Mojaloop
Platform Quality & Security

Product Council update, PI-24 18th June 2024

PQS workstream, Sam Kummary, MLF

Workstream Update

Workstream Name:	Mojaloop platform quality & security (PQS)
Roadmap Pillar:	Quality Product (Foundation)
Lead:	Sam Kummary
Workstream Objectives:	The focus for PI-24 will be on 1) GitHub maintenance of Mojaloop repositories (used in the platform), continuation of 2) Hardening Mojaloop core and addressing any known and reported quality, security issues. 3) We also want to start the activity of identifying all the third party dependencies in Mojaloop to better manage situations when issues arise with any of them or as some of them are not maintained. 4) Bonus: Another objective this PI is to look into achieving OpenSSF badge for Mojaloop.
Progress Against Objectives:	1. Mojaloop GitHub repos maintenance - tightening up on branch protection rules 2. Dependabot alerts 3. SonarCloud features usage on PRs and repositories 4. Projects (github issues) for third-party dependency management created
Anticipated Progress by PI End:	1. GitHub repositories that are all part of Mojaloop platform to follow best practices 2. Mojaloop release made with all high, critical dependabot security alerts addressed
Roadblocks:	1. Resourcing issues, no funded team available.
Support Needed:	1. No dedicated team for the PI, thankful for the contributions so far. 2. Further contributions welcome.

Mojaloop PQS: Objectives

1. Hardening of Mojaloop releases
2. Security testing of Mojaloop
   - Assess feedback from the testing internally ✅
   - Prioritize issues based on criticality and severity ✅
   - Update backlog with stories to address issues
3. Review core and related repositories released with Mojaloop for ✅
   - Ensure dependabot alerts are addressed
   - Ensure Snyk issues are addressed
4. Review any tasks “to-do” in the codebase and related quality issues
5. Review PRs in critical repositories and address (close, approve / reject) ✅
6. Update nodejs version for any services not yet upgraded ✅
7. Update maintenance tooling (license-scanner and such)

Mojaloop PQS: Mojaloop release v16.1.0 RC

Review core and related repositories released with Mojaloop for

1. Snyk alerts for Central-ledger repository are addressed
2. Dependabot alerts for Central-ledger repository are addressed (moderate, high and critical)
3. Ensure main branch is protected and collaborator list is up-to-date
4. Ensure open PRs are addressed, closing stale PRs
5. Update audit exceptions json file to remove exceptions added that are not necessary anymore
6. Close issues on the repository that are fixed / out-of-date
7. Ensure codeowners file is current

Reviewing updates and vulnerabilities (GitHub, NVD, other related media) constantly

1. Take necessary action for Mojaloop services as required
2. Provide guidance and mitigate exposure to Mojaloop

Mojaloop PQS: SBOM for Mojaloop

SBOM of all services included in Mojaloop Platform's core (getting started)

1. Exploring tooling - CycloneDX and SPDX
2. Individual SBOMs for core repositories
3. Centralized list for all core / critical repositories
4. Automate generation during release time
5. Use circleci/cron jobs for maintenance

Mojaloop PQS: Design & Implementation guidance

1. Mojaloop Invariants: https://docs.mojaloop.io/community/standards/invariants.html
2. Mojaloop CVD policy:

   https://docs.mojaloop.io/community/contributing/cvd.html#disclosing-and-receiving-information-regarding-security-vulnerabilities
3. Mojaloop cyber-security architecture: https://docs.mojaloop.io/community/tools/cybersecurity.html#mojaloop-cybersecurity-architecture
4. Guidance around moving from alpha / beta to release quality:

   https://community.mojaloop.io/mojaloop_foundation/pi-22-core-releases-work-stream-reviews-4ami
5. Other Mojaloop standards: https://docs.mojaloop.io/community/standards/guide.html#standards

Mojaloop PQS: Roadmap

1. Hardening of Mojaloop releases - continuation
2. SonarCloud - address issues in detail
3. Improve tooling used in CI/CD - ci tools, license checkers
4. OpenSSF badge
5. Blog posts and guidance to implementers and improve documentation