

A black silhouette of a fox is positioned on the left side of the slide, facing right. The fox's body is partially obscured by the large white text. The background is a solid orange color.

Monitoring: Finding Your Story

Lee Fox
@FoxInATX



A large black silhouette of a fox is positioned on the left side of the slide, facing left. It serves as a background element for the text.

Lee Fox

- **Cloud Architect at Infor**
- **Agile, DevOps, ChatOps evangelist**
- **Past Technology Chair of Agile Austin**
- **Alexa and Google Home Developer**
- **Co-Author of Effect Gradle Implementation Video Series on Packt**
- **Trained Innovation Games Facilitator**
- **Amateur Chef**

Housekeeping

- **Ask questions freely**
- **I'm quite interruptible**
- **Deeper questions may be deferred to the end**

Agenda

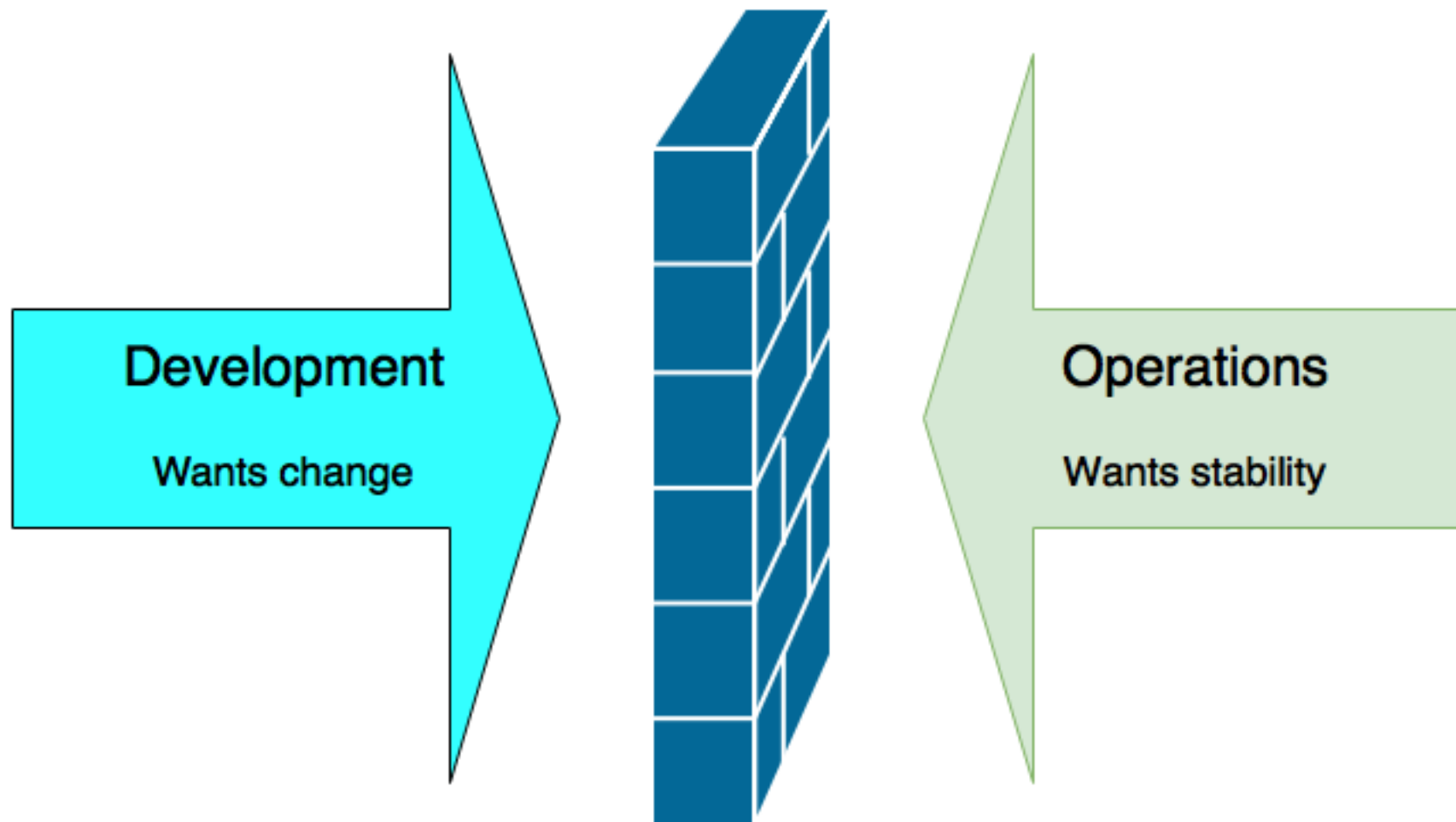
- **What is DevOps**
- **The problem with monitoring**
- **Dealing with the problem**

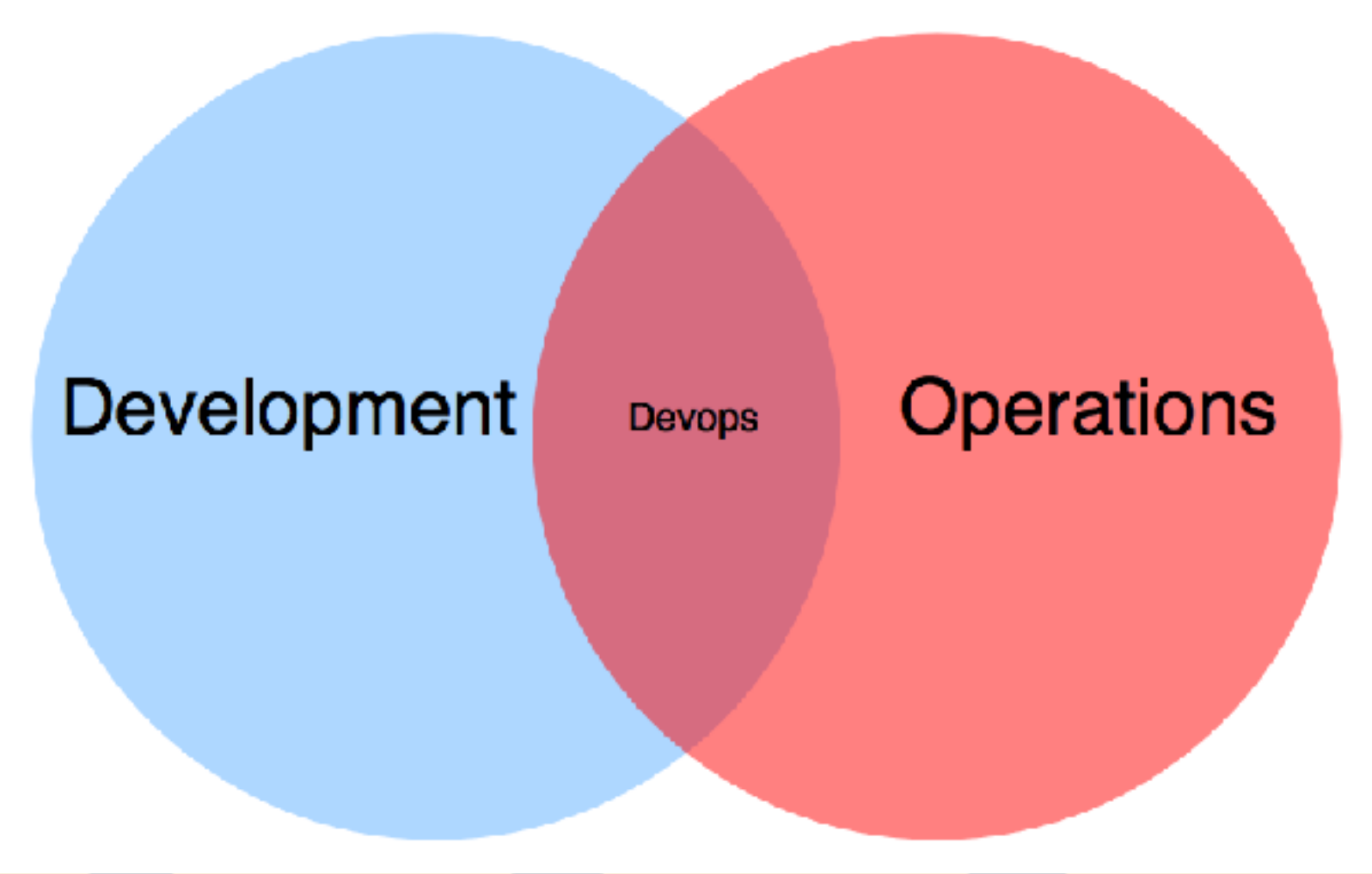
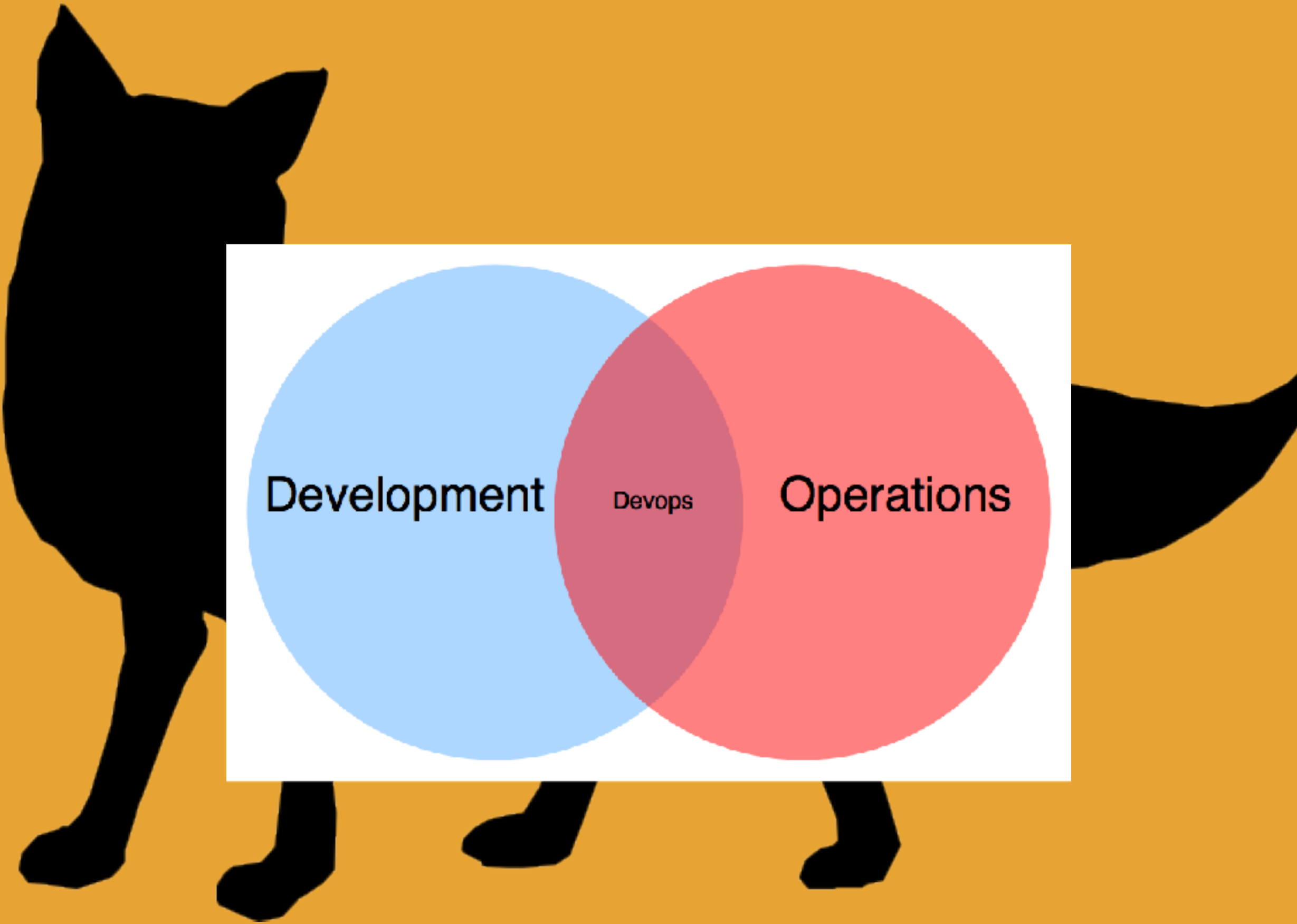
What is DevOps?

