain_detected=mvappend(domain_detected, '<<FIELD>>' . "." . ut_tld)]
| fields orig_domain domain_detected ut_domain count
| eval word1=mvappend(domain_detected, ut_domain), word2 = mvappend("mycompany.com", "company.com", "mycompanylovestheenvironment.com")
| lookup ut_levenshtein_lookup word1 word2
| eval ut_levenshtein= min(ut_levenshtein)
| where ut_levenshtein < 3
| fields - domain_detected ut_domain
| rename orig_domain as top_level_domain_in_incoming_email word1 as domain_names_analyzed word2 as company_domains_used count as num_occurrences ut_levenshtein as Levenshtein_Similarity_Score
    
```

top_level_domain_in_incoming_email ▾
cust.mycompany.com
mycompany.com
mycompany.yourithelpdesk.com

e.g. Increase in Pages Printed

- ▶ Search printer logs for potential resource abuse or data leakage

The screenshot displays a Splunk search interface with three summary cards at the top: 'Outlier(s)' with a count of 1, 'Total Result(s)' with a count of 2, and 'Raw Event(s)' with a count of 1,006. Below these cards is a table titled 'Outliers Only' with one data row for user 'chuck'. The table columns include User, num_data_samples, Pages, avg, lowerBound, upperBound, and isOutlier. Below the table are several action buttons: 'Open in Search', 'Show SPL', 'Schedule Alert', and 'Schedule High Cardinality Alert'. The bottom of the image shows a blurred background of raw search events.

User	num_data_samples	Pages	avg	lowerBound	upperBound	isOutlier
chuck	22	4306	16.700000	0.296855	33.103145	1

e.g. Authentication Against a New DC

Outlier(s) [↗](#)

1

Outlier(s)

Open in Search
Show SPL
Schedule Alert

Total Result(s) [↗](#)

11

Total Result(s)

Open in Search
Show SPL

Raw Event(s)

7,383

Raw Event(s)

Outliers Only [↗](#)

user ↕	anonymized_DomainControllerName ↕	earliest ↕	latest ↕	maxlatest ↕	isOutlier ↕
chuck	anon_DomainControllerName_1	10/22/2016 13:06:37.000	10/23/2016 10:33:39.000	10/23/2016 20:50:29.000	1

Open in Search
Show SPL
Schedule Alert

138.68.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=G1VTS&JSESSIONID=5D15LAF18ADFF10 HTTP 1.1" 404 728 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=PI_5W_01-..."
 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=PI_5W_01-..."
 317.27.168.0.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=PI_5W_01-..."
 10.1.1.1 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=PI_5W_01-..."
 10.1.1.1 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=PI_5W_01-..."
 10.1.1.1 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=PI_5W_01-..."
 10.1.1.1 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=PI_5W_01-..."
 10.1.1.1 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=PI_5W_01-..."
 10.1.1.1 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=PI_5W_01-..."
 10.1.1.1 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=PI_5W_01-..."

Protecting Citizen Data Using Splunk Enterprise Security in the Cloud



“My top priority is to protect the citizens’ data. Making sure that these citizens can trust the government they have with the data that they have entrusted us with is our mission.”

– *CISO, Fairfax County, Virginia*






- ▶ Proactively supporting more than 50 county agencies and protecting citizens’ data
- ▶ Reducing security reporting from two weeks to real time
- ▶ Increasing focus on strategic initiatives by leveraging cloud services

Analytics for the Internet of Things

using analytics on devices and other 'things' to gain actionable intelligence about cloud-connected assets

A World of Connected Assets

   
Transportation | Energy | Utilities | Building
 
Management

  
Retail | Home | Consumer
 
Telemedicine | Connected Cars

Oil and Gas | Manufacturing

Sensors, Pumps, GPS, Valves, Vats,
Conveyors,
Pipelines, Drills, Transformers, RTUs, PLCs,
HMIs, Lighting, HVAC, Traffic
Management, Turbines,
Windmills, Generators,
Fuel Cells,
UPS



Industrial Data

Wearables, Home Appliances,
Consumer Electronics, Gaming
Systems, Personal Security, Set-Top
Boxes, Vending
Machines, Mobile Point of
Sale, ATMs,
Personal Vehicles



Internet of Things



Challenges in IoT Landscape

**Data Volume,
Variety and Velocity**

**Diverse Protocols
and Standards**

**Correlate Data
Across Application/
Infrastructure Silos**

**Complex Device to
Cloud
Architectures**

CHALLENGES

**Human to Machine
Component**

**Security and
Privacy**

IoT and Industrial Machine Data

Industrial Assets



Native Inputs

TCP, UDP, Logs, Scripts, Wire, Mobile

Consumer and Mobile Devices



SDKs and APIs

Java, JS, C#, Python, Ruby, PHP

Modular Inputs

MQTT, AMQP, COAP, REST, JMS

OT



HTTP Event Collector

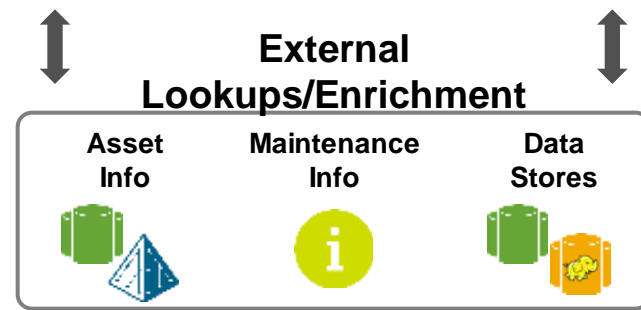
Token Authenticated Events

IT



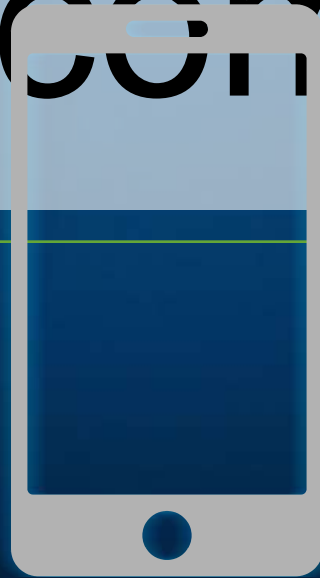
Technology Partnerships

Kepware, ThingWorx, Cisco, Palo Alto



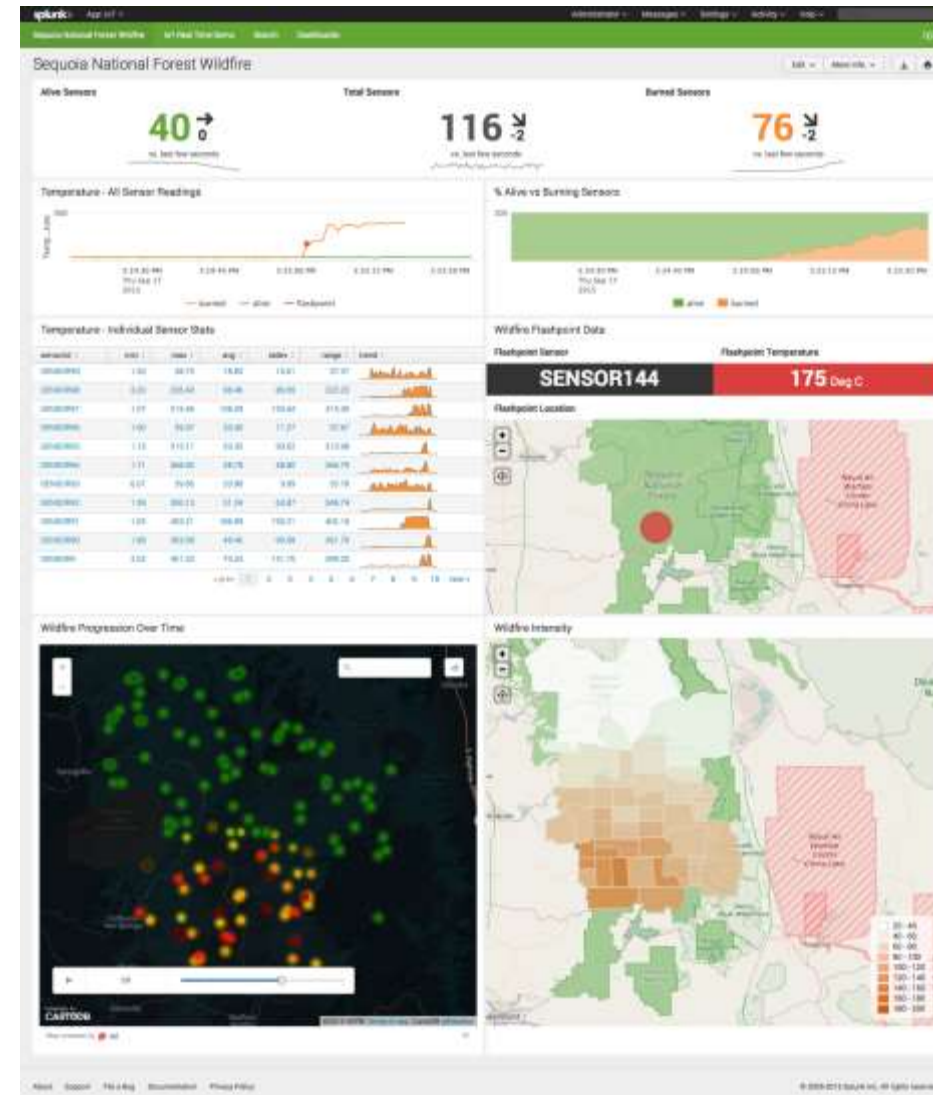
GO TO

splunk.com/shake



AWS and IoT

- ▶ Ingest data in real-time and at scale from AWS IoT Service
- ▶ Search, explore and analyze real-time and historical data with Splunk
- ▶ Correlate and enrich data from AWS IoT service with other data sources – application logs, mobile, databases and data from other IoT platforms
- ▶ Build web-applications using Splunk’s powerful application development, visualization, and machine learning frameworks



Use Cases



Monitoring,
Diagnostics

