

Container Code Classification

Gao, Jeremy, Kostas, Ozan, Rahul

Mentor: Sastry S Duri
(IBM Research)

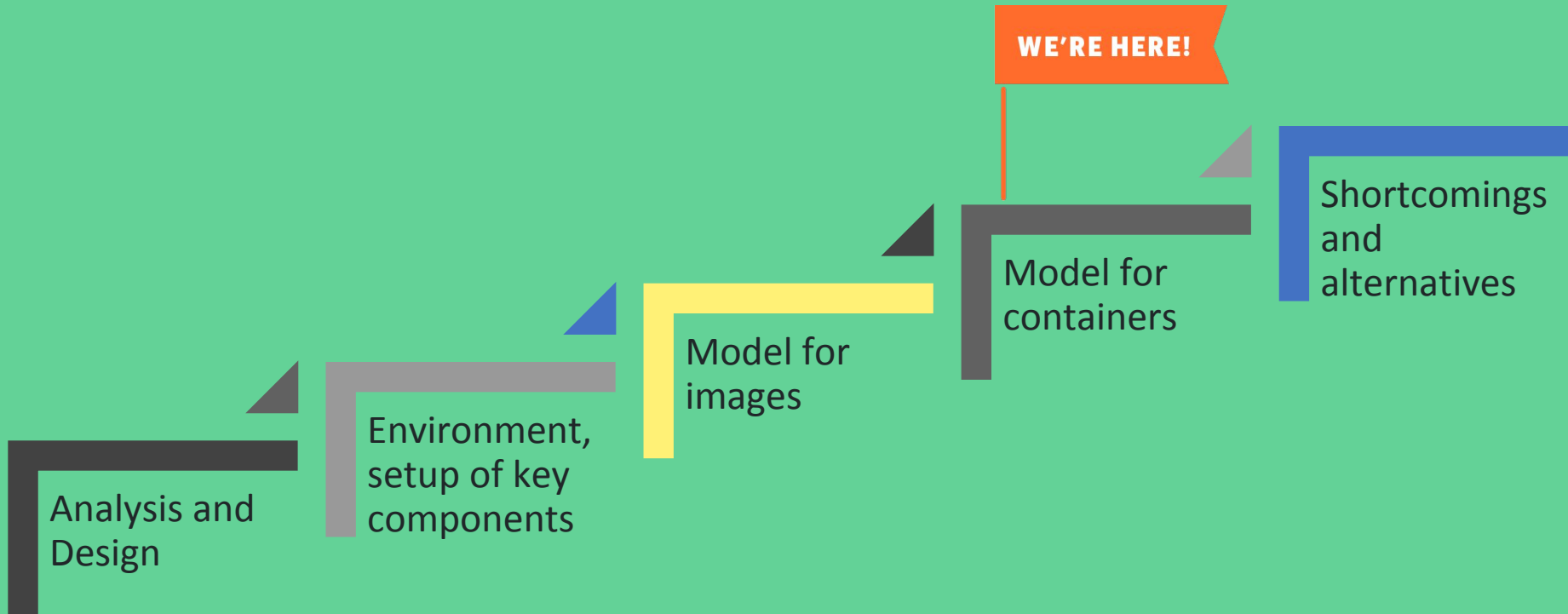
What we've done:

So Far (Sprint 4):

- Implemented Use Case 2 ✓
- Deployed our code in containers ✓
- Tried sdHash alternatives ✓
 - clamAV
 - chkrootkit
- Integrated image push with hash-calculation ✓
- Documentation of project and wiki ✓



