2022-06-14 - ONAP: SECCOM retrospectives for log4j (Istanbul Maintenance) and Jakarta releases

**Topic Leader(s)**
- Pawel Pawlak
- Amy Zwarico

**Topic Description**
Sharing latest lessons learnt for:
- Log4j fix implementation in Istanbul Maintenance Release
- Jakarta security status update

**Topic Overview**
Sharing ONAP SECCOM experience coming from implementation of log4j fixes in the dedicated Istanbul Maintenance Release and Jakarta Release security achievements.

**Slides & Recording**
Live Session to be recorded for YouTube

- **YouTube**
  - Live Interactive Session
    - slides
    - recording

  LFN Staff may elect to publish some videos to YouTube. Please indicate here if you do not want your session to be published to YouTube.

**Agenda**
- Log4j fix implementation in Istanbul Maintenance Release
- Jakarta security status update
- Summary
Minutes

- Lesson Learnt from Log4 Security Alert handled early this year by the ONAP Community
- Review of ONAP Jakarta Security requirements delivery:
  - 299 recommended package upgrades - 60% already completed
  - OpenSSF Badging - 5 projects on their way to "Gold"
- Improvements
  - SBOM ("Software Bill of Materials") can help to identify dependencies early; ONAP Community is taking an action to move forward integrating it as part of our CI/CD pipeline

Action Items

- ODL (Robert Varga) is offering some experience about CycloneDX format and SBOM to be reviewed by the ONAP SECCOM
- To check with Robert Varga and Muddasar Ahmed SBOM proxy