ONAP Security Sub-committee Update

Stephen Terrill, Donald Levey, Pierre Cose,
2017-12-15

Introduction

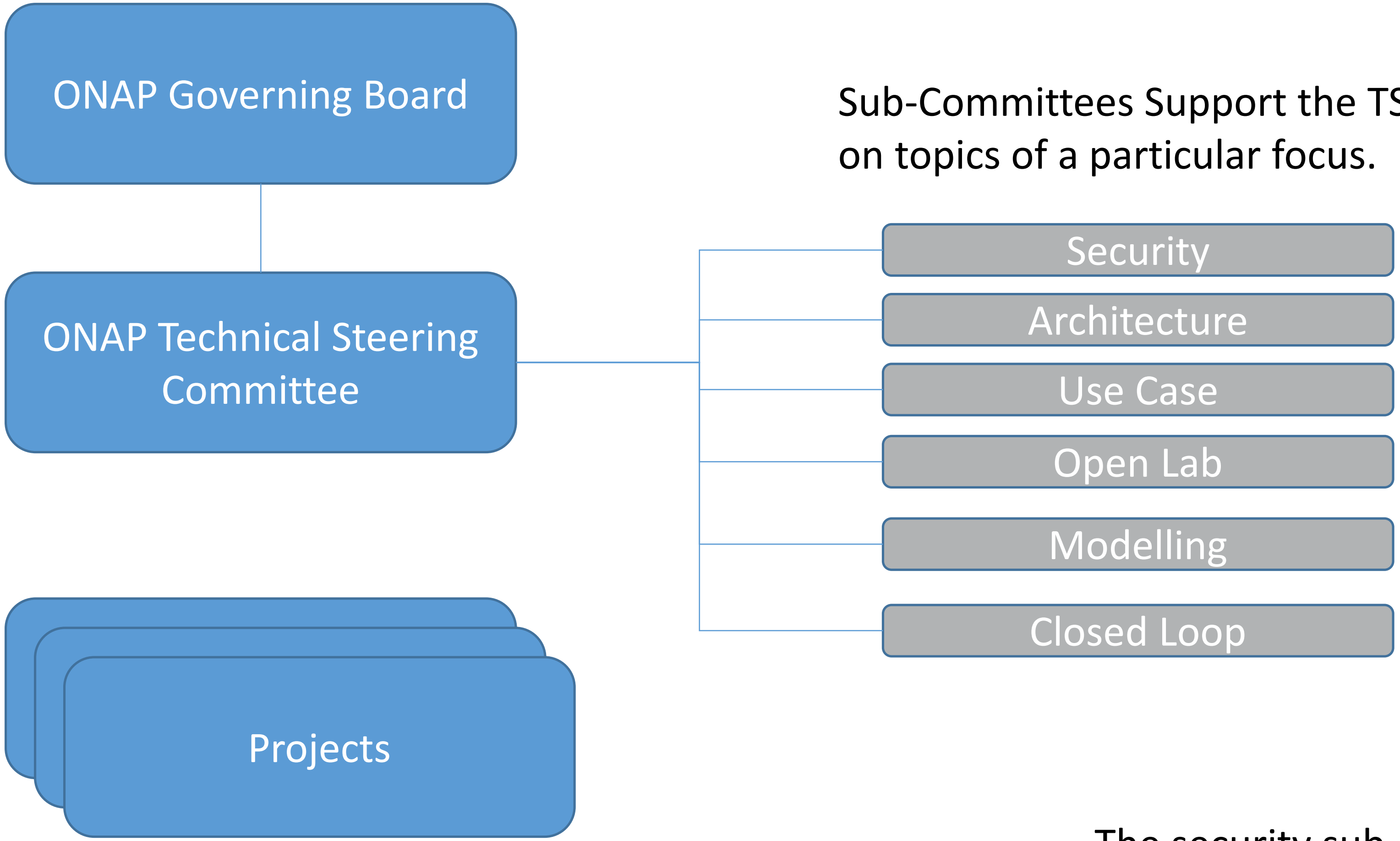
- This presentation is from the ONAP security sub-committee.
- It covers the security aspects that have been put into place, as well as the latest on what is currently on the agenda.

