

# RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: ASD-T07R

## Continuous Security: 5 Ways DevOps *Improves* Security

**David Mortman**



Chief Security Architect & Distinguished Engineer  
Dell Software  
@mortman

**Joshua Corman**



CTO  
Sonatype  
@joshcorman

# CHANGE

Challenge today's security thinking





**“It is not enough to do your best;  
you must know what to do,  
and then do your best”**

- W. Edwards Deming



“It’s not enough to do your best; you must know what to do, and then do your best” Deming @joshcorman @mortman #RSAC #DevOps

LeadershipQuote.org

ON TIME



ON BUDGET



ACCEPTABLE  
QUALITY/RISK



#RSAC  
@mortman  
@joshcorman

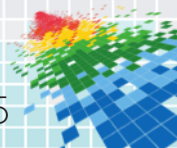


Sonatype



Dev's core motivations are to be OnTime, OnBudget, w/ Acceptable Quality/Risk  
@joshcorman @mortman #RSAC #DevOps

RSA Conference 2015







“Don’t Go Chasin’ Waterfalls” Dev started w/ Waterfall, but modern demands require us to go faster @joshcorman @mortman #RSAC #DevOps

**ON TIME.**

Faster builds.  
Fewer interruptions.  
More innovation.



**ON BUDGET.**

More efficient.  
More profitable.  
More competitive.



**ACCEPTABLE QUALITY/RISK.**

Easier compliance.  
Higher quality.  
Built-in audit protection.



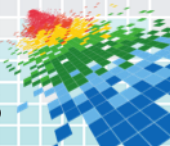
#RSAC  
@mortman  
@joshcorman




Sonatype



Waterfall's Design -> Dev -> Test -> Deploy may go 1.5-3yrs b/w releases.  
@joshcorman @mortman #RSAC #DevOps





Agile goats seek the fruit of Morocco's argan trees. Herders and barriers of thorny branches help thwart the animals.



Agile goats; not goat rodeo. "We need to be agile, but not fragile."  
@RuggedSoftware @joshcorman @mortman #RSAC #DevOps

**ON TIME.**

Faster builds.  
Fewer interruptions.  
More innovation.



**ON BUDGET.**

More efficient.  
More profitable.  
More competitive.

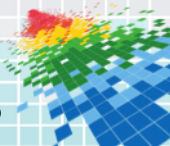


**ACCEPTABLE QUALITY/RISK.**

Easier compliance.  
Higher quality.  
Built-in audit protection.



Agile / CI







DEV OPS IN A BOX



It may feel like DevOps is Pandora's Box, but it's open... and hope remains. ;)  
@joshcorman @mortman #RSAC #DevOps



**ON TIME.**

Faster builds.  
Fewer interruptions.  
More innovation.



