Container Code Classification

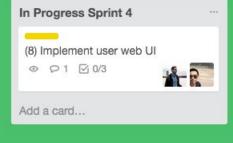
Gao, Jeremy, Kostas, Ozan, Rahul

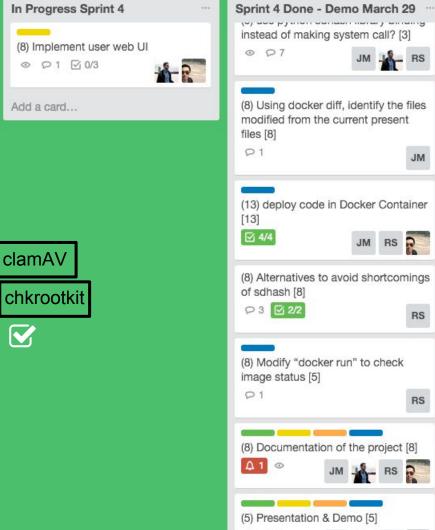
Mentor: Sastry S Duri (IBM Research)

What we've done:

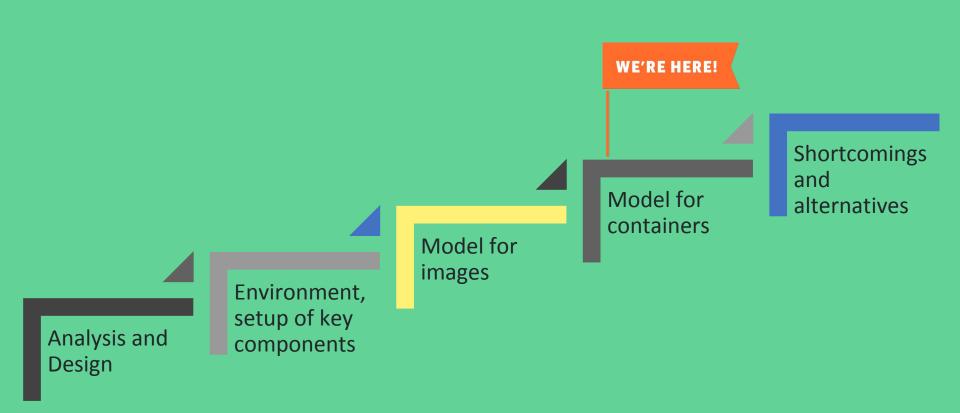
So Far (Sprint 4):

- Implemented Use Case 2 S
- Deployed our code in containers
- Tried sdHash alternatives
- Integrated image push with hash-calculatio
- Documentation of project and wiki





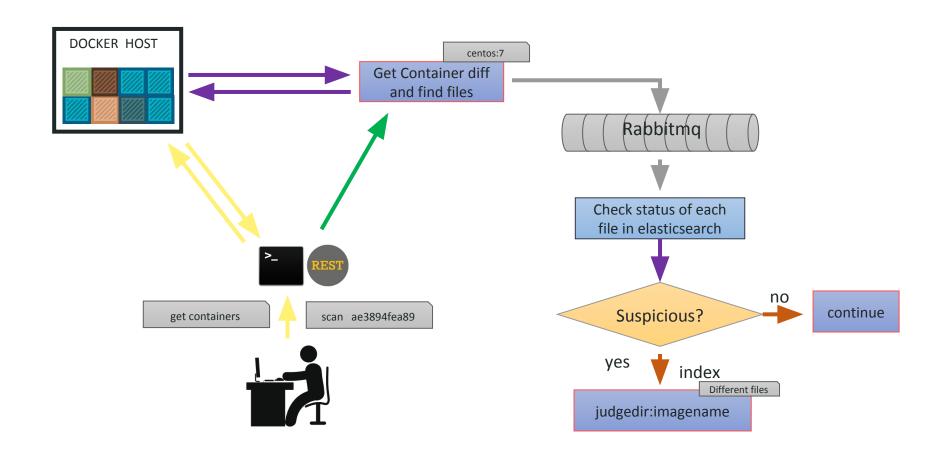
Status with respect to larger plan



Learnings from this sprint

- Using "docker diff" to get changed files and then processing them
- How docker daemon interacts with clients
 - o 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