- **Not a methodology**
- **Not a process**
- **Not something developers do**
- **Not something operators do**
- **Not a person**
- **Not a team**
- **Not a set of scripts**

A solid black silhouette of a cat in a standing, alert pose, facing left. The cat's tail is long and slightly curved. The entire image is set against a solid orange background.

It's a philosophy!

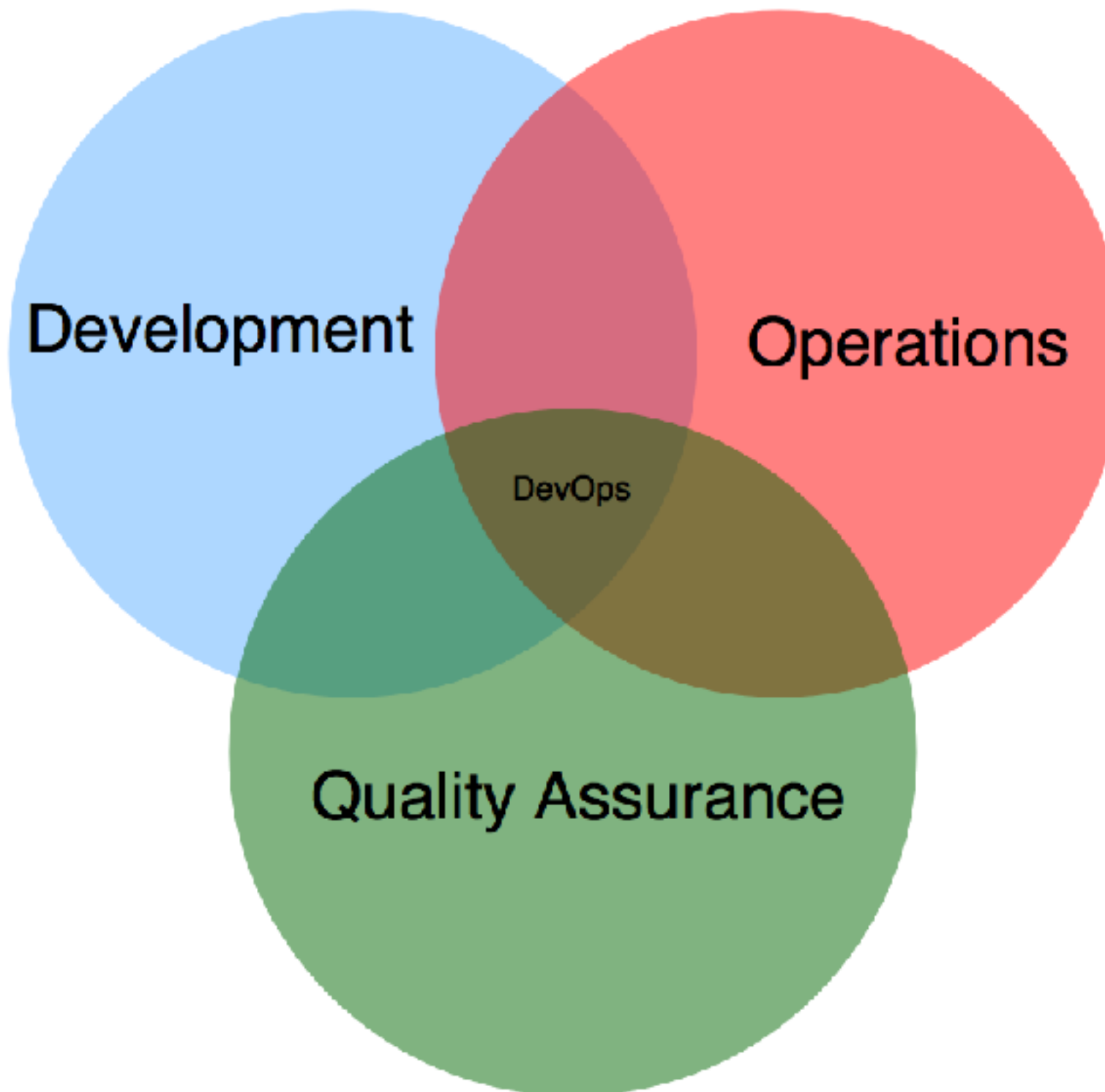


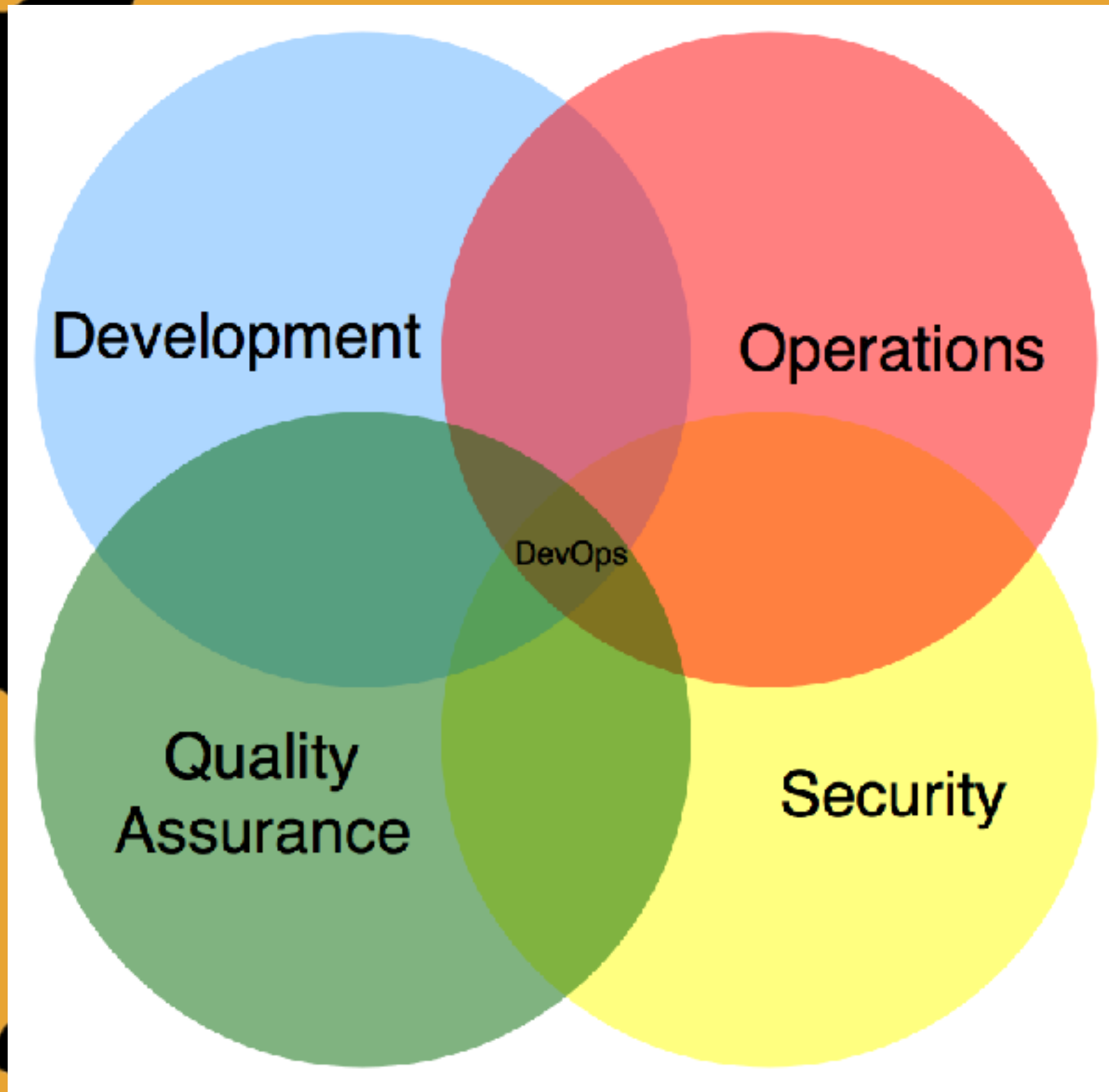


Development

Devops

Operations





Who knows what S.E.T.I. is?