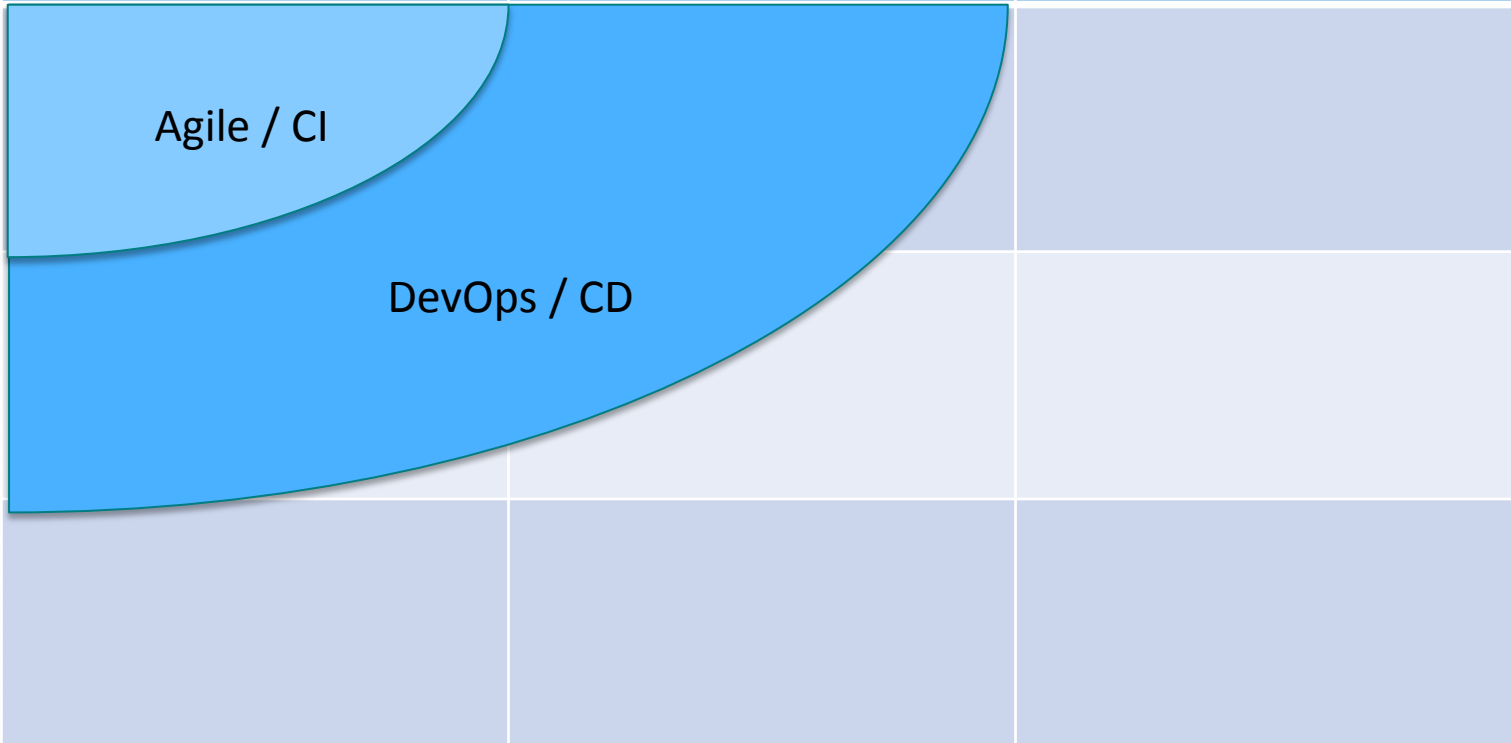
**ON BUDGET.**

More efficient.  
More profitable.  
More competitive.



**ACCEPTABLE QUALITY/RISK.**

Easier compliance.  
Higher quality.  
Built-in audit protection.



#RSAC  
@mortman  
@joshcorman

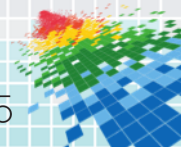


Sonatype



Agile made dev faster but wasn't enough. DevOps extends patterns to Ops 4 mutual gains @joshcorman @mortman #RSAC #DevOps

RSA Conference 2015





Deming drove Toyota Supply Chains. We can EXTEND DevOps w/ his quality/safety patterns @joshcorman @mortman #RSAC #DevOps



**ON TIME.**

Faster builds.  
Fewer interruptions.  
More innovation.



**ON BUDGET.**

More efficient.  
More profitable.  
More competitive.

