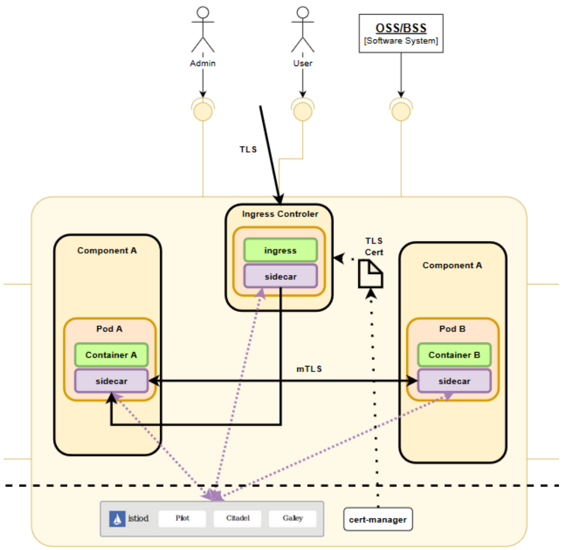
Security Subcommittee (SECCOM) Overview

6 May 2021

SECCOM focus areas

Requirements & Architecture

Defined security requirements for ONAP and VNFs, service mesh, logging



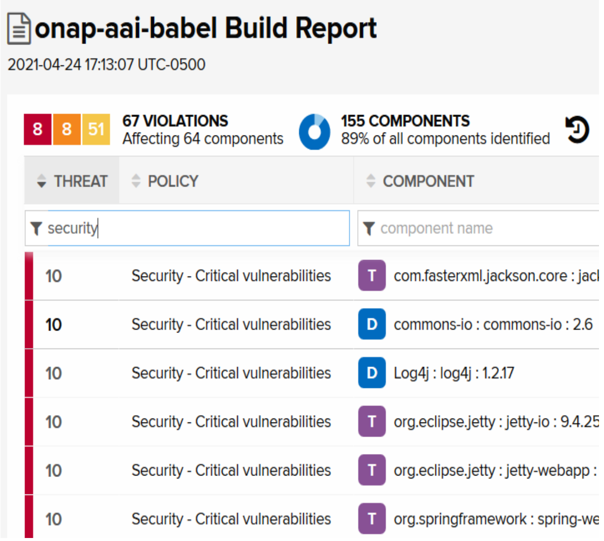
Security Framework

Adopted Core Infrastructure Initiative (CII) Badging as secure development framework

CII Passing Requirements	Total	Non-Security	Security
Basic Requirements	12	10	2
Change Control	9	3	6
Reporting	8	2	6
Code Quality	13	3	10
Security	16	0	16
Analysis	8	0	8
Total	66	18	48

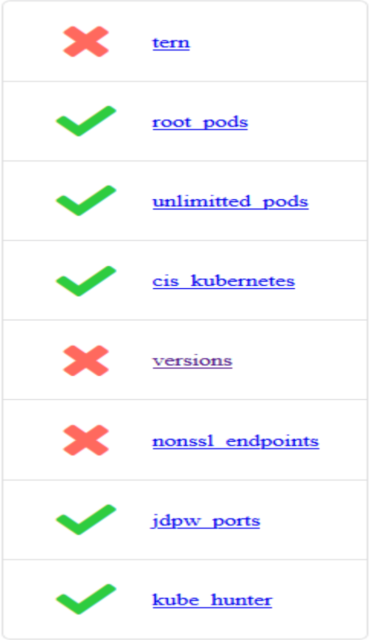
Vulnerability Testing

Integrated software composition analysis and vulnerability scanning into Jenkins



Secure Configuration

Test ONAP configuration during build: language version, HTTPS, Docker/K8s, ports



Requirements and architecture

Requirements

- ONAP platform requirements: ONAP Security Requirements
- VNF security requirements: VNF Security Requirements
- ONAP security model: ONAP Security Model
- Release requirements
- Recommendations for infrastructure packages: Database, Java, Python, Docker, Kubernetes, and Image Versions

Architectures

- Authentication & authorization
- Service Mesh: ONAP Security Model
- Logging

Vulnerability reporting: Reporting Vulnerabilities

Security framework

Core Infrastructure Initiative (CII) Badging

- Open source *secure development framework* based on industry best practices and practices of well-run open source projects
- Increases likelihood of better quality & security
- Designed for any open source project

Badging requirements

- Development environment requirements
  - Stable website, open source license, and user engagement
  - Use of change control tools
- Code requirements
  - Automated vulnerability testing
  - Vulnerability resolution
  - Quality assurance using automated test suites
  - Cryptographic requirements
- CII requirements web site
- ONAP Project CII Badging Status Dashboard

cii best practices passing

cii best practices silver

cii best practices gold

	Passing	*Silver*	*Gold*
Basic	12	28	31
Change Control	9	10	13
Reporting	8	10	10
Code Quality	13	29	34
Security	16	27	29
Analysis	8	9	9
Total	**66**	**113**	**126**

Get Your Badge Now!