ONAP is critical infrastructure

Can you imagine what could be done if compromised?

If security is done right, no-one knows.
We are aware of it when its not!

Security is considered from the start

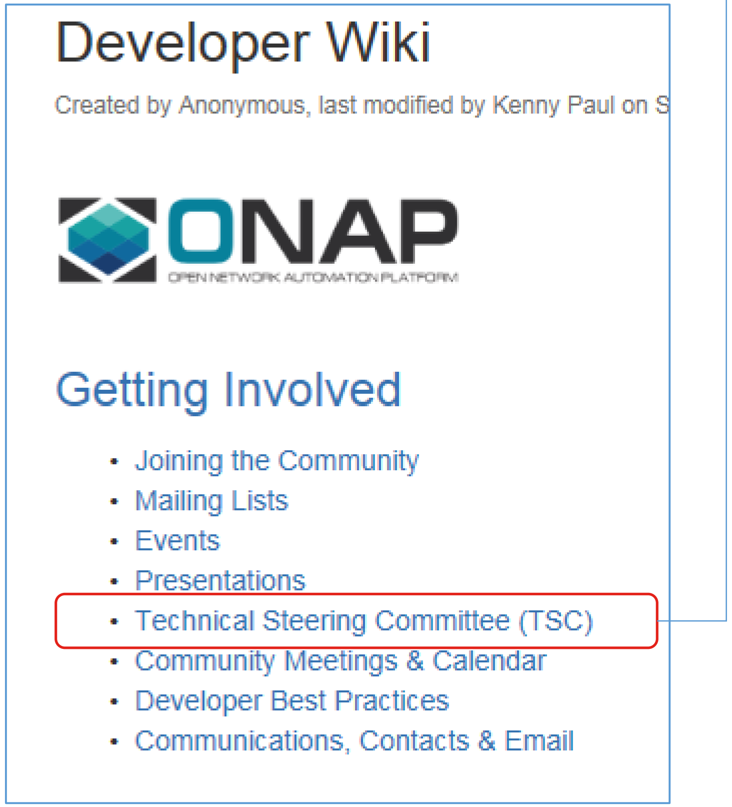


Sub-Committees Support the TSC on topics of a particular focus.

The security sub-committee was one of the first created

Where to find us

http://Wiki.onap.org

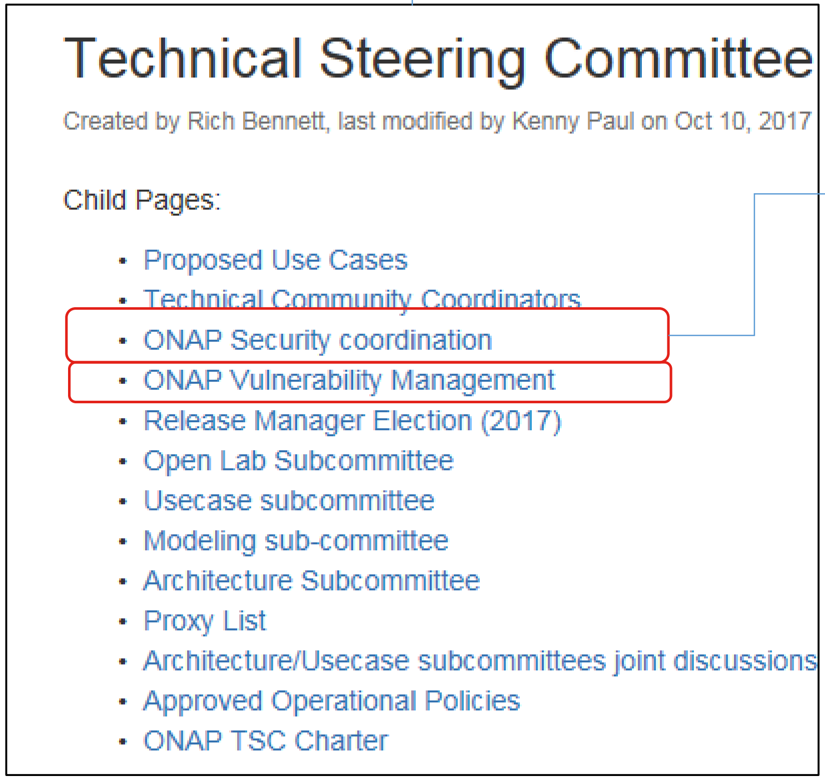


Developer Wiki

Created by Anonymous, last modified by Kenny Paul on S

Getting Involved

- Joining the Community
- Mailing Lists
- Events
- Presentations
- Technical Steering Committee (TSC)
- Community Meetings & Calendar
- Developer Best Practices
- Communications, Contacts & Email

