Appendix A: Worked Example - CNCF Security SIG

Proposal by SAFE Working Group
December 2018

See

SIG Mission Statement

Security has been an area in which open source can flourish and sometimes has done so; however, with cloud native platforms and applications security has received less attention than other areas of the cloud native landscape.

This means that there is less visibility about the internals of security projects, and fewer projects being deeply integrated into cloud native tooling. While there are many open source security projects, there are fewer security experts focused on the cloud native ecosystem. This has contributed to a culture where people feel they cannot understand how to securely set up and operate cloud native systems, due to obscurity and uncertainty. Yet the cloud native principles, although they mean change, have encouraged the development of tools that help manage fast changing environments, and which have the promise of both simplifying and improving security.

Making security more open and understandable is an essential part of this change. Talking to customers, security is the most important and least understood part of the cloud native transition. Security is not an easy field, and it is difficult to measure and value the inputs precisely, which can also cause issues with evaluation of security software and designs.

The SAFE vision aligns with this, focusing on three keys areas:

1. protection of heterogeneous, distributed and fast changing systems, while providing access that is needed,
2. a common understanding and common tooling to help developers meet security requirements, and

3. common tooling for audit and reasoning about system properties.

The projects directly in the security space in CNCF now are quite fragmented, with many security areas not covered at all. Most of the security projects are sandbox level.

We need projects that cover a much wider area that are:
- standards (currently TUF and SPIFFE).
- libraries (OPA)
- standalone projects (Notary, Falco)
- tooling for test, evaluation and audit (none at present)

One aim should be to encourage cross usage between projects, for example in the way that Spiffe is used by Istio and Consul among others, and Notary is part of Harbor.

Encouraging projects that are suitable components of many other projects is a key way to help security become more understandable and expose common interfaces.

Responsibilities & Deliverables

Responsibilities

- users/personas/needs/customer demands in the security space
- identifications of areas of focus eg identity, isolation, network security, authentication, policy etc
- framework for evaluation - how do products and tools fit the users in the area?
- technical evaluations - what is missing, what is difficult to understand, what security gaps are there?
- work on integrating common tooling into different projects, particularly where that tooling is a CNCF project (but the targets may not be)
- cross project focus on the security reviews the CNCF is funding, helping projects make the most of them and conducting reviews to identify areas where issues are common
- recommendations of security development and process tooling, such as static analysis tooling, formal methods, supply chain security and other things that are useful to improve security of CNCF projects, in a similar way to the CI WG does for CI tools.
- growing CNCF external relationships with interested parties, eg NIST and other security standards bodies.

Deliverables to ToC

- framework document for the cloud native security space

- landscape for the security space
- recommendations for sandbox projects where exploration is needed
- recommendations for new CNCF projects where there is clear usage
- scheduled regular reporting to ToC on ongoing and completed work
- reporting on project security for graduation and other events, summarizing the external security reviews and other relevant information
- help with health check of projects in the category

Audiences

- Education - audience is end users and developers
- Project intelligence - audience is TOC / TOC Community
- Who else?

The issue of the Landscape(s)

- Being “deliberate” about what this (these) are for, and for whom?
- Main landscape has become an anti-pattern (kitchen sink effect)

Execution & Focus

- How do we spell out CNCF “work items” that can be executed by both CNCF staff and the TOC community
- Can the TOC ask questions of the SIGs? “Go ruminate on this please”
- Making sure recommendations don’t over-determine users’ tech choices. The storage WG was successful because it provided genuine guidance about a *range* of approaches, in a way that is transparent, unbiased, actionable

Example

From Mark Peek to Everyone: (04:18 pm)
Chris, didn’t you have a tech writer that was going to condense the serverless white paper?
From Chris Aniszczyk to Everyone: (04:18 pm)
Mark, we are happy to do that, we just need a request formally from a project/wg

AR questions:

1. How to make these SIGs actually *effective*
2. Dividing line between TOC & SIGs qua delegation & accountability
3. Being unbiased vs Politics and avoiding vendor anti-patterns (bias)