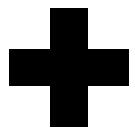


Security, Safety
& Compliance



Preventative
Maintenance

Real-Time Data Platform



TRANSPORTATION – IOT

Improve Customer Service, Reduce Costs by Increasing Locomotive Availability and Reliability



- ▶ Ingest and correlate sensor, diagnostic codes, geolocation data in real time to:
 - Gain insights into asset health, condition
 - Perform root cause analysis
 - Generate locomotive maintenance recommendations

Improving Water Quality



- ▶ Ingest data from water treatment systems, weather, SCADA, buoys, lab testing
- ▶ Monitor, measure water quality; identify factors impacting quality
- ▶ Identify sensor reading anomalies to replace/recalibrate

Managing Airfield Performance

YOUR
LONDON
AIRPORT
Gatwick

- ▶ Real-time monitoring of aircraft turnaround process
- ▶ Tracking real-time metrics to manage airfield performance
- ▶ Increased on-time efficiency and aircraft predictability

Improving Passenger Experience



YOUR
LONDON
AIRPORT
Gatwick

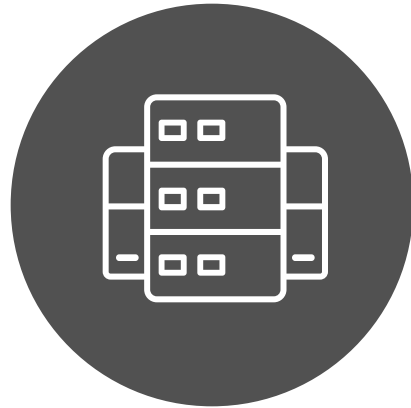
- ▶ Gain visibility into passenger flow
- ▶ Reduce congestion with improved ticket scan validation
- ▶ Monitor travel disruption to understand impact on operations
- ▶ Optimize staffing to improve passenger experience



Measuring New IT Architectures

modern approaches to service delivery incl. Site Reliability Engineering' semantic logging, telemetry, observability

Rethinking and Improving How IT Operates



Traditional IT

- ▶ Brittle tools and integrations
- ▶ Obsession with “faults” and “traps”
- ▶ Focus on components parts
- ▶ Non-stop reactive break-fix
- ▶ Manual ops, one-offs, and heroes



Data Driven IT

- ▶ Robust data integrations
- ▶ Real-time insights from data
- ▶ Focus on the whole service
- ▶ ML and predictive analytics
- ▶ Automation engineering



Site Reliability Engineering

- ▶ A Durable Focus on Engineering
 - No more than 50% time on break-fix; excess ops work goes to backlog
- ▶ Pursuing Maximum Change Velocity Without Violating a Service's SLO
 - “Error budget” to allow for innovation *and* stability
- ▶ Monitoring and Emergency Response
 - Standardize and automate to reduce human impact; issues routed to backlog
- ▶ Engineer for rapid change
 - Real-time self-service provisioning; enable progressive deploy-fail-fix cycles
- ▶ Relentless Automation
 - Software-defined everything; “Automate yourself out of a job”
- ▶ Engineer for Efficiency and Performance
 - Build and test services for resilience; deficiencies go into application backlog

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

Observability

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

The observability and controllability of a system are mathematical duals.”

Wikipedia

“Semantic Logging”

- ▶ You have no control over other systems events
- ▶ You have full control over events that YOU write
- ▶ Most events are written by developers to help them debug
- ▶ Some events are written to form an audit trail

Semantic Events are written explicitly for the gathering of analytics



Semantic Logging Best Practices

Log more than just Debugging Events

- ▶ Log anything that can add value when aggregated, charted or analyzed

Example Bogus Pseudo-Code:

```
void submitPurchase (purchaseId)
{
    log.info("action=submitPurchaseStart, purchaseId=%d", purchaseId)
    //these calls throw an exception on error
    submitToCreditCard(...)
    generateInvoice(...)
    generateFullfillmentOrder(...)
    log.info("action=submitPurchaseCompleted, purchaseId=%d", purchaseId)
}
```

- Graph purchase volume by hour, by day, by month.
- How long are purchases taking at different times of day, or days of the week?
- Are purchases taking longer than they did last month?
- Are my systems getting slower and slower, or are they ok?
- How many purchases are failing? Graph the failures over time.
- Which specific purchases are failing?

SREs Monitor Metrics and Events

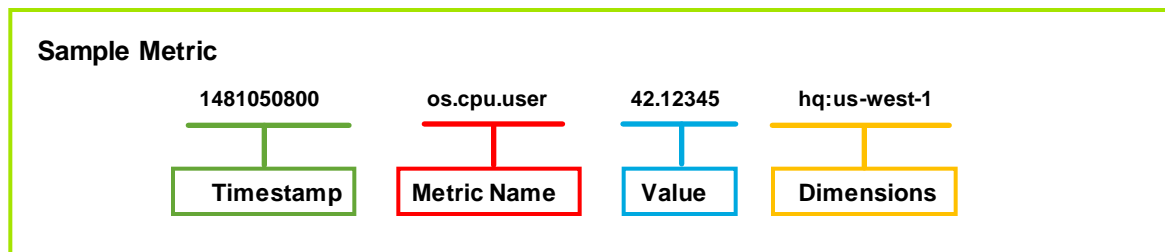
Two distinct machine data sources that have been hard to integrate...until now

Metrics

- ▶ Numbers describing a particular process or activity
- ▶ Measured over intervals of time—
i.e., *time series data*
- ▶ Common metrics sources:
 - System metrics (CPU, memory, disk)
 - Infrastructure metrics (AWS CloudWatch)
 - Web tracking scripts (Google Analytics)
 - Application agents (APM, error tracking)

Events

- ▶ Immutable record of discrete events that happen over time
- ▶ Come in three forms: plain text, structured, binary
- ▶ Common event sources:
 - System and server logs (syslog, journald)
 - Firewall and intrusion detection system logs
 - Social media feeds (Twitter...)
 - Application, platform and server logs (log4j, log4net, Apache, MySQL, AWS)





Dev isn't "done" until the system provides data for Ops



Advanced analytics

advanced data techniques for IT incl. machine learning, operations analytics, anomaly detection, operational intelligence, predictive analytics, and data visualization

Unlock the Value of Data with Analytics

Device Analytics



Security and Privacy



Transport Logistics

High Frequency Analytics



Constituent Engagement



Performance Analytics



Predictive Analytics



Operational Intelligence

Use ML to Forecast Time Series Data

Forecast Time Series

Predict likely future values given past values of a metric (numerical time series).

