

APPSEC PIPELINE В ПРОЦЕССЕ РАЗРАБОТКИ ПО

AppSec Pipeline: как построить централизованный безопасный процесс разработки и интегрировать проверки в РБПО.

APPSEC PIPELINE:

КАК ПОСТРОИТЬ ЦЕНТРАЛИЗОВАННЫЙ БЕЗОПАСНЫЙ ПРОЦЕСС
РАЗРАБОТКИ И ИНТЕГРИРОВАТЬ ПРОВЕРКИ В РБПО



ПЛАН ВЕБИНАРА

ПОГОВОРИМ:

- Точка отправления
- Вызов перед нами
- Как было изначально
- Что хотели получить
- Как мы это реализовали
- Что планируем дальше



НАШИ КОМПЕТЕНЦИИ



DIGITAL
DESIGN

КОМПЛЕКСНЫЙ ПОДХОД К ЗАЩИТЕ

Мы предлагаем полный цикл услуг информационной безопасности: от аудита инфраструктуры и аттестации информационных систем до разработки и внедрения собственных решений.

ЛИЦЕНЗИРОВАНИЕ И СЕРТИФИКАЦИЯ

Наша команда обладает полным набором лицензий ФСТЭК России и ФСБ России, что позволяет легально и без ограничений выполнять проекты любой сложности в сфере информационной безопасности

СПЕЦИАЛИЗАЦИЯ НА ПРОЕКТАХ В КРУПНЫХ КОРПОРАЦИЯХ

Мы успешно реализовали проекты для государственных структур и ведущих коммерческих компаний, понимая их строгие требования и корпоративные стандарты безопасности

ГЛУБОКИЕ ЗНАНИЯ СМЕЖНЫХ ОБЛАСТЕЙ

Наша экспертиза выходит за рамки ИБ: мы координируем работу с подрядчиками, консультируем по интеграции решений и управляем процессами кибербезопасности на всех этапах

СПЕЦИАЛЬНОЕ ПРЕДЛОЖЕНИЕ

DIGITAL
DESIGN



КОНСУЛЬТАЦИОННЫЕ УСЛУГИ ЦЕНТРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

*Для запроса пишите на info@digdes.com
с темой письма «Специальное предложение вебинара»*

О ГРУППЕ КОМПАНИЙ DIGITAL DESIGN

DIGITAL
DESIGN

Входит в топ-20 крупнейших разработчиков
ПО в России

5000+

УСПЕШНЫХ ПРОЕКТОВ

30+

ЛЕТ НА РЫНКЕ

350+

КЛИЕНТОВ В 30+ СТРАНАХ

550+

СПЕЦИАЛИСТОВ

DIGITAL
DESIGN

разрабатывает и внедряет системы автоматизации бизнес-процессов, электронного документооборота, информационной безопасности, а также порталные решения и мобильные приложения.

 docsvision

стоял у истоков автоматизации документооборота в нашей стране и сейчас является одним из лидеров рынка СЭД/ЕСМ/ВРМ. Платформа Docsvision, разработанная компанией для автоматизации управления документами и бизнес-процессами, внедрена более чем в тысяче организаций России и стран ближнего зарубежья. Платформу внедряют более 100 российских и зарубежных партнёров.

6

СТРУКТУРНЫХ ЕДИНИЦ
В КОМПАНИИ

200+

РАЗРАБОТЧИКОВ

10+

ОСНОВНЫХ ПРОДУКТОВ

Десятки продуктов заказной
разработки

ЧТО У НАС ЕСТЬ?



ПРОЦЕССЫ

У каждой БЛ свой независимый процесс свои подходы к разработке, версионированию, сборке, деплою, передачи дистрибутивов и т.д.



ПРОЦЕССЫ

У каждой БЛ свой независимый процесс свои подходы к разработке, версионированию, сборке, деплоя, передачи дистрибутивов и т.д.



ТЕХНОЛОГИИ

У каждой БЛ свой независимые технологии, Gitlab x2, Jenkins, TeamCity, Nexus, Harbor, Tekton, Azure DevOps (TFS) и т.д.



ПРОЦЕССЫ

У каждой БЛ свой независимый процесс свои подходы к разработке, версионированию, сборке, деплоя, передачи дистрибутивов и т.д.



