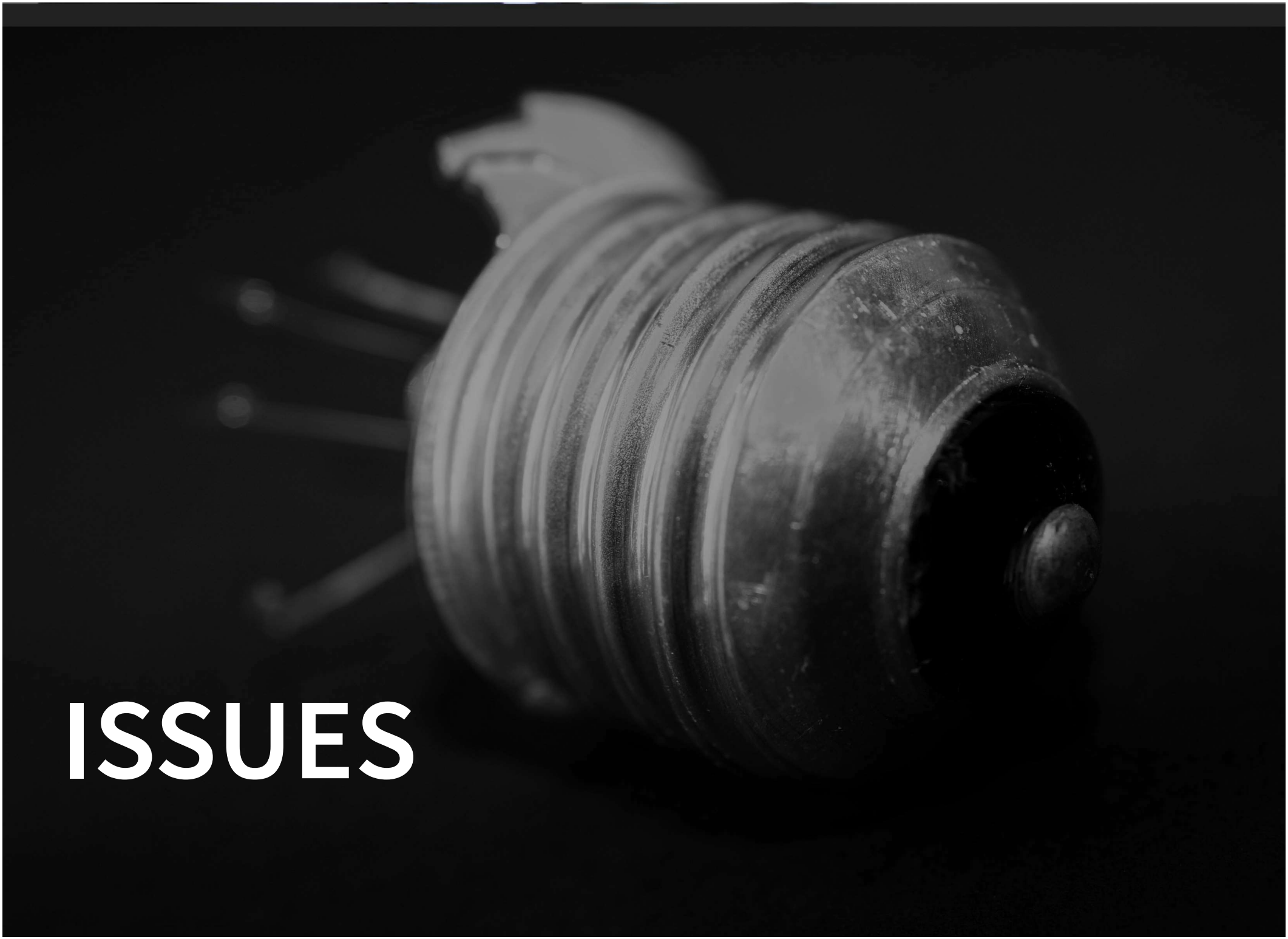
HANDLING OF SECURITY REQUIREMENTS IN SOFTWARE DEVELOPMENT LIFECYCLE