?ETI
•
INSTITUTE

S.E.T.I.

- **Search for Extraterrestrial Intelligence**
- **Began February 1, 1985**
- **Monitors electromagnetic radiation for signs of intelligent life**

Huge problem set

- **$1.0 * 10^{24}$ stars in the universe**
- **Ideally to find at least one with life**

Today's monitoring problem



- **Metrics**
 - **CPU Usage**
 - **Memory Usage**
 - **Disk space**
- **3 metrics**

***Fox's Most
Excellent Application***

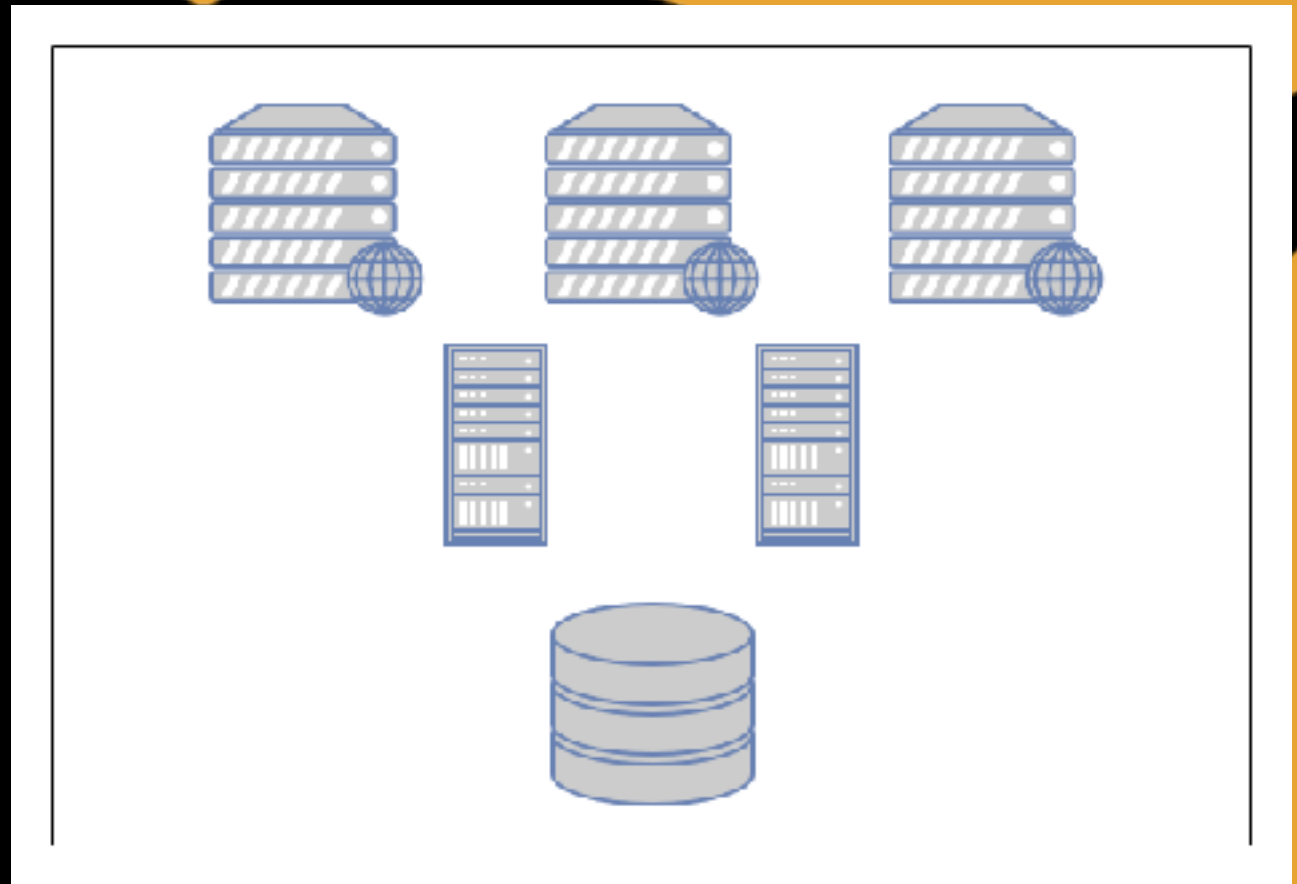
Today's monitoring problem

- **3 tiered system**
- **3 metrics**
- **times 3 tiers**
- **9 metrics**



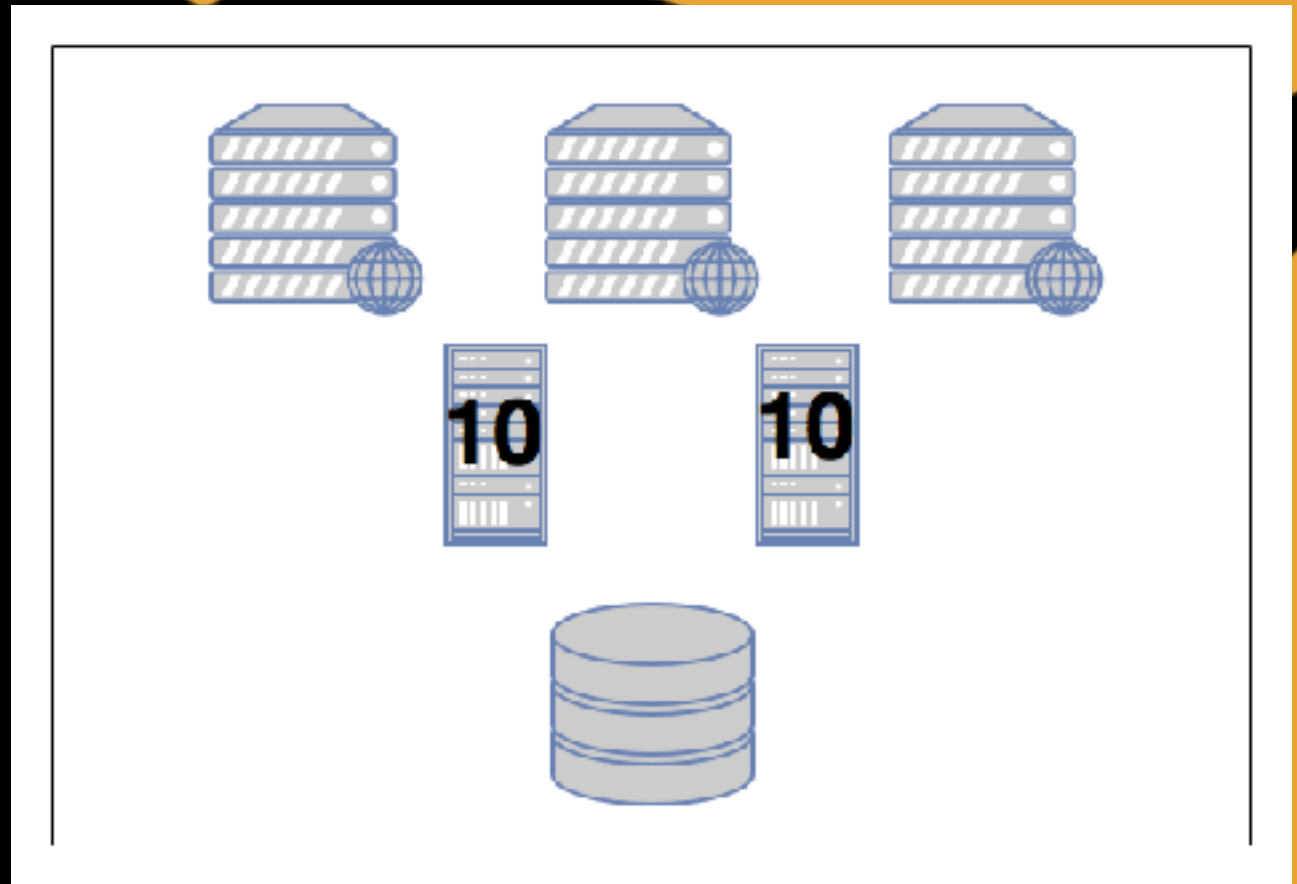
Today's monitoring problem

- **We scaled!**
- **3 metrics**
- **times 6 VMs**
- **18 metrics**



Today's monitoring problem

- **Added docker**
- **3 metrics**
- **times 24 containers**
- **72 metrics**



Today's monitoring problem

- **Per hour: 1,728 metrics**
 - **72 metrics * 24 hours**
- **Per minute: 103,680 metrics**
 - **72 metrics * 24 hours * 60 minutes**
- **Per second: 6,220,800 metrics**
 - **72 metrics * 24 hours * 60 minutes * 60 seconds**



A black silhouette of a cat is positioned on the left side of the slide, facing right. The cat's body is elongated, and its tail is long and curved. The text is overlaid on the cat's body.