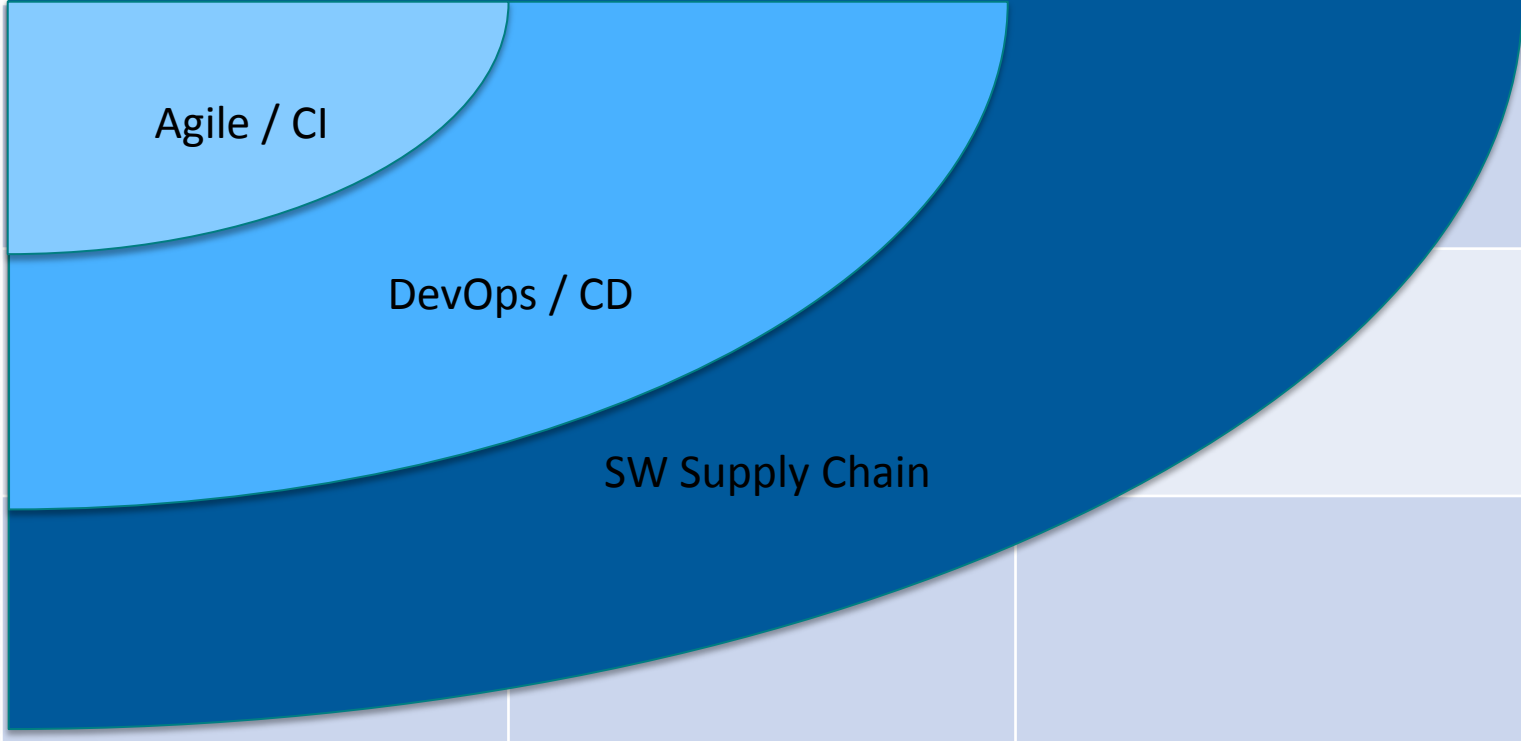


**ACCEPTABLE QUALITY/RISK.**

Easier compliance.  
Higher quality.  
Built-in audit protection.



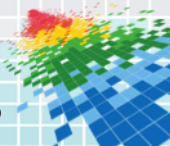
#RSAC  
@mortman  
@joshcorman



Sonatype



SW SupplyChains enable faster, more efficient dev by reducing elective complexity/risk++ @joshcorman @mortman #RSAC #DevOps



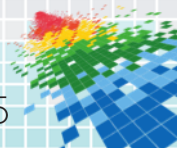


Sonatype



Our SW Supply Chain is only as strong as its weakest link. Can you say #OpenSSL?  
@joshcorman @mortman #RSAC #DevOps

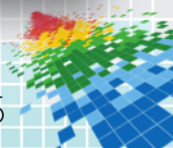
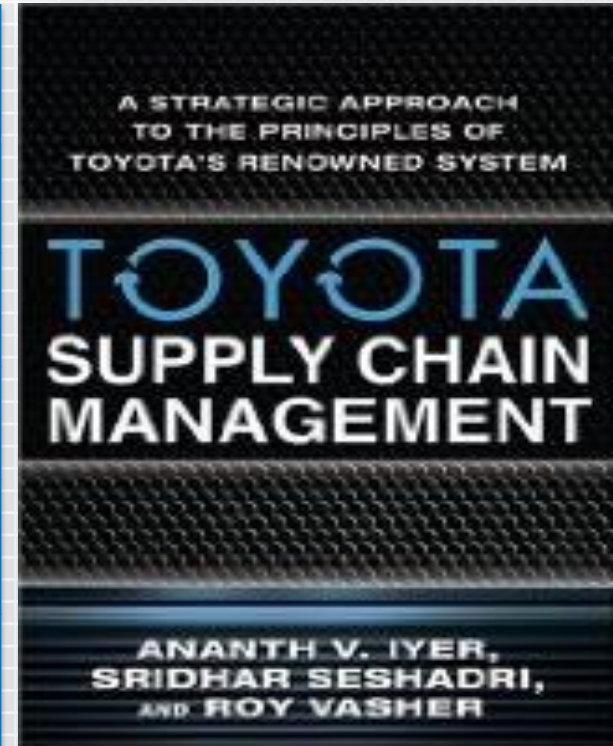
RSA Conference 2015





# Comparing the Prius and the Volt

	Toyota Prius	Chevy Volt
Cost	\$24,200	\$39,900
Units	23,294	1,788
Plant Suppliers	125	800
In-House Production	27%	54%
<i>Firm-Wide Suppliers</i>	224	5,500



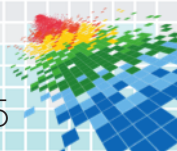


Sonatype



Is #DevOps a Culture? A Process? A Toochain? YES; but the greatest of these is Culture/Empathy @joshcorman @mortman #RSAC

RSA Conference 2015





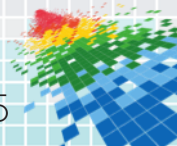


Sonatype



Myths about RE: Security & #DevOps. We FUD-Haters should deal w/ facts  
@joshcorman @mortman #RSAC

