云原生安全技术产业调研

by:LiuShawuji

2023.3.8

目录

01

概念及框架

云原生安全

- 云原生安全是一种将安全性构建到云原生应用程序中的方法。 它确保安全是从开发到生产的整个应用程序生命周期的一部分。 云原生安全旨在确保与传统安全模型相同的标准，同时适应云原生环境的特殊性，即快速的代码更改和高度短暂的基础设施。 云原生安全与称为测试左移 的实践高度相关。

- CNCF-Cloud Native Computing Foundation 云原生计算基金会，2015年由Linux基金会发起，Google、Cisco、Docker等各大厂商加入，共同打造的云原生社区。

- 个人理解：对基于容器化开发和部署的应用，在全软件生命周期的各个阶段采取嵌入式的安全检测和防护技术，以管控风险。

01 Pivotal 最初的定义

- 早在 2015 年 Pivotal 公司写了一本叫做 迁移到云原生应用架构 的小册子，其中探讨了云原生应用架构的几个主要特征：符合 12 因素应用、面向微服务架构、自服务敏捷架构、基于 API 的协作、抗脆弱性

02 CNCF 最初的定义

- 到了 2015 年云原生计算基金会（CNCF）成立，起初 CNCF 对云原生（Cloud Native）的定义包含以下三个方面：应用容器化、面向微服务架构、应用支持容器的编排调度

03 重定义

- 到了 2018 年，原有定义已经限制了云原生生态的发展，CNCF 为云原生进行了重新定位。
- 云原生技术有利于各组织在公有云、私有云和混合云等新型动态环境中，构建和运行可弹性扩展的应用。云原生的代表技术包括容器、服务网格、微服务、不可变基础设施和声明式 API。
- 这些技术能够构建容错性好、易于管理和便于观察的松耦合系统。结合可靠的自动化手段，云原生技术使工程师能够轻松地对系统作出频繁和可预测的重大变更。


访问
存储
计算
部署
分发
开发
生命周期
基础
环境
运行时

01 开发阶段

- 须在软件开发的早期就引入安全需求，在早期阶段解决这些需求可防止在生命周期的后期重新处理，而重新处理则会延缓DevOps 流程，并增加总体成本。
- DevOps 团队还必须利用专门构建的工具在部署应用之前就识别安全配置错误和漏洞。比如可以嵌入IDE的检测插件。

02 分发阶段

- 分发阶段需完成对镜像的功能和安全性测试。
- 镜像扫描及加固
- 对应用的静态安全检测（SAST)和动态安全检测（DAST)
- 为保障镜像的完整性和私密性可以使用签名和加密等技术。

03 部署阶段

- 部署阶段需先检查被部署应用满足安全性和合规性。
- 应用上线后的入侵检测及应急响应，包括攻击行为的检测与报告，和事后的取证调查。

04 运行时环境

- 计算　存储　访问

02

主要厂商

国内云原生安全产品及解决方案

- 阿里云
  - 云原生安全容器解决方案——基于轻量虚拟机技术和ECS神龙的安全容器
- 华为云
  - 新一代云原生防火墙
- 阿里、华为、腾讯、百度等互联网大厂除可以提供云服务之外，也通过云原生防火墙、态势感知、堡垒机等多种产品配合形成云原生安全解决方案。
- 青藤云
  - 青藤蜂巢云原生安全平台
- 奇安信
  - 网神椒图容器安全检测系统
  - 网神开源卫士系统

