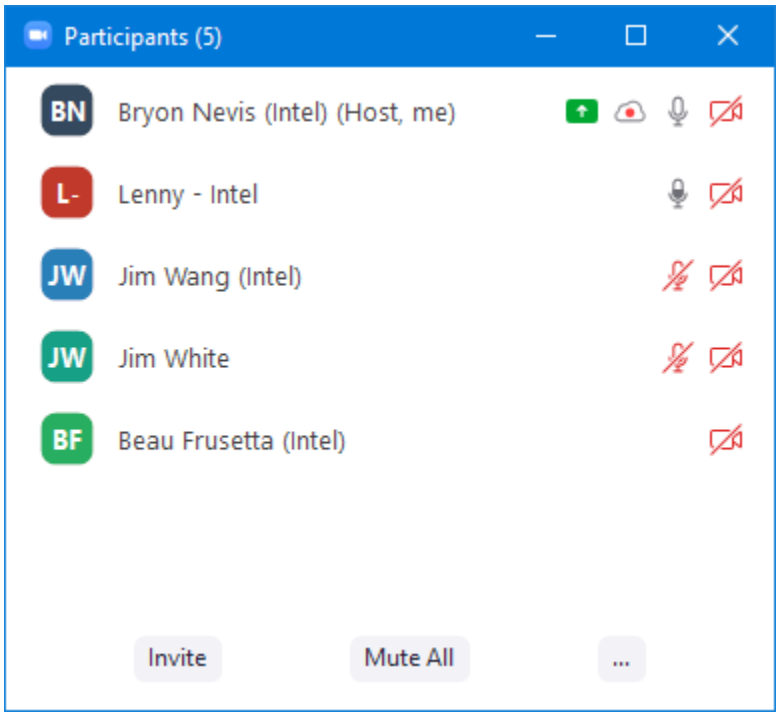
EdgeX Security WG Meeting

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

July 28, 2021

Attendees



Standing Agenda

- Review Security Board

Icebox	New	Backlog	WIP	Done
9	1 (+1)	10 (→2)	3 / 0	3

- Securing Consul Board

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

- Review CIS docker scan (will skip unless something changes) (click latest run, go to classic, view console output). Project still meeting its baseline:

```
[1;32m[PASS][0m 4.1  - Ensure a user for the container has been created
[1;31m[WARN][0m 5.3  - Ensure Linux Kernel Capabilities are restricted within containers
[1;31m[WARN][0m      * Capabilities added: CapAdd=[IPC_LOCK] to edgex-vault
[1;32m[PASS][0m 5.4  - Ensure privileged containers are not used
[1;32m[PASS][0m 5.5  - Ensure sensitive host system directories are not mounted on containers
[1;32m[PASS][0m 5.6  - Ensure ssh is not run within containers
[1;32m[PASS][0m 5.7  - Ensure privileged ports are not mapped within containers
[1;32m[PASS][0m 5.9  - Ensure the host's network namespace is not shared
[1;31m[WARN][0m 5.12  - Ensure the container's root filesystem is mounted as read only
[1;31m[WARN][0m      * Container running with root FS mounted R/W: edgex-vault
[1;32m[PASS][0m 5.15  - Ensure the host's process namespace is not shared
[1;32m[PASS][0m 5.16  - Ensure the host's IPC namespace is not shared
[1;32m[PASS][0m 5.19  - Ensure mount propagation mode is not set to shared
[1;32m[PASS][0m 5.20  - Ensure the host's UTS namespace is not shared
[1;32m[PASS][0m 5.21  - Ensure the default seccomp profile is not Disabled
[1;32m[PASS][0m 5.24  - Ensure cgroup usage is confirmed
[1;31m[WARN][0m 5.25  - Ensure the container is restricted from acquiring additional privileges
[1;31m[WARN][0m      * Privileges not restricted: edgex-vault
[1;32m[PASS][0m 5.29  - Ensure Docker's default bridge docker0 is not used
[1;32m[PASS][0m 5.30  - Ensure the host's user namespaces is not shared
[1;31m[WARN][0m 5.31  - Ensure the Docker socket is not mounted inside any containers
[1;31m[WARN][0m      * Docker socket shared: edgex-sys-mgmt-agent
```

- Review Snyk (Jenkins) (will skip unless something changes) (Imagelist)

Critical	High	Medium	Low
0	40 (-1)	19 (+1)	6 (unch)

  - Remediated but not yet showing:
    - device-coap(-arm64) -24H -8M
  - New vulnerabilities - Docker -- need investigation
    - nexus3.edgexfoundry.org:10004/sys-mgmt-agent:latest
      - Upgrade Alpine:3.12 openssl to version 1.1.1j-r0 or higher.
      - Upgrade Alpine:3.12 openssh to version 8.3_p1-r2 or higher.
      - Upgrade Alpine:3.12 busybox to version 1.31.1-r20 or higher.
      - Upgrade Alpine:3.12 apk-tools to version 2.10.6-r0 or higher.
      - Believe bumping to docker:20.10.7 will fix, Lenny to investigate.
    - nexus3.edgexfoundry.org:10004/docker-security-secretstore-setup-go:master
      - Upgrade Alpine:3.12 curl to version 7.77.0-r0 or higher.
      - Might not need curl any longer. Jim to investigate.
  - Upcoming fixes (not yet released):
    - github.com/dgrijalva/jwt-go@4.0.0 once released

- Review action items from previous week

Agenda

- Younes ABDELOUHAB will file ticket to request that Kong auth be on a per-route basis so that authentication can be mixed-and-matched. Security WG supports.

Action Items

- ~~7/14: Bryon: Update known security issues with Snyk findings~~
- 7/14: Bryon: Update security policy documentation w.r.t. when to use GitHub security advisories to notify users of issues.
- 7/21: Tony: File issue to allow configuration.toml setting to change default token TTL. (cmd/security-secretstore-setup/res/filetokenprovider.toml)
- 7/28: Lenny: Add release note for device-coap base image bump
- 7/28: Jim: Investigate if curl still needed in secretstore-setup.
- 7/28: Bryon: TSC. Update security known issues with current Snyk “highs”.