# Agenda

<table>
<thead>
<tr>
<th>Time</th>
<th>Topic</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Min</td>
<td>DevOps Updates (Hanoi)</td>
<td>Ernesto</td>
</tr>
<tr>
<td>5 Min</td>
<td>Developer Scripts Smoke Tests</td>
<td>Ernesto</td>
</tr>
<tr>
<td>10 Min</td>
<td>Inline Snyk Docker Image Scans Discussion</td>
<td>Ernesto</td>
</tr>
<tr>
<td>15 Min</td>
<td>EdgeX Global Pipeline Documentation</td>
<td>Chinu</td>
</tr>
<tr>
<td>5 Min</td>
<td>Kanban Board Review</td>
<td>All</td>
</tr>
<tr>
<td>5 Min</td>
<td>AOB / Opens</td>
<td>All</td>
</tr>
</tbody>
</table>
Attendees
DevOps WG Update (Hanoi)

• **Pipeline Enhancements**
  - #252 [Watching] Build Snaps natively on Ubuntu
  - #78 [Complete] Implement Functionality to rebuild artifacts during release/code freeze
  - #325 [Complete] Developer Scripts: Run Smoke Tests for PR’s
  - #260 [Backlog] CodeCov results not uploading
  - #261 [In Progress] Research best way to scan docker images pre release
  - [Complete] Misc pipeline library tech debt and bug fixes for git-semver.

• **Other**
  - [Complete] Update ADR10 and ADR07 to include changes for Snaps and GitHub releases
Developer Scripts Smoke Test Automation

- Smoke tests added to the edgex-taf-pipelines repository. Thanks Cherry!
- New [Jenkinsfile](#) has been added to the developer-scripts repository
- [Sample pipeline](#)
- Only run’s smoke tests during the PR stage. Skipped when code is merged to master.
- Note: Smoke test take about 30-40 minutes to run.
Inline Snyk Docker Image Scan

• Snyk CLI offers the `snyk test` command which shows scan results inline

• Pipeline options:
  • Break the build: https://jenkins.edgexfoundry.org/blue/organizations/jenkins/edgexfoundry%2Fsample-service/detail/PR-77/8/pipeline/
  • Mark the build unstable but allow creation of the artifact: https://jenkins.edgexfoundry.org/blue/organizations/jenkins/edgexfoundry%2Fsample-service/detail/PR-77/10/pipeline/279/
Notes

• Inline Snyk Scan
  • Mark the build unstable, do not break the build
  • Generate report to review
  • Notify security via email, person who committed code (attach report)
  • Look into ability to disposition/ignore certain vulns
    https://support.snyk.io/hc/en-us/articles/360003851317-Ignore-vulnerabilities

• Docker CIS Benchmark Demo next WG meeting. Maybe also need to bring the discussion into the Security WG.