Modern day applications
can easily generate 10+
millions metrics daily

It's a real problem

- **Humans have a cognitive limitation for big numbers**
- **We can easily visualize 5 things**
- **We might be able to visualize 100 things**
- **Beyond that, we're generally lost**

How many people are here?



How many people are here?



How many people are here?



Still unsure of this



Some vocabulary

- **Monitoring**
- **Alerting**
- **Paging**

Monitoring

- 
- A black silhouette of a cat is positioned on the left side of the slide, facing left. The cat's body extends across the middle of the slide, and its long tail curves towards the right. The text of the list is overlaid on the cat's body.
- **Simply keeping a watch on your application or system**
 - **Watching for metrics**
 - **Watching for events**

Alerting

- **Send some notification when a threshold has been met**
- **Can't have alerting without monitoring**

Paging

- **Actually notifying someone a person when an alert is generated**
- **Can't have paging without alerting**

Break Down the Metrics

- **Work Metrics**
- **Resource Metrics**
- **Events**

Work Metrics

- **Throughput**
- **Errors**
- **Efficiency**

Resource Metrics

- **CPU Utilization**
- **Memory Usage**
- **Disk Space Free**

Events

- **Scale Up/Scale Down**
- **Login/Logout**
- **Software Deployments**
- **Start of Day/End of Day**
- **Backup Running**

A solid black silhouette of a cat in a standing, alert pose, facing left. The cat's tail is long and curved upwards. The entire image is set against a solid orange background.

Find Your Story

Why a Story?

- **Express meaning**
- **Easy to communicate**
- **Easy to remember**
- **Draw a morale**
- **Determine if relevant**

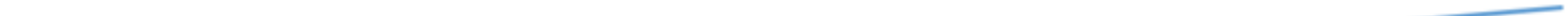
A black silhouette of a cat is positioned on the left side of the slide, facing right. It is standing on all fours with its tail slightly curved. The background is a solid orange color.

Build a Story

- **Metrics convey meaning**
- **More details make for a richer story**
- **Draw meaning from your story**

