EdgeX Security WG Meeting

*3/17/2020*

## Attendees:

## 

## Standing Agenda

* [Backlog progress sheet](https://bit.ly/2UFJWGA)
* [Review Security Provider for All Project Board](https://github.com/orgs/edgexfoundry/projects/37)
* [Review Security Board](https://github.com/orgs/edgexfoundry/projects/28)
* [Securing Consul Board](https://github.com/orgs/edgexfoundry/projects/41)
* [Review CIS docker scan](https://jenkins.edgexfoundry.org/blue/organizations/jenkins/edgexfoundry%2Fcd-management/detail/docker-cis-benchmark/3/pipeline/31/)
* [Review Snyc](https://app.snyk.io/org/edgex-jenkins/projects)
  + Filter With Issues & Active

## Agenda

## Notes

* ~~Bryon: Investigate why CIS benchmark tool thinks edgex-redis is running as root~~
* ~~Lenny: create issues for the bootstrap scripts to run as non-root~~
  + ~~Related:~~ [~~email thread~~](https://lists.edgexfoundry.org/g/EdgeX-TSC-Security/topic/80750077#352) ~~and~~ [~~CIS scan~~](https://jenkins.edgexfoundry.org/blue/organizations/jenkins/edgexfoundry%2Fcd-management/detail/docker-cis-benchmark/3/pipeline/31/)
* ~~Colin: Edgex-device-virtual should mount a volume and not have a R/W filesystem~~
* Colin: Find a way to ignore all vault warnings in the CIS scan
* Colin: Find a way to ignore the edgex-sys-mgmt-agent in the CIS scan
* ~~Lenny: Create issue related to proxy-setup override~~
* Securing consul notes:
  + Phase 1: is backwards compatible and not a breaking change
  + Phase 2: is a non backwards compatible breaking change (if running in secure mode / feature flagged)
  + Phase 3: is not a backwards breaking change with phase 2
  + Lenny: If we feature flag phase 2 and it’s incomplete that’s OK no need to push the release date
* Re-evaluate at the end of April if we can meet / meet with a different release date or skip implementation of [Securing Consul Phase 2](https://github.com/edgexfoundry/edgex-docs/blob/master/docs_src/design/adr/security/0017-consul-security.md#phase-2)
* Colin: have the devops group run the CIS scan weekly
* ~~Next security wg meeting:~~ [~~https://lists.edgexfoundry.org/g/EdgeX-TSC-Security/message/352#~~](https://lists.edgexfoundry.org/g/EdgeX-TSC-Security/message/352#)
* ~~Colin: get the docker security scan ran again~~
* ~~Colin: add a review of the security scan to the weekly security group meetings~~