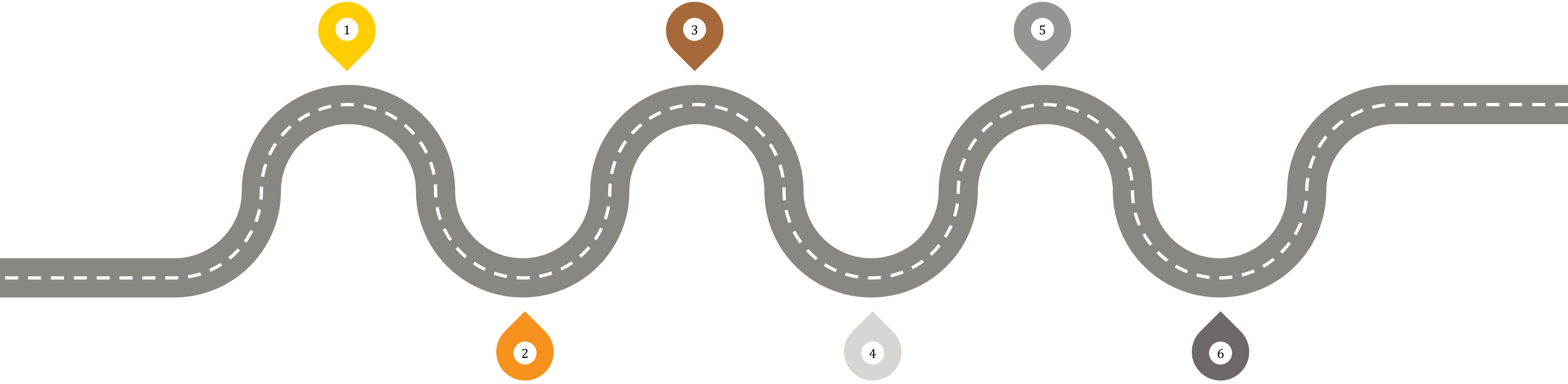
Shift-left and Automate Compliance Checks

Contents

- Introduction
- What is Shift-Left?
- FOSSID
- How to use FOSSID API
- Tasks
- Plans
- Questions

Hello!

I am Arlo



SW Defect Prediction

Configuration Management
Quality

CI/CD
Process
Automation

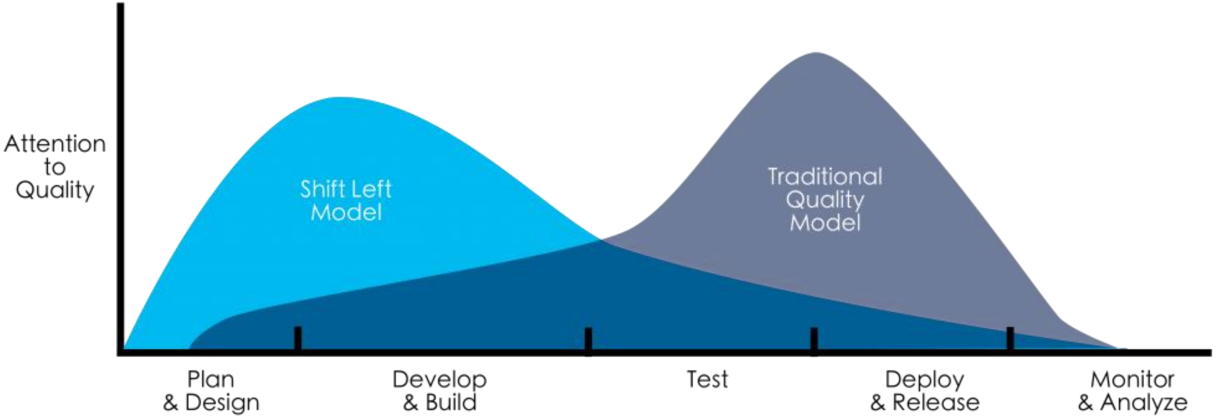
Front-end
Infra

CI/CD
Deployment
Quality
Open Source Manager?

?

What is Shift-Left?