Choose an example dataset or enter a search (should contain "_time" field with unix timestamp values)

Cow Milk Production Data

```
| inputlookup milk.csv | timechart span=1mon values(milk_production) as milk_production |
```

All time

✓ 0 events (12/31/69 4:00:00.000 PM to 9/18/15 4:50:36.000 PM)

Job || Smart Mode

Field to predict

milk_production

Forecasting method

LLP5 (combines LLT and LLP)

Withhold latest k values

24

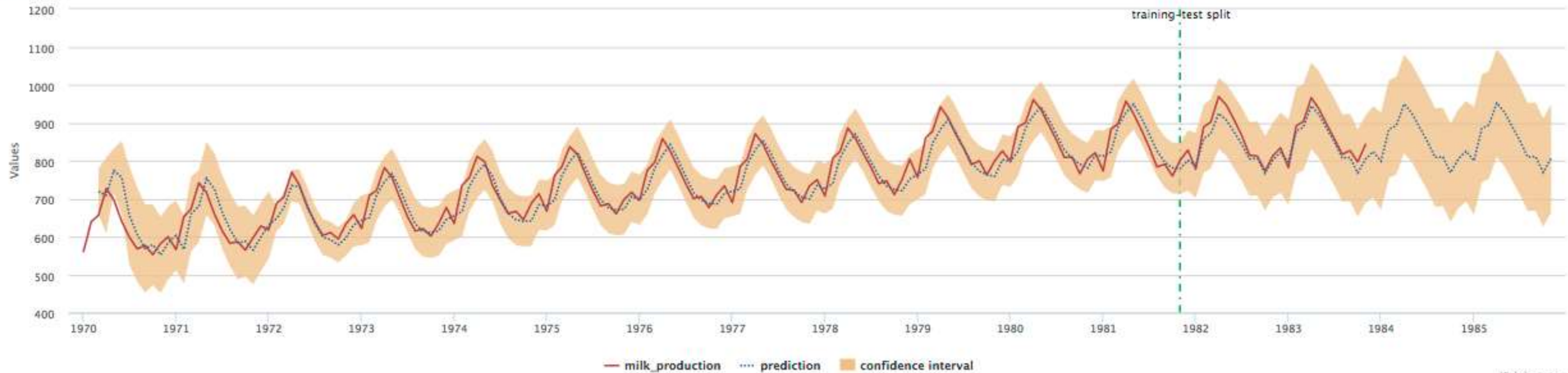
Forecast next k values

24

Period (optional)

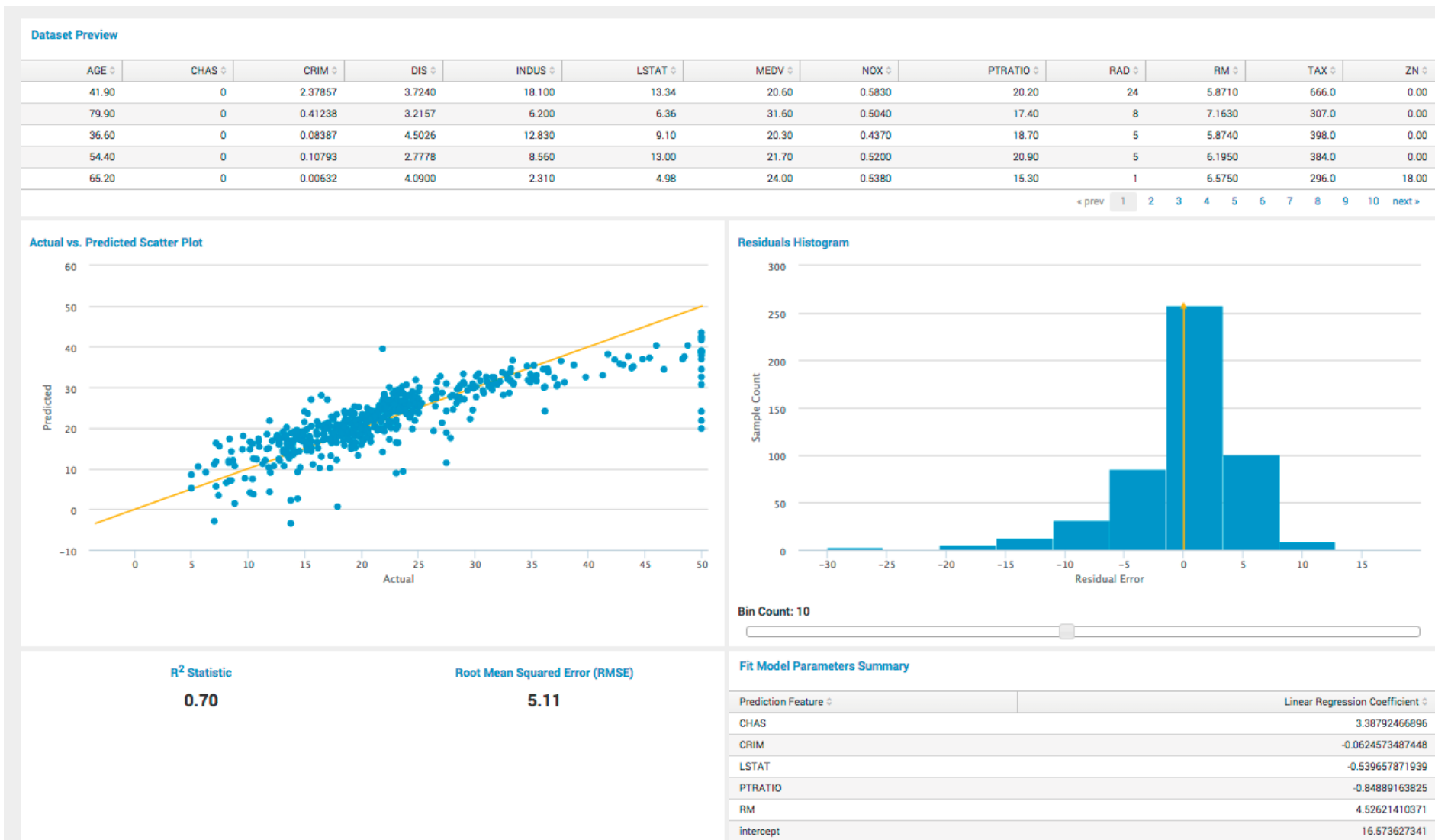
Submit

Prediction



Highcharts.com

Use ML to Detect Metric Anomalies



Baseline Trends to Adapt Thresholds

Thresholding

Use Thresholding Template: 3-hour blocks every day (default weekly)

Set Custom Thresholds: Enable Time Policies: Enable Adaptive Thresholding: Adaptive Thresholding runs every day around midnight and updates the threshold for the KPI based on the settings below. Once updated, old thresholds cannot be recovered.