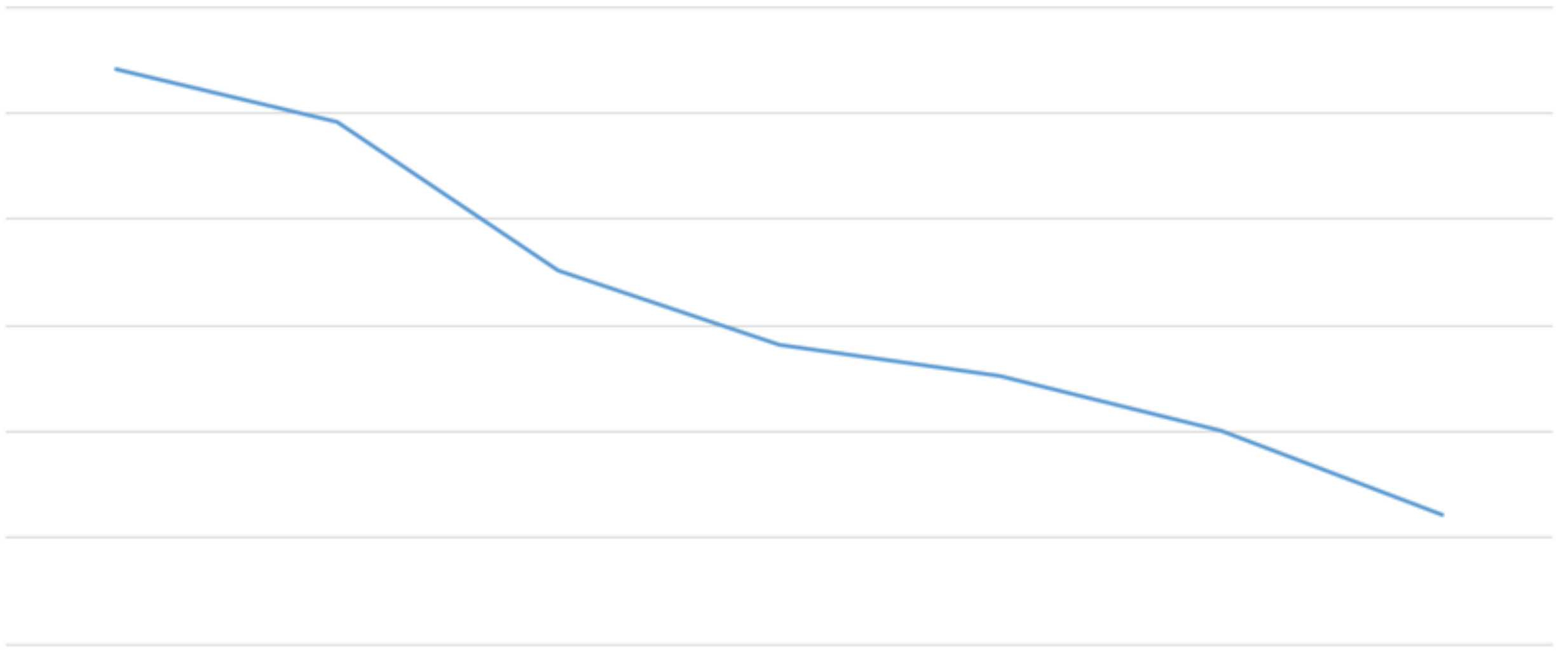
My Development Story

Coverage

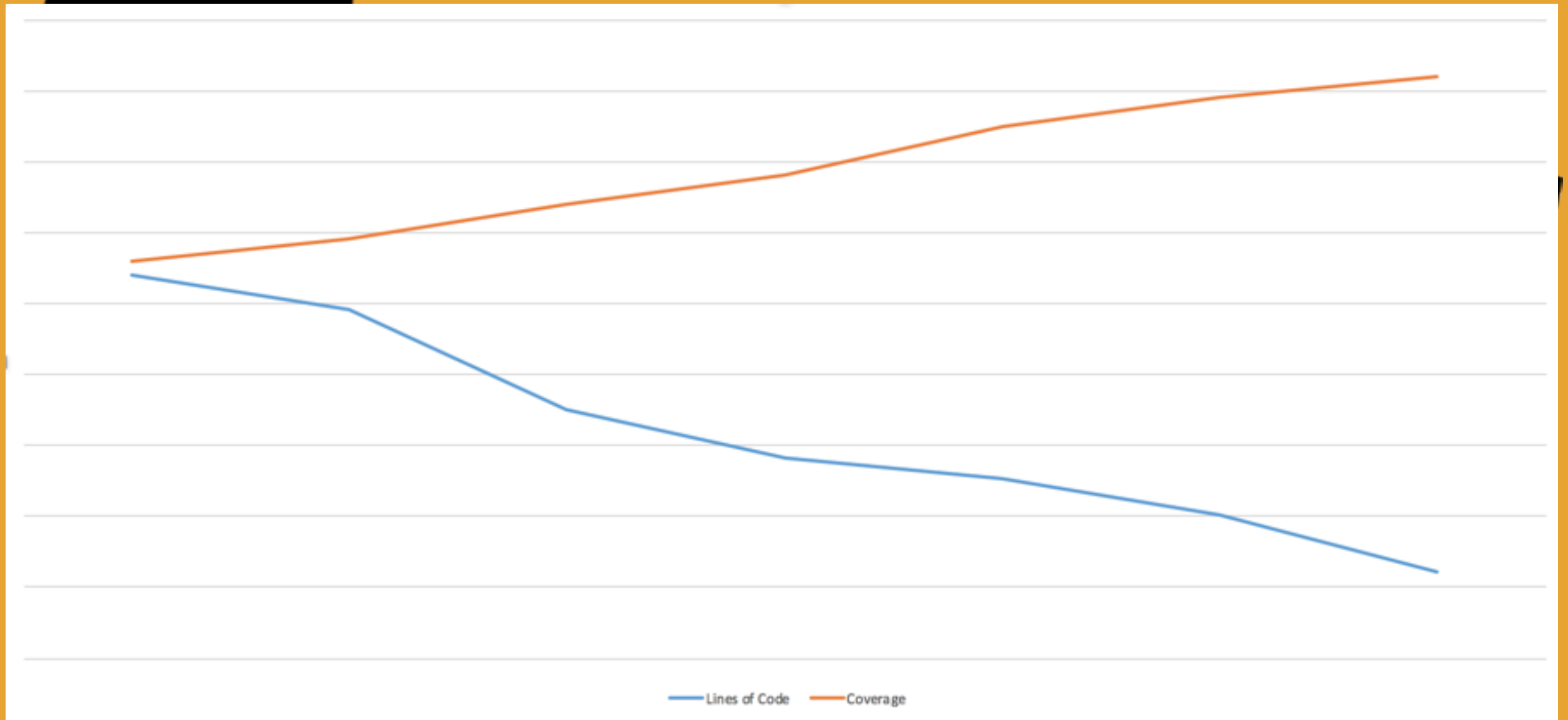


My Development Story

Lines of Code



My Development Story



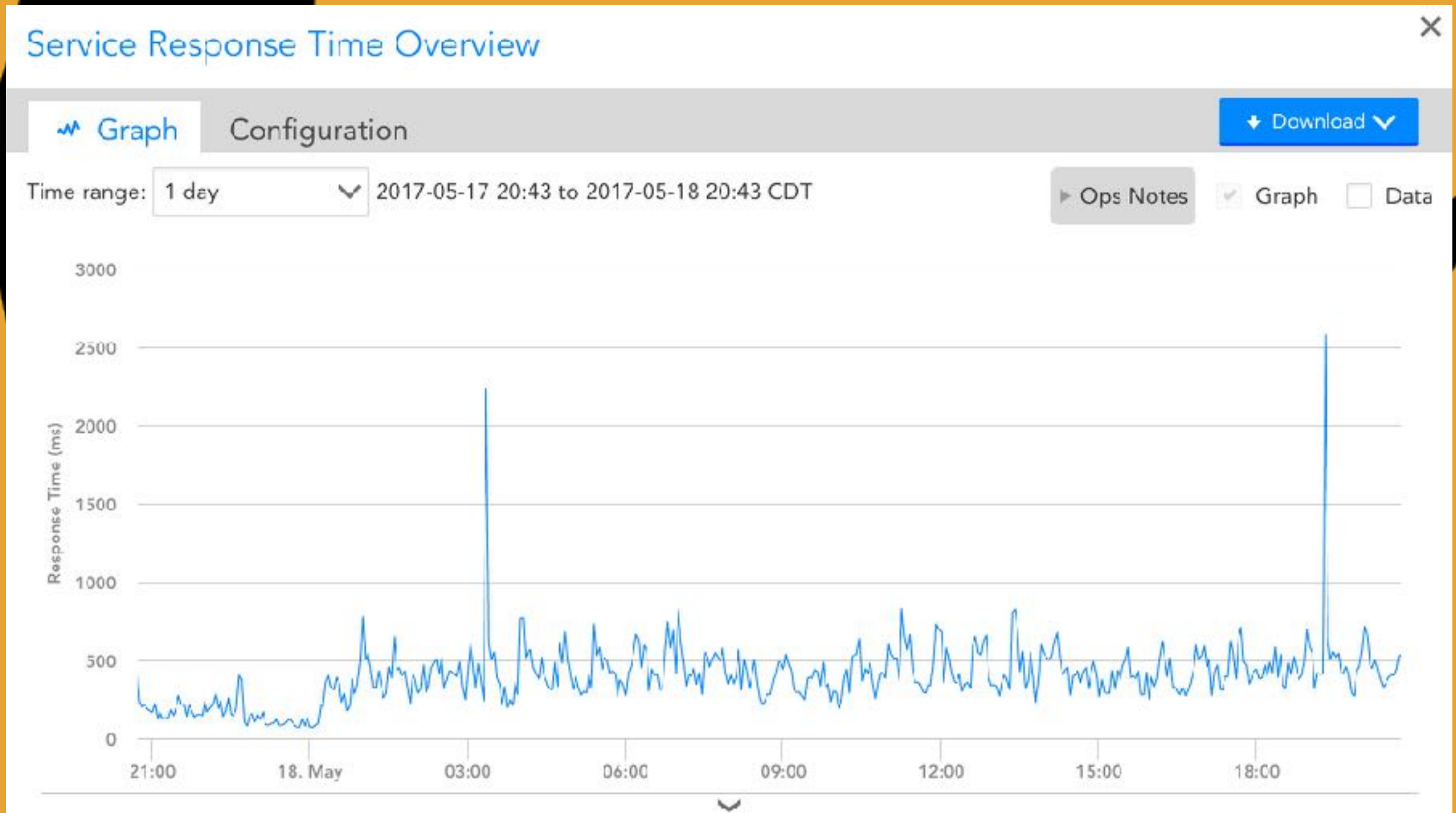
What does it mean?

- **Amount of code is shrinking**
- **Percentage of tested code is growing**
- **Possible: Remove Cruft**
- **Possible: Increasing DRY**
- **Unlikely: New features are added**

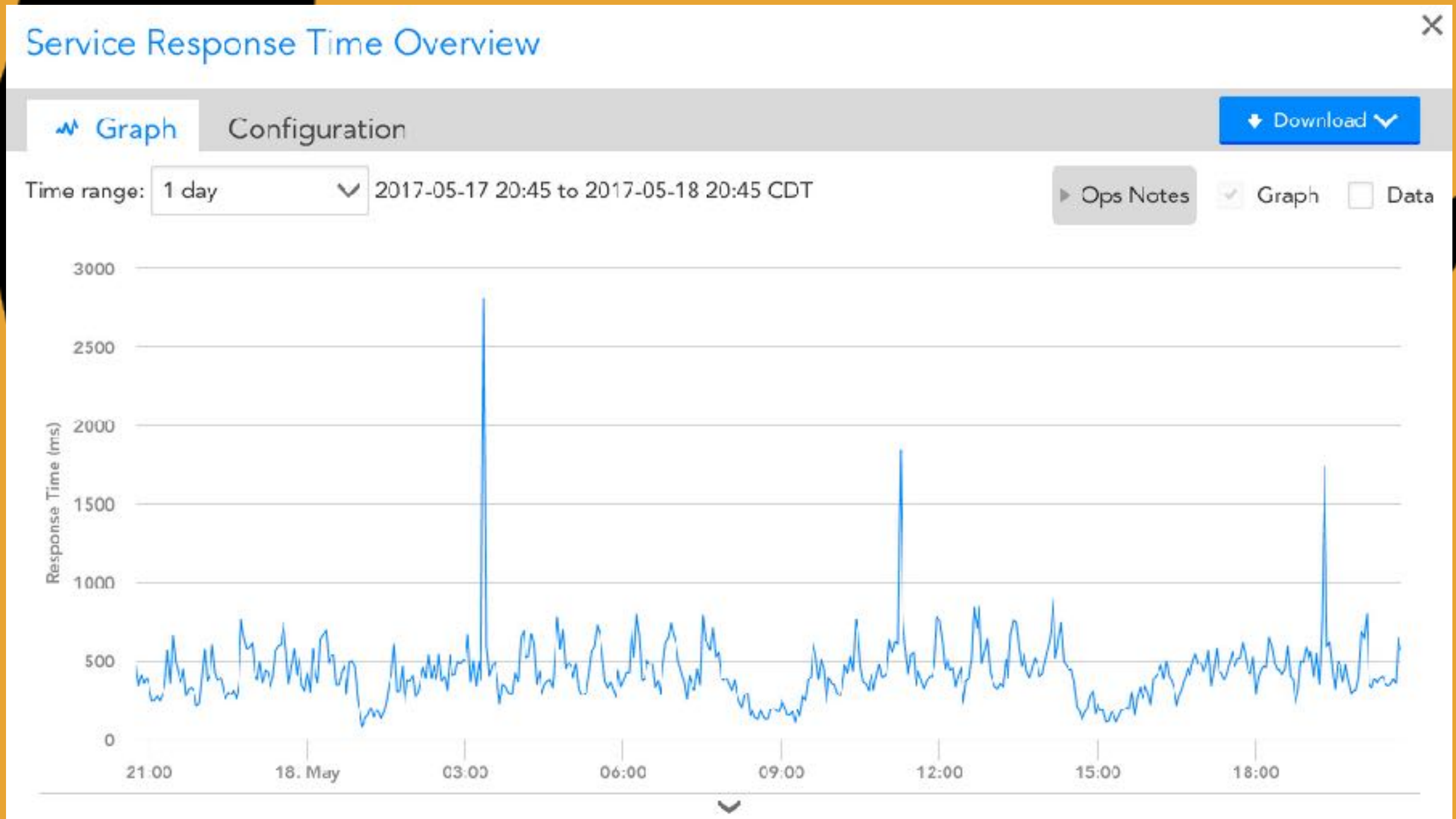
A solid black silhouette of a cat in a standing, alert pose, facing left. The cat's tail is long and curved upwards. The entire silhouette is set against a solid orange background.