RSA Conference 2015



FACTS  
NOT OPINIONS

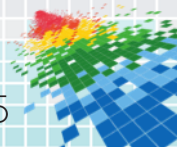


Sonatype

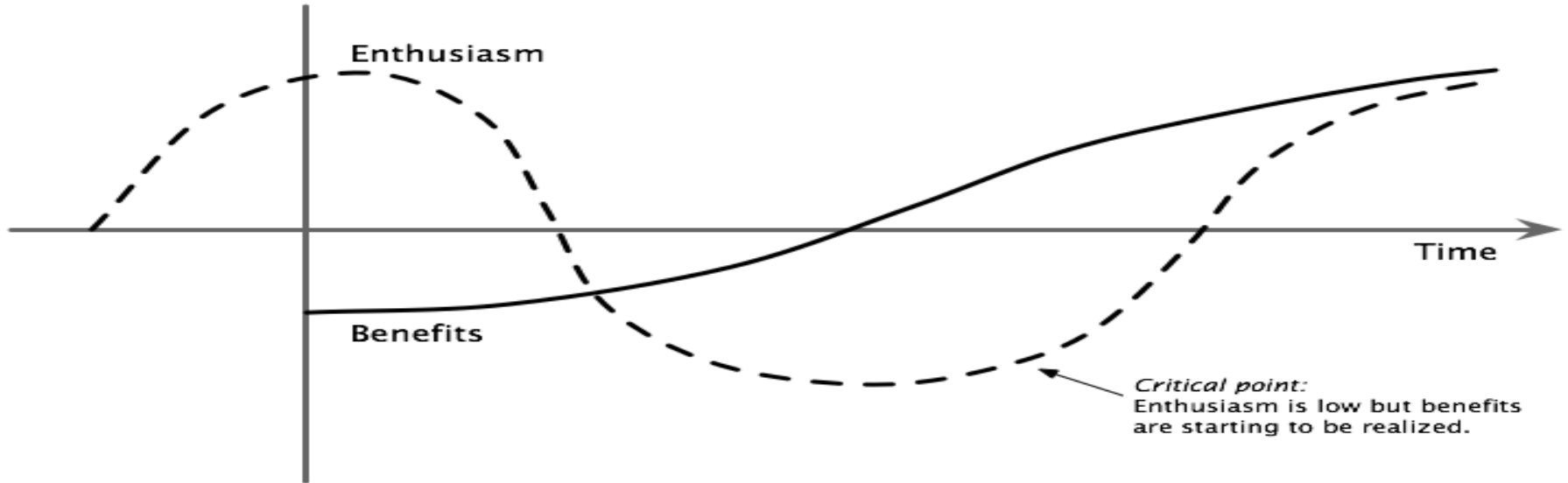


RE: #DevOps & Security: You're entitled to your own opinions, but not to your own facts. @joshcorman @mortman #RSAC

RSA Conference 2015



# "Silver bullet" lifecycle



Reference: Taylor, Sharon, and Ivor Macfarlane. *ITIL Small-scale Implementation*. London: TSO, 2005.

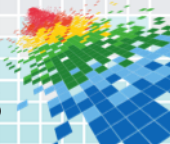


Sonatype



MythBusted: "ITIL & ChangeMngt can't be done w/ #DevOps " <- It can even make it easier/better @joshcorman @mortman #RSAC

RSAC Conference 2015





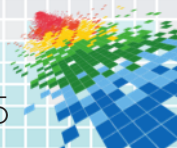


Sonatype



True #DevOps + Security isn't all rainbows & unicorns. Unicorn p00p has to be worked thru @joshcorman @mortman #RSAC

