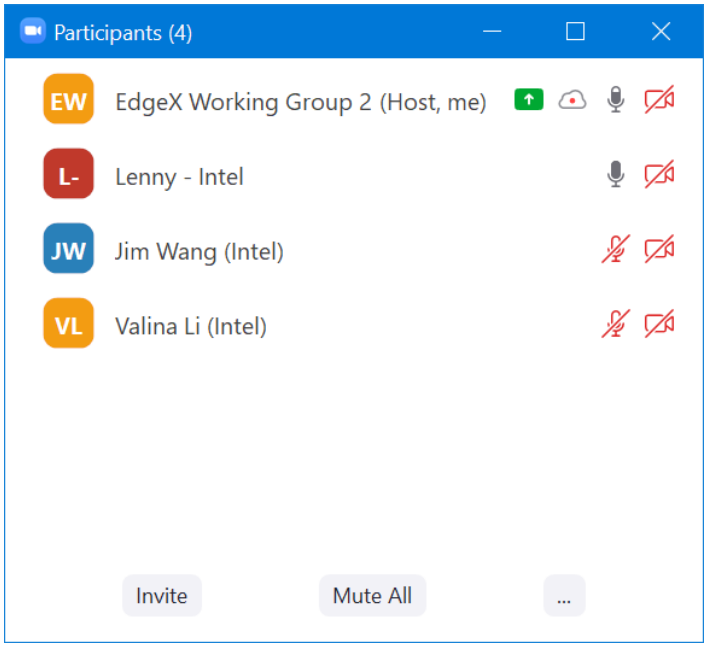
EdgeX Security WG Meeting

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

June 29, 2022

Attendees



Agenda

- Snyk update - added scanning of LTS release - issues to be dispositioned - volunteers?
    a. On or after 21 July we need to go and edit the scan interval for jakarta synk tests to monthly (currently locked right now)
    b. AR: Submit PR against github.com/canonical/edgex-snap-hooks to update testify to non-CVE version.and notify Farshid. (go-mod-outdated, and update)
    c. AR: Bryon: edgexfoundry/app-service-configurable:jakarta:go.mod - need to disposition in snyk and update security wiki regarding AES encryption
    d. https://www.cve.org/CVERecord?id=CVE-2021-38561 needs to be dispositioned as to whether we are affected.
    e. Dispositioning jakarta issues is priority

- What kind of security metrics to we want to collect
    a. How metrics work / requirements
        - Must use go-mod-bootstrap

            - The metrics manager and message bus reporter live here
        - Must add metrics bootstrap handler to the bootstrap init call (late initialization)
            - Depends on message bus handler
            - And thus depends on secrets
        - Must have metrics configuration in writable section
        - Must be connected to message bus to report metrics
        - Can collect metrics at any time, but will be lost until the metrics bootstrap handler is invoked.
    b. Go metrics registration is separate from the go metrics reporter. Metrics can be:
        - Counters e.g. # messages received (increment by value, typically 1)
        - Timers e.g. how long did some action take? (is time based) (“samples” for average min/max reporting)
        - Gauge - current value of something (for things that decrement and increment)
        - Histogram - wrap “samples” e.g. # of bytes exported (integer rather than time)
    c. Asks:
        - Is there anything from system health/dashboard that we want to report from the security services that is valuable?
        - If so, how will that be reported?

- Brainstorming - for security services themselves
    a. Secretstore-setup / file-token-provider - NA too early
    b. Boostrapper - NA too early
    c. Proxy-setup - doesn’t have anything that can’t get from Kong
    d. Kong-db - internal only outside scope
    e. Kong - has its own metrics endpoints
    f. Vault - has its own metrics endpoints
    g. Consul - has its own metrics endpoints
    h. Security-spiffe-token-provider
        - Counter - every token requested
        - Timer - how long does it take go return a new token
        - Counter - known secret requested (tag by secret name)
    i. Spire-server - out of scope
    j. Spire-agent - out of scope
    k. Spire-config - one-shot N/A
- Brainstorming - for every non-security service (tagged by service name automatically)
    a. Counter - secret requested from the store
    b. Counter - consul token requested
    c. Counter - put secret
    d. Timer - how long to obtain secret token
    e. Timer - how long to obtain consul token
    f. (stretch - spiffe-token-provider metrics)

Standing Agenda

- Review Security Board
- Securing Consul Board (skip)
- Review CIS docker scan (will skip unless something changes) (click latest run, go to classic, view console output).
    - Last checked: Tue Nov 16 05:36:01 UTC 2021
- Review Snyk (Jenkins) (will skip unless something changes) (Imagelist)
- Review action items from previous week

Action Items

- 7/14/21: Bryon: Update security policy documentation w.r.t. when to use GitHub security advisories to notify users of issues.
- 6/22/22: Bryon: Update known security issue wiki (add GHSA?)