DANIEL KEFER


@DKEFER


ISSUES

REPEATING MISTAKES

SECURITY DOCUMENTATION

SECURITY BEHIND DEV PROCESSES AND TOOLING

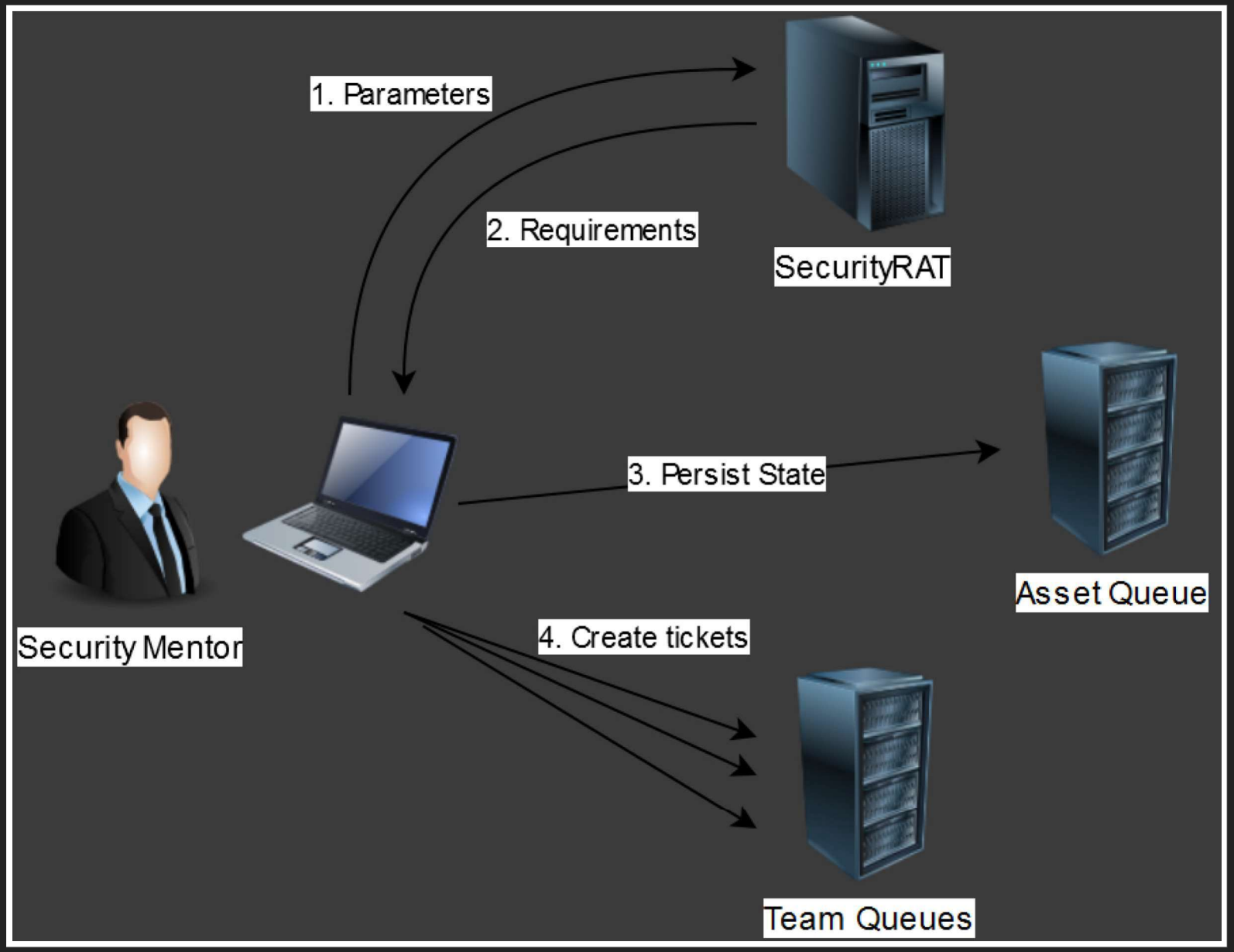

APPROACH

ALIGN THE PROCESS

SCALE

KISS

SECURITYRAT

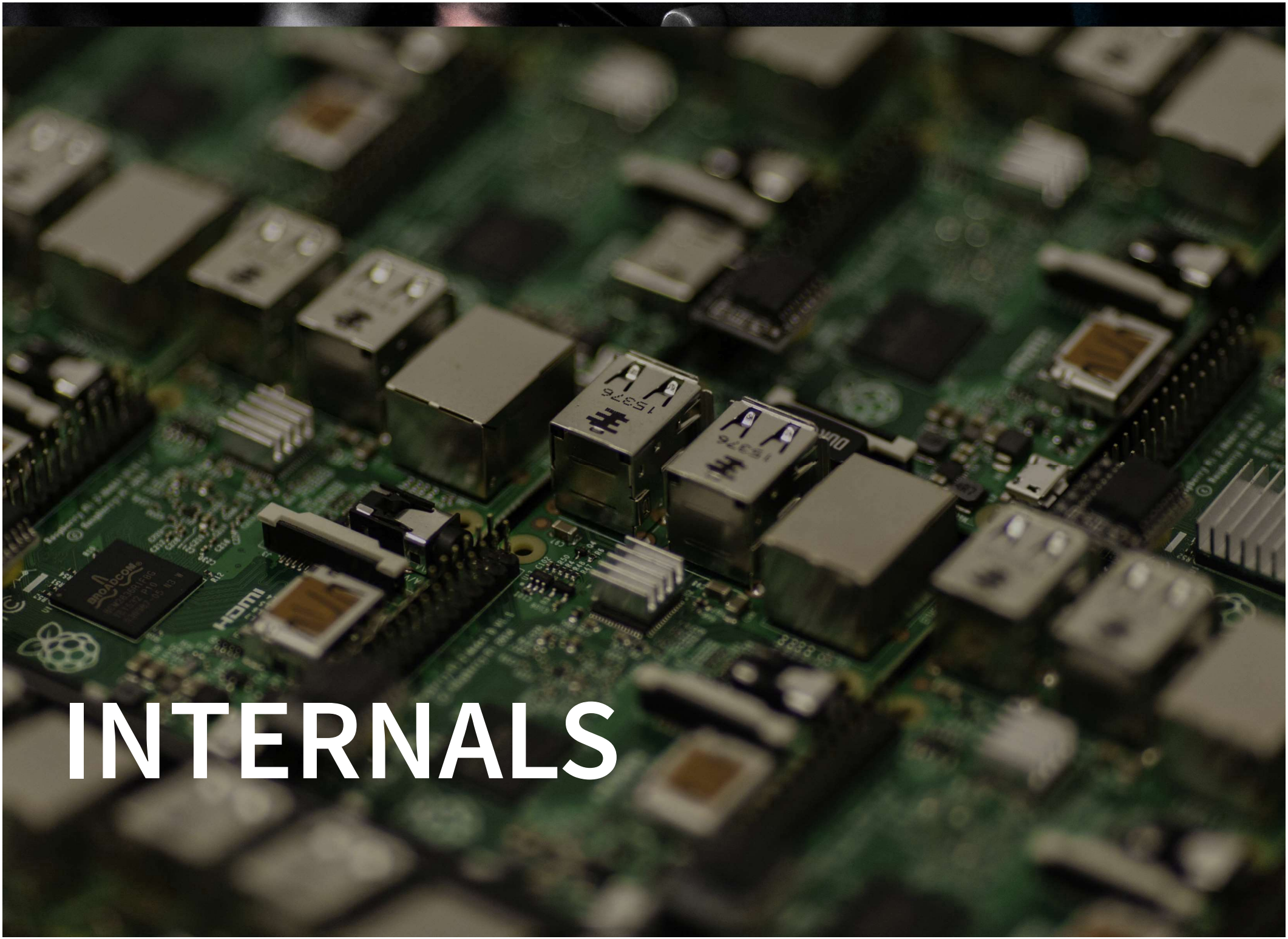

1. Parameters
2. Requirements
SecurityRAT
3. Persist State
Asset Queue
