ON FF ONE 2022

# Актуальные проблемы финансовой безопасности

Морозов Алексей

Руководитель AppSec BP

Москва, 26.08.2022

# Кто я такой?

OFF ONE 2022

Руководитель Appsec BP

- OSCP, OSWE, CEH, eWAPTx
- 6+ опыта работы
- 2 – х кратный победитель PHDays Standoff в составе команды Codeby
- Автор научных статей и CVE
- Выступал на многих конференциях: PHDays, ZeroNight, OFFZone, RuCTF, VolgaCTF

# С чего начать AppSec?

# С чего начать AppSec?

Инвентаризация активов

# С чего начать AppSec?

Оценка текущей зрелости:

BSIMM, OWASP SAMM

Инвентаризация активов

# С чего начать AppSec?

OFF ONE 2022

Оценка текущей зрелости:
BSIMM, OWASP SAMM

Внедрение политик
и регламентов

Инвентаризация активов

# С чего начать AppSec?

Оценка текущей зрелости:
BSIMM, OWASP SAMM

Внедрение политик
и регламентов

Инвентаризация активов

Внедрение
Контролей безопасности

OFF ONE 2022

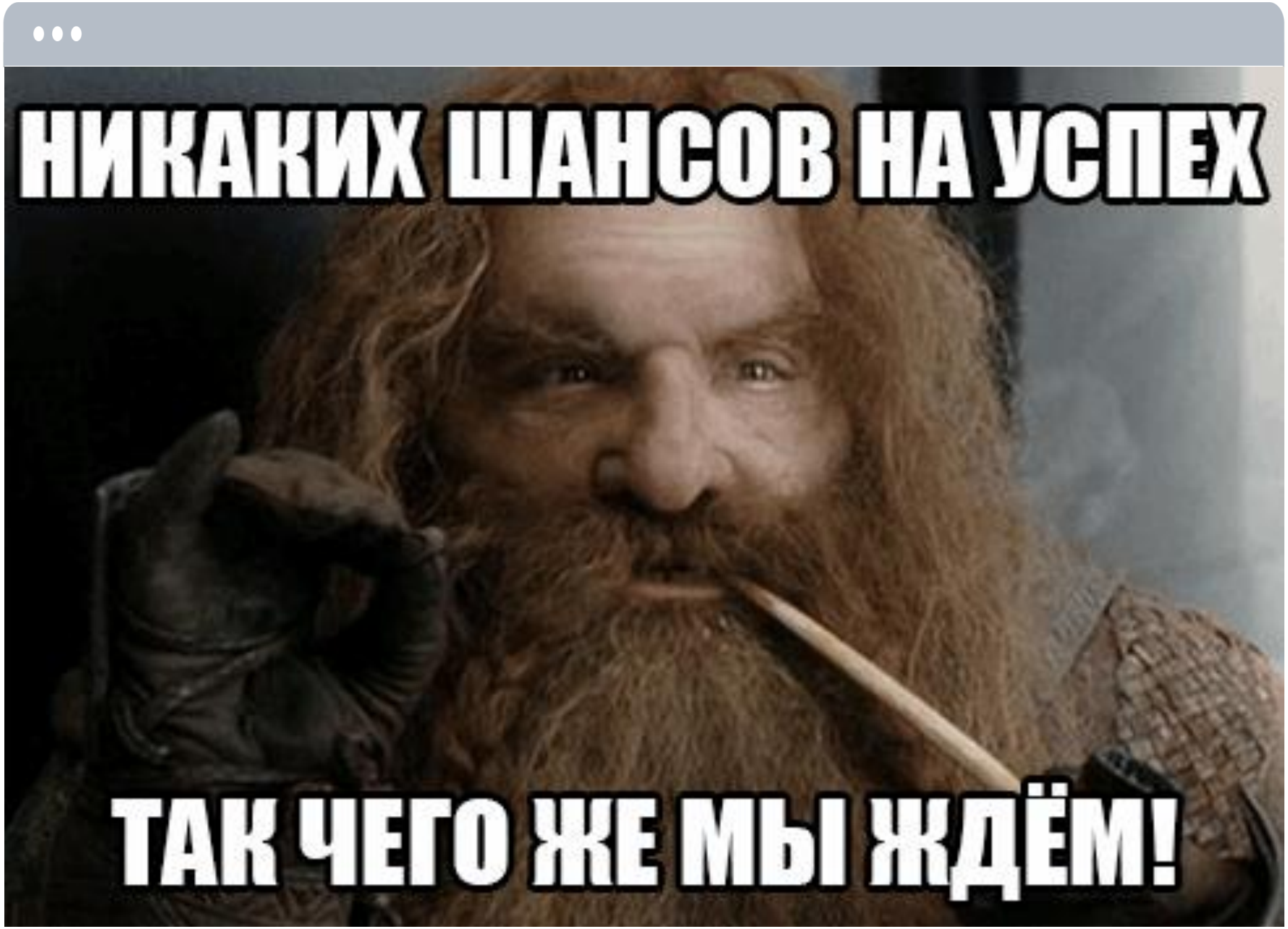
# Загнать пентестеров ⚡

# История развития AppSec

1. 2 человека ищут какие-то уязвимости
2. +1 человек на устранение уязвимостей, появление VM
3. Появление процессов сканирования
4. Появление DevSecOps
5. Появление AppSec BP
6. Появление Awareness
7. Появление Разработки

# Проблемы

- Уязвимости устранялись хаотично и долго
- Нет никакой приоритезации и инвентаризации
- Нет централизованного управления
- Низкая эффективность


НИКАКИХ ШАНСОВ НА УСПЕХ
ТАК ЧЕГО ЖЕ МЫ ЖДЁМ!

Управление уязвимостями

# VM

Create Issue

Configure Fields

Создание задачи* | Risk Scoring* | Роли | Планирование и время

| | |
|---|---|
| Motive* | 0 – No reward |
| Opportunity* | 0 – Full access or expensive resources required |
| Size* | 0 – System administrators |
| Ease of discovery* | 0 – Practically impossible |
| Ease of exploit* | 0 – Theoretical |
| User interaction* | 0 – Complex user interaction |
| Loss of confidentiality* | 0 – No data disclosed |
| Loss of integrity* | 0 – No corrupted data |
| Loss of availability* | 0 – Not affected availability |
