EdgeX Security WG Meeting

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

October 6, 2021

Attendees

Standing Agenda

- Review Security Board

<table>
<thead>
<tr>
<th>Icebox</th>
<th>New</th>
<th>Backlog</th>
<th>WIP</th>
<th>Done</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>2</td>
<td>3</td>
<td>4 / 4</td>
<td>err</td>
</tr>
</tbody>
</table>

- Securing Consul Board

<table>
<thead>
<tr>
<th>Ph-3 ToDo</th>
<th>Ph-2 ToDo</th>
<th>WIP</th>
<th>Done</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>1 / 2</td>
<td>0 / 0</td>
<td>3</td>
</tr>
</tbody>
</table>

- 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)

<table>
<thead>
<tr>
<th>Critical</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
</table>
- 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

- 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](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](https://github.com/edgexfoundry/edgex-go/issues/3690)
  - De-scoping
    - Secret store unsealing daemon (tech debt)
    - Descope Consul Phase 3 hardening
    - [https://github.com/edgexfoundry/edgex-go/issues/3158](https://github.com/edgexfoundry/edgex-go/issues/3158)
    - [https://github.com/edgexfoundry/edgex-go/issues/3257](https://github.com/edgexfoundry/edgex-go/issues/3257)
    - [https://github.com/edgexfoundry/edgex-go/issues/3258](https://github.com/edgexfoundry/edgex-go/issues/3258)
    - [https://github.com/edgexfoundry/edgex-go/issues/3227](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-compose/issues/190)
    - [https://github.com/edgexfoundry/edgex-go/issues/3744](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