RSA Conference 2015

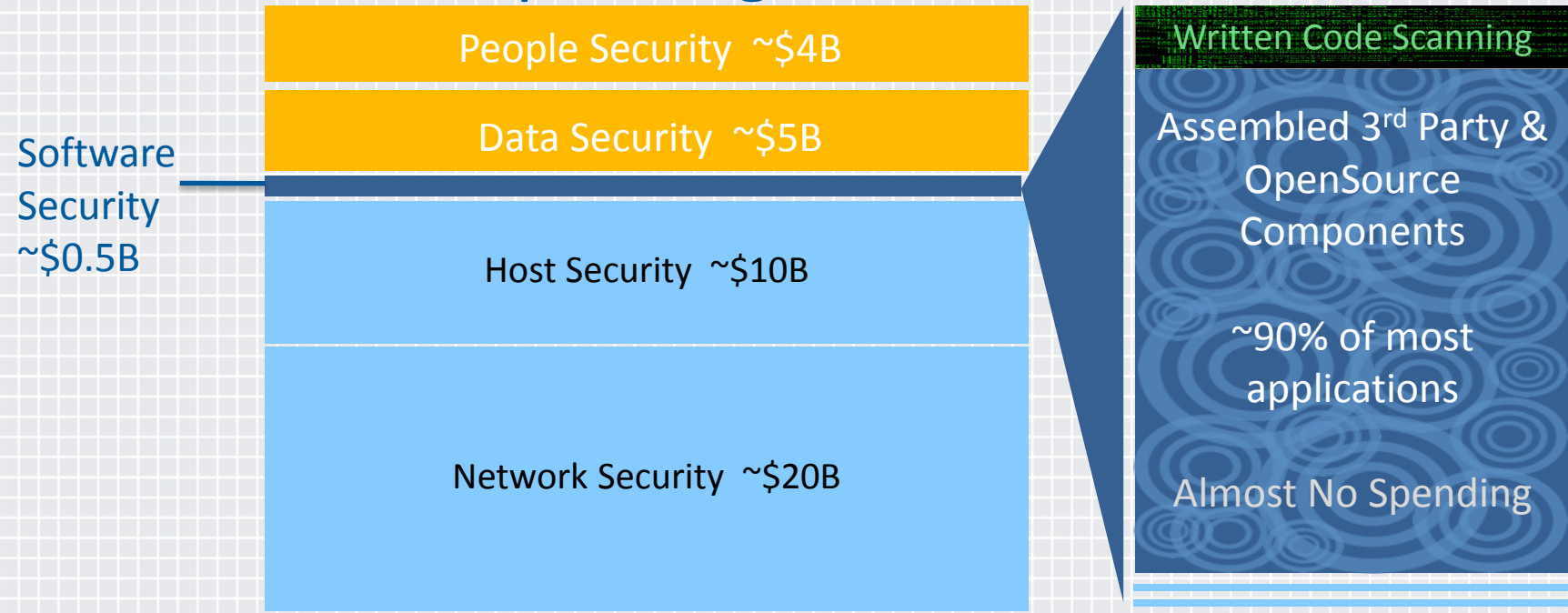


# SW Status Quo: Most attacked; least spend

Worse, w/in Software, existing dollars go to the  $\leq 10\%$  written

## spending

## attack risk



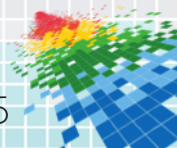
Sonatype



StatusQuo: SW is MOST attacked & gets LEAST SecSpend; most on 10% of code we write @joshcorman @mortman #RSAC #DevOps

Source: Normalized COBIT spending across IDC, Gartner, The 451 Group; since groupings vary

RSA Conference 2015





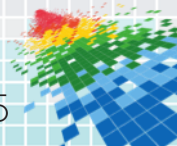


Sonatype



Einstein's Insanity: We could do the same thing over & over expecting different results @joshcorman @mortman #RSAC #DevOps

RSA Conference 2015