An Operational Story

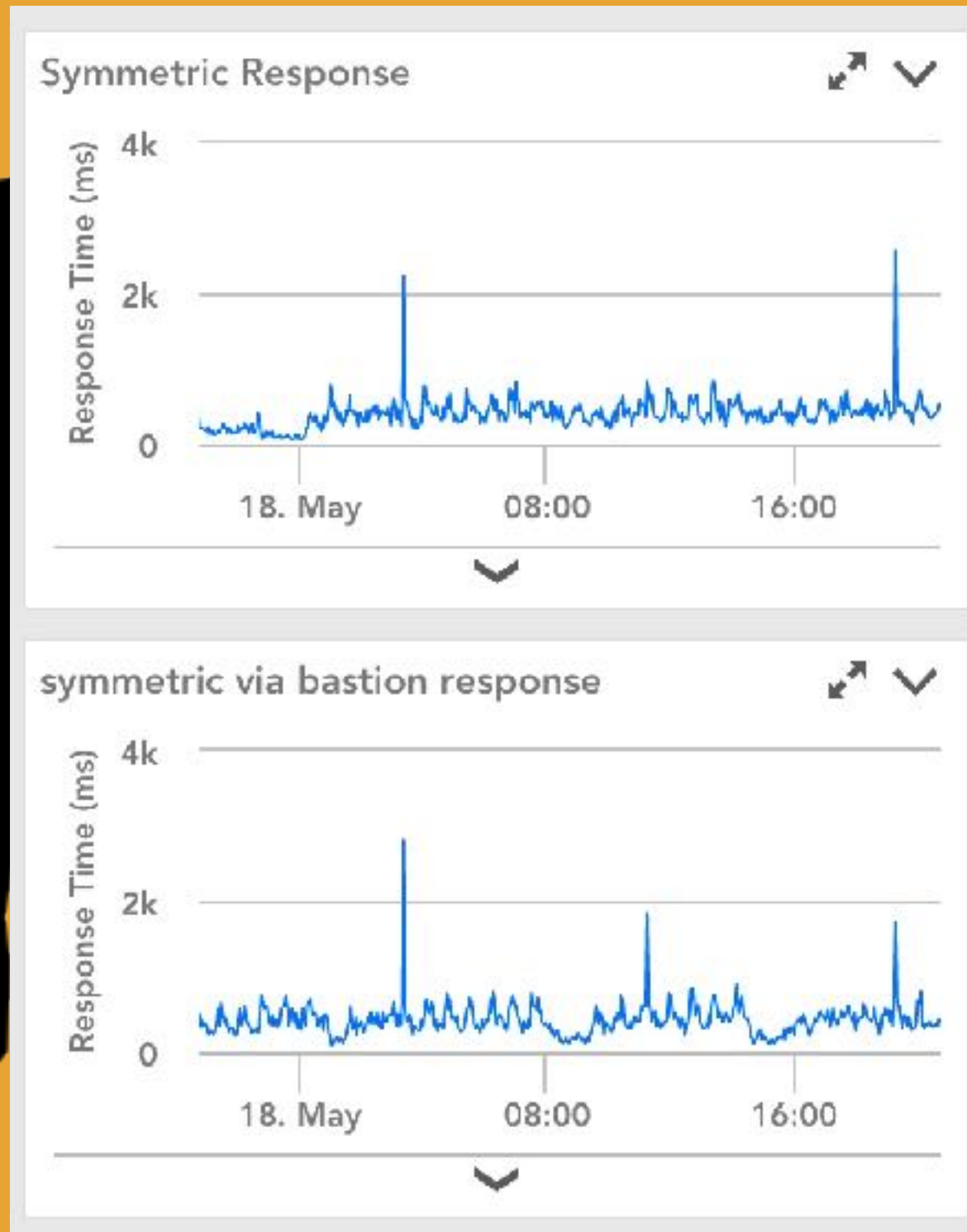
My Operational Story



My Operational Story



My Operational Story



What does it mean?

- **Debugging Story**
- **Network problems if direct good, but bastion bad**
- **Application issue if both bastion and direct are bad**
- **How efficient bastion is performing if both are good**

How to build your story

- **Determine what you want**
- **Start with the details**
- **Start with your vision**
- **Gather your metrics**
- **Tell your story**

Determine what you want

- **Killing time**
- **Persuasion**
- **Information**

Start with the details

- **Focus on a single metric**
- **Add more detail a little at a time**

Start with the vision

- **Compelling reason**
- **Look for supporting detail**

Gather your metrics

- **Resource metrics from monitoring systems**
- **Work metrics from monitoring/logs**
- **Events from logs/ALM**

A black silhouette of a cat is positioned on the left side of the slide, facing right. The cat's body is elongated, with its front legs extended forward and its hind legs slightly behind. The tail is long and curved, extending towards the right edge of the slide. The cat's head is turned slightly towards the viewer, with its ears pointed upwards. The entire silhouette is set against a solid orange background.

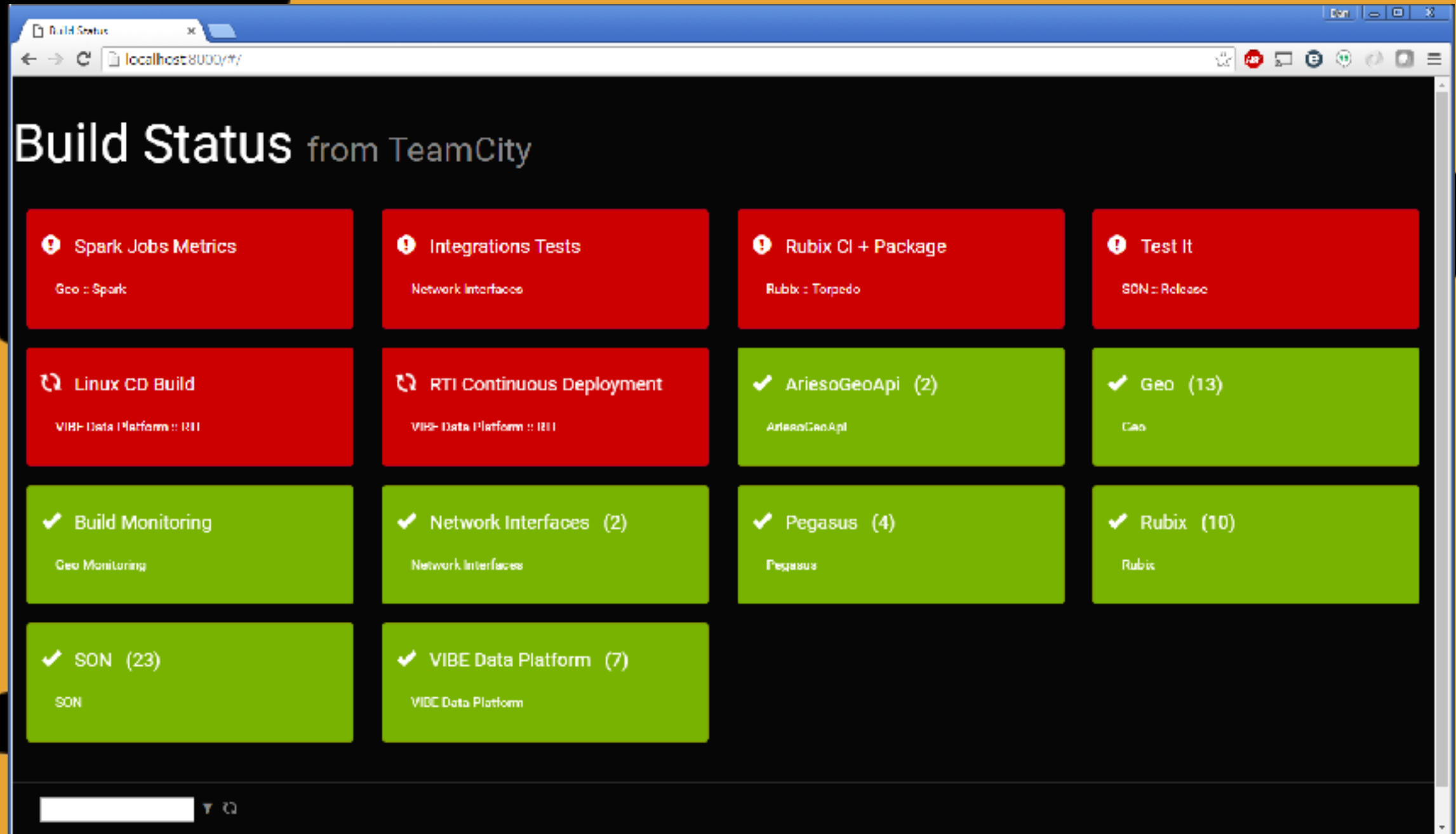
Tell your story

- **Determine the style**
- **Determine the medium**
- **Publish it**

What to do with your story

- **Share them**
- **Action on them**

Information Radiator



Information Radiator



Chatops



jmaupetit 11:46
hubot deploy tailordev-landing



hubot BOT 11:46 ☆
#4376239 - tailordev-landing / master / production
#4376239 : jmaupetit is deploying tailordev-landing to production.

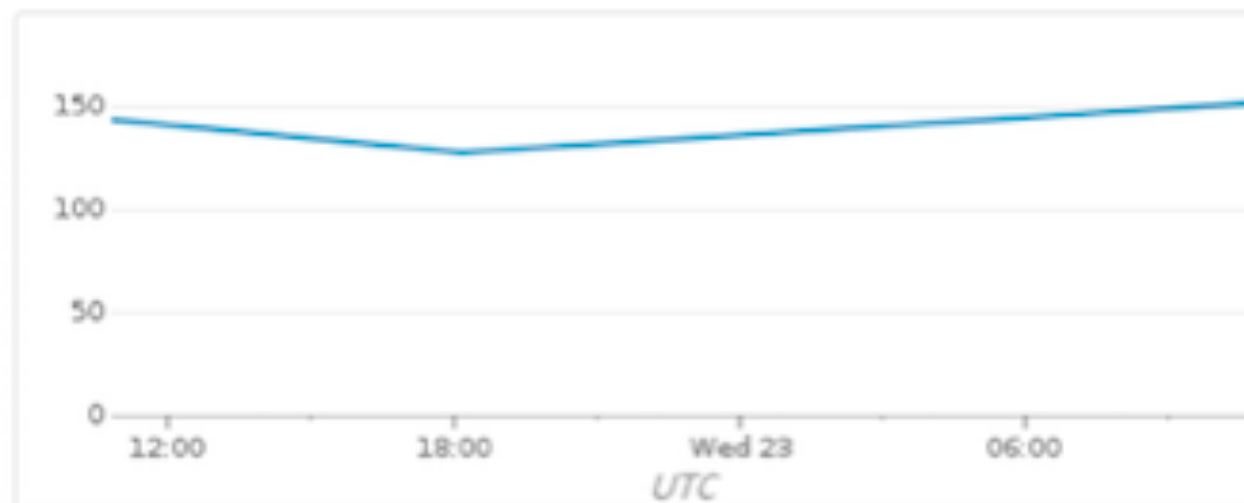
#4376239 : jmaupetit's production deployment of tailordev-landing is done!



jmaupetit 11:49
hubot graph-deploy:td



hubot BOT 11:49
https://p.datadoghq.com/snapshot/view/dd-snapshots-prod/org_50123/2016-03-23/6eea9c279d7ce584303db5899a097ab7ca66149a.png (5KB) ▼



Action on your stories

- **Set up an alert**
- **Set up a page**
- **Create a plan of action**

A solid black silhouette of a cat in a standing, alert pose, facing left. The cat's tail is long and curved upwards. The entire silhouette is set against a solid orange background.

What makes a good
monitoring story?

Good monitoring stories

- **Intuitive**
- **Fast to read**
- **People want to know it**
- **Enable C.A.M.S.**
- **Single Pane of Glass***

A solid black silhouette of a cat in a standing, alert pose, facing left. The cat's ears are pointed, and its tail is long and slightly curved. The silhouette is centered horizontally and occupies most of the frame.