Security Mentor
4. Create tickets
Team Queues

USE CASES

New assets

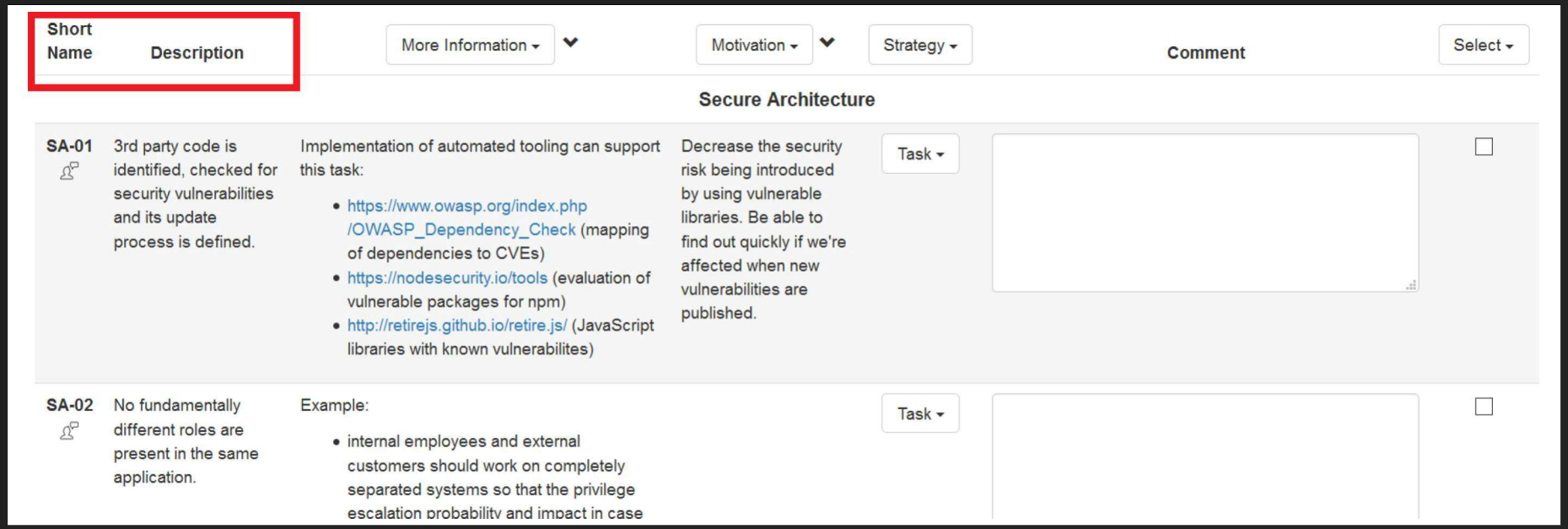
Production assets


BARS
EVF DTL
ZEBRA
LCD
WFM
COUNTER—RESET/TC SET
AUDIO
CH1 SELECT
CH2 SELECT
INT(L)
INT(R)
INPUT1
INPUT2
INPUT2
CH1
CH2
AUTO
MANU
AUTO
MANU
FUNCTION
SHTR/F.RATE
DIAL SEL
R
6h10m
P3.2K
89%
F4.0
NF89
Z31
DEMO