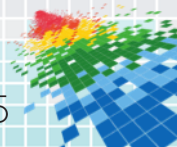


Sonatype



WRT Security & #DevOps We lose things AND we gain things. We'll look at 5 things we gain @joshcorman @mortman #RSAC #DevOps

RSA Conference 2015



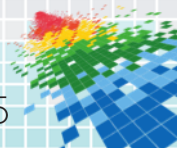


Sonatype



This was added b/c the Red Hat in the "Lost & Found" made @mortman giggle & he forced it upon @joshcorman #RSAC #DevOps

RSAC Conference 2015





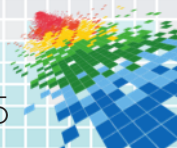


Sonatype



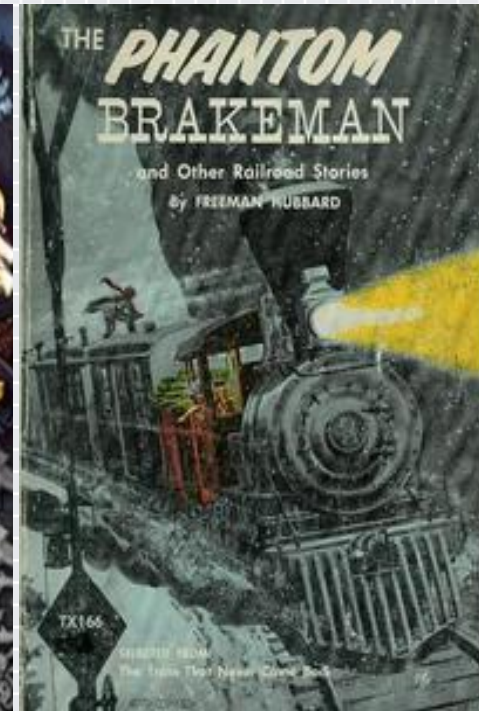
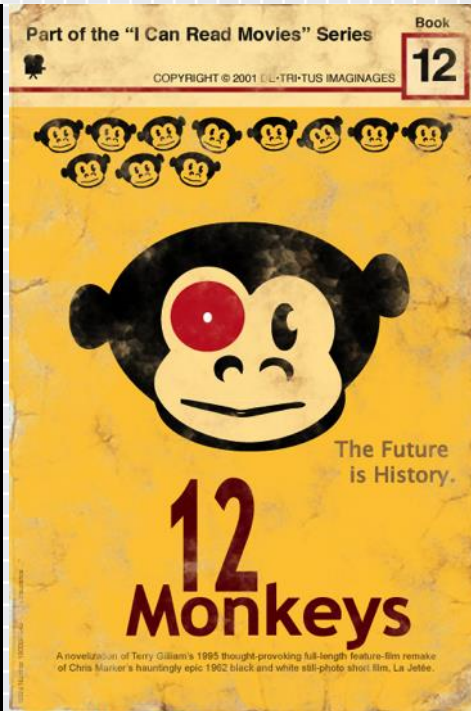
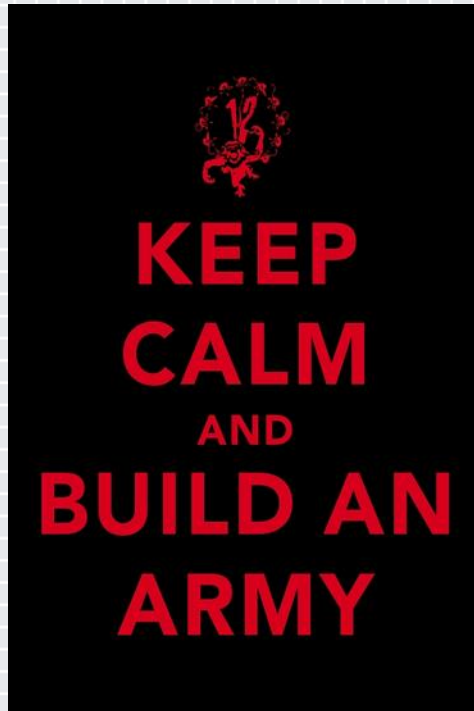
1) Instrumentation! #DevOps instruments EVERYTHING & Security can use it in MANY ways @joshcorman @mortman #RSAC #DevOps

