EDGE FOUNDRY

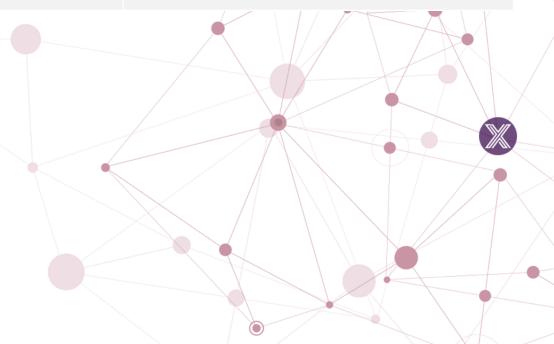
DevOps Working Group

Thursday October 22, 2020



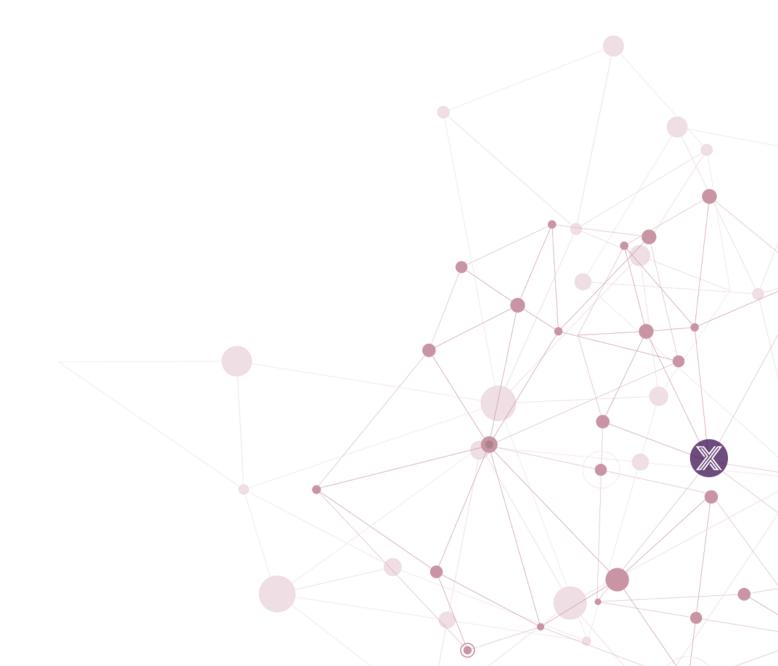
Agenda

Time	Topic	Owner
10 Min	DevOps Updates (Hanoi)	Ernesto
10 Min	Inline Snyk Docker Image Scans Discussion	Ernesto
5 Min	Kanban Board Review	All
5 Min	AOB / Opens	All





Attendees





DevOps WG Update (Hanoi)

Pipeline Enhancements

- #252 [Watching] Build Snaps natively on Ubuntu
- #260 [Backlog] CodeCov results not uploading
- #87 [Complete] Open source components of GitHub release (github3api)
- #261 [In Progress] Research best way to scan docker images pre release
- #137 [In Progress] Spike: CIS Docker Security Benchmark for EdgeX





Inline Snyk Docker Image Scan

- Snyk CLI offers the snyk test command which shows scan results inline
- Pipeline requirements:
 - implement on-demand testing of docker images (after pushed to nexus i.e. master builds)
 - notify distribution list of users when vulnerabilities are found
 - filter only on high severity findings
 - allow ignoring of Snyk findings via the .snyk policy file
 - Another option not used yet
 - --fail-on=<all|upgradable|patchable>
 - Mark the build unstable but allow creation of the artifact: https://jenkins.edgexfoundry.org/sandbox/blue/organizations/jenkins/Functional-Testing%2Fsnyk-testing/detail/snyktesting/17/pipeline





Notes

Enable CodeCov on master builds again

Open questions around Snyk will be presented in next week's Security WG meeting

