EdgeX Security WG Meeting

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

November 9, 2022

Attendees

![Participant List]

Agenda

- EdgeX Minnesota planning conference
### Big Ticket Items / Features

<table>
<thead>
<tr>
<th>Theme / Title</th>
<th>OSSF?</th>
<th>ID</th>
<th>T-Shirt</th>
<th>Breaking? In/Out</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microservice authentication (JWT-based) UCR</td>
<td>✓</td>
<td>#613</td>
<td>L</td>
<td>✓</td>
</tr>
<tr>
<td>Secure microservice distribution (OpenZiti) UCR, ADR, Implementation</td>
<td>TBD</td>
<td>XL</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Capture metrics for additional security events</td>
<td>#374</td>
<td>M</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Delayed start services support in snaps (upstream system attestor)</td>
<td>TBD</td>
<td>L</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

### Security Assurance
- Check in STRIDE threat model
- Jakarta LTS maintenance (version bumps)
- Fuzz testing for REST/MQTT interfaces
- Publish SPDX SBOM for Minnesota release
- Investigate (and integrate?) GoKart static analysis tool
- Put security.txt in our release artifacts
- Help LF/X improve BluBracket scanning of EdgeX

### Tweaks / Tech-Debt
- API gateway dead code removal
- Secret API’s rename “path” to “secretname”
- CamelCase configurename keys
- Pull postgres out of startup services list
- Remove superfluous delay in consul_wait_install.sh
- Cap # of redis connections

#### Update: Secret API’s is a breaking change

- Microservice authentication UCR
  [https://github.com/edgexfoundry/edgex-docs/pull/898](https://github.com/edgexfoundry/edgex-docs/pull/898)

- Microservice authentication ADR
  [https://github.com/edgexfoundry/edgex-docs/pull/659](https://github.com/edgexfoundry/edgex-docs/pull/659)

- OpenZiti investigation update (Clint)
  - Potential benefit from being able to bind to a hardware root - PKCS11
    - Potential integration with Yubikey, Nitrokey, tpm2-pks11 plugin, etc.
  - End-to-end encryption enabled by default
  - Possible Vault + OpenZiti integration coming
  - Note: dockerfile to bring up edgex:
    [https://github.com/edgexfoundry/edgex-compose](https://github.com/edgexfoundry/edgex-compose) (docker-compose.yaml)
  - Clint will work on a proposal for ~1st week December

### 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: August 3, 2022 – as expected
- [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.