| Financial damage* | 0 – No damage |
| Reputation damage* | 0 – No damage |
| Affected users* | 0 – One individual |

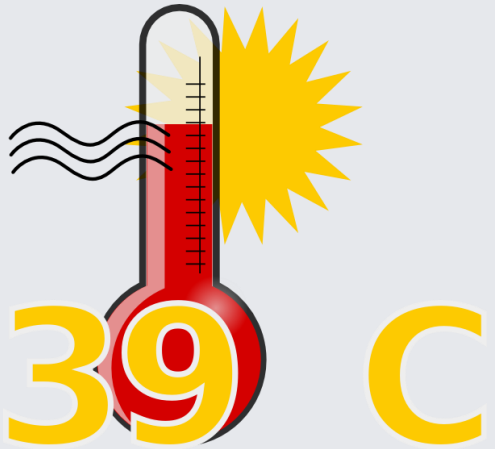
Create another | Create | Cancel

Управление уязвимостями

# VM

| Критичность | Решение |
| --- | --- |
| Blocker | CISO + CTO (3д.) |
| Critical | CISO + CTO (7д.) |
| Major | CISO + CTO (30д.) |
| Normal | CISO + CTO (90д.) |
| Minor | APPSEC (180д.) |
| Trivial | Product Owner |

# Чем померить?




- Количество уязвимостей по критичности
- Количество закрытых/открытых/просроченных
- Количество уязвимостей по источникам

# Безопасность кода

- Complince - CI
- Поиск секретов
- SAST - сканирование
- Обновление правил

# Checkmarx

- Интегрирован Checkmarx в BitBucket
- Немедленное оповещение в Push Request
- Создан механизм APPROVE
- Выделены ключевые проекты

# Проблемы


- Много ложных срабатываний
- Часто возникали ошибки
- Невозможно покрыть всю кодовую базу
- Блокер для разработки

appsec_robot commented on a file 25 Dec 2020

src / main / scala / ru / tcsbank / api / processing / handlers / remoteidentification / **EbsStartVerificationHandler.scala**

```
21 26       ebsClient.startVerificationUri(accessToken).map { uri =>
22    -       val cookie = Uri(uri).query.get("session_id") match {
   27 +       val maybeSession = sessionFrom(uri)
   28 +       val cookie = maybeSession match {
23 29            case Some(value) => Seq(Cookie("ebs_session_id", value, ebsCookieDomain, ebsCookieExpiration, httpOnly = true))
24 30            case None => Seq.empty
25 31          }
26    -       if (user.origin.like(Origin.mobile)) SuccessfulResponse(Uri(uri).query.get("session_id").map(EbsSessionId(_)))
27    -       else RedirectResponse(uri, StatusCodes.Found, cookie)
   32 +       if (user.origin.like(Origin.mobile)) SuccessfulResponse(maybeSession.map(EbsSessionId))
   33 +       else RedirectResponse(uri, Status.Found, cookie)
```