RSA Conference 2015

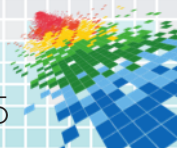




## 2) Be Mean To Your Code!



2) Be Mean To Your Code! To avoid failure; fail all the time #ChaosMonkey #Gauntlt #BrakeMan @joshcorman @mortman #RSAC #DevOps





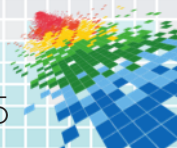


Sonatype

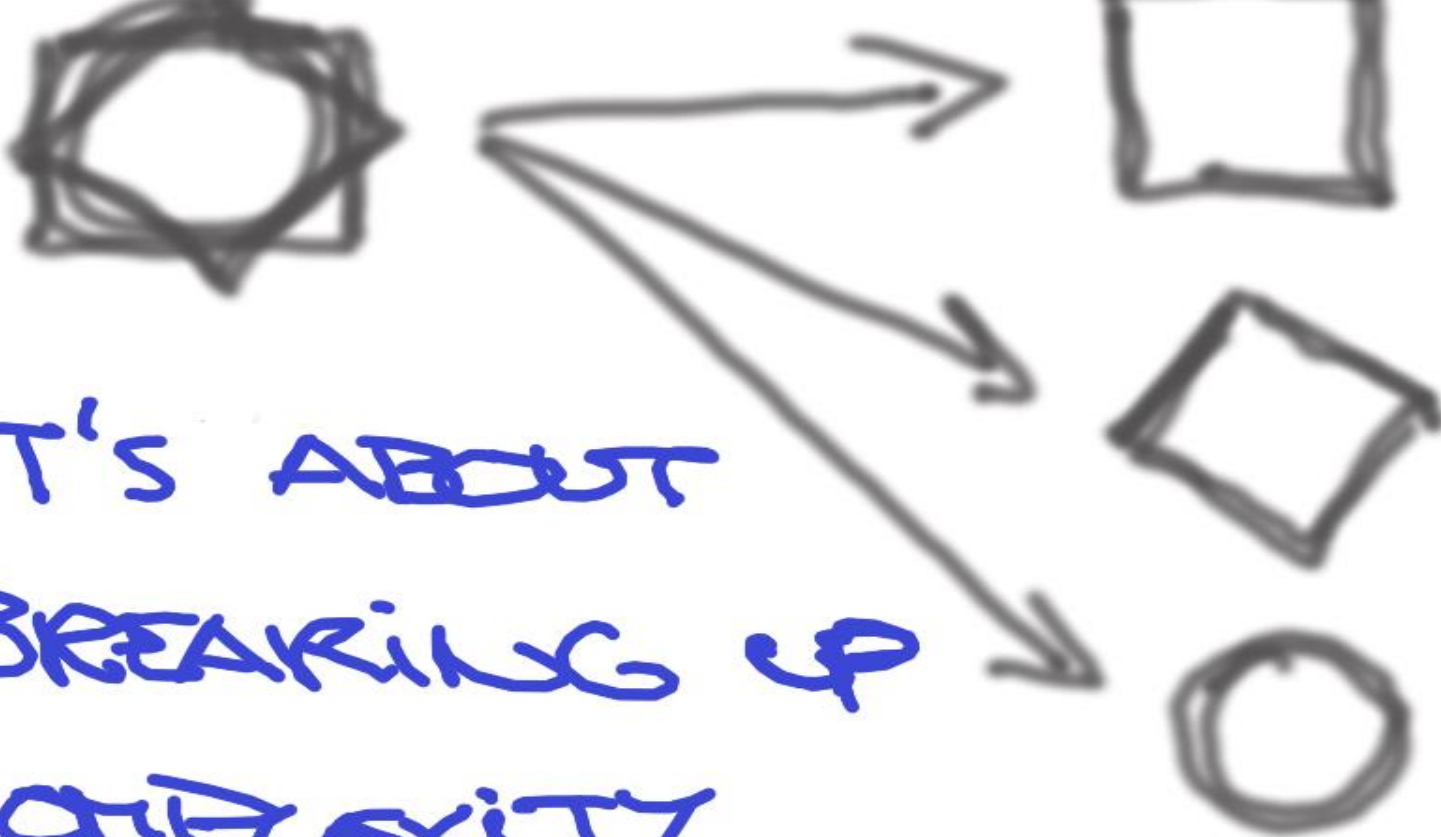


3) Complexity Is Enemy of "All The Things"! All #DevOps parties benefit from reducing complexity @joshcorman @mortman #RSAC

RSAC Conference 2015



IT'S ABOUT  
BREAKING UP  
COMPLEXITY

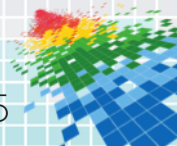


Sonatype



Decomposition lowers complexity adds security and reliability @mortman  
@joshcorman #RSAC #DevOps

RSA Conference 2015







NORTEL

# SIMPLICITY BEATS COMPLEXITY

HYPERCONNECTIVITY.GO.UK

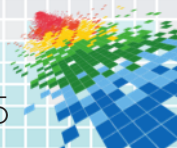


Sonatype



Simple > Complex. Simple != Easy though. There is no easy button, but there is an easiER one. @joshcorman @mortman #RSAC #DevOps

RSA Conference 2015



A photograph of a white surface with a piece of red paper torn out. The red paper has the text "change is good." in white lowercase letters on the top line, and "look hard" in white lowercase letters on the bottom line. The paper is torn at the edges, and there is a black and white spiral graphic above the text.

change is good.