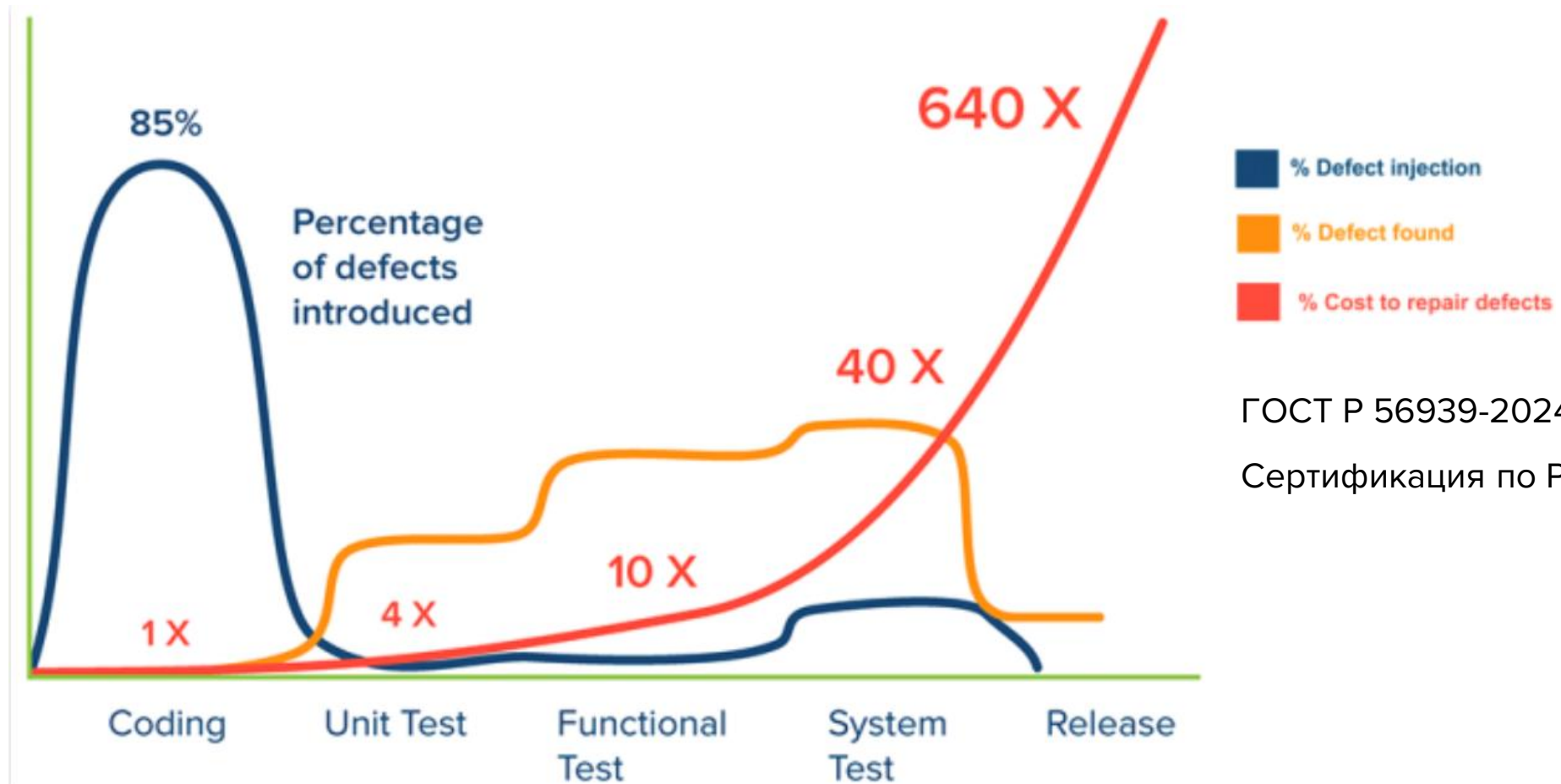
ТЕХНОЛОГИИ

У каждой БЛ свой независимые технологии, Gitlab x2, Jenkins, TeamCity, Nexus, Harbor, Tekton, Azure DevOps (TFS) и т.д.



УРОВЕНЬ ЗРЕЛОСТИ

У каждой команды и БЛ свой уровень зрелости
Часть разработчиков смешана между БЛ и командами



ГОСТ Р 56939-2024

Сертификация по РБПО

**Jones, Capers. Applied Software Measurement: Global Analysis of Productivity and Quality*

КАК ВНЕДРИТЬ SSDLC?



ЗООПАРК ТЕХНОЛОГИЙ:

- Свои системы CI/CD
- Свои процессы разработки
- Свои системы коммуникации
- Свои процессы постановки задачи
- Свои методы и процессы передачи дистрибутивов
- И т.д.

Но делать надо...

DIGITAL
DESIGN



ИЗНАЧАЛЬНЫЙ ПРОЦЕСС APPSEC-PIPELINE

DIGITAL
DESIGN



Запрос от БЛ/Команды
разработки на
сканирование
Или ручная проверка

ЗАПРОС НА СКАН

ИЗНАЧАЛЬНЫЙ ПРОЦЕСС APPSEC-PIPELINE

DIGITAL
DESIGN



Запрос от БЛ/Команды
разработки на
сканирование
Или ручная проверка

ЗАПРОС НА СКАН

ПОДГОТОВКА К СКАНУ



Подготовка скриптов и
набора инструментов
для анализа в рамках
тех процесса БЛ

Bash/Python/Etc

ИЗНАЧАЛЬНЫЙ ПРОЦЕСС APPSEC-PIPELINE

DIGITAL
DESIGN



Запрос от БЛ/Команды
разработки на
сканирование
Или ручная проверка



Ручное или
полуавтоматическое
сканирование
репозитория
VM Runner

ЗАПРОС НА СКАН

ПОДГОТОВКА К СКАНУ

РЕАЛИЗАЦИЯ СКАНОВ



Подготовка скриптов и
набора инструментов
для анализа в рамках
тех процесса БЛ

Bash/Python/Etc

ИЗНАЧАЛЬНЫЙ ПРОЦЕСС APPSEC-PIPELINE

DIGITAL
DESIGN



Запрос от БЛ/Команды
разработки на
сканирование
Или ручная проверка



Ручное или
полуавтоматическое
сканирование
репозитория
VM Runner

ЗАПРОС НА СКАН

ПОДГОТОВКА К СКАНУ

РЕАЛИЗАЦИЯ СКАНОВ

ЗАГРУЗКА РЕЗУЛЬТАТОВ



Подготовка скриптов и
набора инструментов
для анализа в рамках
тех процесса БЛ

Bash/Python/Etc



Загрузка отчетов
в DefectDojo

Bash/Python/Etc

ИЗНАЧАЛЬНЫЙ ПРОЦЕСС APPSEC-PIPELINE

DIGITAL
DESIGN



Запрос от БЛ/Команды
разработки на
сканирование
Или ручная проверка



Ручное или
полуавтоматическое
сканирование
репозитория
VM Runner



Рефакторинг
и триаж уязвимостей
Обработка отчетов
Доступ
для разработчиков

ЗАПРОС НА СКАН

ПОДГОТОВКА К СКАНУ

РЕАЛИЗАЦИЯ СКАНОВ

ЗАГРУЗКА РЕЗУЛЬТАТОВ

АНАЛИЗ РЕЗУЛЬТАТОВ



Подготовка скриптов и
набора инструментов
для анализа в рамках
тех процесса БЛ

Bash/Python/Etc



Загрузка отчетов
в DefectDojo

Bash/Python/Etc



ОСНОВНЫЕ ПРОБЛЕМЫ ТЕКУЩЕГО ПРОЦЕССА

1. Отсутствие понимания Тех стека, процесса и того что происходит в каждой БЛ и что делать ИБ?
2. Как со всем этим работать?
3. Как все это поддерживать?
4. DefectDojo....



Инвентаризация

Отсутствие понимания сущ. репозиторий и проектов в БЛ



Централизация

Зоопарк сервисов и технологий без связи между БЛ и(или) между командами



Подготовка

Длительная подготовка к сканированию
Подключение занимает много времени



Работа с результатами

Сложная работа с триажем уязвимостей и их обработкой, дедубликация, исключения...



Метрики и процессы

Сложность в отслеживании метрик \ приоритетов \ задач по уязвимостям



И так далее..

DEFECTDOJO



ИНТЕРФЕЙС ПЕРЕУСЛОЖНЕН

- Отсутствие понятной конфигурации дедубликации
- Веб интерфейс слишком переусложнен
- Обучать разработчиков процессу работы с веб-интерфейсом
- Контролировать и настраивать доступы
- Как обрабатывать и контролировать исправления/исключения уязвимостей?

