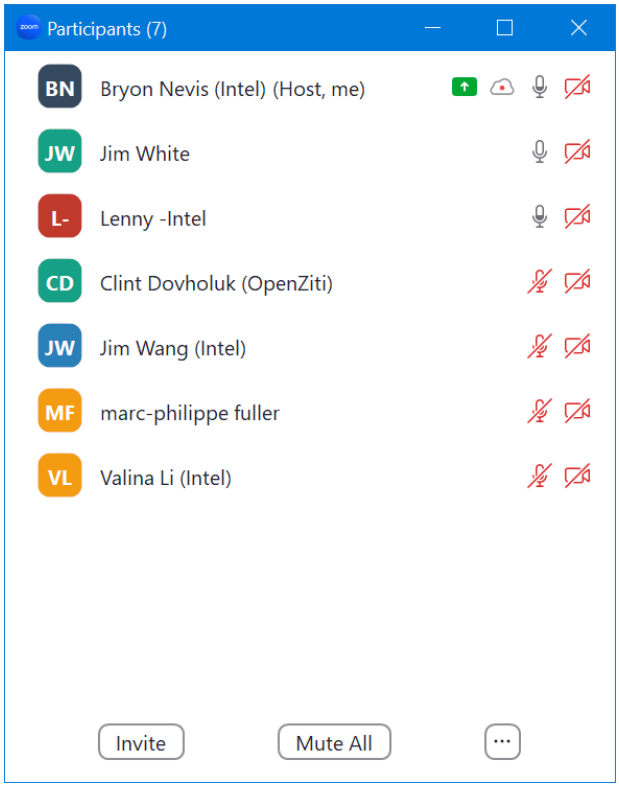
EdgeX Security WG Meeting

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

November 9, 2022

Attendees



Agenda

- EdgeX Minnesota planning conference https://wiki.edgexfoundry.org/display/FA/Nov+14-17%2C+2022%3A+Minnesota+Planning+Conference

Theme / Title	OSSF?	ID	T-Shirt	Breaking?	In/Out
Big Ticket Items / Features					
Microservice authentication (Vault JWT-based) UCR, ADR, Implementation	✓	#613	L	✓	
Secure microservice distribution (OpenZiti) UCR, ADR, implementation		TBD	XL	-	
Capture metrics for additional security events		#374	M	-	
Delayed start services support in snaps (upstream systemd attestor)		TBD	L	-	
Security Assurance					
Check in STRIDE threat model		#858	S	-	
Jakarta LTS maintenance (version bumps)		TBD	M	-	
Fuzz testing for REST/MQTT interfaces	✓	#714	XL	-	
Publish SPDX SBOM for Minnesota release		#4173	M	-	
Investigate (and integrate?) GoKart static analysis tool		#3715	M	-	
Put security.txt in our release artifacts		#4151	S	-	
Help LFX improve BluBracket scanning of EdgeX		#3881	M	-	
Tweaks / Tech-Debt					
API gateway dead code removal		#3583	S	✓	
Secret APIs rename "path" to "secretname"		#370	M	-	
CamelCase configname keys		#352	M	✓	
Pull postgres out of startup services list		#4032	M	-	
Remove superfluous delay in consul_wait_install.sh		#3584	M	-	
Cap # of redis connections		#3594	S	-	

Update: Secret API's is a breaking change

- Microservice authentication UCR
  https://github.com/edgexfoundry/edgex-docs/pull/898

- Microservice authentication ADR
  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-pkcs11 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 (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.