INTERNALS

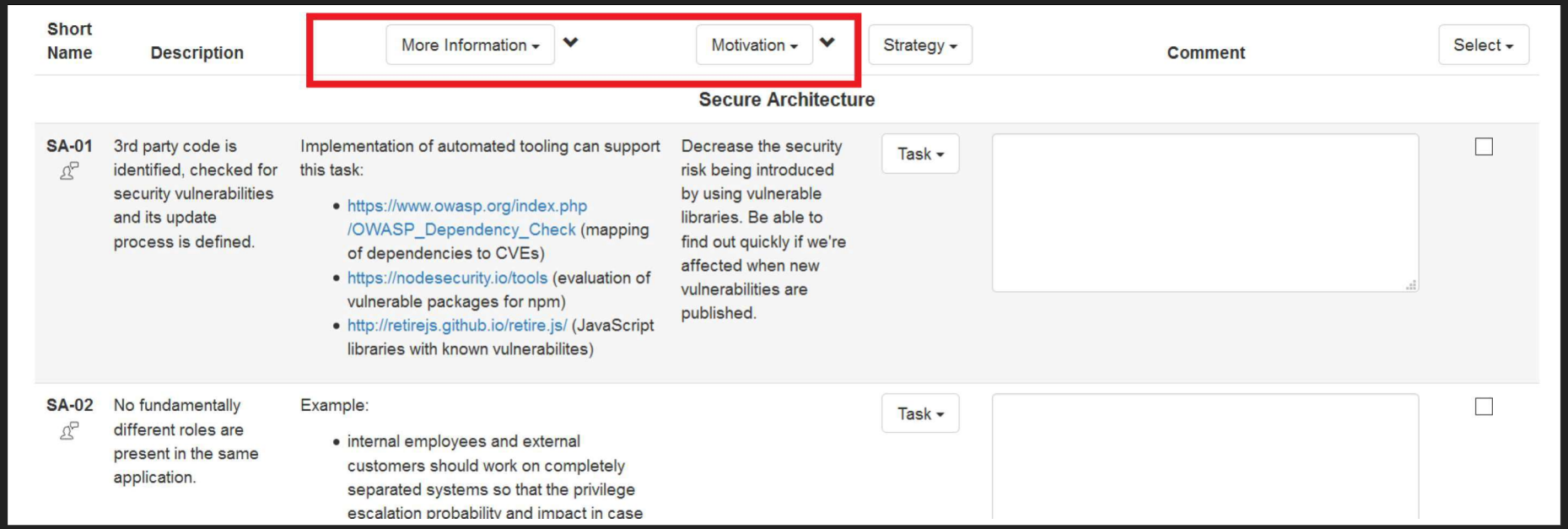
Based on JHipster

Requirement Skeletons



Short Name	Description	More Information	Motivation	Strategy	Comment	Select
			Secure Architecture			
SA-01	3rd party code is identified, checked for security vulnerabilities and its update process is defined.	Implementation of automated tooling can support this task: • https://www.owasp.org/index.php/OWASP_Dependency_Check (mapping of dependencies to CVEs) • https://nodesecurity.io/tools (evaluation of vulnerable packages for npm) • http://retirejs.github.io/retire.js/ (JavaScript libraries with known vulnerabilites)	Decrease the security risk being introduced by using vulnerable libraries. Be able to find out quickly if we're affected when new vulnerabilities are published.	Task		☐
SA-02	No fundamentally different roles are present in the same application.	Example: • internal employees and external customers should work on completely separated systems so that the privilege escalation probability and impact in case		Task		☐

Optional Columns



Short Name	Description	More Information	Motivation	Strategy	Comment	Select
			Secure Architecture			
SA-01	3rd party code is identified, checked for security vulnerabilities and its update process is defined.	Implementation of automated tooling can support this task: • https://www.owasp.org/index.php/OWASP_Dependency_Check (mapping of dependencies to CVEs) • https://nodesecurity.io/tools (evaluation of vulnerable packages for npm) • http://retirejs.github.io/retire.js/ (JavaScript libraries with known vulnerabilites)	Decrease the security risk being introduced by using vulnerable libraries. Be able to find out quickly if we're affected when new vulnerabilities are published.	Task		☐
SA-02	No fundamentally different roles are present in the same application.	Example: • internal employees and external customers should work on completely separated systems so that the privilege escalation probability and impact in case		Task		☐

Alternatives to Option Columns

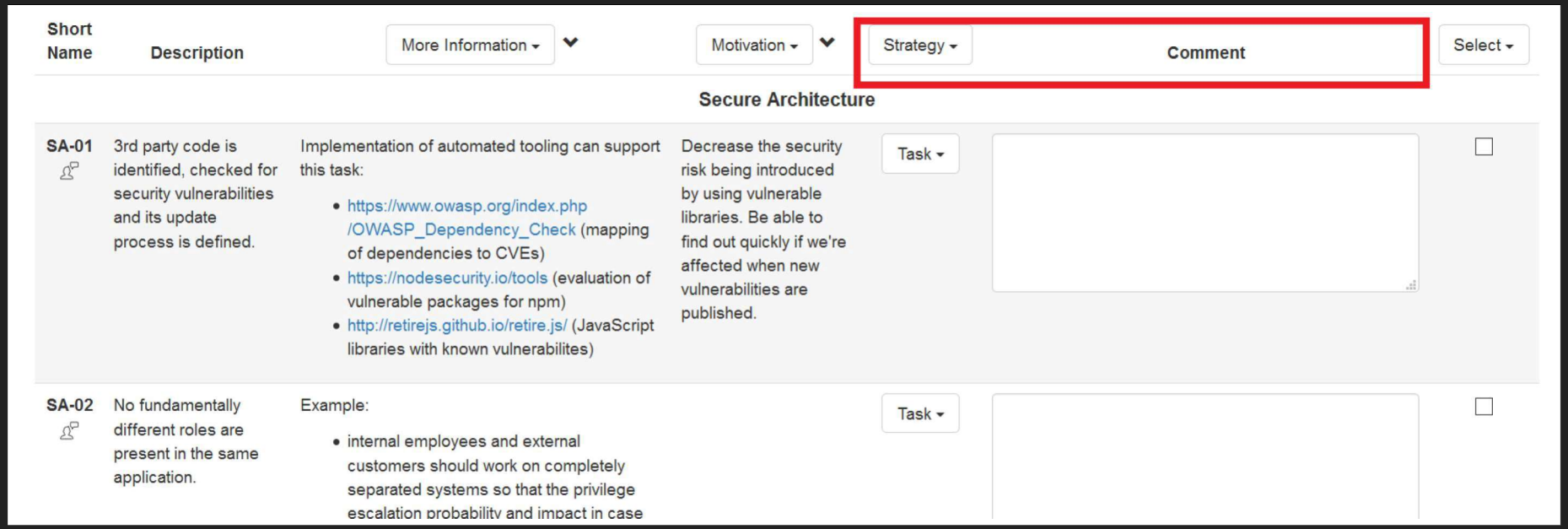
Short Name	Description	JAVA Application	Motivation	Strategy
		Output Encoding		
OE-01	All untrusted data outputted to any interface are properly escaped for the particular context using a common and standardized approach.	These interfaces can include (but are not limited to): • SQL • NoSQL • Web Services • LDAP • ... Parametrized queries should be used in all cases.	Prevent injection attacks, e.g.: • SQL Injection • LDAP Injection	Task