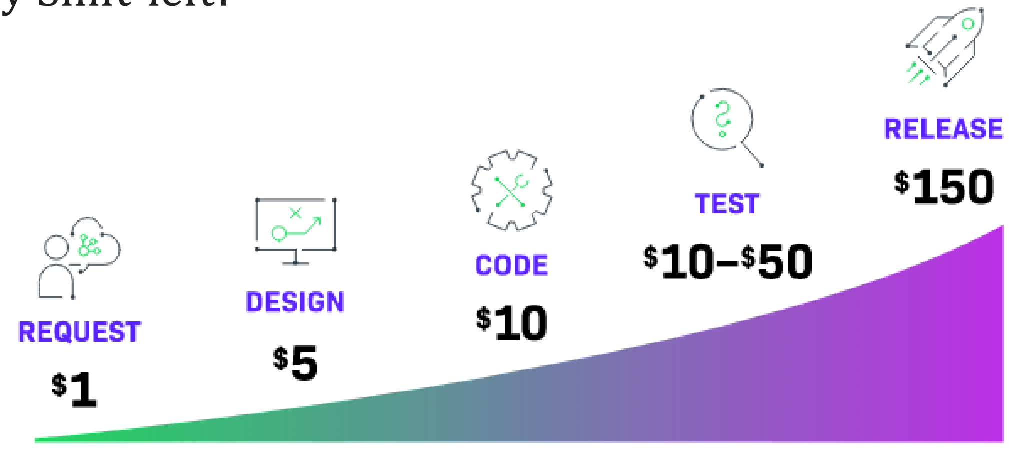
- Shift-left Testing ?



Shift Left is about doing things earlier in the development cycle. Source: van der Cruijsen

What is Shift-Left?

- Why Shift-left?

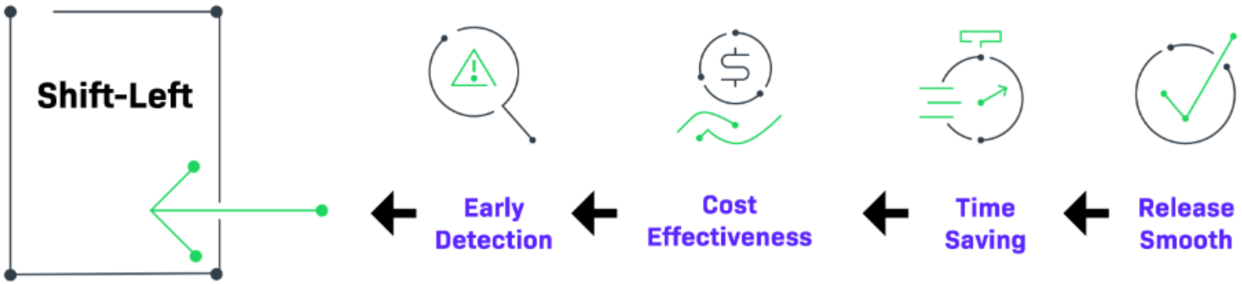


Cost to mitigate risk increases if identified later in the development lifecycle

Shift-Left and Automate Compliance Checks. Ref. revenera.