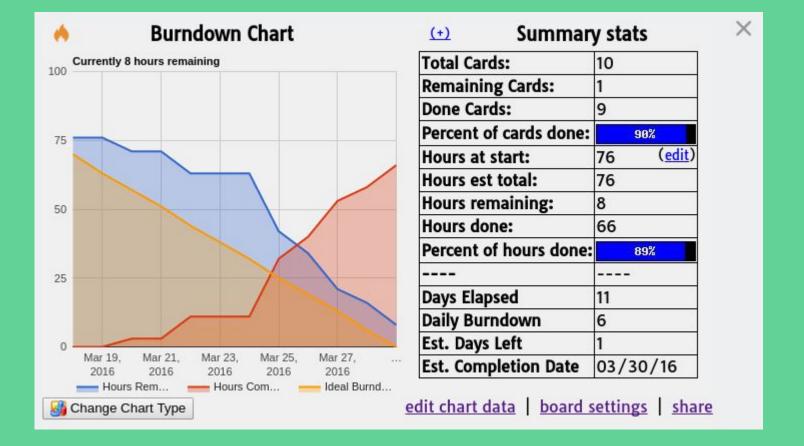


DEMO

```
W W DO DO NO TELEVISION &
                                                                                                                                                                               OTHER MANAGEMENT OF SERVICE ASSESSMENT OF STREET, STRE
                                                                                                                                                                             mendati@best-1:-/Container-Code-Classiffications
                                                                                                                                                                              -mendatiguest-1:-)Container-Code-Classifications decker po
                                                                                                                                                                             CONTACOUR 19
                                                                                                                                                                                                                       THACK.
                                                                                                                                                                                                                                                                        STREET, SQUARE
                                                                                                                                                                                                                                                                                                                             CHEATER'
                                                                                                                                                                                                        PMIS
                                                                                                                                                                                                                                                                                                                  WANTS.
                                                                                                                                                                             170079079496
                                                                                                                                                                                                                       ubanto (Laters)
                                                                                                                                                                                                                                                                        "AR CARBORNE"
                                                                                                                                                                                                                                                                                                                            F daes age
                                                                                                                                                                                                                                                                                                                  herten excited
                                                                                                                                                                                                       etasticusarchitatest "Adober entrypetar s" Days age
8.8.0.0500-5000-5000-500 8.8.0.012771-0388752 evil bapter
registrycs. 8.8.0.012771-0388752 evil bapter
registrycs. 8.8.0.012771-0388752 evil bapter
                                                                                                                                                                              AMERICAN STREET
                                                                                                                                                                             int A.A.S. SPEC-1000/U/D
possibilitation -1:-/Container-Code Classiffications
weakington: -1:-/Container-Code Classifications
weakington: -1:-/Container-Code Classifications desher ps
                                                                                                                                                                                                                                                                                                                  restativ_restativ_3
       C THATESE & C. O. B AR 1
              CONTRACTOR OF
                                                                                                                                                                                                                       I MHUE
                                                                                                                                                                                                                                                                                                                             CHEATER
    STATES - 7 - E 4 Stoday - Baycon 3 N. 7 5
                                                                                                                                                                                                       POSTS
    Start[] - 7 - [ | A.Lon(Mon(1) | Start[7] | N.7 |
Start[] - | A.Lon(Ann(2) + Start[2] | N.7 |
                                                                                                                                                                              - Nachtstelle.
                                                                                                                                                                                                                                                                         "(fringhash"
                                                                                                                                                                                                                                                                                                                             Zinencińki ago
                                                                                                                                                                             combs.
                                                                                                                                                                                                                                                                                                                   abete beautie
    for (believe bitter) ( while ( therefol on 7 ) therefol on 7 )
                                                                                                                                                                             (FUELDACTRACK)
                                                                                                                                                                                                                                                                        "Althought
                                                                                                                                                                                                                                                                                                                             T days age
                                                                                                                                                                                                                        Mantin Catent
    for Constituted Constituted C
                                                                                                                                                                                                                                                                                                                  mering exclisi
        if ( Year[ex] to Year[ex-1] )
                                                                                                                                                                              VALUE STORMST
                                                                                                                                                                                                                       elasticsegratitatect "Macker-entrypolatio" 7 days ago
           printft 'me
                                                                                      Waller's and West [ren], as
                                                                                                                                                                                                        8.4.6.0:008-0006/hpp. 0.6.8.9:32771-0008/fep - mil.hoppe
        of ( on on 1 ) printf( 'No. No. Mailto', no. Header(felf), no )
                                                                                                                                                                                                                                                                        "Jhin/registry fatchs" "A seeks ago
                                                                                                                                                                              TENNESS BREET
                                                                                                                                                                                                                       regionrych.b
        3 - 8 - 1
                                                                                                                                                                                                        B.A. R. B. SERRY - SHEEL/SHE
                                                                                                                                                                                                                                                                                                                 Deglishry_registry_1
                                                                                                                                                                             1465
                                                                                                                                                                             -wends tighect-1:- (Container-Core Classification)
        white I I -- I can benched ) !
                                                                                                                                                                             Twendstiglend: 1:-/Container-Code-Clessifications
Twendsfiglend: 1:-/Container-Code-Clessifications purhow endokeck.pp dhafacements
            Shifter of the
            für (betitenfiter) (
                if | thanking = 0 || ] = n_han|med|en|| | | Sate = "" | Stark[en]-- |
etse dans = ber
                                                                                                                                                                             100POCTORS FILES
                                                                                                                                                                              Imperply services
                tf [ per es 2 dik date es tentos 3 f Ser = ou ; Ser = ou 3
                                                                                                                                                                             DOM
                    eine | Se o fe o " 1
                                                                                                                                                                             b) /ww/share/doc/setted quested/margins/settrelay
vi. our/share/doc/sed/margins/doc/sed
                 tion - spring! "managem ", time, to, dame, to I
            AS - Substition_base(max(red)),bee,b)
            printfi "No Bio No Bobe Walle", no, etc. pe, time, no, as 3
                                                                                                                                                                              wendall@test:1:-JContateer-Code-Class&Floatherd []
    artistff time_fet, so, time_ts, time_se )
fate +"SOATE AMOS" | Blass (unask) of Sprey amount medical
**11 *
# 207 "block" - Toe Bes. 18 29:19:19 257 1984
# finb Litoch larr - bribgtruber Lighen poor - CES: TERIG. #52
```

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