A few suggestions

Avoid Clutter

SecurityCenter

Dashboard ▾ Analytics ▾ Scores ▾ Reporting ▾ Assets ▾ Workflows ▾ Users ▾

PCI Continuous Monitoring

Switch Dashboard ▾ Options ▾

PCI Monitoring - Mitigated Vulnerabilities by Severity

	Mitigated v1.00	Mitigated v2.00	Mitigated v3.00
Total Vulnerabilities	62%	5%	8%
Critical	88%	1%	1%
High	81%	7%	7%
Medium	68%	7%	10%
Low	78%	7%	14%

Last Updated: 23 hours ago

PCI Monitoring - Most Vulnerable Hosts

IP Address	OS	Score	Total	Vulnerability
192.168.1.100	Windows Server 2016 Standard	4040	571	11
192.168.1.101	Windows Server 2016 Standard	4070	580	12
192.168.1.102	Windows Server 2016 Standard	4040	580	12
192.168.1.103	Windows Server 2016 Standard	4020	591	13
192.168.1.104	Linux	4040	590	14

Last Updated: 4 hours ago

PCI Monitoring - Most Mitigated Vulnerabilities

Plugin ID	Name	Severity	Total
000001	Windows 10: Security Updates (000001)	High	50
000002	Windows 10: Security Updates (000002)	Critical	50
000003	Windows 10: Security Updates (000003)	Critical	50
000004	Windows 10: Security Updates (000004)	High	48
000005	Windows 10: Security Updates (000005)	High	47

Last Updated: 1 hour ago

PCI Monitoring - Vulnerabilities and Compliance Trends



Last Updated: 1 hour ago

PCI Monitoring - Vulnerability Summary

	Mitigated	Unmitigated	Medium	High	Critical
Total	10440	30110	1%	10%	10%
Last 24 Hours	81	6360	20%	20%	20%
Last 7 Days	1200	13800	10%	10%	10%
Last 30 Days	7100	9000	14%	10%	10%
Last 90 Days	10400	11000	10%	10%	10%

Last Updated: 20 hours ago

PCI Monitoring - Configuration Summary

	Passed	Manual Check	Failed
Check Count	11100	10100	4000
Check Ratio	88%	8%	20%
System Count	657	497	0%
System Ratio	87%	64%	15%

Last Updated: 1 hour ago

Understanding Risk - Remediation Capabilities

Reference	Risk Reduction	Hosts Affected
Apply WS18-014: Security Update for Microsoft Windows to Address Remote Code Execution (012422)	2.11%	160
Apply WS18-009: Security Update for Microsoft Graphics Component (014852)	2.01%	161
Apply WS18-046: Security Update for Windows OS (014873)	2.01%	161
Apply WS18-120: Security Update for Microsoft Windows to Address Remote Code Execution (011619)	2.11%	160
Apply WS18-006: Security Update for JET Framework to Address Security Feature Bypass (014119)	2.27%	171

Last Updated: 4 hours ago

OS - Compliance Checks by Keyword

	Systems	Score (Last 7 Days)	Passed	Manual	Failed
All	146	100%	60%	5%	20%
Account	121	100%	21%	4%	18%
Auth	131	100%	61%	3%	20%
Disable	100	100%	84%	4%	12%
Enforce	130	100%	21%	8%	17%
Log	126	100%	61%	4%	20%
Password	110	100%	50%	4%	46%
Permissions	114	100%	35%	7%	23%
User	211	100%	25%	4%	18%

Last Updated: 30 hours ago

PCI Monitoring - Top Failures and Manual Checks

Name	Severity	Total
VMware vCenter/ESXi Compliance Checks Initialization Failed	Medium	274
BS-100-2: 5.4.20.1 It is possible to prevent the device driver for USB storage media from starting up	High	181
Compliance Check Test Error	High	172
BS-100-2: 5.4.21 Preventing unauthorized acquisition of administrator rights - Mode for for administrative accounts	High	151
BS-100-2: 5.4.10 Every SID must be unique - Careful allocation of identifiers	High	140