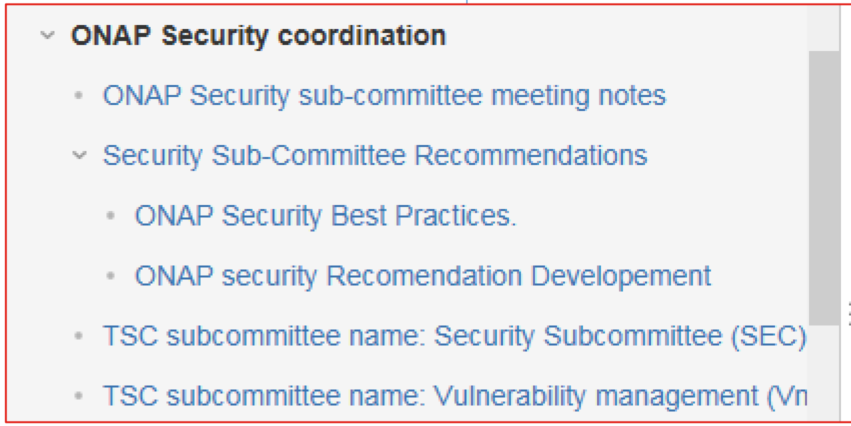


Technical Steering Committee

Created by Rich Bennett, last modified by Kenny Paul on Oct 10, 2017

Child Pages:

- Proposed Use Cases
- Technical Community Coordinators
- ONAP Security coordination
- ONAP Vulnerability Management
- Release Manager Election (2017)
- Open Lab Subcommittee
- Usecase subcommittee
- Modeling sub-committee
- Architecture Subcommittee
- Proxy List
- Architecture/Usecase subcommittees joint discussions
- Approved Operational Policies
- ONAP TSC Charter



ONAP Security coordination

- ONAP Security sub-committee meeting notes
- Security Sub-Committee Recommendations
  - ONAP Security Best Practices.
  - ONAP security Recomendation Developement
- TSC subcommittee name: Security Subcommittee (SEC)
- TSC subcommittee name: Vulnerability management (Vn

How to contact us

- Onap-seccom@onap.org

- To subscribe: https://lists.onap.org/mailman/listinfo

- We meet Wednesdays, 15:00 – 16:00 CET.

Vulnerability Management

- Vulnerability management is the process to handle identified vulnerabilities
  - Approved Vulnerability Management procedures: https://wiki.onap.org/display/DW/ONAP+Vulnerability+Management
    - How to submit a vulnerability, acknowledge a vulnerability, and manage the process to conclusion including communication.
    - Email: security@lists.onap.org

  - Vulnerability management team (volunteers) are in place:
    - Will follow a
      - Case lead on a “step-up” approach on per case by case basis.
      - Support team to step in to ensure nothing falls through.
      - Security coordinator also to ensure that all is working ok.

Current Focus

- Core Infrastructure Initiative Badging Program
- Static Code Scanning
- Credential Management
- Communication Security
- Known vulnerability informing