Generate Product Report

Filters

Name	SLA Start Date	CVE	CVSS v3	CVSSv3 score	Severity	Steps to Reproduce			
<input type="text" value="Name"/>	<input type="text" value="SLA Start Date"/>	<input type="text" value="CVE"/>	<input type="text" value="CVSS v3"/>	<input type="text" value="CVSSv3 score"/>	<input type="text" value="Nothing s"/>	<input type="text" value="Steps to Repro"/>			
Severity Justification	Active	Verified	False Positive	Duplicate	Duplicate Finding	Out Of Scope	Risk Accepted	Under Review	Last Status Update
<input type="text" value="Severity Justifir"/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value="Unk"/>	<input type="text" value="Unk"/>	<input type="text" value="Last Status Upd"/>
Review Requested By	Reviewers	Under Defect Review	Defect Review Requested By	Is Mitigated	Thread ID	Mitigated Date	Mitigated By	Last Reviewed By	
<input type="text" value=""/>	<input type="text" value="Nothing s"/>	<input type="text" value="Unknown"/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value="Thread ID"/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	
Line Number	Source File Path	Source File	Parameter	Payload	Hash Code	Line number			
<input type="text" value="Line Number"/>	<input type="text" value="Source File Pal"/>	<input type="text" value="Source File"/>	<input type="text" value="Parameter"/>	<input type="text" value="Payload"/>	<input type="text" value="Hash Code"/>	<input type="text" value="Line number"/>			
File path contains	Component name	Component version	Found by	Static finding (SAST)	Dynamic finding (DAST)	Created			
<input type="text" value="File path contai"/>	<input type="text" value="Component nai"/>	<input type="text" value="Component ver"/>	<input type="text" value="Nothing s"/>	<input type="text" value="Unknown"/>	<input type="text" value="Unknown"/>	<input type="text" value="Created"/>			
Scanner confidence	SonarQube issue	Unique ID from tool	Vulnerability ID from tool	SAST Source Object	SAST Sink Object	SAST Source Line number			
<input type="text" value="Scanner confid"/>	<input type="text" value=""/>	<input type="text" value="Unique ID from"/>	<input type="text" value="Vulnerability ID"/>	<input type="text" value="SAST Source C"/>	<input type="text" value="SAST Sink Obj"/>	<input type="text" value="SAST Source L"/>			
SAST Source File Path	Number of occurrences	Publish date	Tags	Tags (Test)	Tags (Engagement)				
<input type="text" value="SAST Source F"/>	<input type="text" value="Number of occi"/>	<input type="text" value="Publish date"/>	<input type="text" value="Enter some tags (comma separated,"/>	<input type="text" value="Enter some tags (comma separated,"/>	<input type="text" value="Enter some tags (comma separated,"/>				

Bulk Edit

Choose wisely...

Severity

Choose...

Date

mm/dd/yyyy

Planned Remediation Date

mm/dd/yyyy

Status

☐ Active

☐ Verified

☐ False Positive

☐ Out of scope

☐ Mitigated

Risk Acceptance

☐ Accept

☐ Unaccept

Notes

Tags

tag-group-charlie

tag-group-delta

Submit

Print

Search:

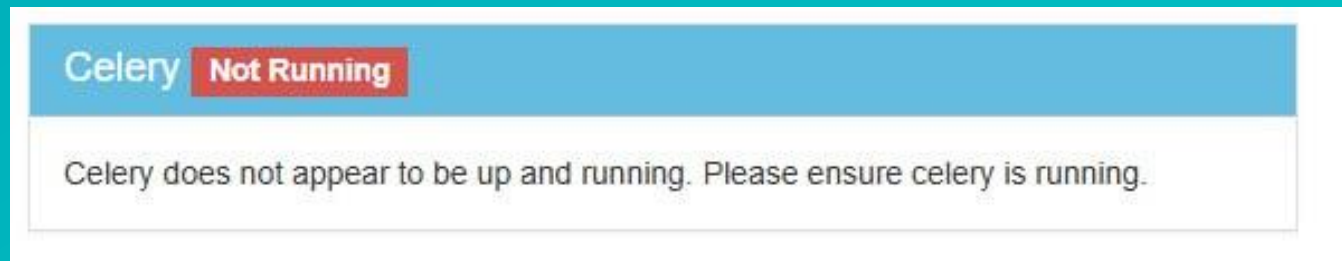
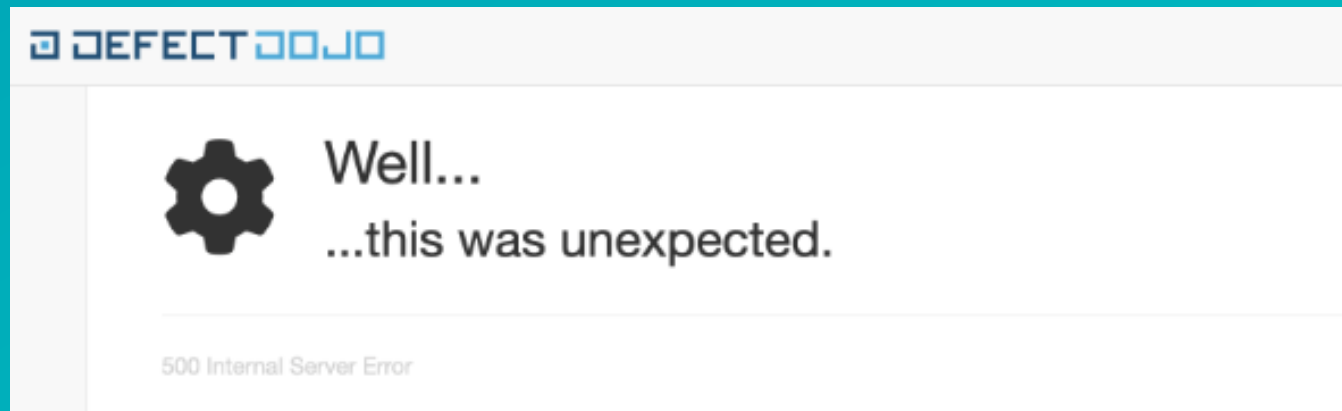
CWE	Vulnerability Id	Date	Age	SLA	Reporter	Found By	Status	Service	Planned Remediation
Signature Signed	CVE-2004-2761	May 11, 2023	0	90	Admin User (admin)	Nessus Scan	Active, Verified		
Signature Cannot		May 11, 2023	0	90	Admin User (admin)	Nessus Scan	Active, Verified		
Signature Signed		May 11, 2023	0	90	Admin User (admin)	Nessus Scan	Active, Verified		
Cipher Suites	CVE-2013-2566	May 11, 2023	0	90	Admin User (admin)	Nessus Scan	Active, Verified		

Page Size

DEFECTDOJO

ПОСТОЯННЫЕ ПАДЕНИЯ

- Постоянные падения
- Загрузка веб Flinging может достигать до 5-10 минут
- Дедубликация крашит сервер и БД
- Сложная интеграция с JIRA
- Затратен по ресурсам
- Устаревшие фреймворки



DEFECTDOJO

КАК РАБОТАТЬ С ИСКЛЮЧЕНИЯМИ И СТАТУСАМИ?