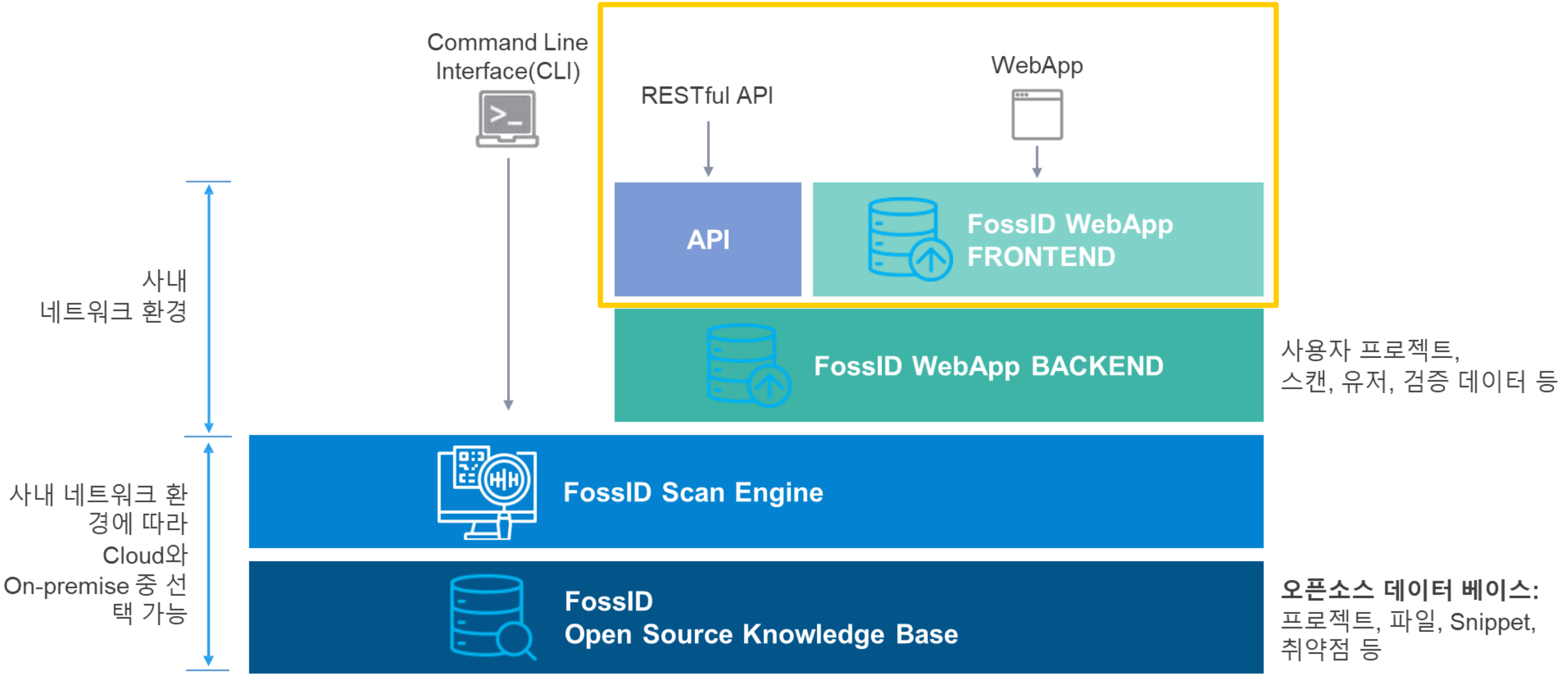
What is Shift-Left?

- Benefits? -> Shift-left Compliance Checks !



Shift-Left and Automate Compliance Checks. Ref. revenera.

FOSSID



Command Line Interface(CLI)

