2016-05-05 Meeting notes

Date

05 May 2016

Attendees

- Houshang
- Rita McKissick
- Jon Zeolla

Goals

- Discuss ‘Single Pane of Glass’

Discussion items

1. What goal does a ‘Single pane of glass’ achieve?
    a. Need Easy Start and stop Services - JZeolla
    b. Need to easily troubleshoot - JZeolla
    c. Get Basic operational - JZeolla
    d. Health monitoring in general. - JZeolla
    e. Alert when something is broken - JZeolla
    f. Dashboard gets to everything or just high level. -RMcKissick
    g. How functional is it? Or it just a navigation point with a lot of useful info. - JZeolla
    h. That first page needs to be on a 60inch screen - JZeolla
2. What are some Examples?
    a. iPhone - HLivian
    b. Windows 10 - HLivian
3. Hub & Spoke UI Model
    a. Flatten a hierarchy
    b. Dashboard needs to be customizable - JZeolla
    c. Need profiles for Servers and People - JZeolla
    d. Need Slices and different views of things - JZeolla
    e. Need to generate a report everyday on this, an Executive View - JZeolla
    f. Need a concept for saved searches, shortcuts - JZeolla
    g. Need to see what's being executed exactly. Debugging style view. - JZeolla
    h. Output snapshots need to be escalate to me. - JZeolla
    i. IS there some kind of Case Management system? - JZeolla
    j. Want to share a link of where I am with someone else - JZeolla
    k. Visualization Needs - JZeolla
        i. Time based trending with focus on anomalies
        ii. Ordered lists by geo regions
        iii. How much data over protocols or ports
        iv. How are things trending over time.
        v. Health check, what's having issues?
        vi. Constant visual for health
    l. Very quickly it's going to get detailed, very important to drill down, drilling in is most important use case.
4. Filter Lake Concept
    a. Really like telling you the choices - JZeolla
    b. Want to be able export these metrics as a report - JZeolla
5. Should roles have different UI? - JZeolla
    a. Roles should have a baseline. Then tweak
    b. Data science wants custom only interface, they are rarely satisfied with any stock visuals, they always want to create their own.
    c. Big Team versus small Team
        i. Big Team has major separation of duty
        ii. Novice users might have little training but need to dig into the data
        iii. A lot more detailed needs in larger
        iv. Smaller Team: All senior level in smaller team
6. Would making Learning Models proprietary keep them safe?
    a. Determined attacker will get it anyway.
    b. They will pay just to reverse engineer the algorithm
    c. Has seen some buzz and even classes on subverting Machine Learning Models
7. App Store
    a. Open Exchange would be great for Learning Models or enrichments - JZeolla
        i. Would like to submit enrichments to the community - JZeolla

    b. Splunk has an App Store - JZeolla
8. Jon Zeolla Interview
    a. Carnegie Mellon University (CMU) SOC Team
        i. SOC Team has 12 Members
        ii. Has a 60inch monitor that shows status when they walk in the office
        iii. He supports Operations and provisions access as a Platform Engineer
        iv. Very interested in Metron wants to know how committed we are looking to invest in building a system
        v. Metron Architecture exactly matches what he was hoping to build for CMU
        vi. Two years ago he set out to redesign the system. OpenSOC Architecture inspired him.
    b. Runs Meetups and Conferences in Pittsburgh
    c. Invited Hortonworks to visit if we are in Pittsburgh
    d. Open to giving perspective
        i. Really excited. Looking at doing seam implementation. Make this 80% of day to day.

Action items

- [ ] @Houshang to mockup Saved Search