- Через Веб интерфейс?
- Через API? (снова скрипты и обертки)
- Задавать в конфигурации сканеров?
- Подключение сканеров для анализа репозиторий – рутинная и простая операция. Однако при большом количестве объектов анализа это может длиться неделями

```
Updating 11 findings as closed due to exclusions...
[OK] Finding 210911 updated successfully.
[OK] Finding 210921 updated successfully.
[OK] Finding 210933 updated successfully.
[OK] Finding 210459 updated successfully.
[OK] Finding 210943 updated successfully.
[OK] Finding 210949 updated successfully.
[OK] Finding 210962 updated successfully.
[OK] Finding 210974 updated successfully.
[OK] Finding 217020 updated successfully.
[OK] Finding 217026 updated successfully.
[OK] Finding 217034 updated successfully.
Uploading artifacts for successful job
Uploading artifacts...
request.json: found 1 matching artifact files and directories
```

```
Traceback (most recent call last):
  File "/opt/cib-engagement-creator.py", line 111, in <module>
    DD_PRODUCT_TYPE_ID = get_product_type_id(os.environ["DD_PROJECT_TYPE"], headers)
  File "/opt/cib-engagement-creator.py", line 59, in get_product_type_id
    response.raise_for_status()
  File "/usr/local/lib/python3.13/site-packages/requests/models.py", line 1026, in raise_for_status
    raise HTTPError(http_error_msg, response=self)
requests.exceptions.HTTPError: 502 Server Error: Bad Gateway for url: des.com:8080/api/v2/product_types/?name=
Cleaning up project directory and file based variables
ERROR: Job failed: command terminated with exit code 1
```

ЧТО ХОТЕЛИ ПОЛУЧИТЬ?

Централизацию систем
и процессов, понятную
документацию по РБПО



Единый AppSec-Pipeline. Иной ASOC?
Единый процесс работы
с SAST/DAST/SG/etc



Возможность работы
с исключениями
и приоритетами



Возможность отслеживать метрики, задачи
и процессы исправлений



Кратко:

1) Аудит сущ. процессов:

- Паспорт ПО и Паспорт Процессов (todo -> YAML)
- Понятная вики по процессам РБПО

2) Перевод всех репозиторий и процессов в единое место (Gitlab/GitLab CI/CD/Nexus/Build Cluster/Etc)

3) Построение единого Appsec-Pipeline

- Подключение новых сканеров / новых конфигов не должно влиять на разработку и мешать им
- Конфигурация переменных на БЛ/Репозиторий/
- Использовать по максимуму возможность девелопоцентричного подхода и возможности Gitlab

ЕДИНЫЙ APPSEC-PIPELINE

Что получилось:

Appsec-tools (Закрытый для остальных):

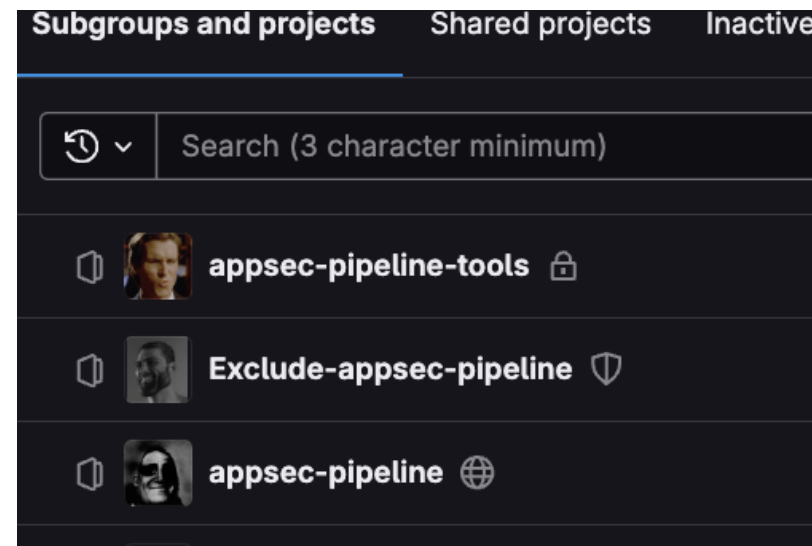
- Наши сканеры с доработками упакованными в контейнеры
- Скрипты для работы или автоматизаций

Exclude-appsec-pipeline (Общедоступный):

- Единое место для добавления исключений\конфигурации под БЛ и репозитории для ASOC
- Апрувы от ИБ через MR

Appsec-pipeline (Общедоступный):

- Централизованный CI с проверками и SecGate для всех репозиторий и БЛ с возможностью конфигурации под конкретные проекты