Preview Aggregate Thresholds

Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday, Monday

Configure Thresholds for Time Policies

Policy	Aggregate Threshold Values
1PM - 3PM	2
3AM - 5AM	1
3PM - 6PM	2
5AM - 8AM	1
6PM - 9PM	1

Use statistics to dynamically adapt KPI thresholds by time

Maintain and preserve learned thresholds to monitor KPI and service behavior

Detect and Predict Anomalies

Percentage of Time Anomalies were Detected: 3% (Expected <15%)

Trending AD Preview - KPI Value for Last 7 Days



Entities Analyzed: 57

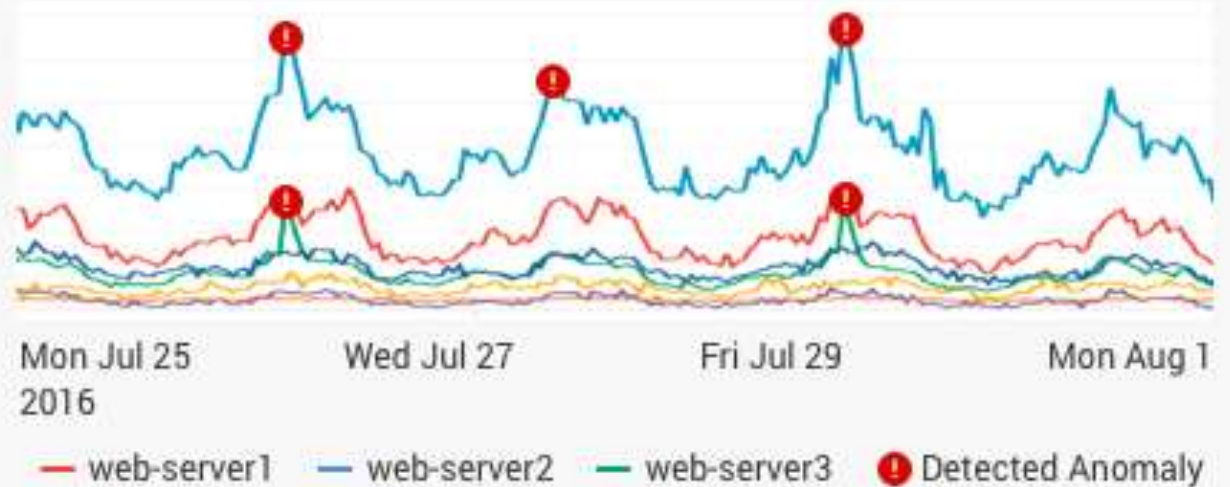
Entities with Detected Anomalies: 33

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



Learn What's Normal and Abnormal



Baseline normal operations and alert on anomalous conditions

Identify abnormal trends and patterns in KPI data

138.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=G1VTS&JSESSIONID=SD1SLAFF18ADF10 HTTP 1.1" 404 728 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=PI_0W_01 -
 128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FFDADF0 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-2&product_id=MK-CW-01 -
 317.27.168.0.0 - - [07/Jun 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FFDADF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1&product_id=AV-CN-01&JSESSIONID=SD5SL7FFDADF0 HTTP 1.1" 200 380
 itemId=EST-5V1; - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=G1VTS&JSESSIONID=SD1SLAFF18ADF10 HTTP 1.1" 404 728 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=PI_0W_01 -
 //buttercup-shopping.com/cart.do?action=purchase&itemId=EST-2&product_id=MK-CW-01 -
 //buttercup-shopping.com/cart.do?action=purchase&itemId=EST-2&product_id=MK-CW-01 -
 //buttercup-shopping.com/cart.do?action=purchase&itemId=EST-2&product_id=MK-CW-01 -
 //buttercup-shopping.com/cart.do?action=purchase&itemId=EST-2&product_id=MK-CW-01 -

But Good Data Is Not Enough



Find The Value In The Data

Planning	Development	Build	Verification	Deployment	Post-Deploy
100 (0%)	100 (0%)	94.74 (-5.3%)	100 (0%)	100 (0%)	100 (0%)
160 stories	0 in progress	100% success	100% success	364 deploys	0 CFDs
100 stories	95 complete	8.8 MTTB	3.95 MTTT	0.54 success	
	1 ticket	2.489 MTTR			
	30 points/dev				
		94 (-6%)			
		15.12 days			

Find The Value In The Visualization



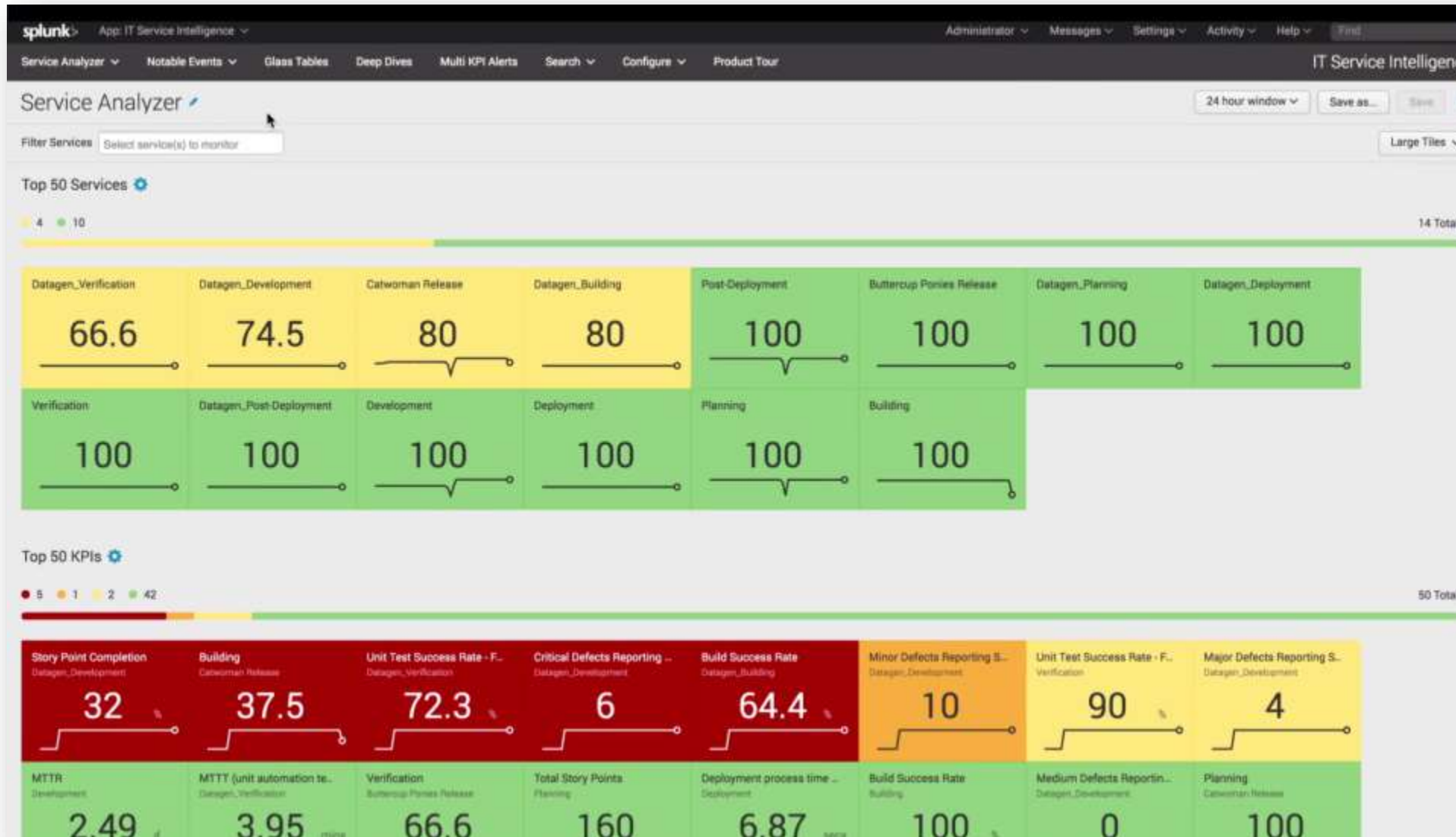
Find The Failure in the Visualization



BUTTERCUP GAMES DEVELOPMENT HEALTH



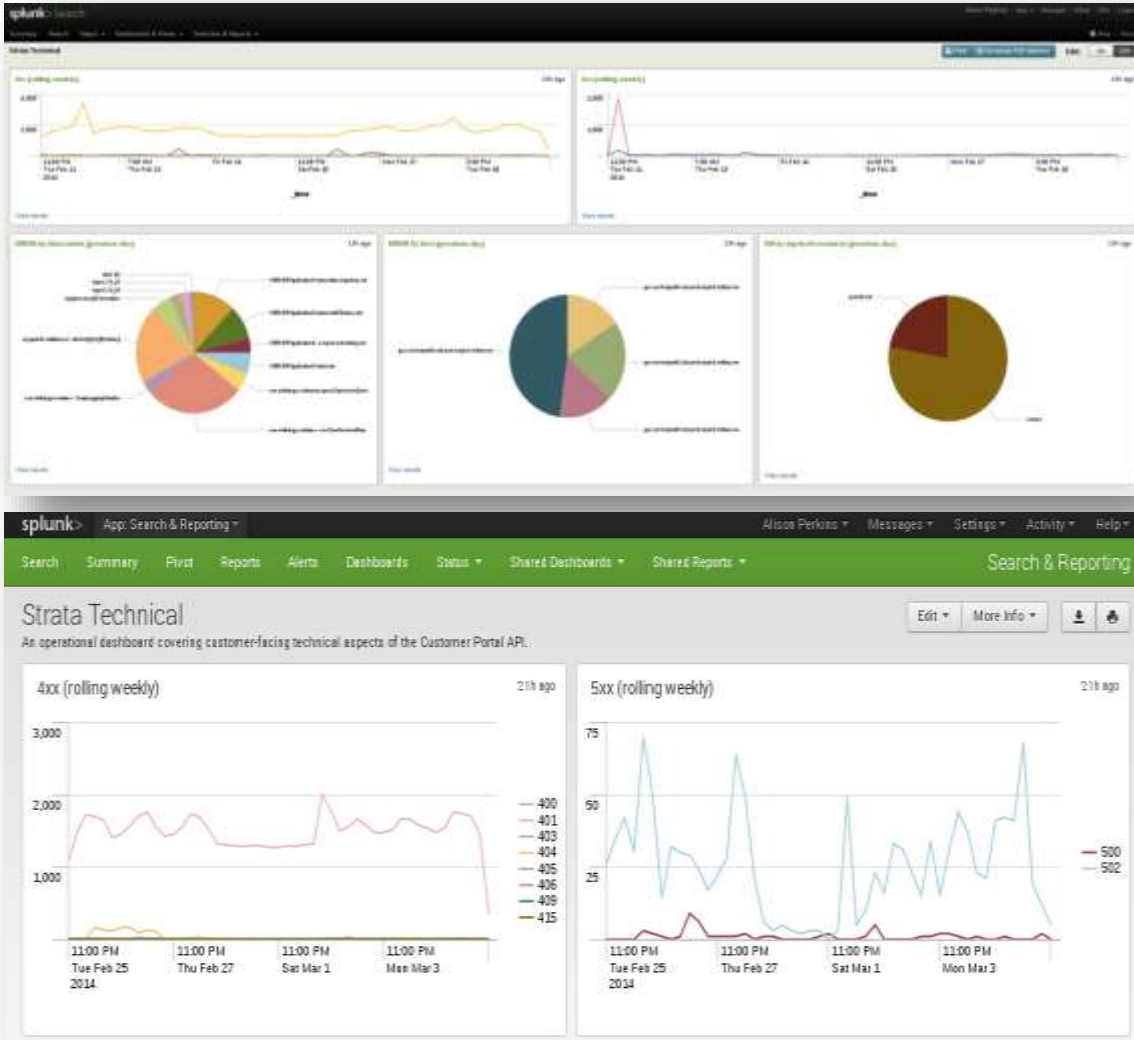
How About Now?