CII (core infrastructure initiative) badging program

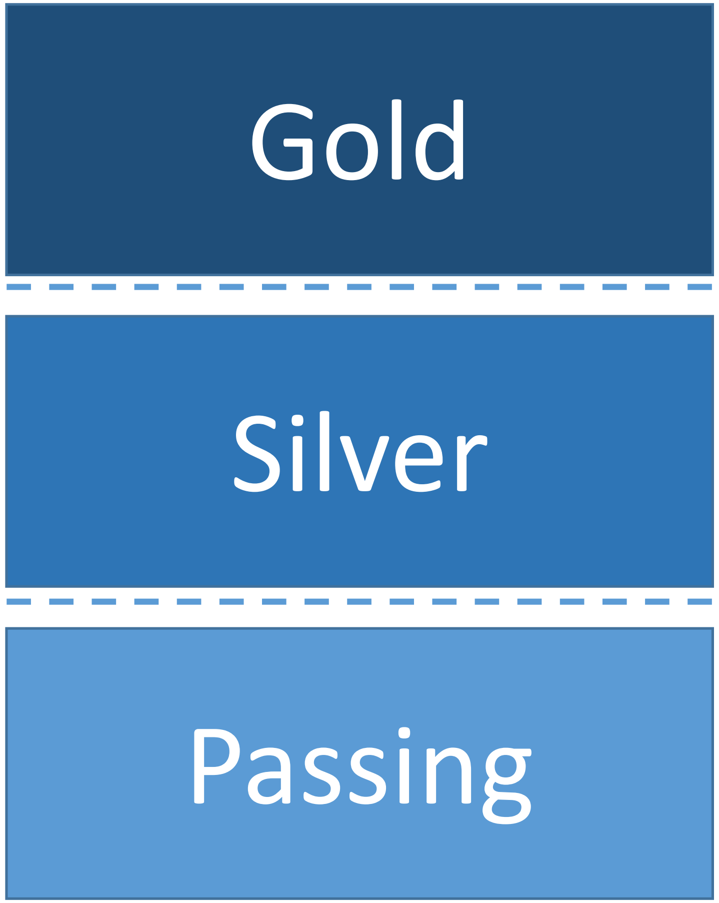
- CII (core infrastructure initiative) has been created by the linux foundation in response to previous security issues in open-source projects (Heartbleed in openSSL).

- The CII has created a badging program to recognize projects that follow a set of identifies best practices that could be adopted.
    - There are three levels passing, silver and gold.

- The security sub-committee has looked at these and feels that given ONAP is managing core critical infrastructure, *the ONAP projects should follow the gold level*.
    - This is a challenge!

- The CII Badging program levels are now part of the S3P (carrier grade) focus of Release 2.

CII Badging program, 3 levels



Gold

- More stringent criteria
  - Security Review, project continuity, continues test integration, 70%+ test coverage, secure design, ….

Silver

https://github.com/coreinfrastructure/best-practices-badge/blob/master/doc/other.md

Passing

- Basic practices
- Largely also covered by Release Best Practices

https://github.com/coreinfrastructure/best-practices-badge/blob/master/doc/criteria.md

Example Criteria

Passing:

The project website MUST succinctly describe what the software does (what problem does it solve?).

The project MUST use at least one automated test suite that is publicly released as FLOSS (this test suite may be maintained as a separate FLOSS project).

Silver:

The project MUST document what the user can and cannot expect in terms of security from the software produced by the project. The project MUST identify the security requirements that the software is intended to meet and an assurance case that justifies why these requirements are met. The assurance case MUST include: a description of the threat model, clear identification of trust boundaries, and evidence that common security weaknesses have been countered

Gold:

The project MUST have at least 50% of all proposed modifications reviewed before release by a person other than the author, to determine if it is a worthwhile modification and free of known issues which would argue against its inclusion.

The Questionnaire

- Editing rights is limited to a subset of users
  - Main editor can nominate other users as editors
- Divided into clear sections
  - For each section, a set of questions is provided, addressing best practices relating to the parent section
- Each question asks if a criterion is
  - Met, unmet, not applicable, or unknown
- Criteria are generally high-level as targeted to best practices, e.g.
  - “The project MUST have one or more mechanisms for discussion”
  - “The project SHOULD provide documentation in English”

The Goals

CLAMP project Perspective:
Xue Goa, Pierre Close, Anael Clossson

- Give confidence in the project being delivered
  - By quickly knowing what the project supports
- See what should be improved
  - Self-questioning helps project stakeholders identifying strengths and weaknesses, do’s and don'ts
- Align all projects using the same ratings
  - Makes projects connected together to follow the same practices
- Call for continuous improvement
  - Increase self rating and reach better software quality