AppSec-pipeline

Подключение appsec-pipeline в проект

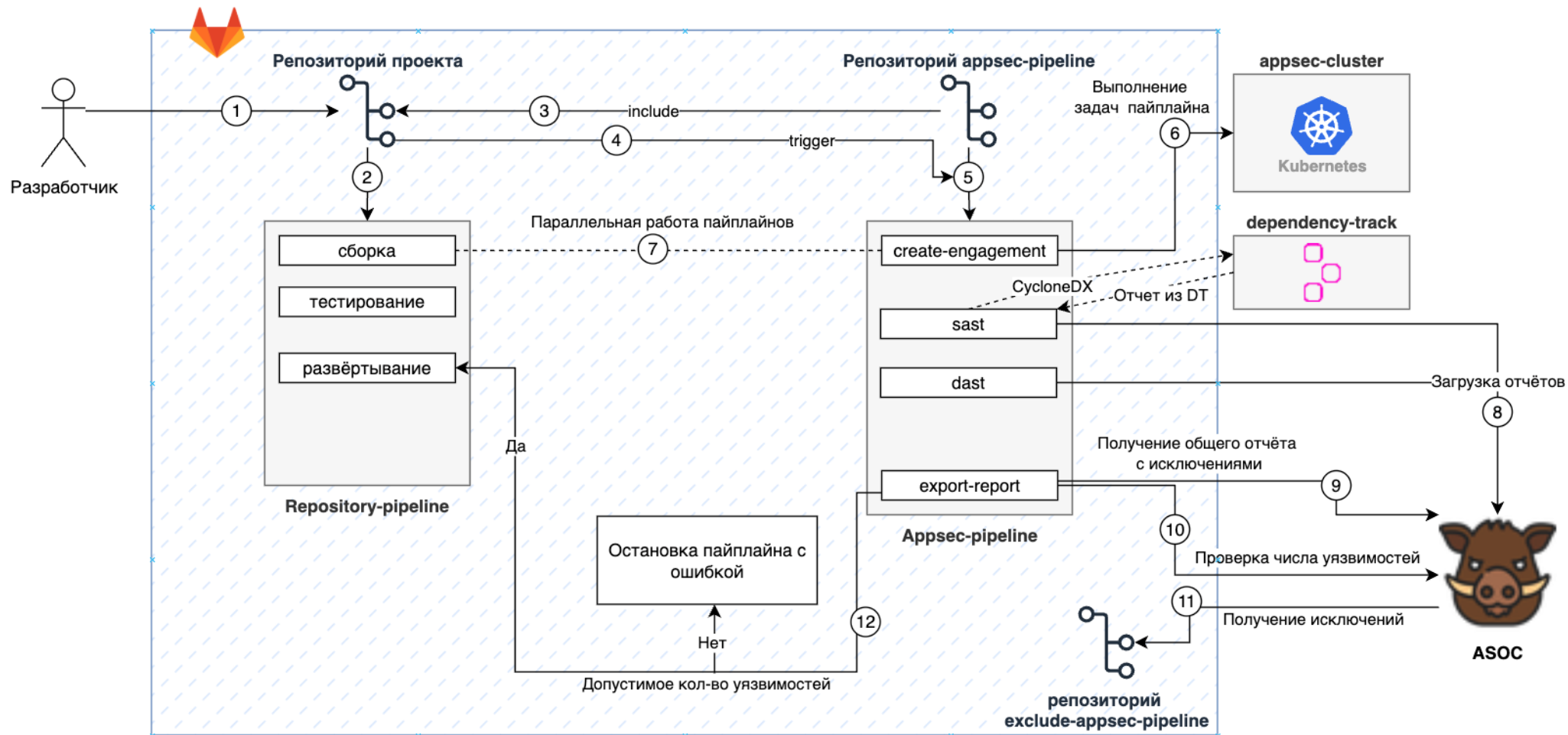
Добавьте данный код в .gitlab-ci.yml:

```
stages:
  - trigger-appsec

include:
  - project: '$APPSEC_PROJECT'
    ref: '$APPSEC_BRANCH'
    file: 'appsec-pipeline-job.yml'
```