RESTful API

WebApp

API

FossID WebApp FRONTEND

FossID WebApp BACKEND

FossID Scan Engine

FossID
Open Source Knowledge Base

사내
네트워크 환경

사내 네트워크 환경에 따라 Cloud와 On-premise 중 선택 가능

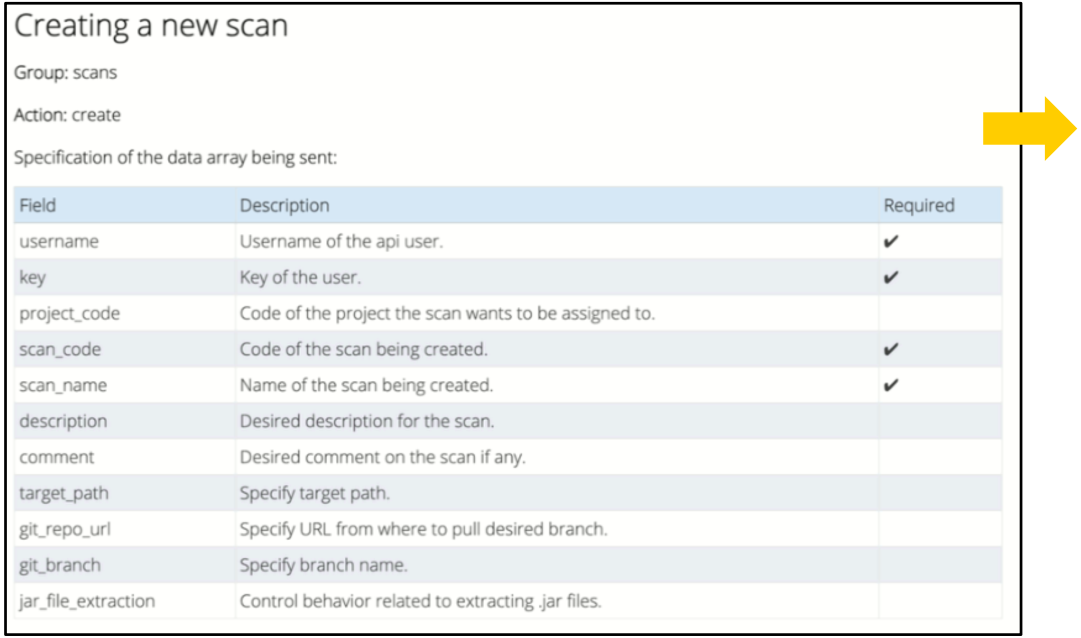
사용자 프로젝트,
스캔, 유저, 검증 데이터 등

오픈소스 데이터 베이스:
프로젝트, 파일, Snippet,
취약점 등

How to use FOSSID API

- Projects
- **Scans**
    - create
    - list_scans
    - get_information
    - get_pending_files
    - update
    - download_content_from_git
    - check_status_download_content_from_git
    - run
    - check_status
    - get_results
    - get_scan_identified_component
    - generate_report
    - ….
- Quick Scans
- Components
- Licenses
- Users
- Files and Folders
- Jira

How to use FOSSID API



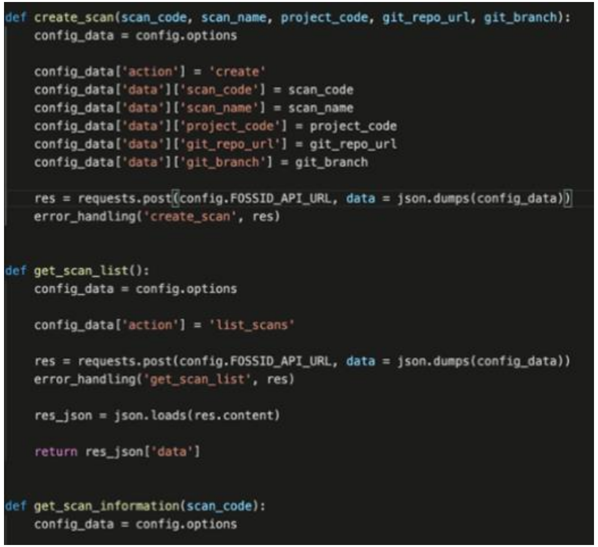
Creating a new scan

Group: scans

Action: create

Specification of the data array being sent:

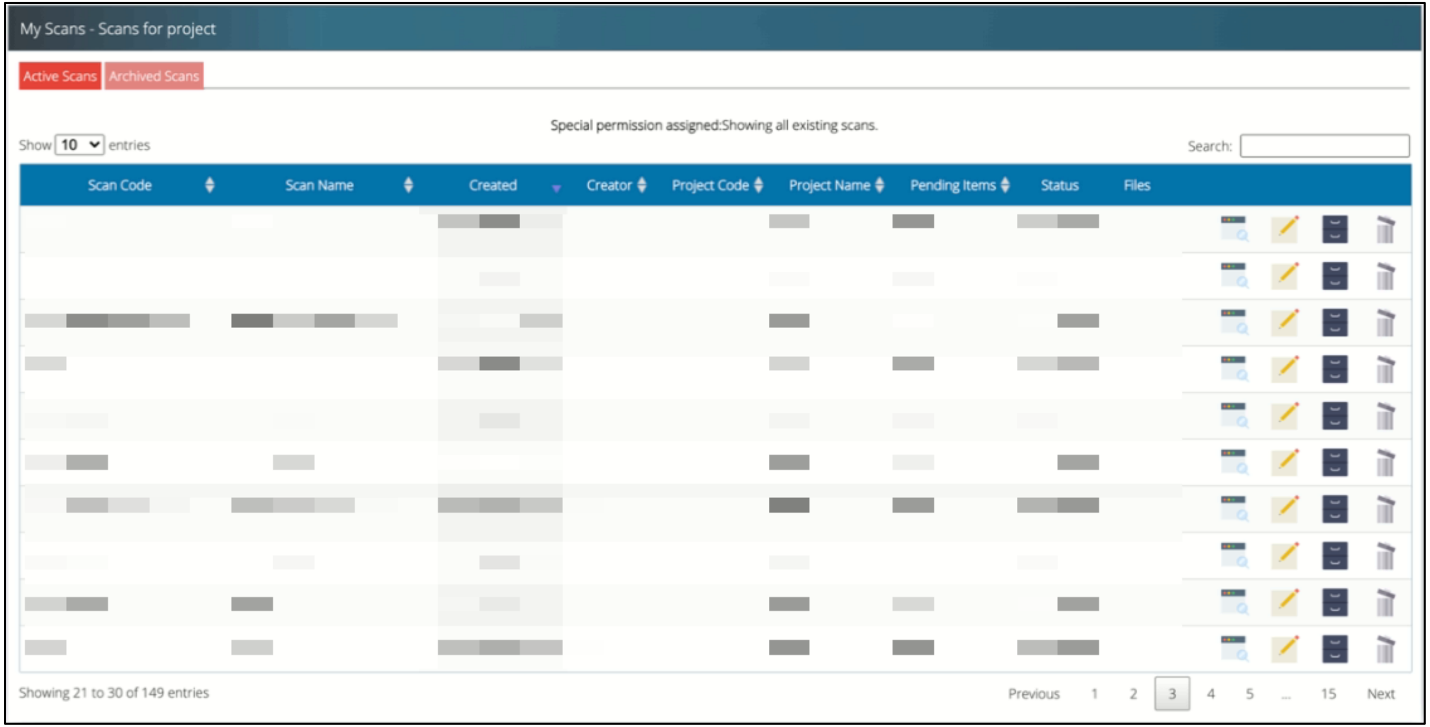
Field	Description	Required
username	Username of the api user.	✔
key	Key of the user.	✔
project_code	Code of the project the scan wants to be assigned to.	
scan_code	Code of the scan being created.	✔
scan_name	Name of the scan being created.	✔
description	Desired description for the scan.	
comment	Desired comment on the scan if any.	
target_path	Specify target path.	
git_repo_url	Specify URL from where to pull desired branch.	
git_branch	Specify branch name.	
jar_file_extraction	Control behavior related to extracting .jar files.	



```
def create_scan(scan_code, scan_name, project_code, git_repo_url, git_branch):
    config_data = config.options

    config_data['action'] = 'create'
    config_data['data']['scan_code'] = scan_code
    config_data['data']['scan_name'] = scan_name
    config_data['data']['project_code'] = project_code
    config_data['data']['git_repo_url'] = git_repo_url
    config_data['data']['git_branch'] = git_branch

    res = requests.post(config.FOSSID_API_URL, data = json.dumps(config_data))
    error_handling('create_scan', res)


def get_scan_list():
    config_data = config.options

    config_data['action'] = 'list_scans'

    res = requests.post(config.FOSSID_API_URL, data = json.dumps(config_data))
    error_handling('get_scan_list', res)

    res_json = json.loads(res.content)

    return res_json['data']


def get_scan_information(scan_code):
    config_data = config.options
```

FOSSID API 사용하는 코드로 당행에 대한 정보는 제외함

How to use FOSSID API



My Scans - Scans for project

Special permission assigned:Showing all existing scans.

Show 10 entries

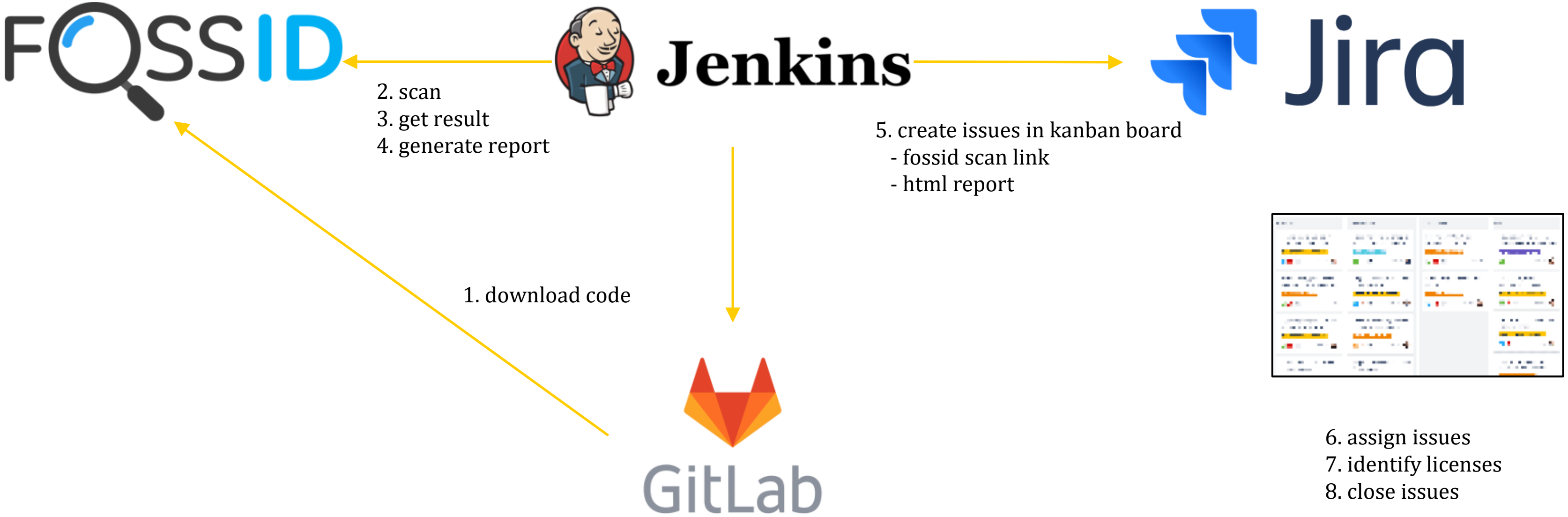
Search:

Scan Code	Scan Name	Created	Creator	Project Code	Project Name	Pending Items	Status	Files

[redacted]

Showing 21 to 30 of 149 entries

How to use FOSSID API



2. scan
3. get result
4. generate report

5. create issues in kanban board
   - fossid scan link
   - html report

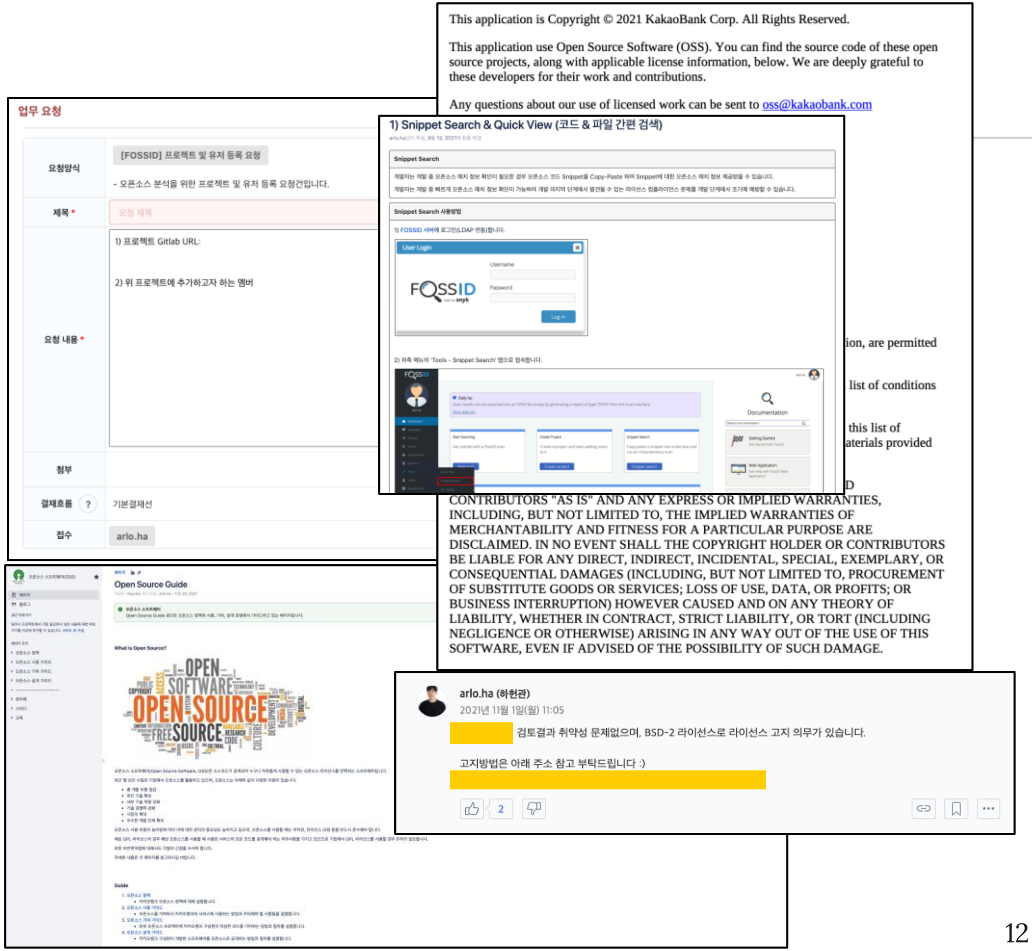
1. download code

6. assign issues
7. identify licenses
8. close issues

Automatically !