How About Now?



Shared Data Helps Find and Fix Issues Faster

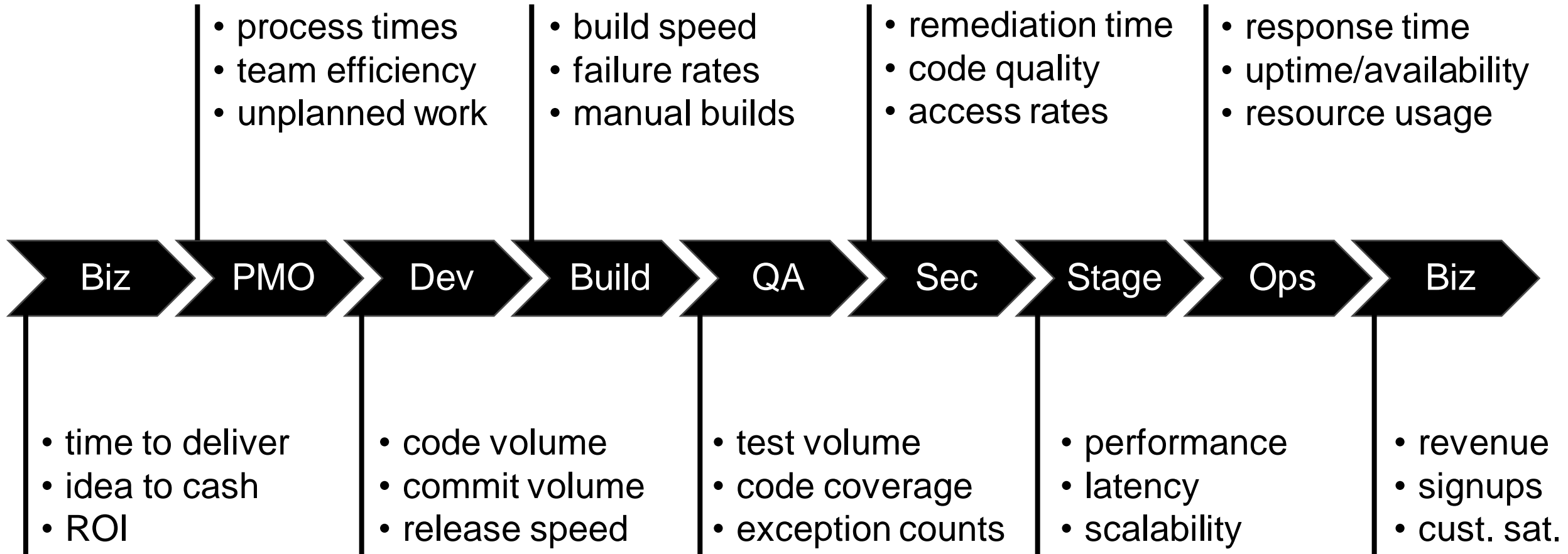


Common alerting notify devs and ops as soon as a problem arises

Developers can search and visualize production logs and tools —without production access

Real-time data sharing shows error rate in production and impact of pushing new builds

Specific Data For Each Stakeholder

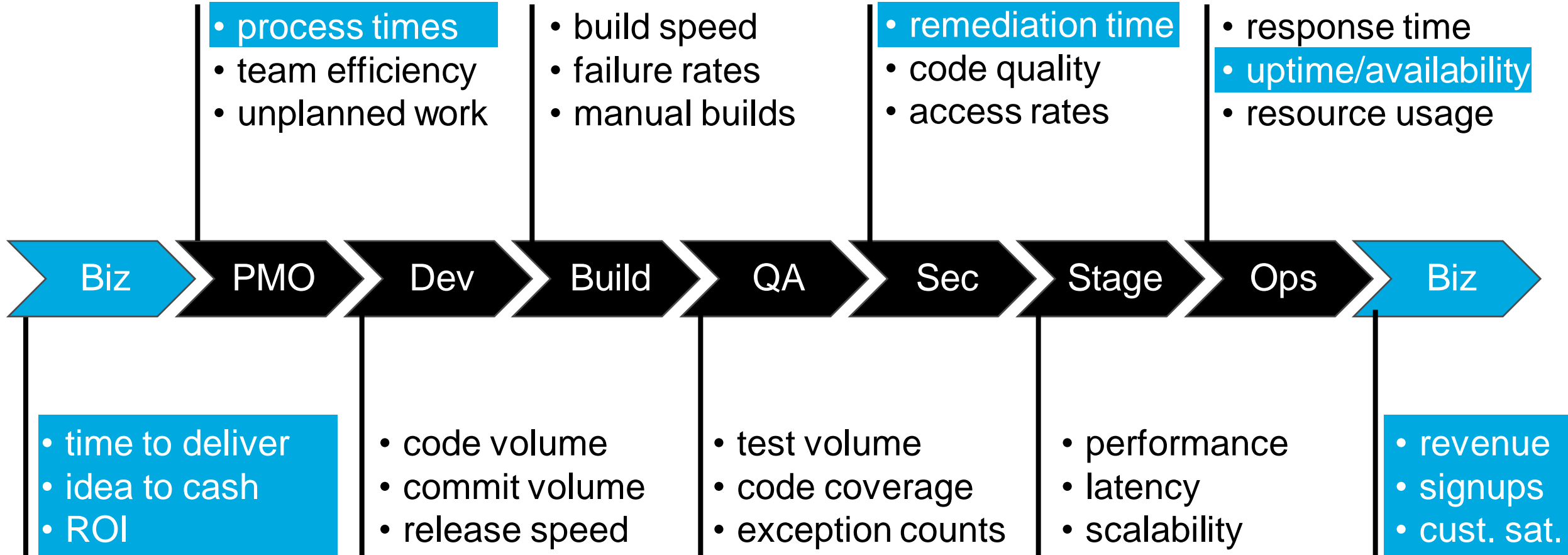


```

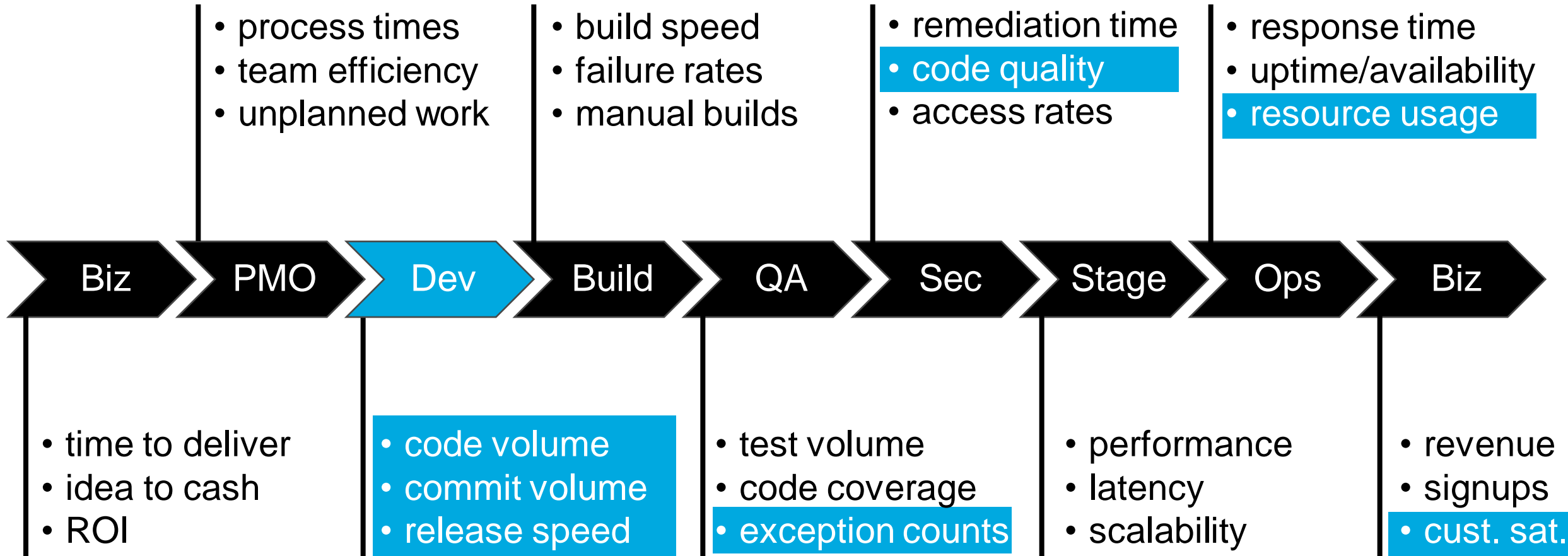
138.68.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=61VTS&JSESSIONID=5D15LAF18ADFF10 HTTP/1.1" 404 728 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-68product_id=215w-01-
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 404 322 "http://buttercup-shopping.com/category.screen?category_id=61VTS-
ows NT 27.168.0.0 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=61VTS&JSESSIONID=5D15LAF18ADFF10 HTTP/1.1" 404 728 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-68product_id=215w-01-
itemId=EST-16&JSESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=61VTS&JSESSIONID=5D15LAF18ADFF10 HTTP/1.1" 404 728 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-68product_id=215w-01-