Security testing

Static application software tests (SAST): SonarCloud

- Weak crypto, insecure config, injection, SSRF, XXE, XSS

Software composition analysis (SCA): NexusIQ

- Use mean time to upgrade strategy (MTTU)

Samsung penetration testing

- ONAP Casablanca Security Assessment
- ~200 findings
- 23 CVEs issued for ONAP

Sample SCA Upgrade Recommendation

Component name and version	CVE	Threat level	Recommended version
okhttp : 2.7.5	CVE-2021-0341	7 5	com.squareup.okhttp3 : okhttp : 4.9.1
log4j : 1.2.17	CVE-2019-17571	9 7	2.14.1 (log4j-core)
: tomcat-catalina : 9.0.30	CVE-2020-9484 CVE-2021-24122	7 5	10.0.5

Secure configuration

Java and Python upgrades

- Update to Java 11: 22/95 containers with Java 8
- Update to Python 3: 19/55 containers with Python 2

Pods running as root

Containers exposing HTTPS outside cluster

Kubernetes configurations

Developer tools (jdwp)

[Integration tests]()

Sample Java/Python Version Test

holmes-rule-mgmt	['11.0.6']
message-router	['1.8.0_212']
message-router-kafka	['1.8.0_212']
message-router-kafka	['1.8.0_212']
message-router-kafka	['1.8.0_212']
message-router-zookeeper	['1.8.0_212']
message-router-zookeeper	['1.8.0_212']
message-router-zookeeper	['1.8.0_212']
msb-discovery	['1.8.0_131']
msb-eag	['1.8.0_131']
msb-iag	['1.8.0_131']
framework-artifactbroker	['1.8.0_252', '11.0.8']

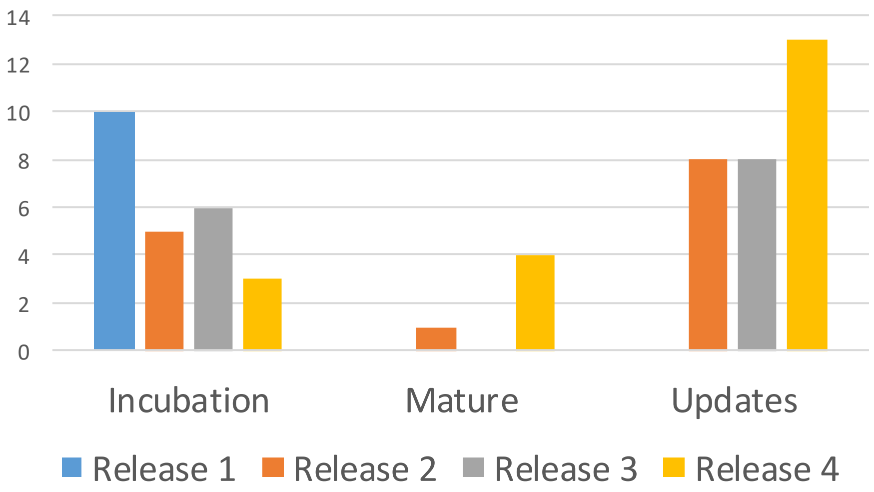
Akraino

AKRAINO

Overview

- Akraino is an opensource software stack that improves the state of edge cloud infrastructure for carrier, provider, and IoT networks through the development of Edge and Virtual Network Function (vNF) applications.

Release Blueprint History



Current Security Scans

- Vuls – agentless Linux vulnerability scanner
- Lynis – Linux system hardening/compliance verification
- Kube-Hunter – Kubernetes vulnerability scanner

2021 Security Sub-Committee Plans

- Minimum OS Version Support Document
  - Ubuntu, CentOS, RHEL CoreOS, Debian
- Formalize/Document Lynis Incubation vs Maturity Requirements
- Require minimum version for Vuls, Lynis and Kube-Hunter used by Bluval
- Process for updating OVAL database to improve scanning accuracy of Vuls
- Platform Security for Akraino Blueprints
  - Arm
  - X86
  - Version 1.0 Platform Security Whitepaper
- Investigate using LFX Security Tools
- Automate Vuls and Lynis Log Output Analysis (Pass/Fail)

Fabian Rouzaut Slides