Tasks

- FOSSID
- OSS Process
- Wiki
- License Feedback
- Notice
- Vulnerability
- Education
- OSRB
- ISO/IEC 5230



This application is Copyright © 2021 KakaoBank Corp. All Rights Reserved.

This application use Open Source Software (OSS). You can find the source code of these open source projects, along with applicable license information, below. We are deeply grateful to these developers for their work and contributions.

Any questions about our use of licensed work can be sent to oss@kakaobank.com

ion, are permitted

list of conditions

this list of
aterials provided

D
CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

업무 요청

요청양식	[FOSSID] 프로젝트 및 유저 등록 요청 - 오픈소스 분석을 위한 프로젝트 및 유저 등록 요청건입니다.
제목 *	요청 제목
요청 내용 *	1) 프로젝트 Gitlab URL: 2) 위 프로젝트에 추가하고자 하는 멤버
첨부	
결재흐름 ?	기본결재선
접수	arlo.ha

1) Snippet Search & Quick View (코드 & 파일 간편 검색)

Snippet Search

개발자는 개발 중 오픈소스 매치 정보 확인이 필요한 경우 오픈소스 코드 Snippet을 Copy-Paste 하여 Snippet에 대한 오픈소스 매치 정보 제공받을 수 있습니다.

개발자는 개발 중 빠르게 오픈소스 매치 정보 확인이 가능하여 개발 마지막 단계에서 발견될 수 있는 라이선스 컴플라이언스 문제를 개발 단계에서 조기에 예방할 수 있습니다.

Snippet Search 사용방법

1) FOSSID 서버에 로그인(LDAP 연동)합니다.

2) 좌측 메뉴의 'Tools - Snippet Search' 탭으로 접속합니다.

Open Source Guide

What is Open Source?

Guide

1. 오픈소스 정책
2. 오픈소스 사용 가이드
3. 오픈소스 기여 가이드
4. 오픈소스 공개 가이드

arlo.ha (하현관)
2021년 11월 1일(월) 11:05

[redacted] 검토결과 취약성 문제없으며, BSD-2 라이선스로 라이선스 고지 의무가 있습니다.

고지방법은 아래 주소 참고 부탁드립니다 :)

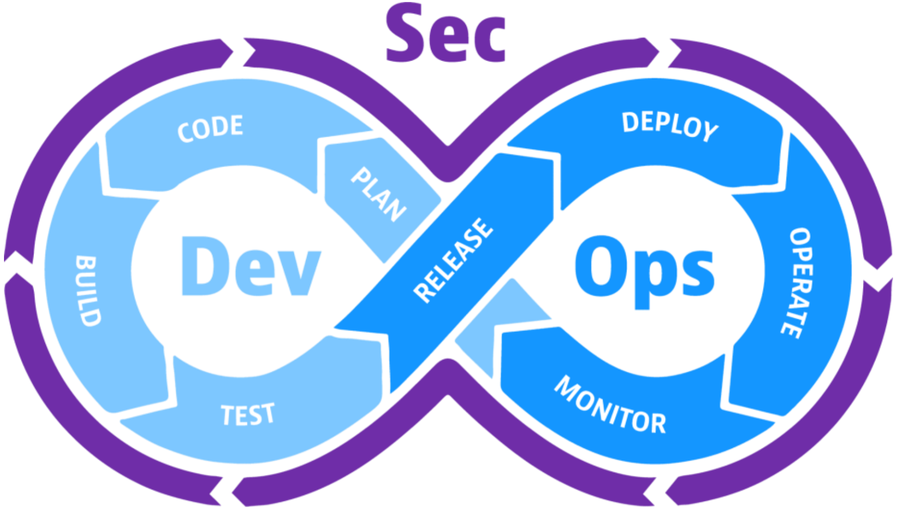
[redacted]

2

Plans

DevSecOps

- Vulnerability
- Dependency
- Checklist
- Cultures
- Automation
- Containers
- ...



References

- https://nipa-openup.github.io/oss-governance-guide/
- https://sktelecom.github.io/guide/
- https://fossid.com/

Thanks!

*Any **questions** ?*

You can find me at

- arlo.ha@kakaobank.com