//buttercup-shopping.com/category.screen?category_id=61VTS&JSESSIONID=5D15LAF18ADFF10 HTTP/1.1" 404 728 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-68product_id=215w-01-
shopping.com/category.screen?category_id=61VTS&JSESSIONID=5D15LAF18ADFF10 HTTP/1.1" 404 728 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-68product_id=215w-01-
http://buttercup-shopping.com/category.screen?category_id=61VTS&JSESSIONID=5D15LAF18ADFF10 HTTP/1.1" 404 728 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-68product_id=215w-01-
http://buttercup-shopping.com/category.screen?category_id=61VTS&JSESSIONID=5D15LAF18ADFF10 HTTP/1.1" 404 728 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-68product_id=215w-01-
http://buttercup-shopping.com/category.screen?category_id=61VTS&JSESSIONID=5D15LAF18ADFF10 HTTP/1.1" 404 728 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-68product_id=215w-01-

```

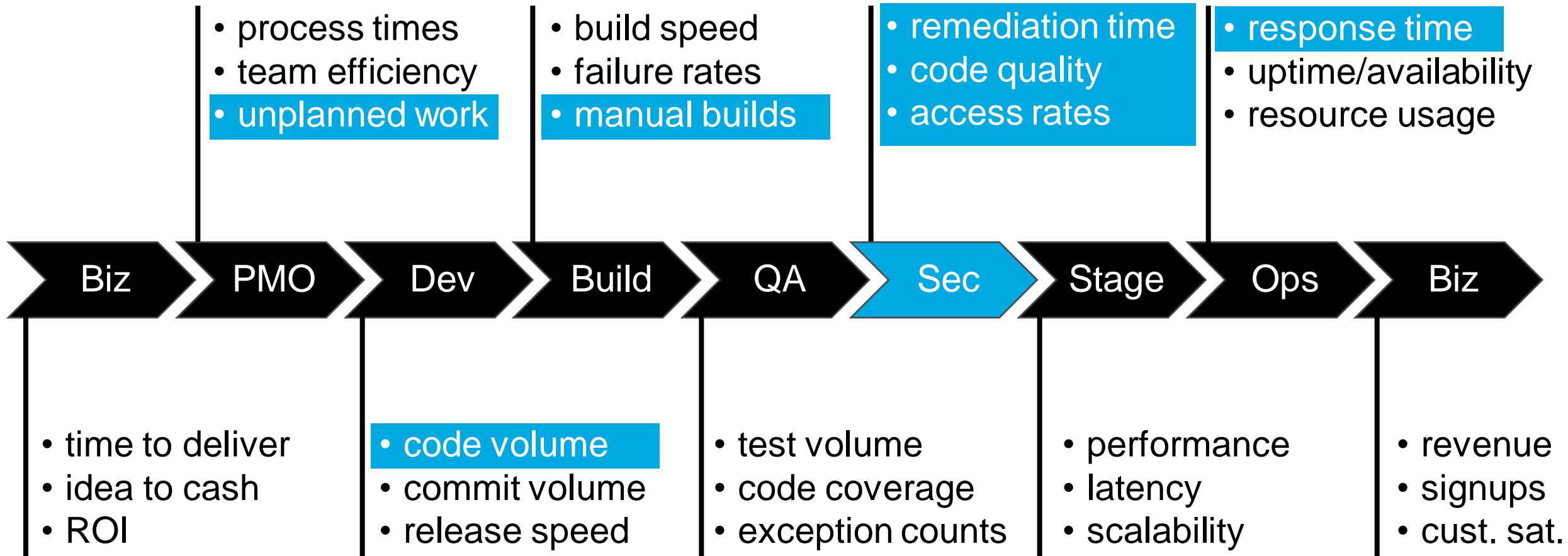
Shared Data for Multiple Stakeholders



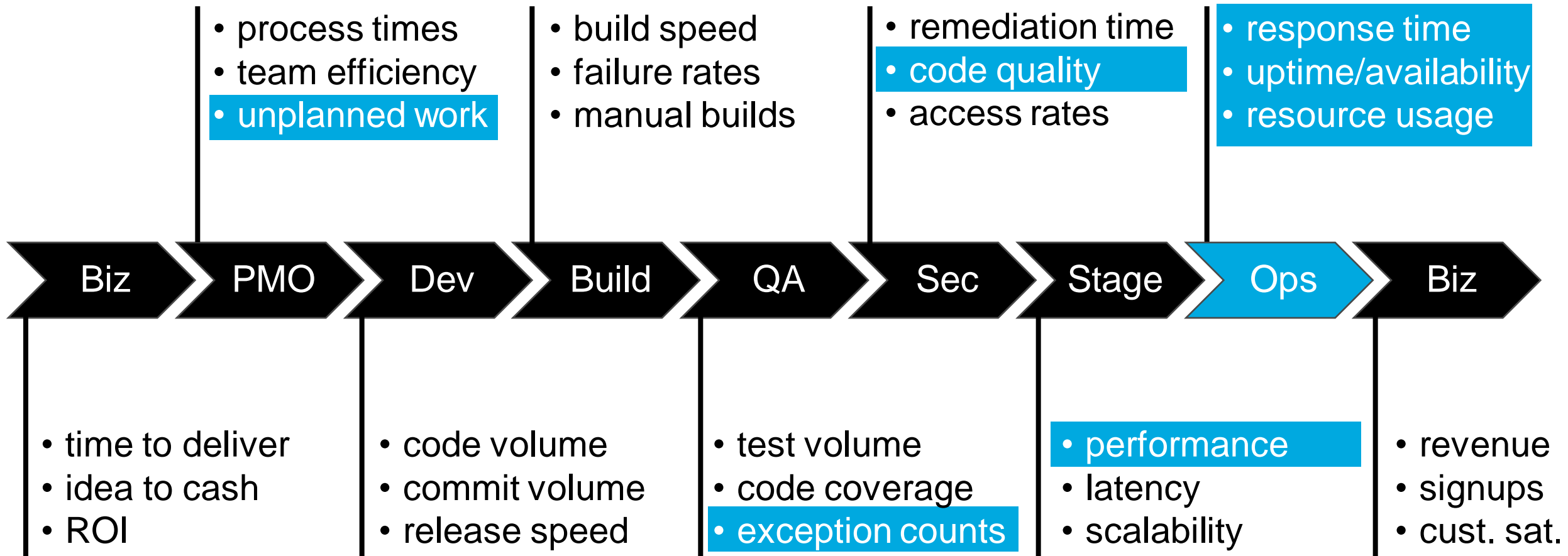
Shared Data for Multiple Stakeholders



Specific Data For Each Stakeholder



Specific Data For Each Stakeholder





City of Los Angeles: Sharing Security Intel Across 40+ Agencies

“As the number and sophistication of risks increase, our cloud-based Splunk solution levels the playing field by making our security team more effective.”

