Pacing Security in Containerworld

@justinjsmith
WHAT ARE YOU GONNA DO?
Well over 400 engineers building enterprise platforms
NOT ON THE “CONFERENCE CIRCUIT”
BACK TO THE RIVER/CONTAINER
METAPHOR
Shadow IT
HOW DO WE DEAL?
What doesn’t work so well

• Invent enemies
• Freeze (do nothing, obsess, panic)
• Control-monger
• Blame
More things that don’t work

• Use existing security policy and process (P&P)
• Change P&P out of sync with apps and devops
• Get stuck in transition
The “web” wins when it meets the enterprise.

EVERY TIME.
What seems to work?
Everyone is a tech company.

Do what big tech companies do.
A word on culture.
Strive for:
Awareness, Focus, and Flexibility
Start with small projects with exec blessing & clear outcomes.

Learn & build trust.
Awareness, Focus, and Flexibility:
In your org and your tech.
Awareness

• What are developers using and asking for?
• What’s your inventory?
• What types of vulns have been most trouble?
• Who can do what to what?
• How are things configured?
• Platform vs. Dev
• Is the “undone” stuff visible?
Focus

• “Where the attention goes, the energy flows”
• Can you zero-in on a type of action in logs?
• Centralize auth
• Centralize pipelines and tooling
• Blocking and tackling
• METRICS METRICS METRICS METRICS
Flexibility

- Systems that welcome change
- Run towards the pain
- Rotate creds often
- Embed capabilities into the platform
- MOATs around legacy
Example AFF Metrics

- Consider by app and by org
- Time to deploy patch (OS, middleware, app)
- Container lifetime
- Cluster lifetime
- Credential lifetime
Vulnerabilities
Make it RAIN!

- **R**ecognize
- **A**llow / Acknowledge / Accept
- **I**nvestigate
- **N**eutralize
RAIN Example (1)

- Amplification attack on auth system
  - **Recognize** - Simple idea
  - **Allow** - No judgment
  - **Investigate** - Look around for other examples
  - **Neutralize** – logs, IP filtering, 😊
• **Credential leaks to a log file**
  
  – **Recognize** – How did we find out?
  – **Allow** – Very easy do
  – **Investigate** - Look around for other examples
  – **Neutralize** – education, platform, scanning, rotate