Continuous Security: 5 Ways DevOps *Improves* Security

David Mortman
Chief Security Architect & Distinguished Engineer
Dell Software
@mortman

Joshua Corman
CTO
Sonatype
@joshcorman
“It is not enough to do your best; you must know what to do, and then do your best”

- W. Edwards Deming
Dev’s core motivations are to be OnTime, OnBudget, w/ Acceptable Quality/Risk
@joshcorman @mortman #RSAC #DevOps
“Don’t Go Chasin’ Waterfalls” Dev started w/ Waterfall, but modern demands require us to go faster @joshcorman @mortman RSAC #DevOps
<table>
<thead>
<tr>
<th>ON TIME.</th>
<th>ON BUDGET.</th>
<th>ACCEPTABLE QUALITY/RISK.</th>
</tr>
</thead>
</table>

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
<table>
<thead>
<tr>
<th>ON TIME.</th>
<th>ON BUDGET.</th>
<th>ACCEPTABLE QUALITY/RISK.</th>
</tr>
</thead>
</table>

Agile / CI

Agile & Lean tightened Design -> Build -> Test cycle releasing 6-12+ smaller batches/yr @joshcorman @mortman #RSAC #DevOps
It may feel like DevOps is Pandora’s Box, but it’s open... and hope remains. ;)
@joshcorman @mortman RSAC #DevOps
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Agile / CI</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DevOps / CD</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Deming drove Toyota Supply Chains. We can EXTEND DevOps w/ his quality/safety patterns @joshcorman @mortman #RSAC #DevOps
SW Supply Chains enable faster, more efficient dev by reducing elective complexity/risk++ @joshcorman @mortman RSAC #DevOps
Our SW Supply Chain is only as strong as its weakest link. Can you say #OpenSSL?
@joshcorman @mortman RSAC #DevOps
# Comparing the Prius and the Volt

<table>
<thead>
<tr>
<th></th>
<th>Toyota Prius</th>
<th>Chevy Volt</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cost</strong></td>
<td>$24,200</td>
<td>$39,900</td>
</tr>
<tr>
<td><strong>Units</strong></td>
<td>23,294</td>
<td>1,788</td>
</tr>
<tr>
<td><strong>Plant Suppliers</strong></td>
<td>125</td>
<td>800</td>
</tr>
<tr>
<td><strong>In-House Production</strong></td>
<td>27%</td>
<td>54%</td>
</tr>
<tr>
<td><strong>Firm-Wide Suppliers</strong></td>
<td>224</td>
<td>5,500</td>
</tr>
</tbody>
</table>

Toyota Prius (v Volt) used 1/6th suppliers, better leveraged, for 60% price & 12x sales @joshcorman @mortman #RSAC #DevOps
Is #DevOps a Culture? A Process? A Toochain? YES; but the greatest of these is Culture/Empathy @joshcorman @mortman #RSAC
Myths abound RE: Security & #DevOps. We FUD-Haters should deal w/ facts @joshcorman @mortman #RSAC
RE: #DevOps & Security: You’re entitled to your own opinions, but not to your own facts. @joshcorman @mortman #RSAC
"Silver bullet" lifecycle


MythBusted: “ITIL & ChangeMngt can’t be done w/ #DevOps ” <- It can even make it easier/better @joshcorman @mortman #RSAC
True #DevOps + Security isn’t all rainbows & unicorns. Unicorn p00p has to be worked thru @joshcorman @mortman #RSAC
SW Status Quo: Most attacked; least spend
Worse, w/in Software, existing dollars go to the <= 10% written spending

- People Security ~$4B
- Data Security ~$5B
- Host Security ~$10B
- Network Security ~$20B

Software Security ~$0.5B

Software Status Quo: 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

Almost No Spending

Assembled 3rd Party & OpenSource Components
~90% of most applications

Written Code Scanning
Einstein’s Insanity: We could do the same thing over & over expecting different results @joshcorman @mortman #RSAC #DevOps
WRT Security & #DevOps We lose things AND we gain things. We’ll look at 5 things we gain @joshcorman @mortman #RSAC #DevOps
This was added b/c the Red Hat in the “Lost & Found” made @mortman giggle & he forced it upon @joshcorman #RSAC #DevOps
1) Instrumentation! #DevOps instruments EVERYTHING & Security can use it in MANY ways @joshcorman @mortman RSAC #DevOps
2) Be Mean To Your Code!

To avoid failure; fail all the time #ChaosMonkey #Gauntlt #BrakeMan @joshcorman @mortman RSAC #DevOps
3) Complexity Is Enemy of “All The Things”! All DevOps parties benefit from reducing complexity @joshcorman @mortman RSAC
IT'S ABOUT BREAKING UP COMPLEXITY
Simple > Complex. Simple != Easy though. There is no easy button, but there is an easier one. @joshcorman @mortman RSAC #DevOps
4) Implicit and Explicit Change Management. Change is good and leads to stability and fights stagnation. @joshcorman @mortman rsac devops
All of Chuck Norris's Change Controls are Full-Cycle... and they're always APPROVED!!!
5) Empathy is the killer app! Silos prohibit sharing and empathy.... #RSAC #DevOps
@mortman @joshcorman
Madame CISO, Tear Down This Wall! #RSAC #DevOps @mortman @joshcorman
The software & hardware we build, buy, and deploy. 90% of software is assembled from 3rd party & Open Source.

DefensibleIT & OpsExcellence have MOST Security impact, but elude CISO influence

BUT... @joshcorman @mortman #RSAC #DevOps
Defensible Infrastructure

[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
❖ Read “The Phoenix Project” by Gene Kim
❖ http://itrevolution.com/books/phoenix-project-devops-book/
❖ Watch videos from RSAC “DevOps Connect” Rugged DevOps Day
❖ Grab tooling:
❖ Gauntlt, BrakeMan, Chaos Monkey, and the Simian Army
❖ Start small, start anywhere, start TODAY!

Get on the train before the train gets on you! Don’t delay, start today!
@joshcorman @mortman RSAC #DevOps
Conclusion/Wrap-Up

Follow Us & Rugged #DevOps at:
@mortman @joshcorman @RuggedSoftware @RuggedDevOps @iamthecavalry