– *Chief Information Security Officer, City of Los Angeles*

- ▶ Prompt responses to cyberthreats with real-time situational awareness of citywide infrastructure
- ▶ Timely intelligence sharing with local, state and national law enforcement
- ▶ Reduced Total Cost of Ownership

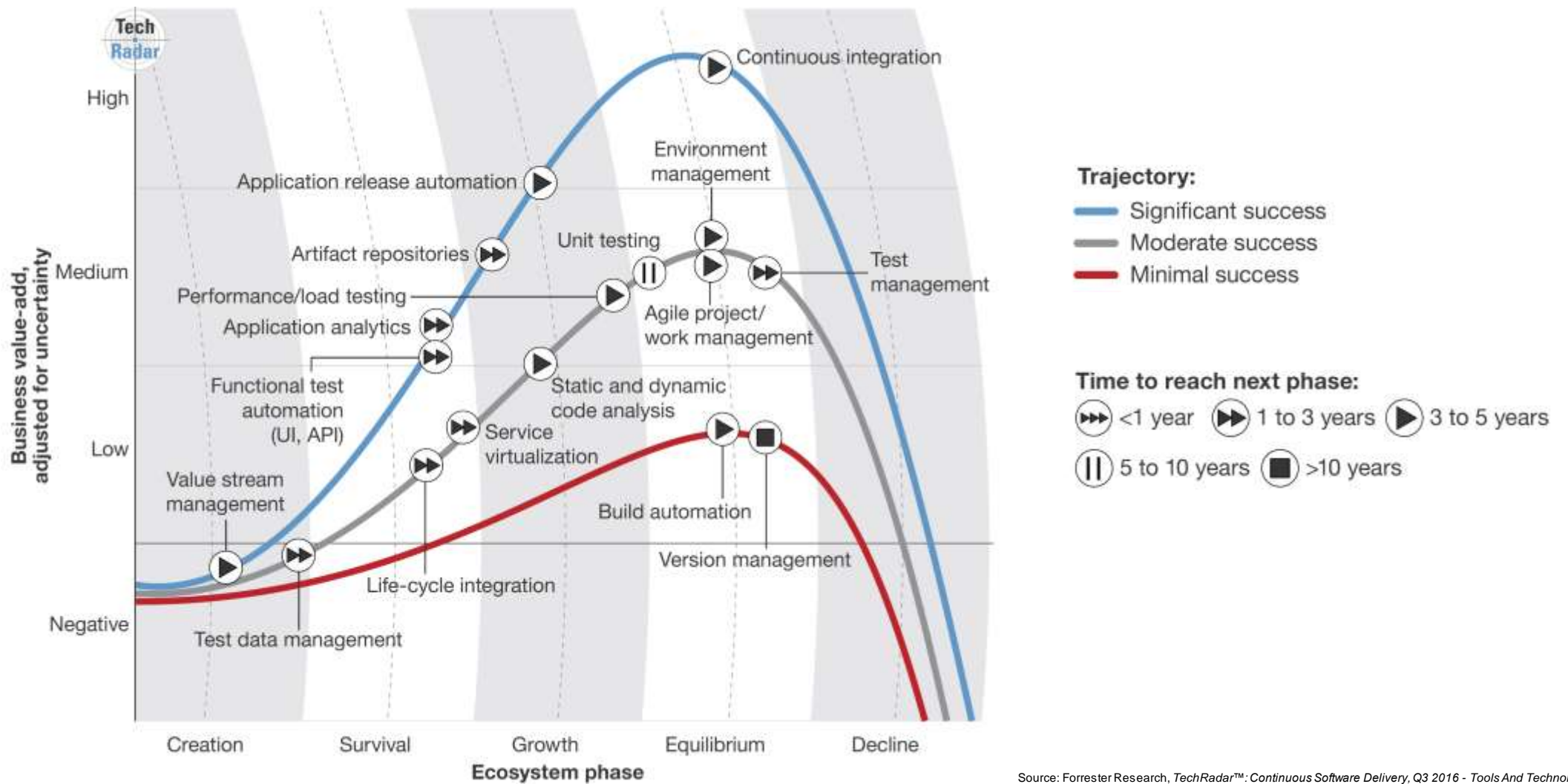
Data-driven automation

coupling data analytics with process automation to surface actionable data points, make real-time decisions, and act to remediate

Automate Dev and Ops Activity



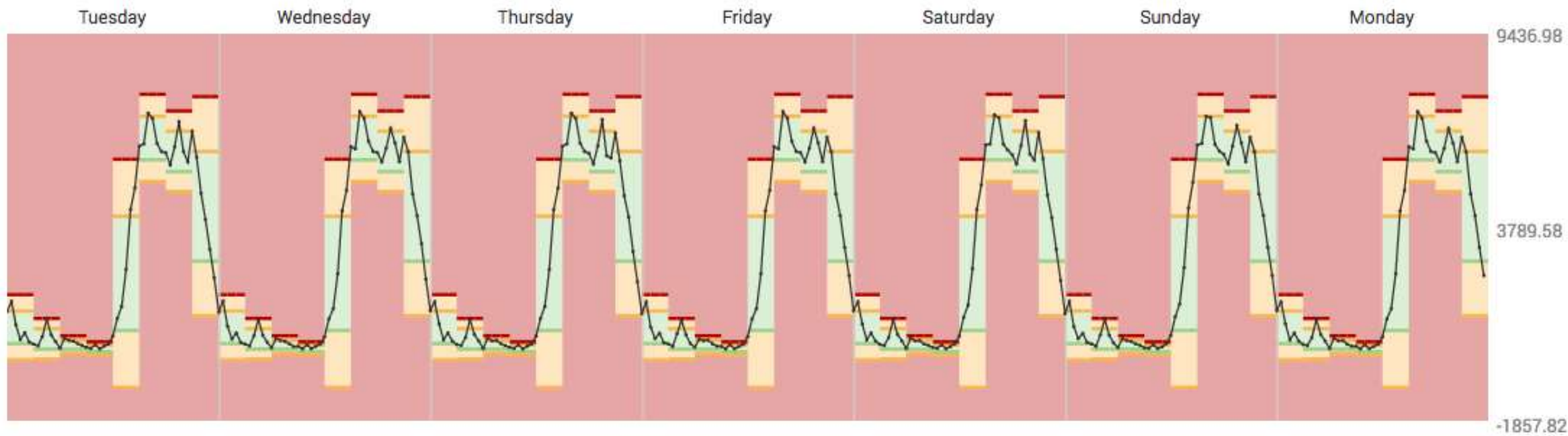
Automation in the SDLC



Source: Forrester Research, TechRadar™: Continuous Software Delivery, Q3 2016 - Tools And Technology: The Modern Application Delivery Playbook, by Diego Lo Giudice and Kurt Bittner, August 31, 2016

Detect Patterns, Anomalies with Machine Learning

Preview Aggregate Thresholds



138.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=61VTS&JSESSIONID=SD15LAF18ADFF10 HTTP 1.1" 404 728 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-0&product_id=PI_0W_01-
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FFADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-20&product_id=PKA-01-0-
ows NY 27.168.0.0 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=61VTS&JSESSIONID=SD15LAF18ADFF10 HTTP 1.1" 404 728 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-0&product_id=PI_0W_01-
itemId=EST-16&product_id=RP-LI-02" 468 125.17 14.1 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-20&product_id=PKA-01-0-
://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-20&product_id=PKA-01-0-
shopping.com/cart.do?action=purchase&itemId=EST-20&product_id=PKA-01-0-
://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-20&product_id=PKA-01-0-

Learn What's Normal and Abnormal

The screenshot displays the Splunk ITSI Anomaly Detection interface. On the left, a sidebar lists various KPIs under 'Service Health', including 'CPU Utilization: % User' (selected), 'DB Service Errors', 'DB Service Queues', 'DB Service Response Time', 'Memory Free: % System', 'Storage Free Space: % System', and 'Storage Operations: Total'. The main area is titled 'Anomaly Detection' and contains the following information:

- ITSI Anomaly Detection:** A descriptive paragraph explaining that it learns normal patterns in real-time and alerts on deviations.
- Analysis Time Window:** Set to 'Last 7 days' with an 'Analyze KPI Data' button.
- Trending Anomaly Detection:** Shows an 'Algorithm Analysis Result' of 'Recommended' (green checkmark) and an 'Enable Trending AD Algorithm' toggle set to 'Yes'.
- Analysis Breakdown:** A table showing 'Percentage of Time Anomalies were Detected: 3% (Expected <15%)'.
- Trending AD Preview:** A line graph titled 'Trending AD Preview - KPI Value for Last 7 Days' showing a blue line for 'KPI Value' and red dots for 'Detected Anomaly' over the period from Mon Jul 25 to Mon Aug 1, 2016.
