User Interviews Debrief

Napolean

What stood out:

- Laura: ICR (IBM Container Registry) will tell you theres a problem but not how to fix it
  - "Hey you have a problem but doesn't tell you which version to use to fix it"
  - Shripad - Since we are at the source and shifting left we can delivery this capability
- GitSecure using Static Scan Napolean asks about Dog Fooding
  - Shripad - This capability is in progress
  - Should be able to use for repositories on ibm.github.com
- Conflict between Laura and Christophe persona
  - Laura - security is a huge priority
  - Christophe - just want to focus on features and need to educate developer
  - Shripad - Opinionated approach to security
- Static scan scans lines in code vs GitSecure scans dependency versions
- Main take away: Need to have steps to have to fix vulnerabilities
- Classifying improvements vs Vulnerability notifications
  - Provide justification to developers
  - Shripad - Go beyond vulnerabilities, like a IPhone update
    a. Notifications when dependencies change (MVP)
    b. Why you should fix
    c. How you should fix
- Already have vulnerability notifications as best practice
  - This project goes beyond vulnerability notifications

Nicholas

What stood out:

- Laura and Christophe were different in their approach to security
- Security as an inhibitor vs Security as a priority
- Shirpad
  - Notification that can be blocked
  - Manager of Christophe knows that notification was given
  - Don't block developers (Christophe mentioned soft-block)
  - Laura will look for notifications from services
- Other tools may provide steps foward

Next steps

- Next week's meeting we go over as-is and hills