Click to edit Master title style

Static Code Scanning

- The purpose is for Looking for unknown vulnerabilities
  - Currently investigating the tool
    - Primary Recommendation: Coverity Scanning
  - Looking at the process to apply it within ONAP
- Supported Languages:
  - C/C++, C#, Java, Javascript, Python, Ruby

- Possible scan frequency (per project):
  - < 100K LoC: Up to 28 builds per week, with a maximum of 4 builds per day
  - 100K-500 K LoC: Up to 21 builds per week, with a maximum of 3 builds per day
  - 500K – 1M LoC Up to 14 builds per week, with a maximum of 2 build per day
  - > 1M LoC: Maximum of 1 build per day
- Next Step:
  - Evaluate output report
  - Recommendation for inclusion in ONAP Processes

Static Code Scanning

- The purpose is for Looking for unknown vulnerabilities
  - Currently investigating the tool
    - Primary Recommendation: Coverity Scanning
  - Looking at the process to apply it within ONAP
- Supported Languages:
  - C/C++, C#, Java, Javascript, Python, Ruby

Possible scan frequency (per project):

< 100K LoC: Up to 28 builds per week, with a maximum of 4 builds per day

100K-500 K LoC: Up to 21 builds per week, with a maximum of 3 builds per day

500K – 1M LoC Up to 14 builds per week, with a maximum of 2 build per day

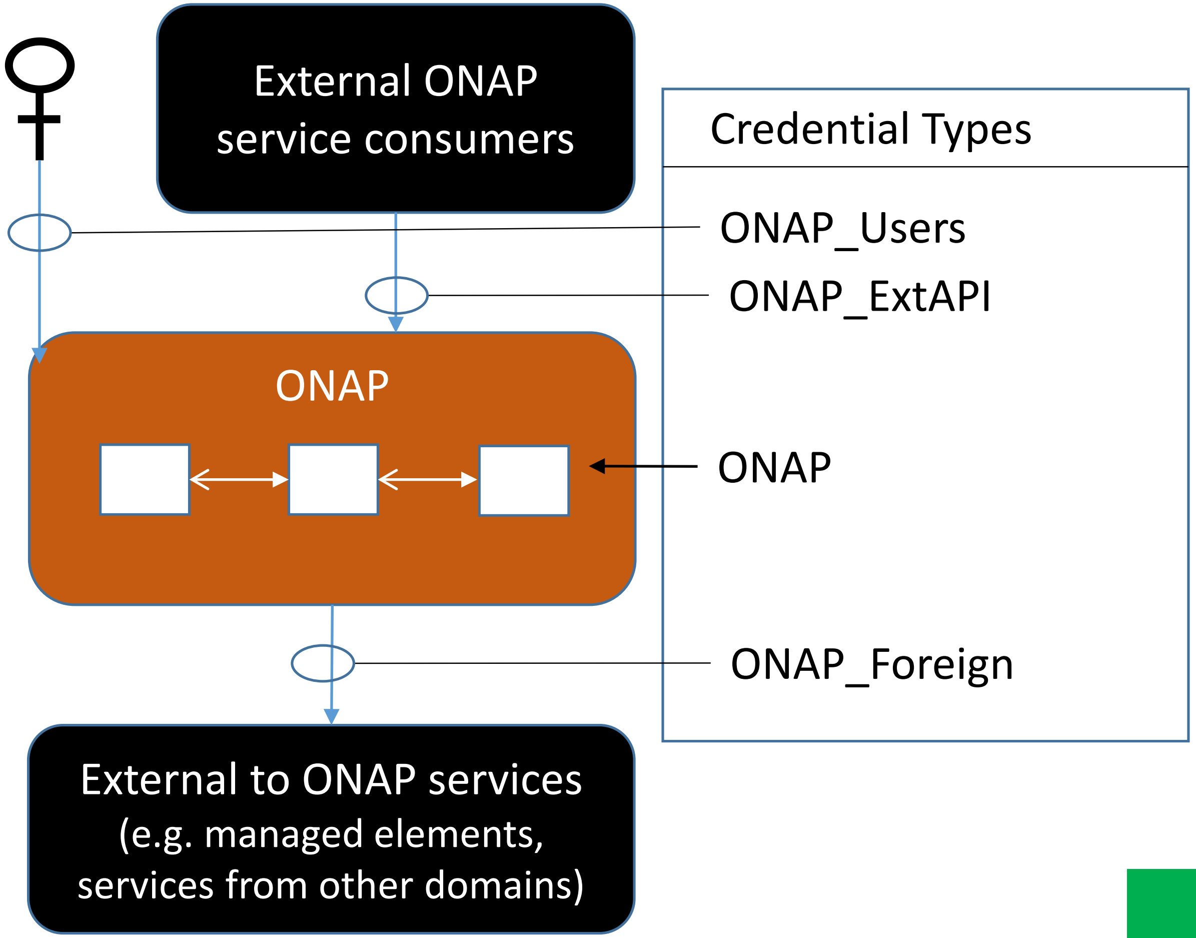
> 1M LoC: Maximum of 1 build per day

Next Step:

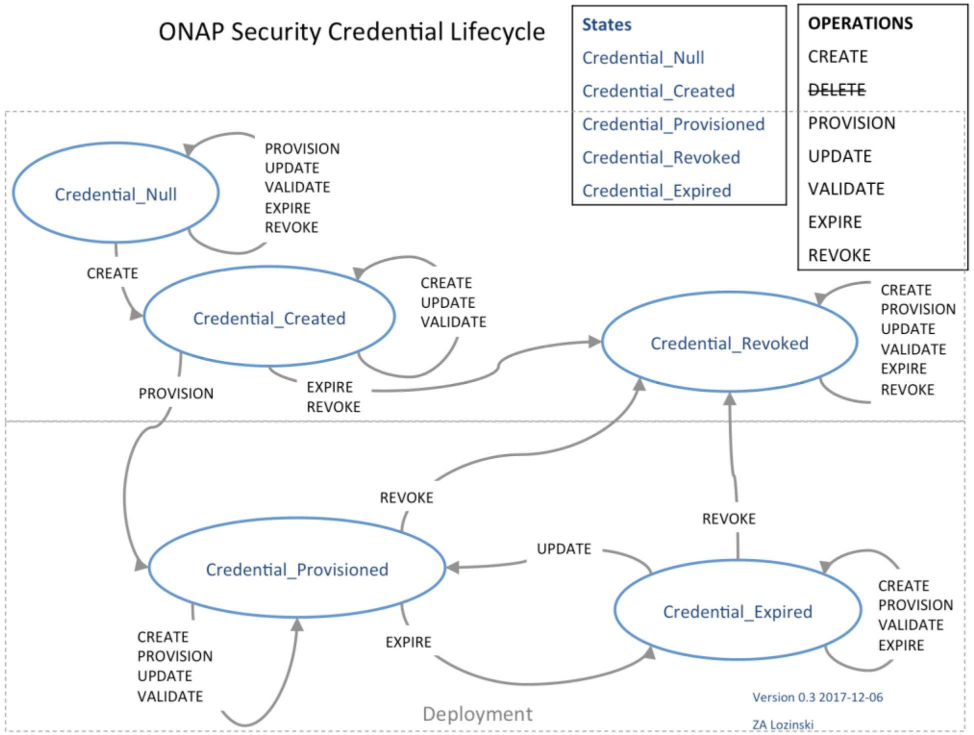
Evaluate output report

Recommendation for inclusion in ONAP Processes

Credential Management



External ONAP service consumers
Credential Types
ONAP_Users
ONAP_ExtAPI
ONAP
ONAP
ONAP_Foreign
External to ONAP services (e.g. managed elements, services from other domains)



