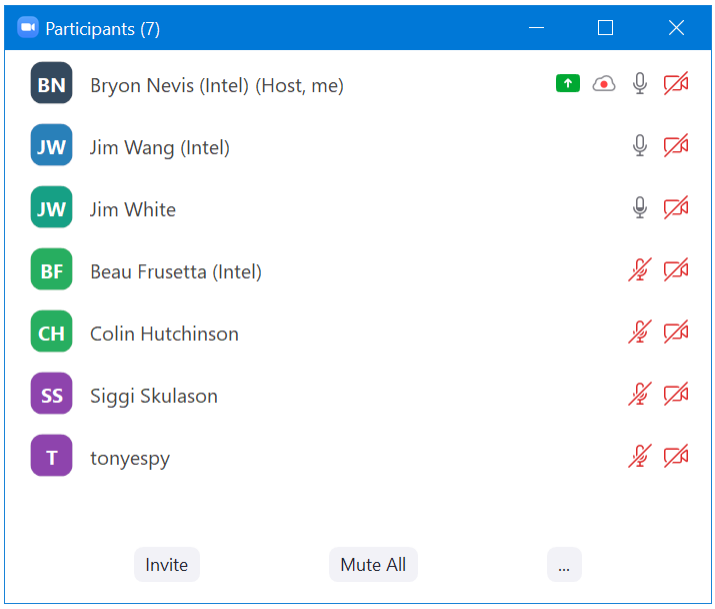
EdgeX Security WG Meeting

https://wiki.edgexfoundry.org/display/FA/Security+Working+Group

September 1, 2021

Attendees



Standing Agenda

- Review Security Board
  - Finished codeQL enabling
  - Added documentation task for Vault TTL

Icebox	New	Backlog	WIP	Done
9	0	12 (+1)	1 / 2 (+0/1)	9 (+1)

- Securing Consul Board

Ph-3 ToDo	Ph-2 ToDo	WIP	Done
4	1 / 2	0 / 0	3

- Review CIS docker scan (will skip unless something changes) (click latest run, go to classic, view console output).
- Review Snyk (Jenkins) (will skip unless something changes) (Imagelist)

Critical	High	Medium	Low
36!	28	23	2

    - Alpine 3.12 became vulnerable this week.
    - New Snyk reports regarding vulnerability in openssl/libssl1.1 1.1.1k-r0
    - Q: Do we want to move from alpine to busybox or distroless for most base images?
        - Decision might be more clear if we looked at LTS policies of busybox vs alpine vs distroless. Distroless has bash-static.
        - Looking at (1) availability of patches for an LTS and (2) minimizing the number of times we need to update the base image.
        - Research CVE rate of busybox vs alpine vs others. Concerned about doing this in Jakarta.
        - Should also look at the LTS policy of go 1.16 and go 1.17 (go doesn't have an LTS policy)
    - DevOps will be leading the upgrade.

- Review action items from previous week

Agenda

- No progress on the Consul security after-the-fact-disable.

Action Items

- 7/14: Bryon: Update security policy documentation w.r.t. when to use GitHub security advisories to notify users of issues.
- 8/25: Jim/Tony: Report back progress on Consul security after-the-fact disable. (Look at a snap configure hook to see if it will work to modify ACL config.)
- 9/1: Test the VaultTTL enhancement.
- ~~8/25: Bryon: Document Alpine 3.12 issues.~~ https://wiki.edgexfoundry.org/display/FA/Known+Security+Issues
- ~~8/25: Bryon: Add issue to Jakarta documentation board to document new Vault TTL setting.~~ https://github.com/edgexfoundry/edgex-docs/issues/553
- 9/1: Bryon: Research base image alternatives -- add to backlog