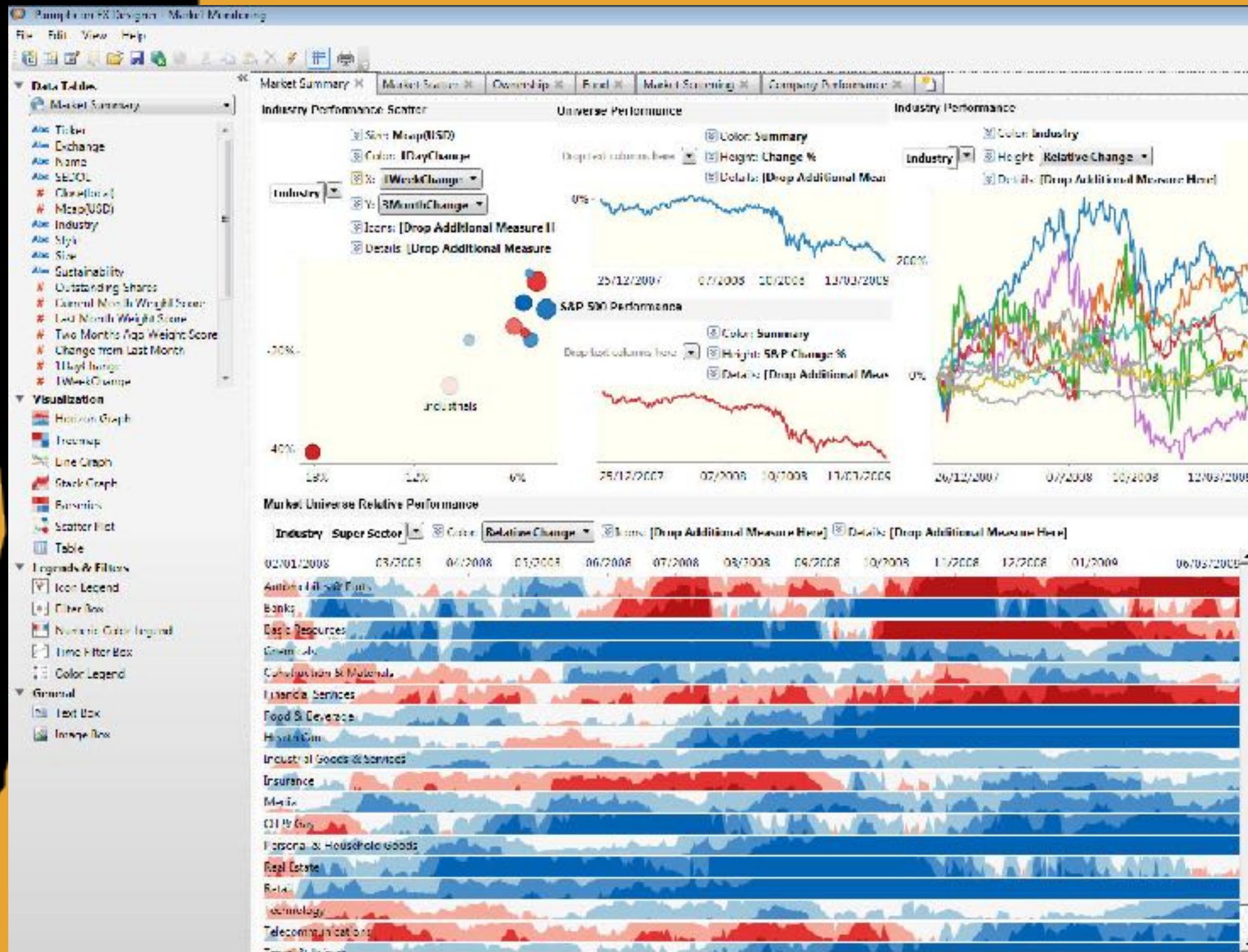
Last Updated: 2 hours ago

Priorities - Top Hosts with Compliance Concerns

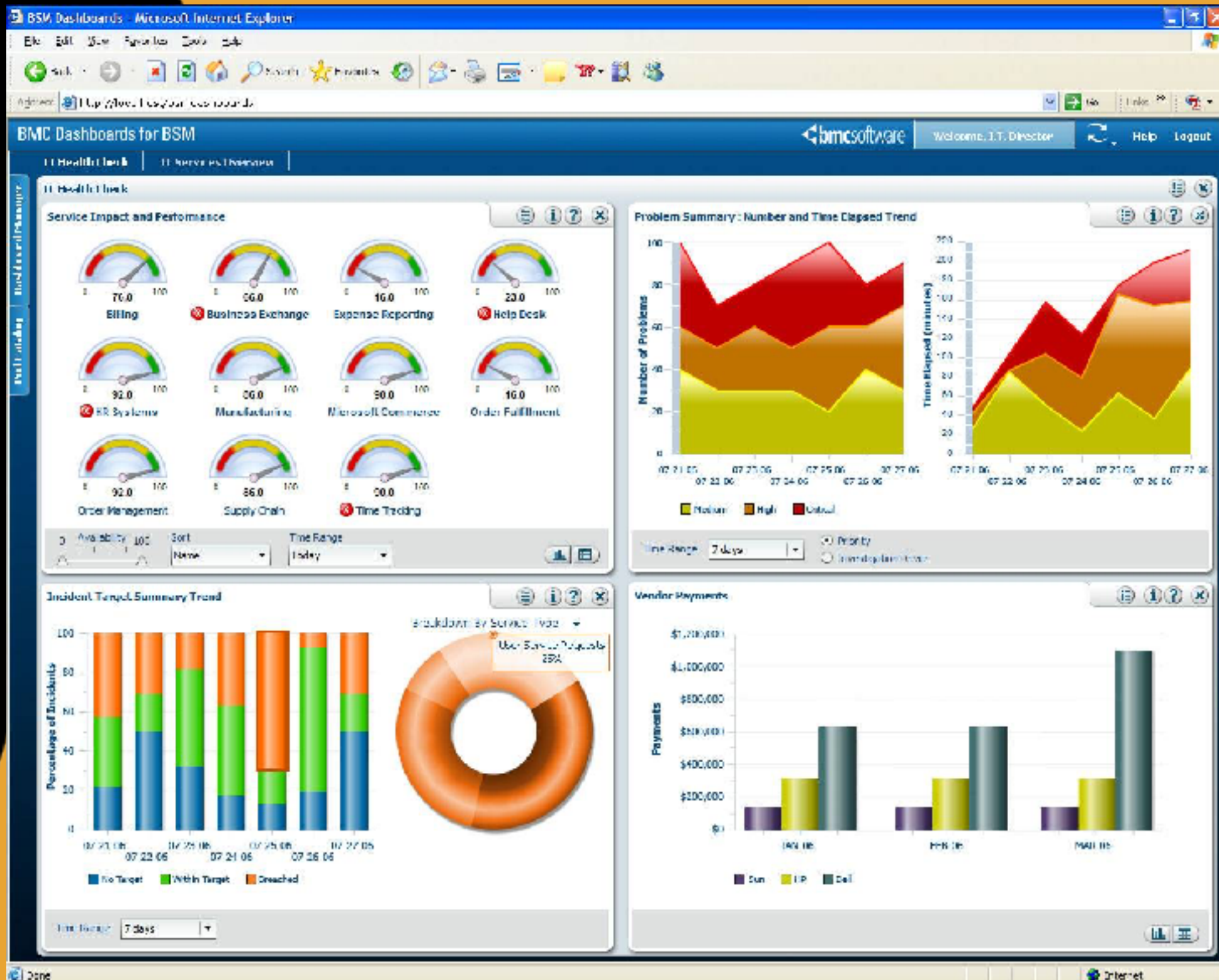
IP Address	OS	Total	Vulnerabilities
192.168.1.100	Windows Server 2016 Standard	1007	990
192.168.1.101	Windows Server 2016 Standard	1104	997
192.168.1.102	Windows Server 2016 Standard	1000	958
192.168.1.103	Windows Server 2016 Standard	1012	909
192.168.1.104	Linux	1078	1000

Last Updated: 3 hours ago

Seriously...Avoid Clutter



Less is More

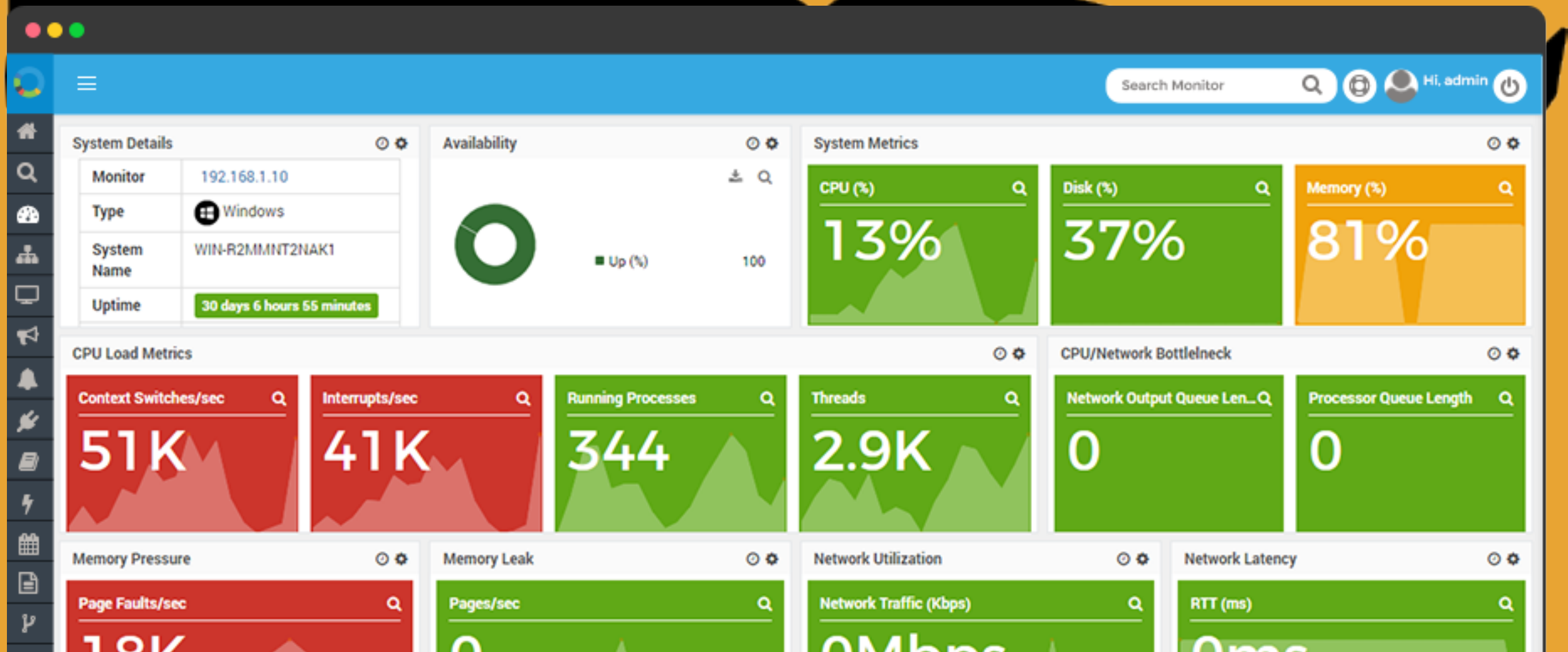




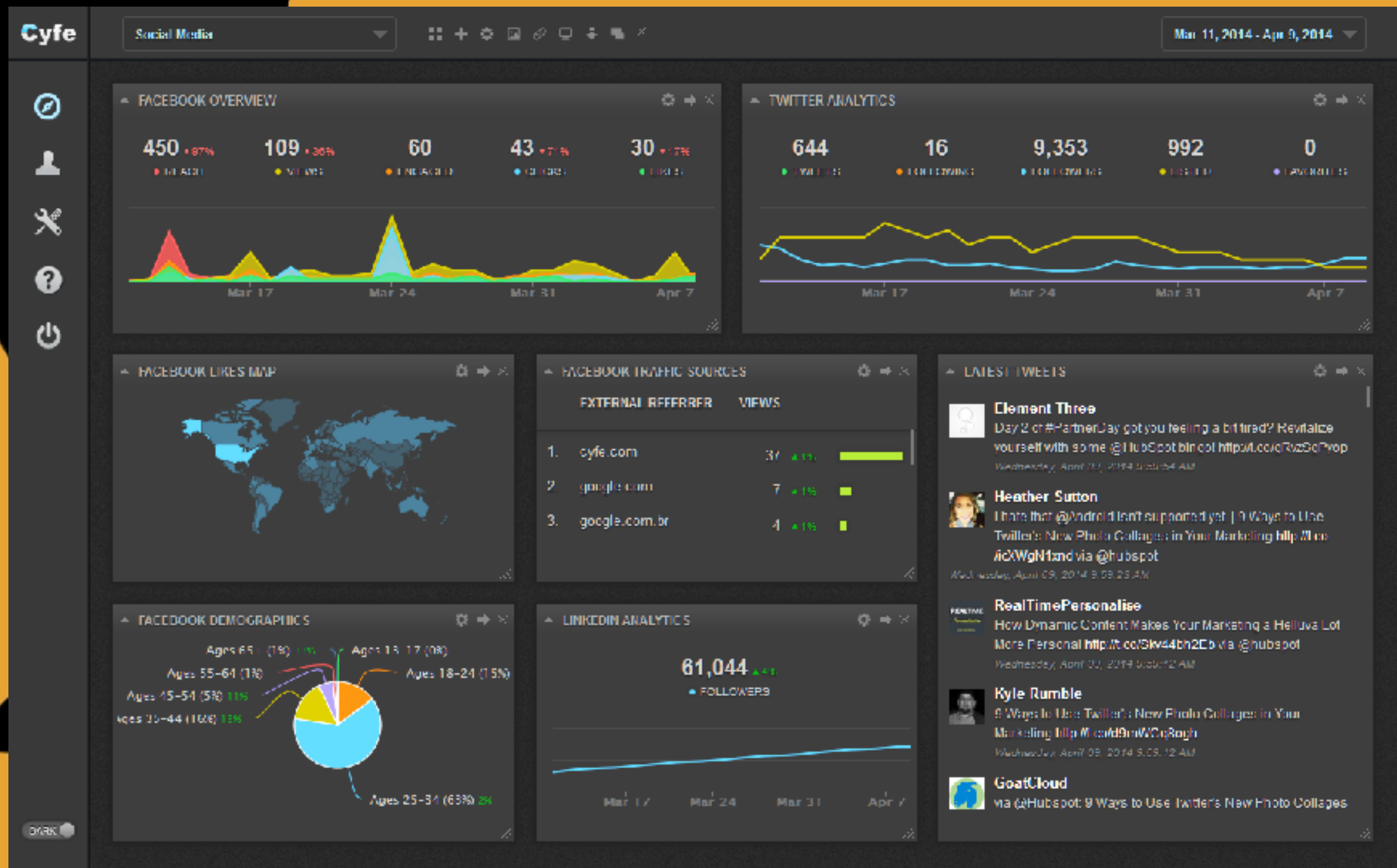
Less is More



Use Colors



Differ Visualizations



A black silhouette of a dog, possibly a Weimaraner, is positioned on the left side of the slide, facing right. It serves as a background element for the text.

Source Links

- <https://www.datadoghq.com/blog/monitoring-101-collecting-data/>
- <http://io9.gizmodo.com/how-to-comprehend-incomprehensibly-large-numbers-1521604757>