JAVA Application

Example of a prepared statement for SQL queries:

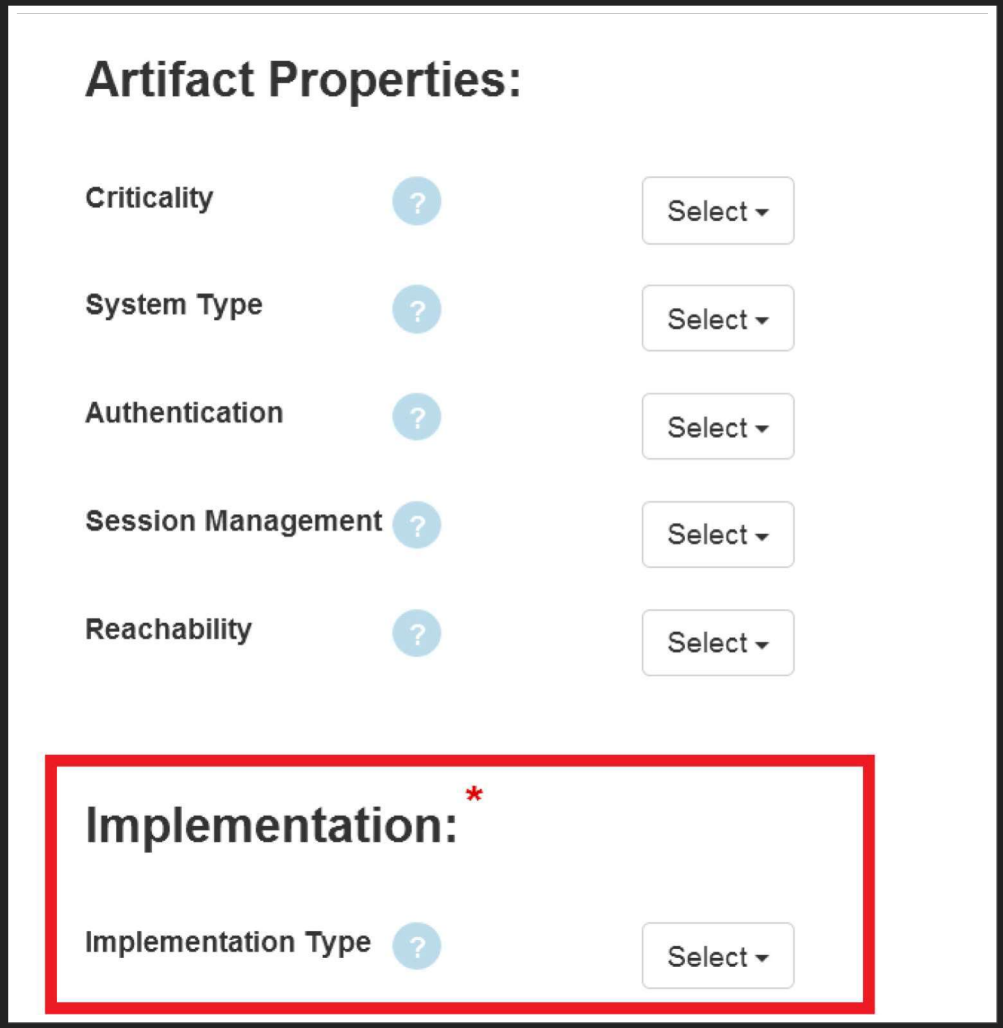
```
String selectSQL = "SELECT USER_ID, USERNAME FROM DBUSER
WHERE USER_ID = ?";
PreparedStatement preparedStatement = dbConnection.prepar
eStatement(selectSQL);
preparedStatement.setInt(1, 1001);
ResultSet rs = preparedStatement.executeQuery(selectSQL )
;
while (rs.next()) {
    String userid = rs.getString("USER_ID");
```

