ONAP
OPEN NETWORK AUTOMATION PLATFORM

ONAP El Alto Security SoW proposal

Pawel Pawlak

12th June 2019

El Alto SoW proposal to ONAP community

1. Work on OJSI tickets to solve penetration tests findings/CVEs – 60 days ticking clock!
2. Update ONAP environment (java, python, kubernetes, docker, ubuntu, alpine…) to commonly agreed versions
3. Focus on known vulnerabilities by **upgrading** libraries to commonly agreed versions – coordination with ONAP Release Manager, stakeholders: OOM, Integration, PTLs
4. Focus on known vulnerabilities by **replacing** libraries with commonly agreed versions and components – coordination with ONAP Release Manager, stakeholders: OOM, Integration, PTLs
5. Update CII Badging answers within release LCM
6. Contribute to ONAP security communication matrix creation

El Alto SoW proposal to SECCOM community

1. Support ONAP community in achieving El Alto goals
2. Update Security by Design with: CII Badging gates, https communication update for M3, revamping of the vulnerability review tables
3. Update Oparent.pom file with SECCOM recommended and consulted versions, including dependency management from Maven
4. Create communication matrix based on inputs from PTLs and validate it with scripts with Integration team – coordinate with architecture team
5. Support Integration team with security testing enhancements
6. Consider security features scope and perform comparative analysis of AAF and ISTIO
7. Design CMPv2 implementation – stakeholder: AAF
8. Benchmark Nexus-IQ with Whitesoftware for Dan's project
9. Continue known vulnerabilities management and CII Badging answers reviews

ONAP

OPEN NETWORK AUTOMATION PLATFORM