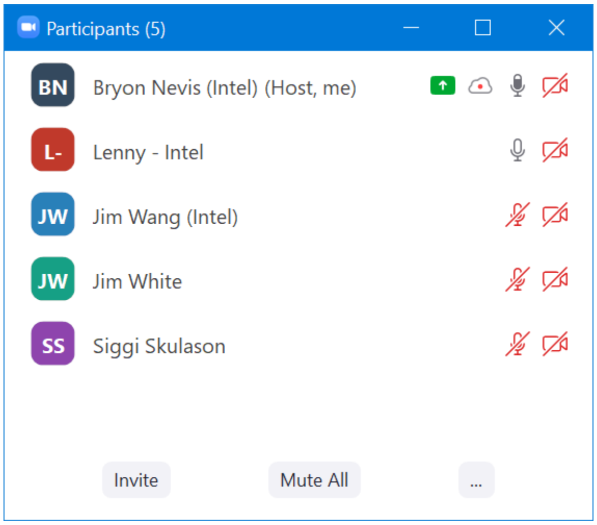
EdgeX Security WG Meeting

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

October 6, 2021

Attendees



BN Bryon Nevis (Intel) (Host, me)

L- Lenny - Intel

JW Jim Wang (Intel)

JW Jim White

SS Siggi Skulason

Standing Agenda

- Review Security Board

Icebox	New	Backlog	WIP	Done
9	2	3	4 / 4	err

- Securing Consul Board

Ph-3 ToDo	Ph-2 ToDo	WIP	Done
7	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

0	4 (false positive)	16	0

  - Performed major cleanup on Snyk project; removed 2.0.0 and 2.0.1 containers from dashboard. Prefer more accurate CLI-based go.mod scans over inaccurate web-based scans of go.mod. (Web-based scan can’t distinguish submodules of a github-based project: web only analyzes top-level URL.)

- Review action items from previous week

Agenda

- ADR for delay start service secret store token - ready for 2nd round review https://github.com/edgexfoundry/edgex-docs/pull/389.
- CORS support
  - Status: We backed up support in API gateway and planned to implement CORS in server middleware
  - Have code in https://github.com/edgexfoundry/edgex-go/blob/main/internal/pkg/correlation/middleware.go that adds output headers. Have code go-mod-bootstrap where we create a request router that we can plug in to. Also has required implementation for C device services.
- Review work left for final stretch for Jakarta
  - Dispositioning:
    - Research base image alternatives to limit CVE exposure
      - https://github.com/edgexfoundry/edgex-go/issues/3690
  - De-scoping
    - Secret store unsealing daemon (tech debt)
      - https://github.com/edgexfoundry/edgex-go/issues/1944
    - Descope Consul Phase 3 hardening
      - https://github.com/edgexfoundry/edgex-go/issues/3158
      - https://github.com/edgexfoundry/edgex-go/issues/3257
      - https://github.com/edgexfoundry/edgex-go/issues/3258
      - https://github.com/edgexfoundry/edgex-go/issues/3227
  - AR: Create ticket on edgex-compose to expose Consul on host IP when Consul is in secure mode (need mirror ticket in edgex-go for the snap)
    - https://github.com/edgexfoundry/edgex-compose/issues/190
    - https://github.com/edgexfoundry/edgex-go/issues/3744
- Postponed: ~~More data on being able to switch in- and out- of insecure Consul mode in snaps~~

Action Items

- 7/14: Bryon: Update security policy documentation w.r.t. when to use GitHub security advisories to notify users of issues.
- ~~9/15: ALL: Review #3709 proposal~~
- ~~9/15: Lenny: Submit issue for resiliency on Consul token~~
- 9/15: Bryon: Go back and check with users who requested remote gateway user management and see if they are OK with installing a persistent key of their choice to do this? If not, may have to not rotate kong admin key every boot.
- ~~9/28: Bryon: Create ticket to figure out how consul UI protects the consul token.~~ https://github.com/edgexfoundry/edgex-ui-go/issues/448