Status Columns

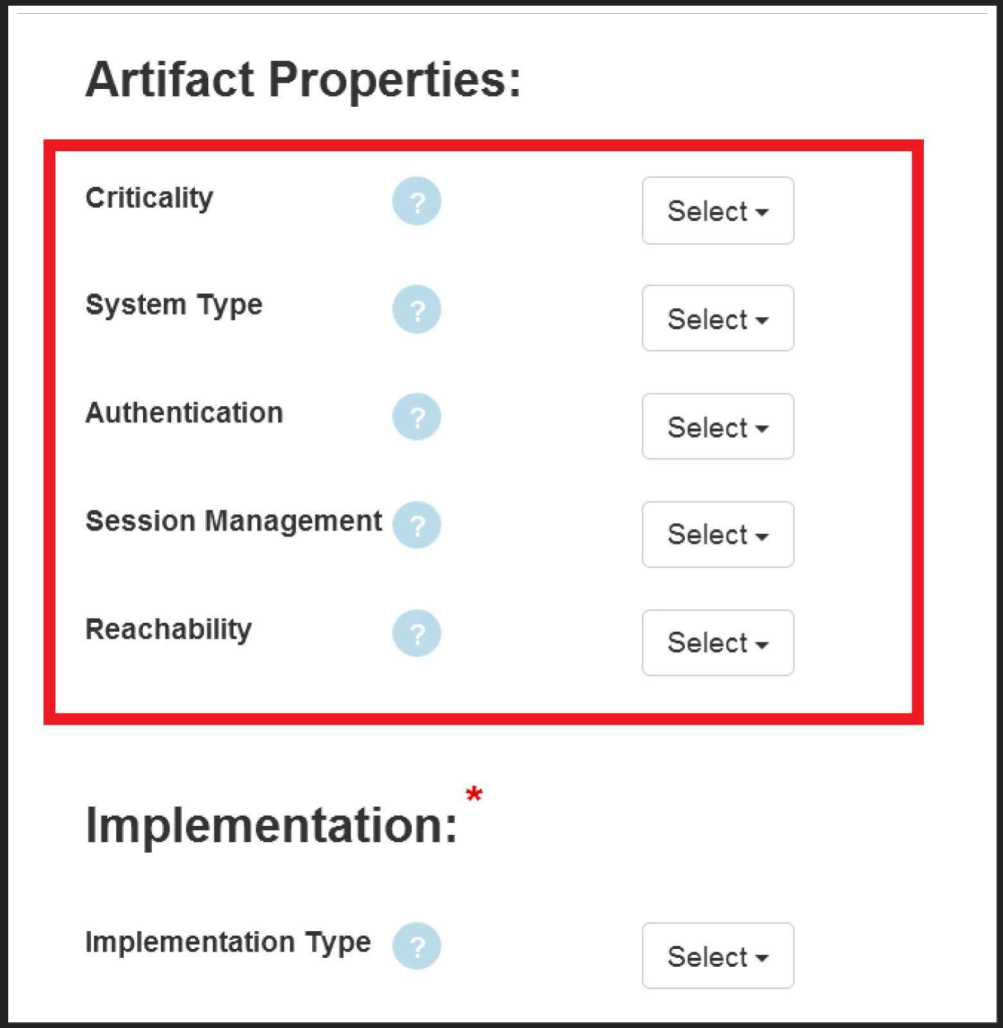


Short Name	Description	More Information	Motivation	Strategy	Comment	Select
				Secure Architecture		
SA-01	3rd party code is identified, checked for security vulnerabilities and its update process is defined.	Implementation of automated tooling can support this task: • https://www.owasp.org/index.php/OWASP_Dependency_Check (mapping of dependencies to CVEs) • https://nodesecurity.io/tools (evaluation of vulnerable packages for npm) • http://retirejs.github.io/retire.js/ (JavaScript libraries with known vulnerabilites)	Decrease the security risk being introduced by using vulnerable libraries. Be able to find out quickly if we're affected when new vulnerabilities are published.	Task		☐
SA-02	No fundamentally different roles are present in the same application.	Example: • internal employees and external customers should work on completely separated systems so that the privilege escalation probability and impact in case		Task		☐