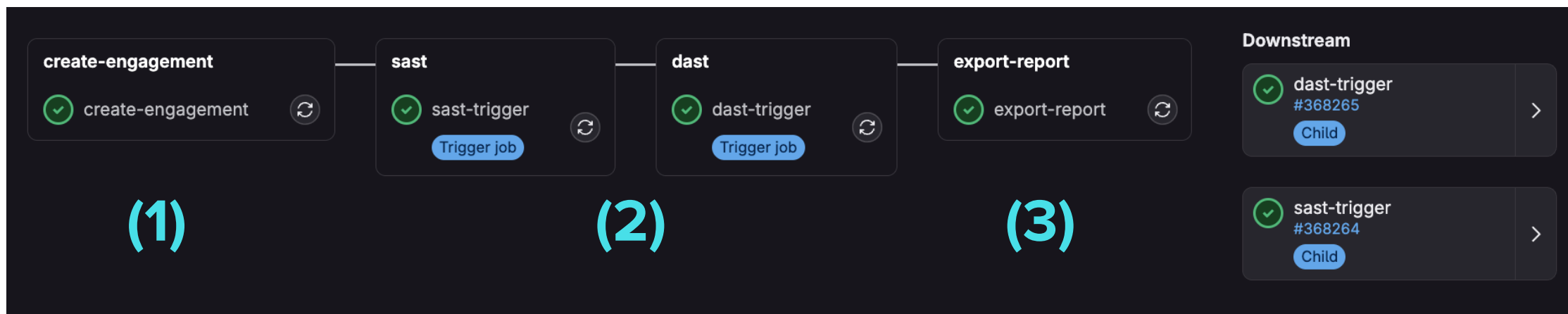

ЕДИНЫЙ APPSEC-PIPELINE

DIGITAL
DESIGN



ЕДИНЫЙ APPSEC-PIPELINE

DIGITAL
DESIGN



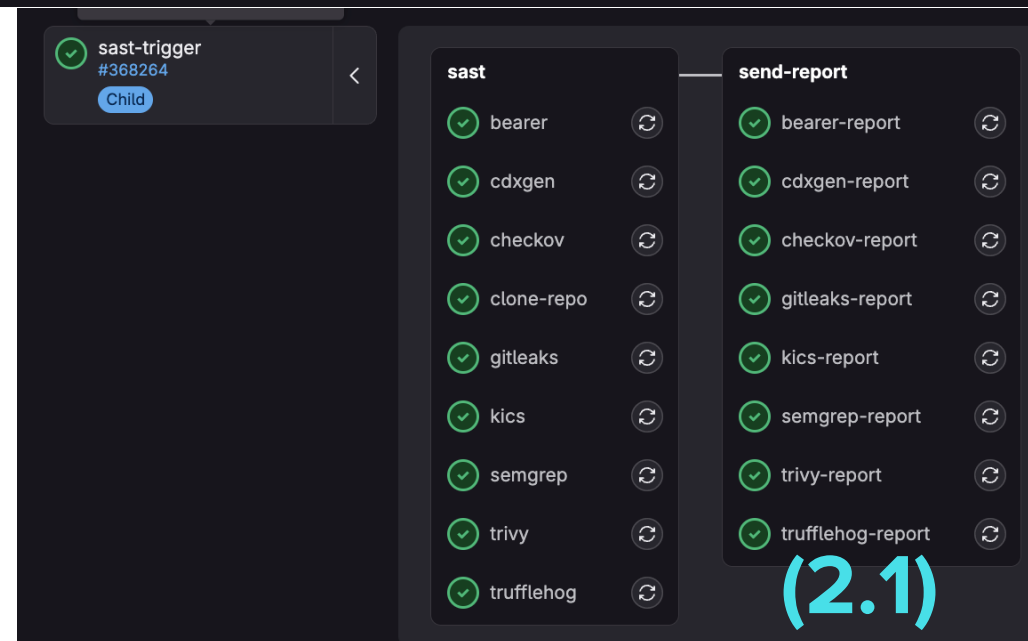
1) Create-engagement

- Подготовка и применение настроек
- Получение информации по проекту

2) SAST и DAST – Анализ сканерами исх. кода\образов\стендов

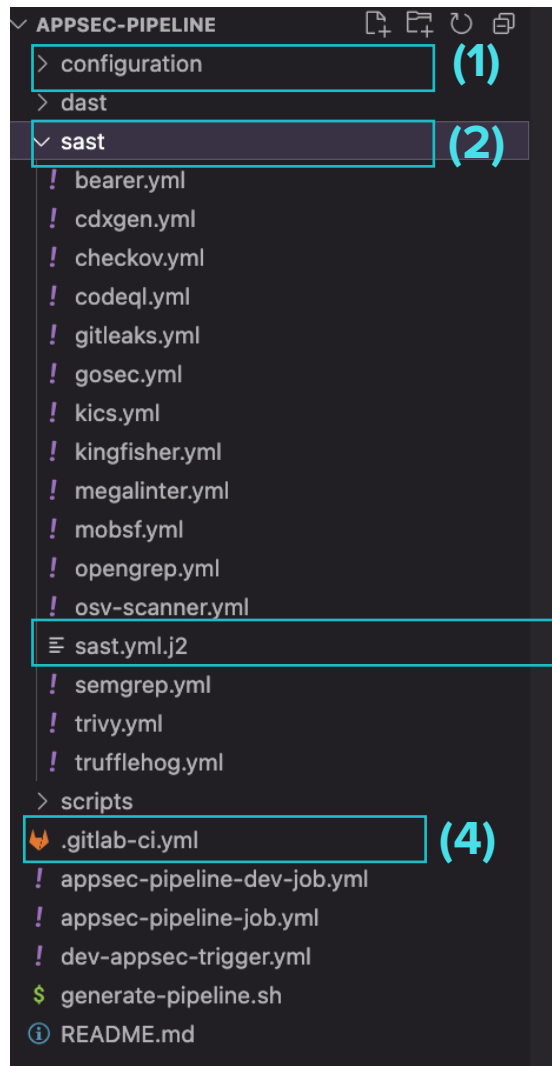
2.1) Send-report – Загрузка отчетов в ASOC

3) Export-Report – Вывод информации по уязвимостям в Pipeline и артефакты



ЕДИНЫЙ APPSEC-PIPELINE

DIGITAL
DESIGN



```
create-engagement:
  rules:
    - if: $UPSTREAM_BRANCH =~ /^(dev|test|prod|master|main)$/
      when: always
    - if: '$UPSTREAM_BRANCH =~ /^(develop|release-[^ ]+)/ && $UPSTREAM_PROJECT_ROOT_NAMESPACE == "devsecops"'
      when: always
    # АРЕОПАД (develop - ветка для сборки мобильной версии под заказчиков
    # dev-* - ветки фронта и бека для сборки артефактов под заказчика на дев стенды
    # release-* - ветки фронта и бека для отгрузки сборки заказчику
    # на всех них активно смотрим отчеты по уязвимостям и устраняем их) [Kulakov Daniil]
    - if: '$UPSTREAM_BRANCH =~ /^(develop|dev-[^ ]+|release-[^ ]+)/ && $UPSTREAM_PROJECT_ROOT_NAMESPACE == "areopad"'
      when: always
```

```
# Generate sast.yml pipeline
if [[ -n "${APPSEC_ANALYZERS_SAST}" ]]; then
  echo Variable APPSEC_ANALYZERS_SAST found, generating sast pipeline with ${APPSEC_ANALYZERS_SAST} scanners...
  jinja2 sast/sast.yml.j2 -D tools="${APPSEC_ANALYZERS_SAST}" > sast/sast.yml
else
  echo Variable APPSEC_ANALYZERS_SAST not found, creating dummy sast/sast.yml...
  cat > sast/sast.yml <<'YAML'

stages: [noop]
noop:
  stage: noop
  tags:
    - appsec-runner-cib
  image: bash:5.0.18-alpine3.22
  script:
    - echo "Variable APPSEC_ANALYZERS_SAST not found"

YAML
fi
```

```
----- Vulnerability: 691 -----
[1] Наименование: Usage of weak hashing library (MDx).
[2] Категория CWE: null
[3] Критичность: high
[4] Оценка CVSS: 0
[5] Описание:
## Description
Using a weak hashing library, such as MD5, increases the risk of data breaches. MD5 itself is vulnerable to collision
uce the same hash value, compromising data integrity and security.
## Remediations
- **Do not** use MD5 for hashing. This algorithm is considered weak and vulnerable to attacks.
  ```php
 $encrypted = md5($input); // unsafe
  ```
- **Do** opt for stronger hashing algorithms like SHA-256 to enhance security.
  ```php
 $encrypted = hash('sha256', $input);
  ```
[6] Файл: vulnerabilities/captcha/source/high.php
[7] Строка: 27
[8] Хеш: 0a96aa7578442c0517cce3de2ec077e8075309d95f501f046e1cdf1bfde7f23d
[9] Идентификатор: 691
----- End: 691 -----
```

active_findings.csv 7.45 KiB

| ID | Title | Severity | Description | Scanner name | Scanner type | Status |
|-------|---|----------|--|--------------|--------------|-----------|
| 28076 | SQL Server is a relational database management system | info | SQL Server is a relational database management system developed by Microsoft. SQL Server credentials can be used to access and manage databases. | trufflehog | secrets | recurrent |

