EdgeX Security WG Dec 18, 2019

Attendees: Beau, Colin Hutchinson, Diana, Jim Wang, Jim White, Lenny, tonyespy, Trevor, Michael Estrin, Bryon, Eno

Agenda:

- Adding Security Metrics - Jim White
- Update on Blackbox testing with Security Enabled -- Bryon
- Windows related Secret Store Setup issues -- Jim Wang https://github.com/edgexfoundry/developer-scripts/issues/188
- New API for secrets for use by App Func SDK -- Jim Wang
- Meetings - Next Meeting Jan 8, 2020
  - Meeting next week - Dec 25 cancelled. Merry Christmas!!!
  - Meeting the week after - Jan 1 cancelled. Happy New Year!!!
  - Jan 8 expected outs: Tonyespy and Malini

Jim White: Metrics across EdgeX -- that SMA would expose

From a Security Admin Perspective -- what would somebody want to know from a single pane of glass?

Example: how many intrusions through Kong?

How many logins? Unique requests? Traffic density in various time intervals- DOS

Question: Bryon -- asking very high high level or something we might scrape from logs, or build instrumentation into the code?

Answer: Jim White -- yes, yes, and yes.

Question: Also how might we want to expose this information, UI, SMA APIs

Jim White to create an ADR for tracking this feature request.

Blackbox -- update from Bryon

Bryon has been hacking on the BB test -- on the VM

Discovered that there were write permission issues when attempting to save auth tokens, CA certificate etc. Pertains to volume sharing between containers and/or host in an SELiinux environment.

From Colin Hutchinson to Everyone: (09:17 AM)

re -Z "Labeling systems like SELinux require proper labels be placed on volume content mounted into a container, otherwise the security system might prevent the processes running inside the container from using the content. By default, volumes are not relabeled."

Bryon added a **Z switch for volume mounts** -- which resulted in progress - moved beyond the write stage. (Note that having a separate volume for service specific secrets was considered but discarded as overkill.)

Currently failing in Rules Engine stage. JVM is panicking, ZMQ.
Help is needed. AMD64/X86. Failing consistently.
Tonyespy question: Export Services was removed, would this be a problem?
Bryon, Jim Wang and Lenny answer: Unlikely because this is a Fuji BB tests. Lenny: Version check -- turned off in BB for now/semver.
Jim White question: Might this be a network issue?
Bryon answer: Volume mount should not be a network issue. Jenkins having issues that is gating merging of patches.
Jim White: James is doing his causal analysis. Working with LF and devops.
Note originally BB tests with security was failing 50% of the time on ARM.

Context:

> **Michael Estrin (Dell)** 5:02 AM
> @Big-B (Intel) I want to discuss
> https://github.com/edgexfoundry/blackbox-testing/pull/349 with you. Several concerns: issues with developer-scripts' docker-compose files (I want to understand this issue better), coverage of https://github.com/edgexfoundry/blackbox-testing/issues/342 and https://github.com/edgexfoundry/blackbox-testing/issues/307 (why aren't these issues corrected with their own pull requests?), overlap with https://github.com/edgexfoundry/blackbox-testing/pull/350, and it's not completely clear to me what other concerns are being addressed by the PR. Please ping me so we can sync on this PR.

> **Big-B (Intel)** 7:59 AM
> The current blackbox test docker-compose is completely busted. The changes in the PR get it into a state where vault, vault-worker, kong, edgex-proxy, secretstore-setup will all boot. This includes:
>
> Using the custom consul container that has the new dependency checking scripts
> Switching to a stock version of Vault (secret-secrets-setup is now its own container)
> Sharing the dependency checking scripts (/consul/scripts) with all of the containers that need it

Sharing the TLS CA certificate with all of the core services (no longer shared in the same location as the Vault root token in order to protect the Vault root token)
Putting in workarounds for Kong dependency checking due to use of -centos/-ubuntu.
Sharing the proxy TLS private key with edgex-proxy.
Synchronizing dependency checks with developer scripts for mongo and edgex-proxy.
Workaround for app-service-configurable static sdk version check
The general request in #342 to sync these scripts
The "remove insecureSkipVerify arg" request #307 (entrypoint script that invokes secretstore-setup is now added to the container, and it defaults to false) -- there is nothing to do here.

(edited)

Jim Wang - update on Windows support -- docker-compose file

The secret path is not working as originally as designed.
Using two kinds of shells: native windows and cygwin - variations
Problem stemming from Windows
Environment variable -- handling shell variable. -- Mike to send information on this.

Jim Wang -- new API to save secrets into secret store

The Get implementation exists
Jim's code provides storage of secrets ability

Anything Else?

1) Tony question for Bryon -- security and tokens. Shall sync offline.
   ETA for token
   Bryon - PR to do logic approved .. but not yet merged

   Token provider and Snaps issue .. old master token.

2) Diana Developer Scripts is all on Master. How does one handle release specific changes.
   Outstanding PR for documentation. Looking at developer scripts. MongoDB javascripts -- remove/update? Developer scripts has only master branch. Should we have a branch of developer scripts.
   Trevor: Developer and Mongo scripts should exist to help folks who develop natively.

Diana: Export Services -- if removed -- How do we capture this in developer scripts?
Diana: Why EdgeX Mongo not part of EdgeX GO
Jim White: developer scripts -- buyer beware. There are sub-folders for each of the releases.
A topic to discuss in Core WG. Should we have branches, propose, discuss, and then escalate out to TSC.
Good ideas and suggestions, bring a proposal to Trevor.