EdgeX Security WG Meeting 09/23/2020

**Attendees:**



**Agenda**

* Action Items from last meeting
	+ Action item: adjust proxy setup to use kong acl allow / deny (possibly Ireland scoped) and upgrade Kong to above 2.0 (Colin)
	+ Action item: [edgex-go/issues/1955](https://github.com/edgexfoundry/edgex-go/issues/1955) should become a here to there plan wiki doc / google doc / possibly becomes an ADR
		- Let’s document the hurdles (as a checklist) for what needs to adjust
	+ Action item: ack edgexfoundry/docker-edgex-mongo and edgexfoundry/docker-edgex-volume as won’t fix
	+ Action Item: James Gregg present a POC of what a CIS docker benchmark guide may look like
	+ Action Item: Document the vulnerabilities on our disclosure page. Include details that we haven’t evaluated if the vulnerability is exploitable, fixing is upgrading (Colin)
	+ ~~Action Item: coordinate an application service release to verify we have fixes for the zeromq vulnerabilities (Colin create issue on edgex-go)~~
	+ Action Item: snyk reports are for past images not for future images / work in progress. (ping devops if snyk can scan nexus not docker hub - Jim White)
	+ ~~Action Item: validate new builds get 4.3.3 of zeromq (Lenny)~~
	+ ~~Action Item: create a github issue to validate we’re not vulnerable to edgex-go:go.mod~~ [~~https://app.snyk.io/vuln/SNYK-GOLANG-GITHUBCOMDGRIJALVAJWTGO-596515~~](https://app.snyk.io/vuln/SNYK-GOLANG-GITHUBCOMDGRIJALVAJWTGO-596515)
	+ Action Item: will <https://github.com/edgexfoundry/edgex-go/issues/2495> slip how critical is it? (Tony)
	+ Action Item: <https://github.com/edgexfoundry/edgex-docs/pull/220> needs approval / a read (Colin / Tony)
	+ Action Item: confirm at TSC <https://github.com/edgexfoundry/edgex-docs/issues/136> likely not making Hanoi
	+ Action Item: <https://github.com/edgexfoundry/edgex-go/issues/2537> (Colin)
* Review Snyk
* Anything at risk of not making Hanoi?
* Review
	+ QA code review
	+ In Progress
	+ New
	+ Release backlog if necessary
* Open

### Notes

* Action Item: adjust snyc such that we’re only scanning 1.2.latest. Device and app services might be an exception -- tread carefully
* Action Item: <https://github.com/edgexfoundry/edgex-docs/pull/140> review prior to end of October (Tony)
* Action Item: contact brett preston of linux foundation get on **security-issues@lists.edgexfoundry.org** distribution list (Colin)