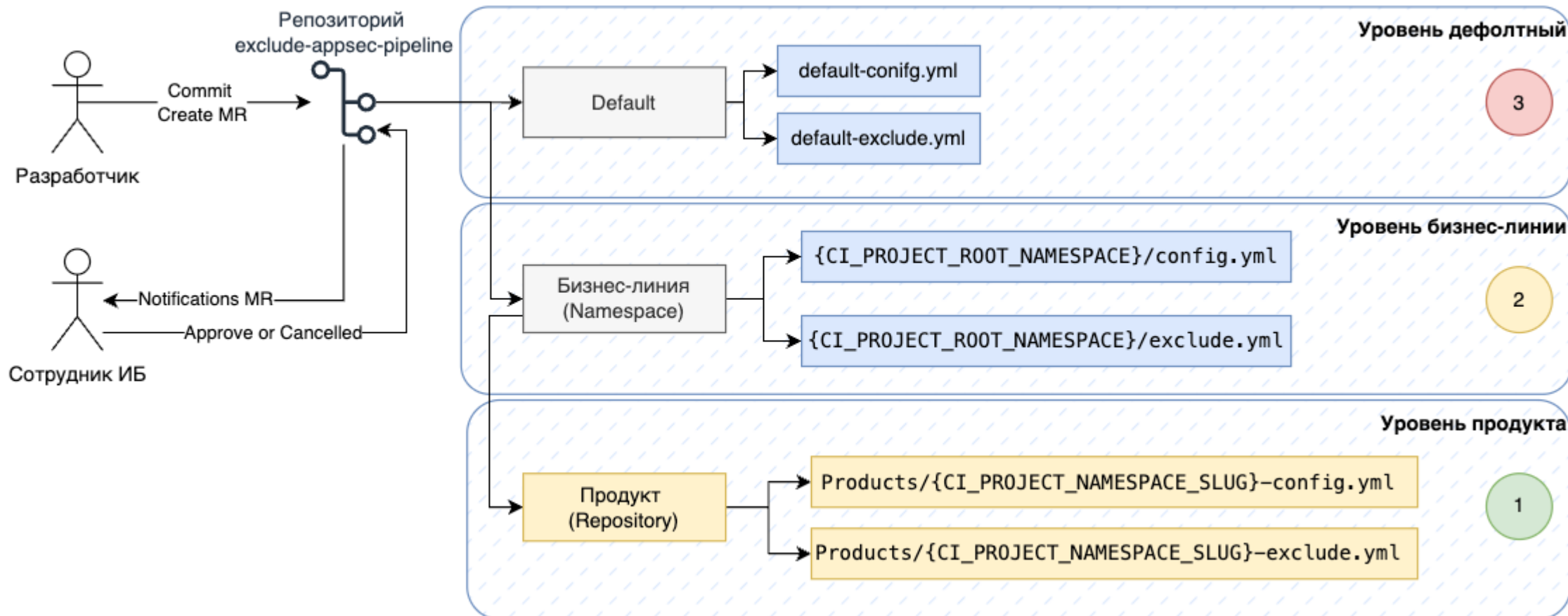
УЯЗВИМОСТИ В КОДЕ!



Findings

| Критичность | Значение | Ограничение |
|-------------|----------|-------------|
| critical | 0 | 10 |
| high | 175 | 20 |
| medium | 30 | 50 |
| low | 9 | 100 |
| info | 3 | 200 |
| Bcero | 217 | 100 |
| risk_score | 8.81106 | 500 |

ЕДИНЫЙ APPSEC-EXCLUDE



1) Пример стандартных исключений

```
3  exclusions:
20  - type: file_path
21    pattern: "**/wwwroot/lib/**/*.*js"
22    reason: "Legacy library are excluded from security scans"
23  - type: file_path
24    pattern: "**/wwwroot/app/**/cadesplugin_api.js"
25    reason: "CryptoPro library are excluded from security scans"
```

2) Пример объединённых исключений

```
- type: "compound"
  logic: "AND"
  conditions:
    - type: "file_path"
      pattern: "**/wwwroot/app/controllers/UI-secretary/question/*Question.js" #createEditQuestion.js, editQuestion.js
    - type: "rule_id"
      pattern: "javascript_lang_observable_timing"
  reason: "False-positive Observable Timing Discrepancy vulnerability, when on fact comparison is between enum and number, but enum is called Secret"
```

Пример настроек Security-Gate

```
# Настройки для Security Gate
security_gate:
  severity_counts: # Ограничения по количеству уязвимостей по уровням критичности
    max_critical: 0
    max_high: 20
    max_medium: 100
    max_low: 500
    max_info: 1000
  max_findings: 1700 # Максимальное общее количество уязвимостей
  max_risk_score: 8.0 # Максимальный риск-скор
```

```
asoc_config:
  # Настройки для создания issues
  issues:
    issue_enabled: false # Включение или отключение создание issues в gitlab issues
    severity_threshold: "critical" # Порог критичности для создания issues
    allowed_labels:
      - vulnerability
      - asoc
    allowed_scanners: # Список разрешённых сканеров
      - semgrep oss
      - bearer
      - checkov
    allowed_tool_types: # Список разрешённых типов инструментов
      - sast
      - sca
      - iac
```

Пример настроек для создания Issues

Примеры создания Issues

[iac] Ensure that arrays have a maximum number of items.

Open Issue created 2 months ago by devsecops devsecops

Title: Ensure that arrays have a maximum number of items.

Description: Ensure that arrays have a maximum number of items Resource: paths

File: app/src/test/resources/scheme.json

Line Number: 161

Severity: high

CVSS: 0.0

CVE:

Scanner Name: checkov

Scanner Type: iac

Code Snippet:

```
"schema": {
  "type": "array",
  "items": {
    "type": "string",
    "enum": [
      "ADMIN",
      "USER",
      "DESIGNER",
      "COORDINATOR",
      "MANAGER",
      "AUDITOR"
    ]
  }
}
```

CWE: None

[sast] Unsanitized external input in SQL query.

Open Issue created 2 months ago by devsecops devsecops

Title: Unsanitized external input in SQL query.

Description: ## Description

Using unsanitized data, such as user input or request data, or externally influenced data passed to a function, in SQL query exposes your application to SQL injection attacks.

Remediations

- Do not concatenate external input directly into SQL queries. This practice can lead to SQL injection vulnerabilities.

```
String query = "update user set name='"+uri.getQueryParameter("name")+"' where id='"+uri.getQueryParameter("userId")+"'";
return jdbcTemplate.update(query);
```

- Do use `PreparedStatement` with parameterized SQL queries to safely include external input. This method ensures that input is treated as data, not executable code.

```
new PreparedStatementCreator() {
    public PreparedStatement createPreparedStatement(Connection conn) throws SQLException {
        String updateString = "update user set name = ? where id = ?";
        return conn.prepareStatement(updateString);
    }
}

new PreparedStatementSetter() {
    public void setValues(PreparedStatement preparedStatement) throws SQLException {
        preparedStatement.setString(1, uri.getQueryParameter("name"));
        preparedStatement.setInt(2, uri.getQueryParameter("userId"));
    }
}
```

References

- JDBC Template class
- OWASP SQL injection explained
- OWASP SQL injection prevention cheat sheet

File: services-access-rights/src/main/java/com/digdes/idmfenix/rights/service/impl/AccessGroupImportServiceImpl.java

Line Number: 275

ЧТО С МЕТРИКАМИ?