根据CNCF landscape可见主要的云原生安全供应商如图。

03

主要风险

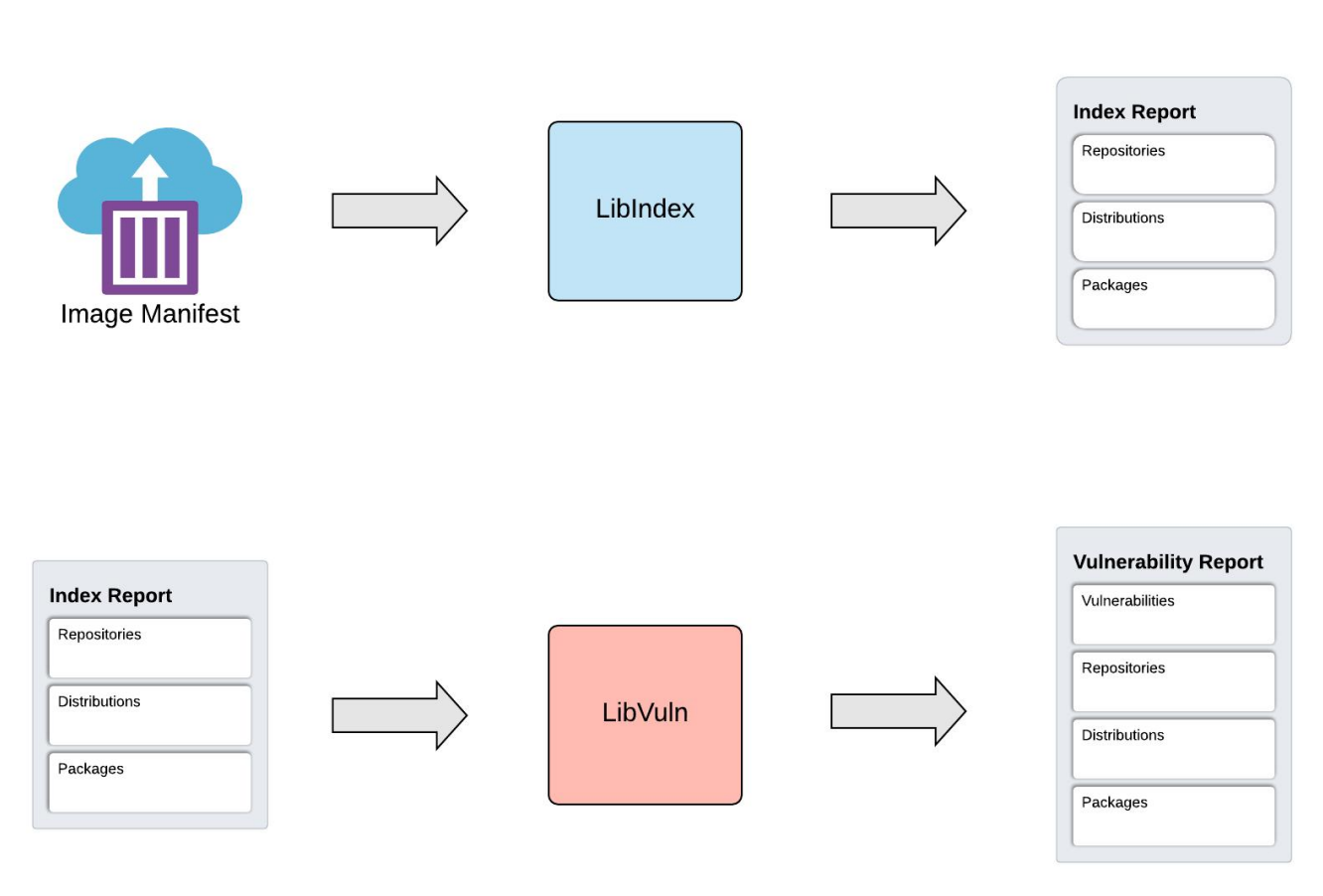
云原生安全主要风险

- 2022年4月，OWASP 针对云原生应用系统发布了最新的云原生应用安全（Cloud-Native Application Security）TOP10风险指南。
- CNAS-1: 不安全的云、容器或编排配置
- CNAS-2: 注入漏洞（应用层、云事件、云服务）
- CNAS-3: 身份认证和授权不当
- CNAS-4: CI/CD 管道和软件供应链缺陷
- CNAS-5: 不安全的密钥存储
- CNAS-6: 过度宽松或不安全的网络策略
- CNAS-7: 使用有已知漏洞的组件
- CNAS-8: 资产管理不当
- CNAS-9:未对容器或者pod资源进行有效限制
- CNAS-10: 未能有效的进行日志记录和监控（如：容器运行时）

04

个人实践及思考

Clair——开源镜像安全检测工具



- 主要功能分为三部分：镜像中组件的检索、组件漏洞扫描、漏洞库的更新。
- 以Docker镜像为例，镜像image由layer构成。ClairCore的LibIndex模块通过解析layer的内容检索出镜像中的组件名称及版本。
- LibVuln模块通过将组件名称及版本与漏洞库中信息比对，输出漏洞检测报告。
- 漏洞信息的来源主要有Alpine、Aws、Debian、Oracle、Photon、Ubuntu等。

对于云原生安全发展趋势的思考

- 由于云原生安全与软件生命周期需要紧密结合，如何将安全平台或工具更透明地结合到DevOps过程中以达到在不过度拖慢流程的情况下保障安全性，未来还可能探索更完善的落地方式。

- 如果由多个工具结合形成解决方案，那么不同工具之间的数据流转能否畅通，检测的信息是否冗余，管理后台能否统一。

- 如何结合不同的企业的合规和安全要求，调整其合适的检测规则和策略。

感谢各位老师指导