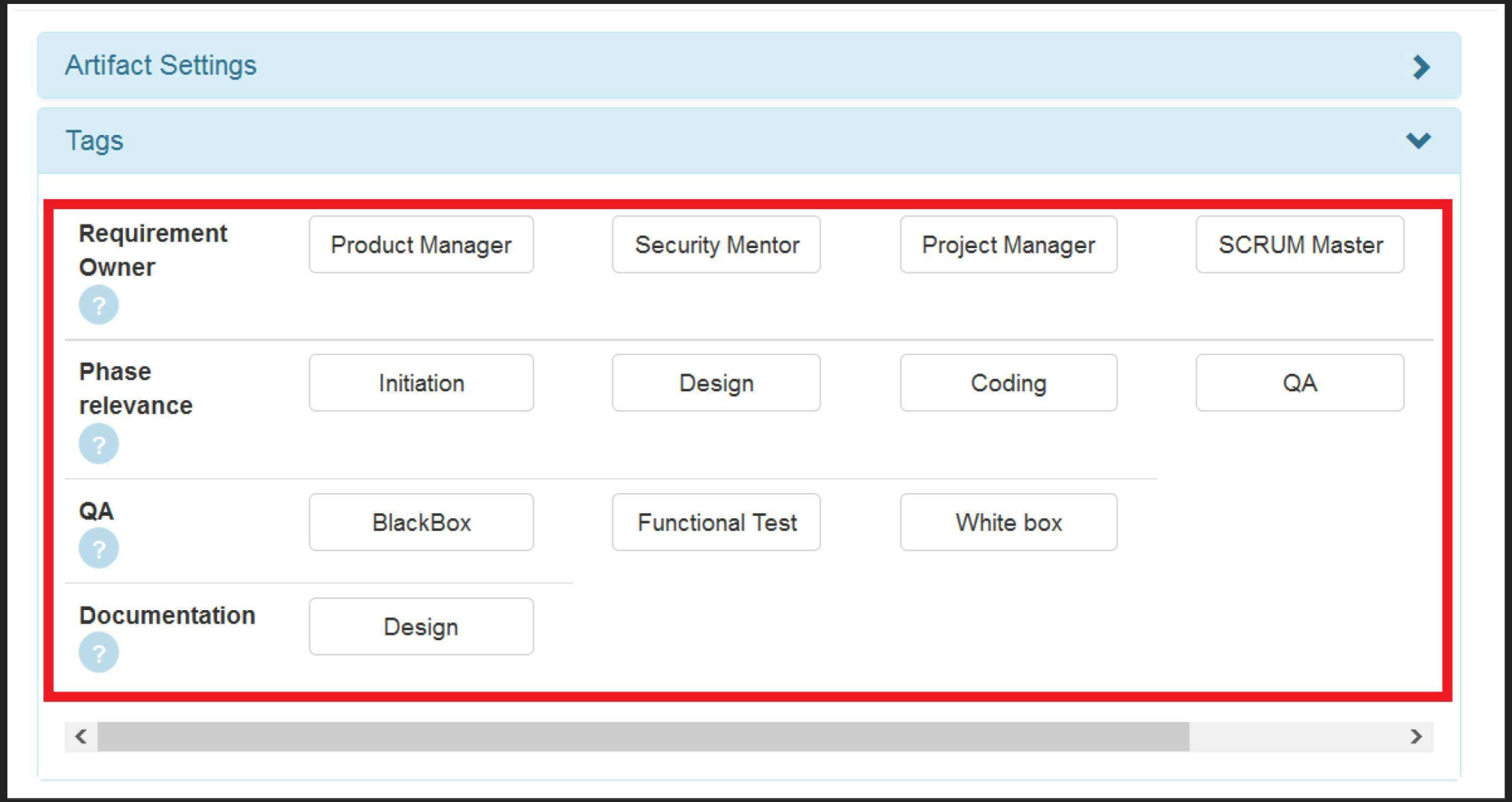
Implementation Type



Collections



Tags


Artifact Settings
Tags
Requirement Owner
Product Manager
Security Mentor
Project Manager
SCRUM Master
Phase relevance
Initiation
Design
Coding
QA
QA
BlackBox
Functional Test
White box
Documentation
Design

AUTHENTICATION

Own authentication scheme

CAS (Central Authentication Service)