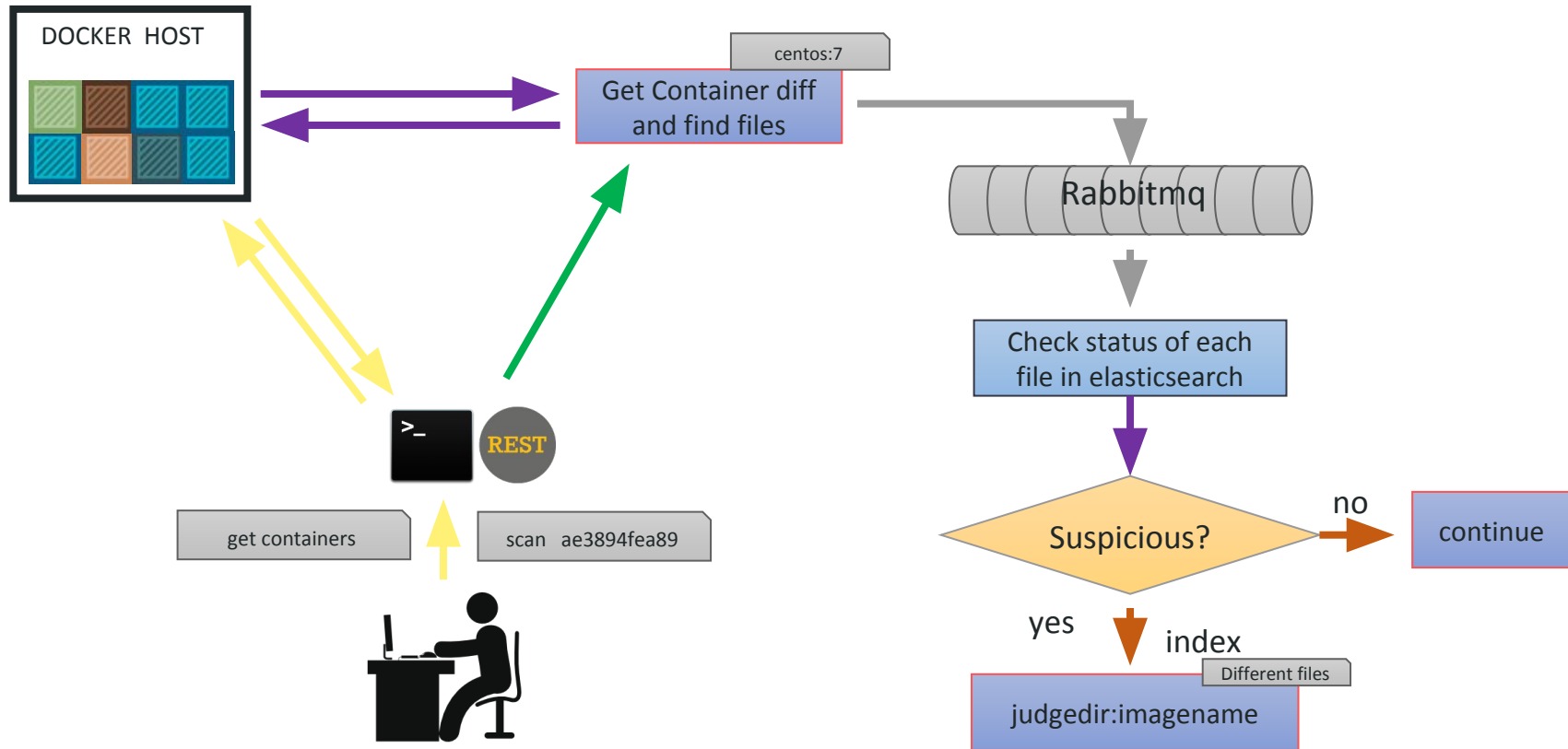
Status with respect to larger plan



Learnings from this sprint

- Using “docker diff” to get changed files and then processing them
- How docker daemon interacts with clients
 - CLI
 - REST API's
- Use of clamAV to scan for malicious files
- Packaging of code within containers and running it
- Shortcomings of sdhashes and things where it's useful