look hard

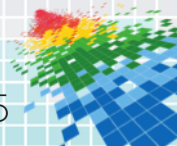


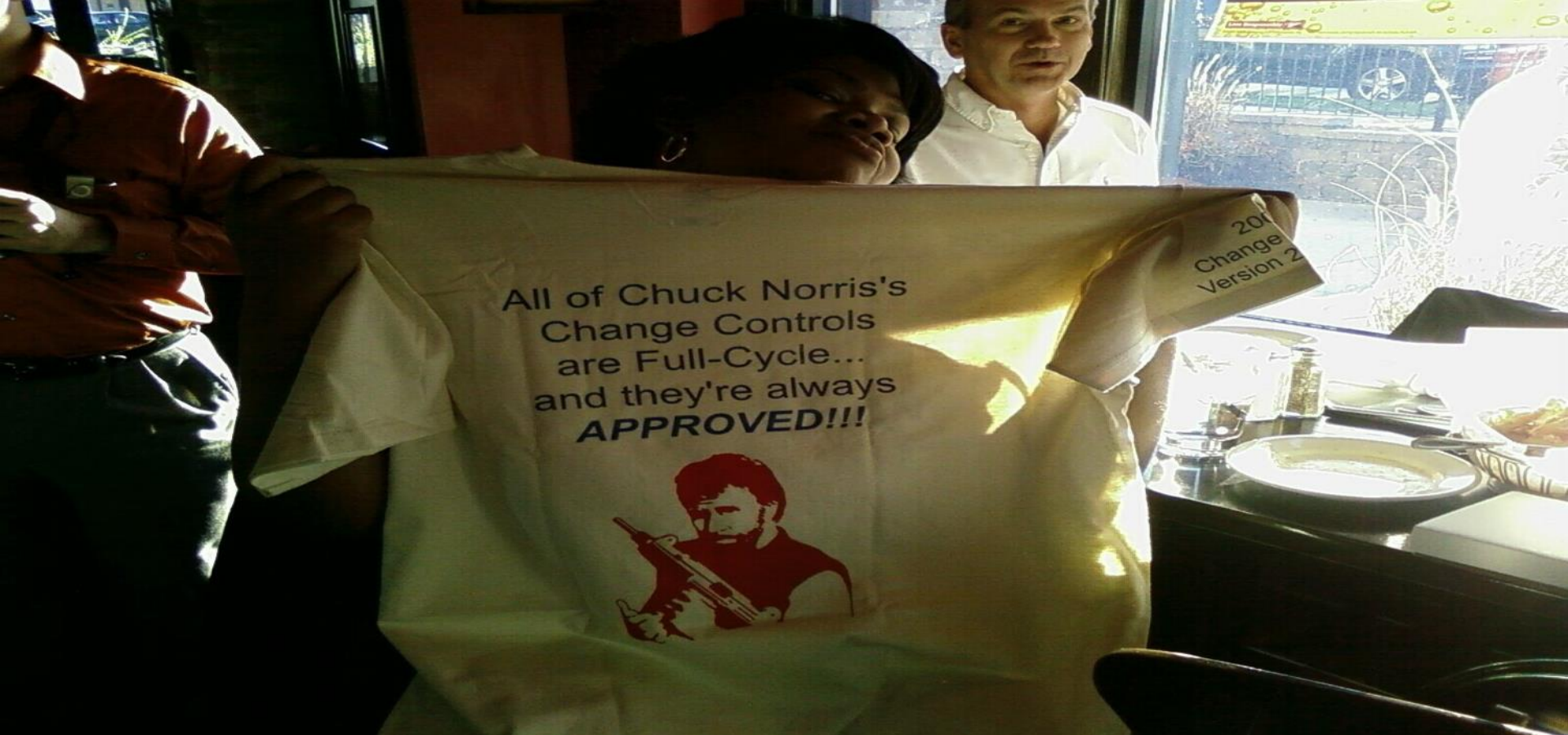
Sonatype



4) Implicit and Explicit Change Management. Change is good and leads to stability and fights stagnation. @joshcorman @mortman #rsac #devops

RSA Conference 2015



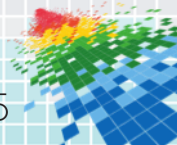


Sonatype



All of Chuck Norris's Change Controls are Full Cycle and they're always approved!  
@joshcorman @mortman #RSAC #DevOps

RSAC Conference 2015





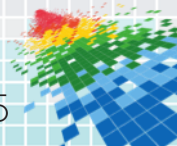


Sonatype



5) Empathy is the killer app! Silos prohibit sharing and empathy.... #RSAC #DevOps  
@mortman @joshcorman

RSA Conference 2015



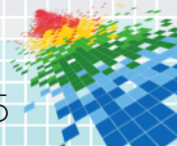


Sonatype



Madame CISO, Tear Down This Wall! #RSAC #DevOps @mortman @joshcorman

RSA Conference 2015



# MOST IMPACT: BUY/BUILD DEFENSIBLE SOFTWARE

#RSAC  
@mortman  
@joshcorman

Counter-measures

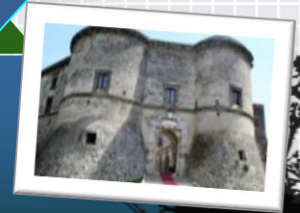
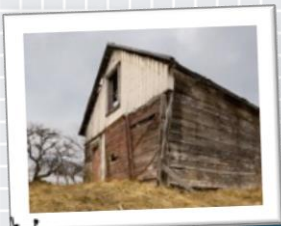
Situational Awareness

Operational Excellence

10%  
Written

Defensible Infrastructure

The software & hardware we build, buy, and deploy. 90% of software is assembled from 3<sup>rd</sup> party & Open Source



DefensibleIT & OpsExcellence have MOST Security impact, but elude CISO influence  
BUT... @joshcorman @mortman #RSAC #DevOps



Counter-  
measures

Situational Awareness

Operational Excellence

Defensible Infrastructure

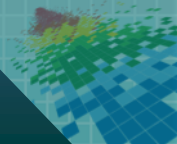
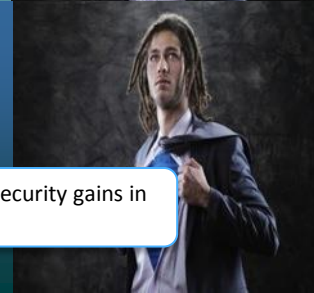
DevOps

DevOps

DevOps

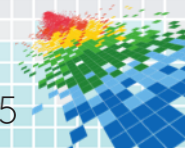


[cont] #DevOps smashes silos & finally enables the MUCH LARGER Security gains in both @joshcorman @mortman #RSAC #DevOps



# Apply!

- ◆ Stop resisting... “Survival isn’t mandatory” – Deming
  - ◆ Josh’s RSAC EU Keynote [http://youtu.be/m4Y\\_K7MXQxQ](http://youtu.be/m4Y_K7MXQxQ)
- ◆ Read “The Phoenix Project” by Gene Kim
  - ◆ <http://itrevolution.com/books/phoenix-project-devops-book/>
- ◆ Watch videos from RSAC “DevOps Connect” Rugged DevOps Day
  - ◆ <http://www.sonatype.org/nexus/2015/04/13/devops-connect-secops-edition-at-rsac-2015-speakers-and-schedule/>
- ◆ Grab tooling:
  - ◆ Gauntlt, BrakeMan, Chaos Monkey, and the Simian Army
- ◆ Start small, start anywhere, start TODAY!





# RSA<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

## Conclusion/Wrap-Up



Follow Us & Rugged #DevOps at:  
[@mortman](#) [@joshcorman](#) [@RuggedSoftware](#) [@RuggedDevOps](#) [@iamthecavalry](#)