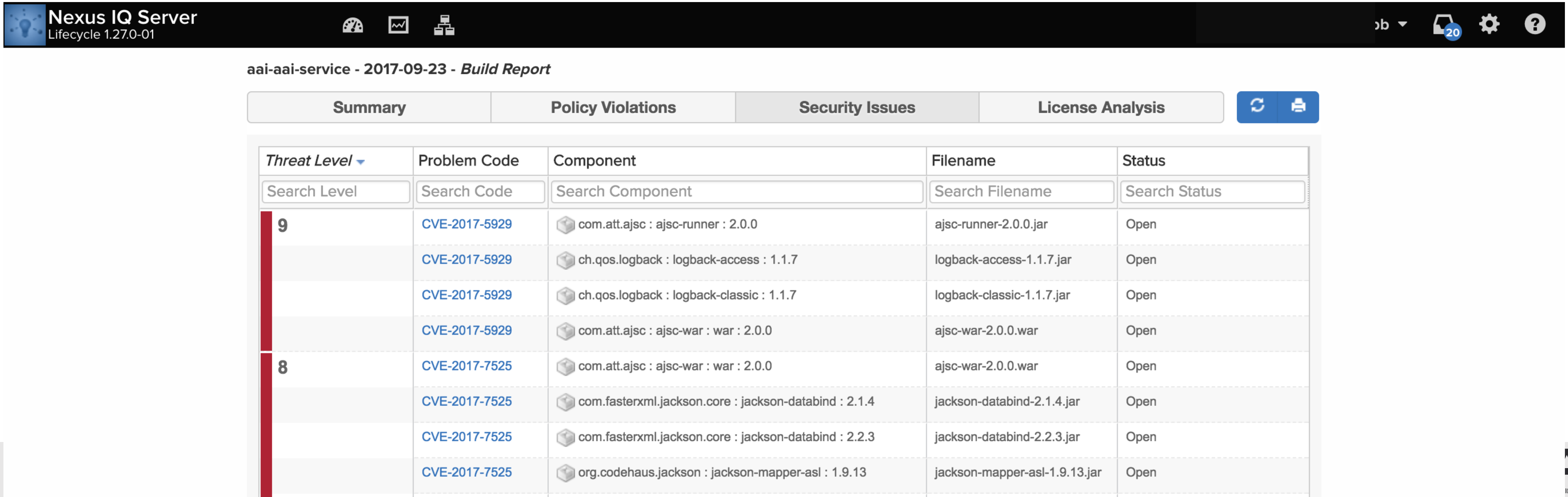
Proposal exists to extend ONAP with the capabilities for :
- ONAP certificate authority
- ONAP secret storage service

Presented:"Securing onap using trusted infrastructure solutions" (TUE)

Credential Examples: Certificates, traditional credentials

Managing known vulnerabilities – FOR DISCUSSION

- Managing known vulnerabilities
  - Sonatype CLM/ Nexus IQ Tool
  - Can be used to inform the projects of known vulnerabilities in the components that a project has.
  - DISCUSSION – how do we want to use it?
    - Make the report available to PTLs (See “IPR Tools & CLA process” presentation on Tuesday)
    - Include in milestone criteria?



aai-aai-service - 2017-09-23 - *Build Report*

Threat Level ▾	Problem Code	Component	Filename	Status
Search Level	Search Code	Search Component	Search Filename	Search Status
9	CVE-2017-5929	com.att.ajsc : ajsc-runner : 2.0.0	ajsc-runner-2.0.0.jar	Open
	CVE-2017-5929	ch.qos.logback : logback-access : 1.1.7	logback-access-1.1.7.jar	Open
	CVE-2017-5929	ch.qos.logback : logback-classic : 1.1.7	logback-classic-1.1.7.jar	Open
	CVE-2017-5929	com.att.ajsc : ajsc-war : war : 2.0.0	ajsc-war-2.0.0.war	Open
8	CVE-2017-7525	com.att.ajsc : ajsc-war : war : 2.0.0	ajsc-war-2.0.0.war	Open
	CVE-2017-7525	com.fasterxml.jackson.core : jackson-databind : 2.1.4	jackson-databind-2.1.4.jar	Open
	CVE-2017-7525	com.fasterxml.jackson.core : jackson-databind : 2.2.3	jackson-databind-2.2.3.jar	Open
	CVE-2017-7525	org.codehaus.jackson : jackson-mapper-asl : 1.9.13	jackson-mapper-asl-1.9.13.jar	Open

Summary

ONAP is critical infrastructure

Can you imagine what could be done if compromised?

If security is done right, no-one knows.
We are aware of it when its not!

We welcome your input!

ONAP

OPEN NETWORK AUTOMATION PLATFORM