Flow for container scan

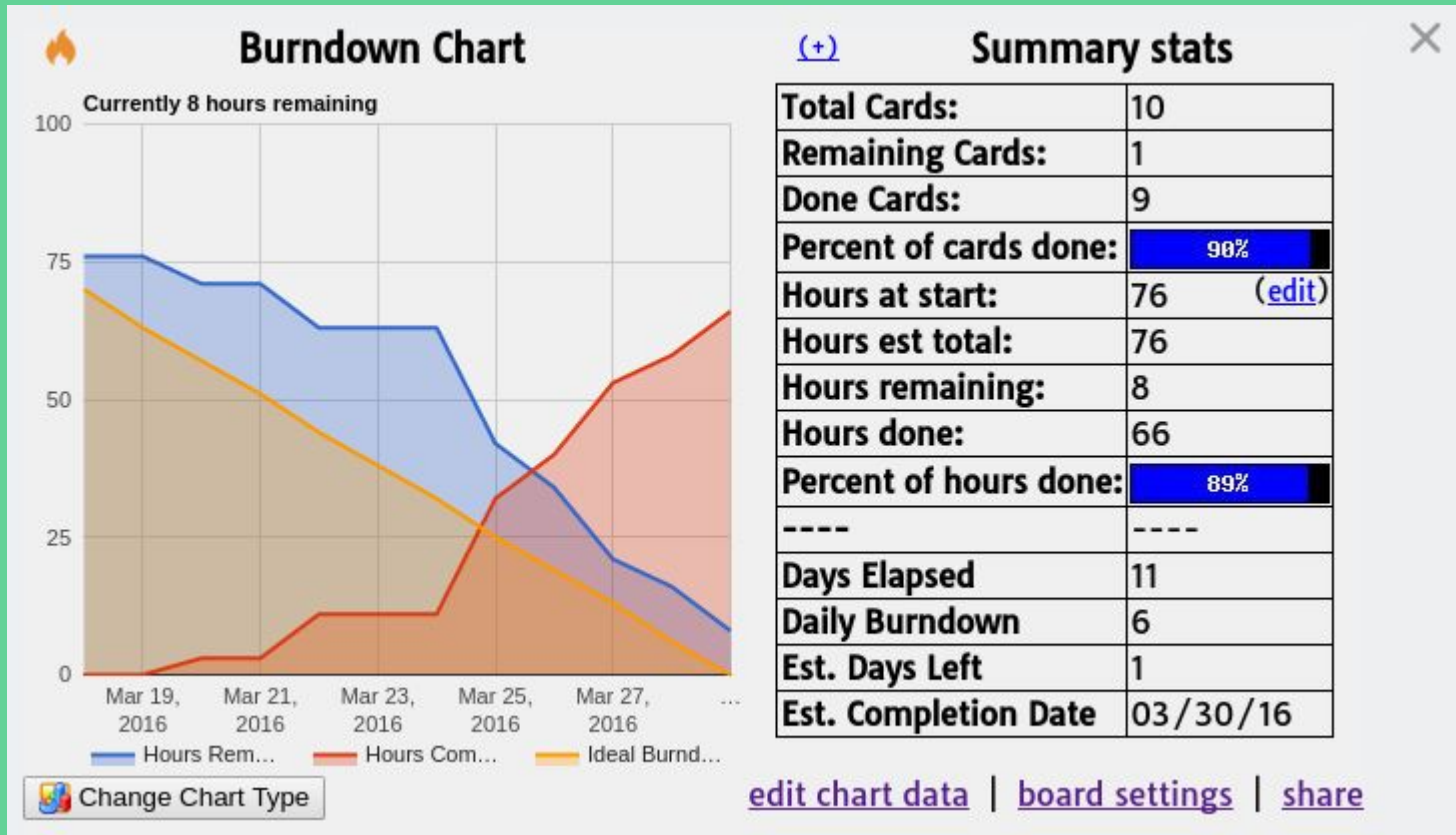


DEMO

[illegible]

Video: <https://www.youtube.com/watch?v=2cRBCUmx0vE>

Burndown chart



Next sprint

- Using alternatives like clamAV
- Single script to deploy development environment
- Code refactoring
- Modifying dockerUI and integrate our project

Thank you
&
Q/A