ROLES

Frontend User

User

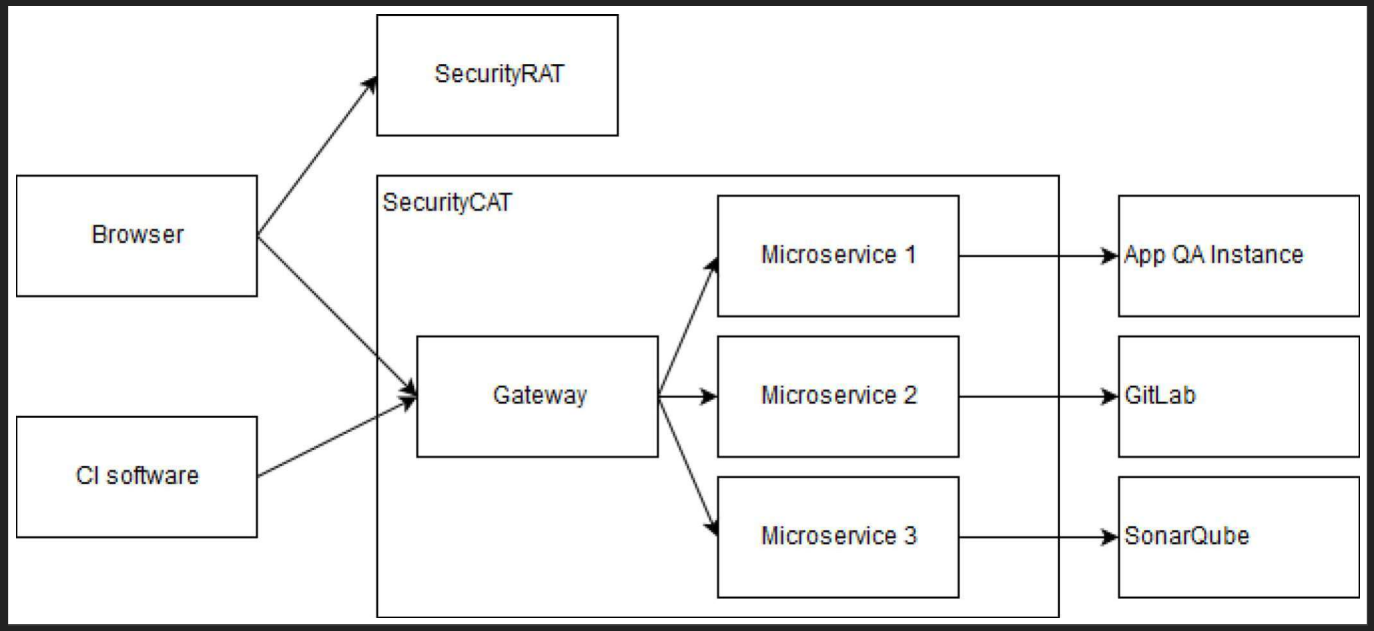
Admin

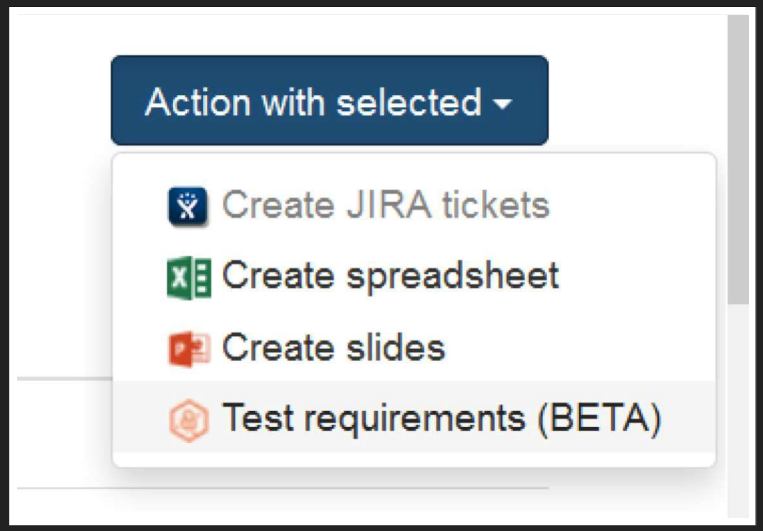
JIRA INTEGRATION

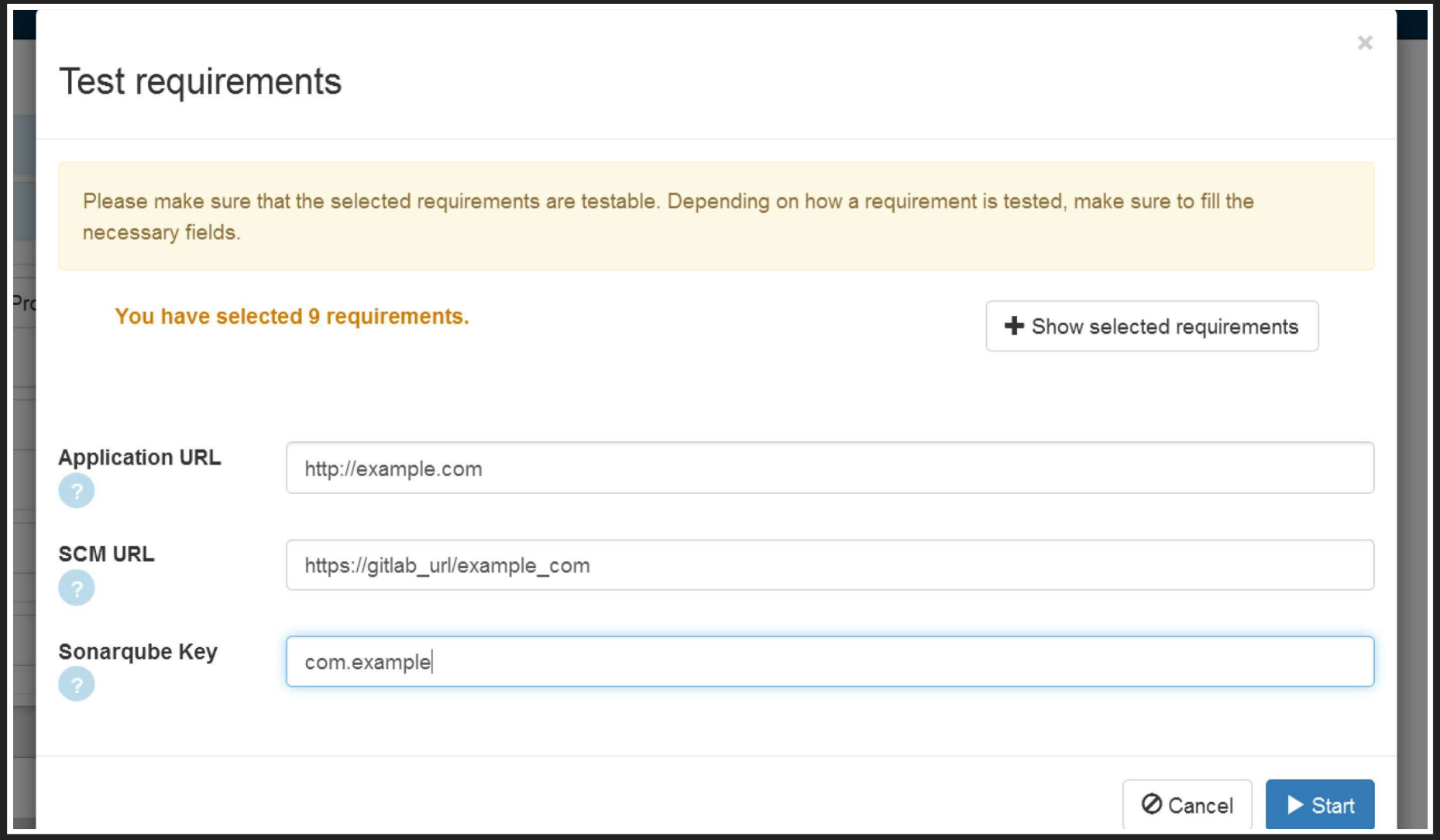
Cross Origin Request Sharing

SecurityRAT inherits user‘s rights in JIRA

SECURITYCAT


SecurityRAT
Browser
SecurityCAT
Microservice 1
App QA Instance
Gateway
Microservice 2
GitLab
CI software
Microservice 3
SonarQube


Action with selected
Create JIRA tickets
Create spreadsheet
Create slides
Test requirements (BETA)


Test requirements
Please make sure that the selected requirements are testable. Depending on how a requirement is tested, make sure to fill the necessary fields.
You have selected 9 requirements.
Show selected requirements
Application URL
http://example.com
SCM URL
https://gitlab_url/example_com
Sonarqube Key
com.example
Cancel
Start

Test results

Alternatively is the result available at https:// ./serviceapi/resource/46 for a week as from now.

Short Name	Description	Result	Confidence level	Message	Tool
IV-08	Buffer overflow attacks are mitigated.	✓	90%	The test was successful.	sonarMS
EHL-01	The system does not output error messages data that could assist an attacker.	✗	70%	The test was unsuccessful. Check for the sonarqube vulnerabilities to your projects with tag(s) error-handling.	sonarMS
SA-01	3rd party code is identified, checked for security vulnerabilities and its update process is defined.	✓	70%	The test was successful.	sonarMS
IV-04	Cross-Site Request Forgery attacks are mitigated.	✓	50%	The test was successful.	sonarMS
OE-01	All untrusted data outputted to any interface are properly escaped for the particular context using a common and standardized approach.	✓	90%	The test was successful.	sonarMS


FUTURE PLANS

SECURITYRAT 2.0

https://github.com/SecurityRAT/SecurityRAT/wiki/Version-2.0-Brainstorming

COMMUNITY

Issues

Pull requests

Derived projects

THANK YOU FOR YOUR ATTENTION!

https://securityrat.github.io

dan.kefer@gmail.com