DIGITAL
DESIGN



ЧТО С МЕТРИКАМИ ПО БЛ?

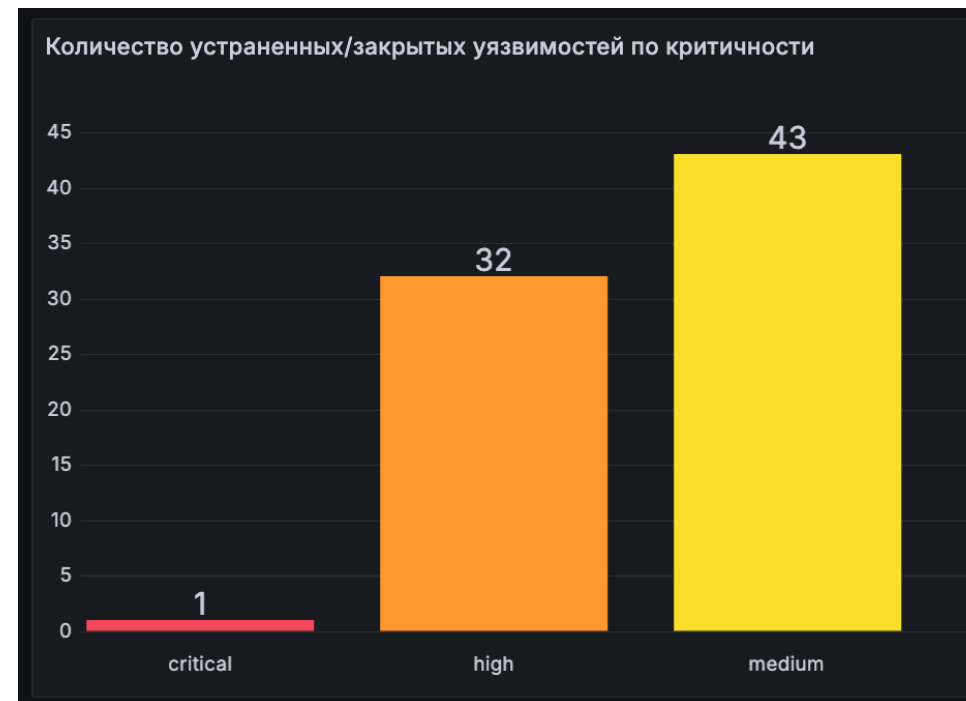
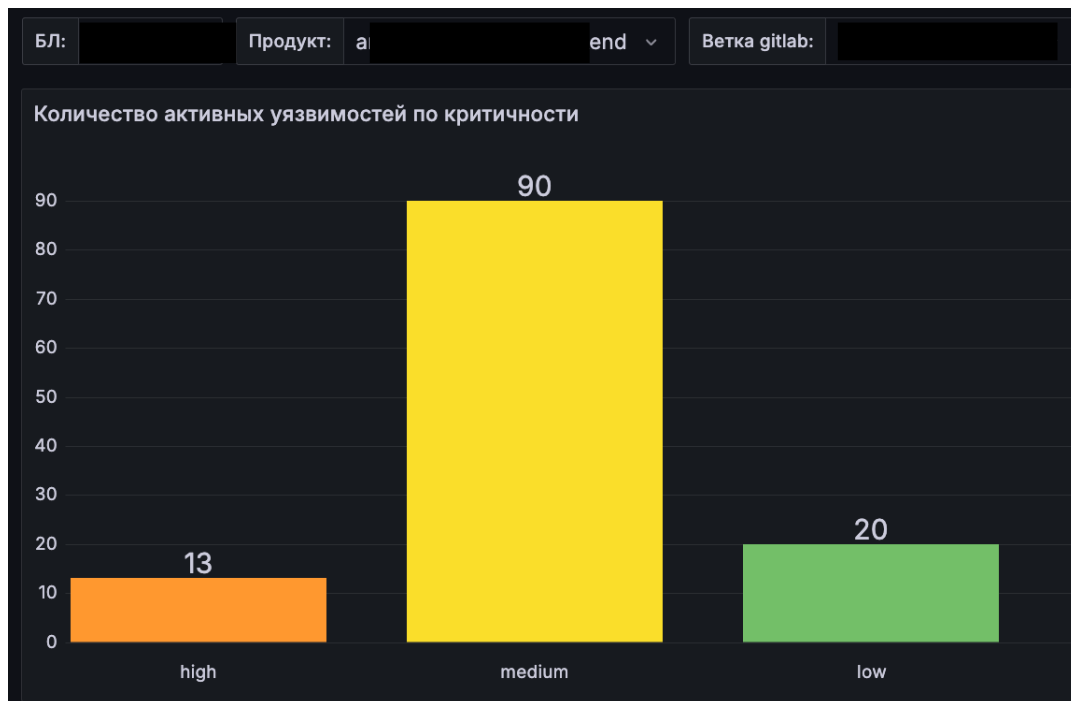


| Product name | Risk score |
|-------------------------------------|------------|
| [REDACTED] ut | 1.13 |
| [REDACTED] | 5.59 |
| [REDACTED] unicon
versionservice | 1 |
| [REDACTED] digde | 1.13 |

| Список активных уязвимостей | | | | | | | | |
|-----------------------------|--|----------|--------|--------------|-----------------|------|---------|--------------|
| Title | Description | Severity | Status | Product name | File path | Line | Branch | Scanner type |
| Using Unnamed Build Stages. | This query is used to ensure that build stages are named. This way even if the Dockerfile is re-ordered, the COPY instruction doesn't break. | low | new | [REDACTED] | [REDACTED] kerf | 16 | develop | iac |

ЧТО С МЕТРИКАМИ ПО ПРОДУКТУ?

DIGITAL
DESIGN



| | | |
|--|------------------------------------|------------|
| Количество исправленных/закрытых уязвимостей | Количество исключенных уязвимостей | Risk score |
| 97 | 515 | 5.25 |

ЧТО ПЛАНИРУЕМ ДАЛЬШЕ?

DIGITAL
DESIGN





DIGITAL
DESIGN

ПРОДОЛЖИМ СОТРУДНИЧЕСТВО?

Для получения консультации, дополнительных
материалов, запроса демонстрации

Санкт-Петербург
Наб. реки Смоленки, дом 33
+7 (812) 346 58 33

Москва
Одесская ул., дом 2, корпус С
+7 (499) 788 74 94

digdes.ru

info@digdes.com