- Entity Cohesion Anomaly Detection:** Shows an 'Algorithm Analysis Result' of 'Not Recommended' (red X) and an 'Enable Cohesive AD Algorithm' toggle set to 'No'.
- Analysis Breakdown:** A table showing 'Entities Analyzed: 67', 'Entities with Detected Anomalies: 39', 'Average Anomalies Per Entity: 16.3', 'Percentage of Time Anomalies were Detected: 5.8% (Expected <3%)', and 'Percentage of Data Points with Anomalies: 7.3% (Expected <10%)'.
- Cohesive AD Preview:** A line graph titled 'Cohesive AD Preview - Top 5 Entities With Most Anomalies for Last 7 Days' showing multiple colored lines for different entities (web-server1, web-server2, web-server3) and red dots for 'Detected Anomaly' over the same time period.

Baseline normal operations and alert on anomalous conditions

Identify abnormal trends and patterns in KPI data

138.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=61&product_id=61 HTTP/1.1" 404 728 "http://buttercup-shopping.com/cart.do?action=view&item_id=EST-6&product_id=61" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322) 468 125.17.14.108

Integrate ML With Existing Workflows

The screenshot displays a Splunk incident management interface. At the top right, there is a 'Show Timeline' dropdown. Below it, filters for 'Medium', 'New', and 'Unassigned' are visible. The main content area shows an incident titled 'Cross Tier Response Time - Rule' with a date of 'Thu A'. A context menu is open over the incident, listing actions: 'Create ServiceNow Ticket', 'Ping host', 'Run a script', and 'Send email'. Below the incident title, there are tabs for 'Overview', 'Comments', and 'Activity'. The 'Description' section contains the text: 'Cross Tier Response Time - Rule status was high (Health Score=30.91) at 2016-08-25 16:09:00.000 PM'. The 'Contributing KPIs' section includes 'Open all in Deep Dive' and a list of KPIs: 'Middleware Service Response Time' and 'Web Service Response Time'.

Automatically initiate defined incident and remediation responses

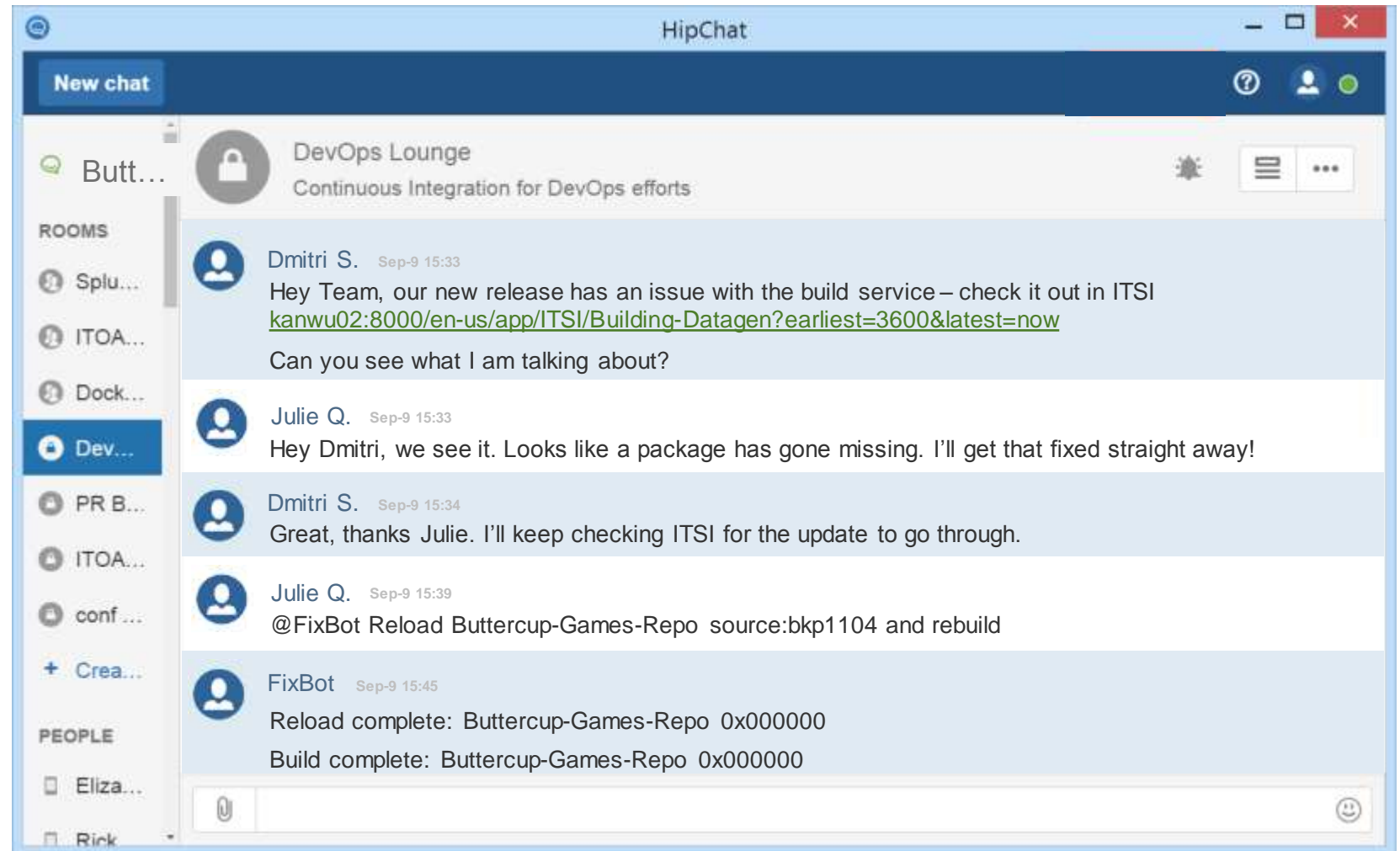
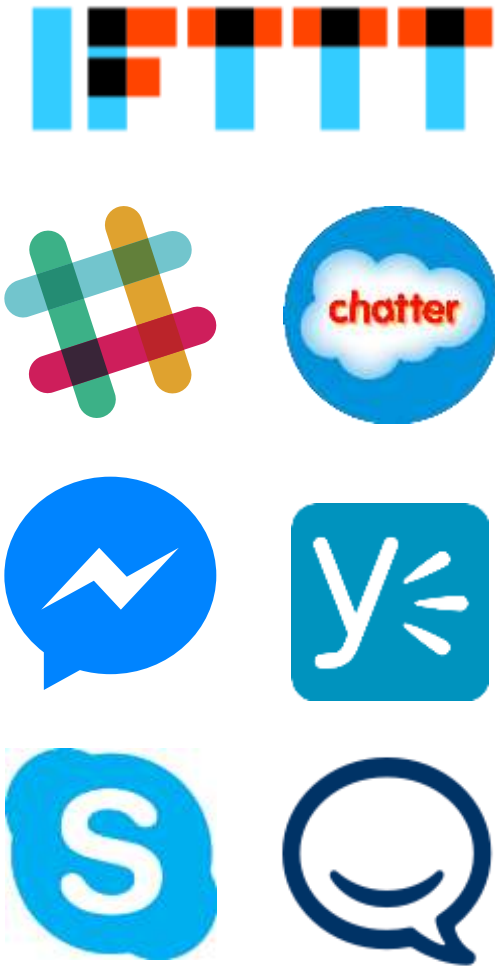
Integrate with ServiceNow to create tickets and accelerate triage

Use Adaptive Responses to Security Breaches

The screenshot shows the Splunk Adaptive Responses interface. At the top, there is a 'Category' dropdown menu set to 'All' and a search bar. Below this, a list of responses is displayed, each with an icon, a title, a description, and a metadata string. The responses listed are:

- STM Stream Capture**: Creates stream capture. Category: Information Gathering | Task: create | Subject: network.capture | Vendor: Splunk
- Nbtstat**: Runs the nbtstat command. Category: Information Gathering | Task: scan | Subject: device | Vendor: Operating System
- DNS Nslookup**: Runs the nslookup command. Category: Information Gathering | Task: scan | Subject: device | Vendor: Operating System
- PAN : Block Traffic**: Category: Device Control | Task: update | Subject: network | Vendor: PAN
- PAN : Quarantine Host**: Category: Device Control | Task: update | Subject: network | Vendor: PAN
- PAN : Tag to Dynamic Address Group**: (partially visible)

Integrate Data, Chat, Bots for Collaborative Troubleshooting and Triage (aka 'ChatOps')





Wrap-up

Q&A, Summary, Close

Thank You!

Questions?