appsec_robot 25 Dec 2020

**SAST Issue**

Уязвимость: Find_OpenRedirects

Уровень риска: Low

# DevPlatform

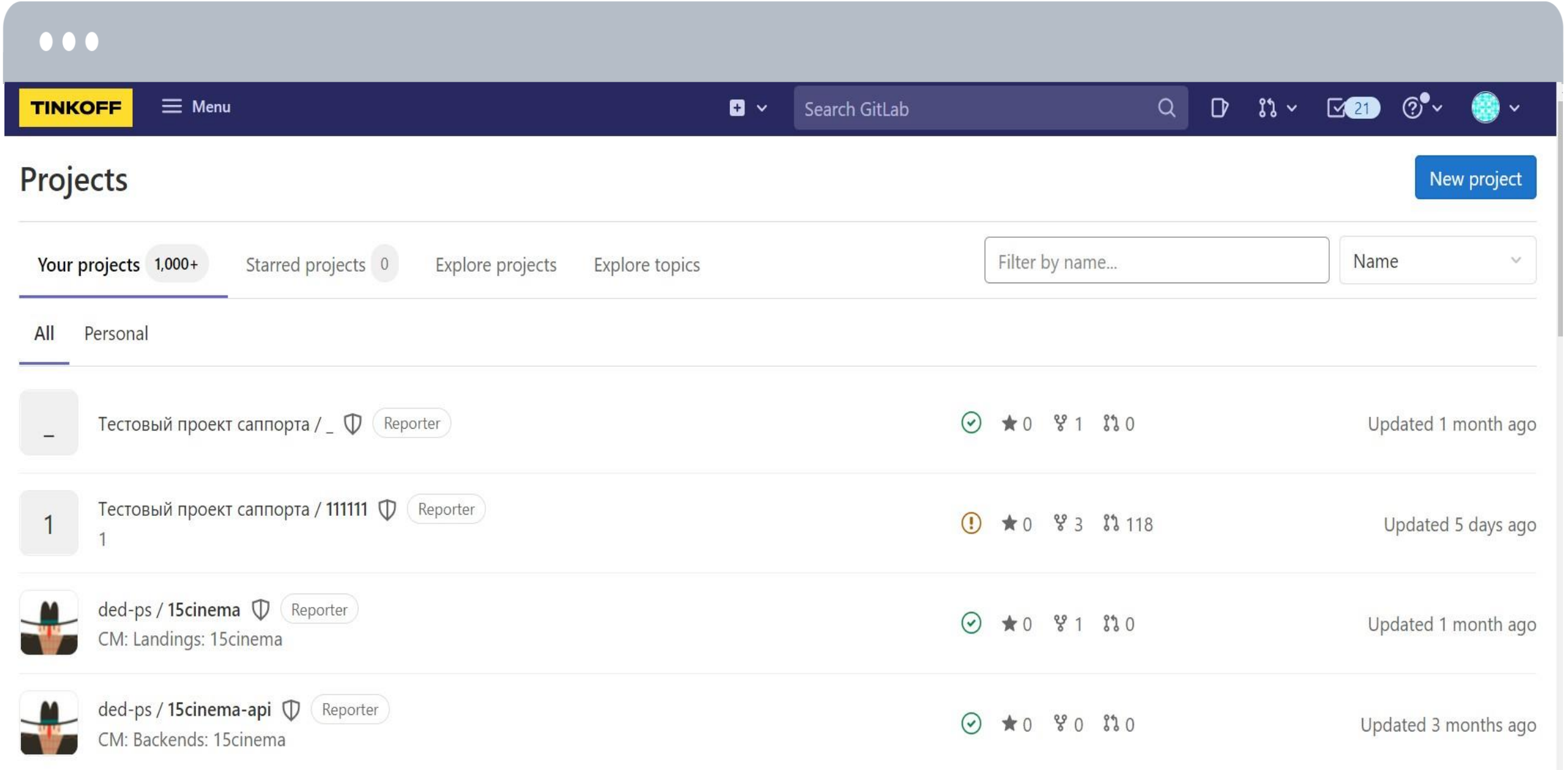
OFF ONE 2022

На **базе Git-Lab** построена платформа для разработки

Появление **Complince - CI**

Интеграция **SemGrep, GitLeaks**

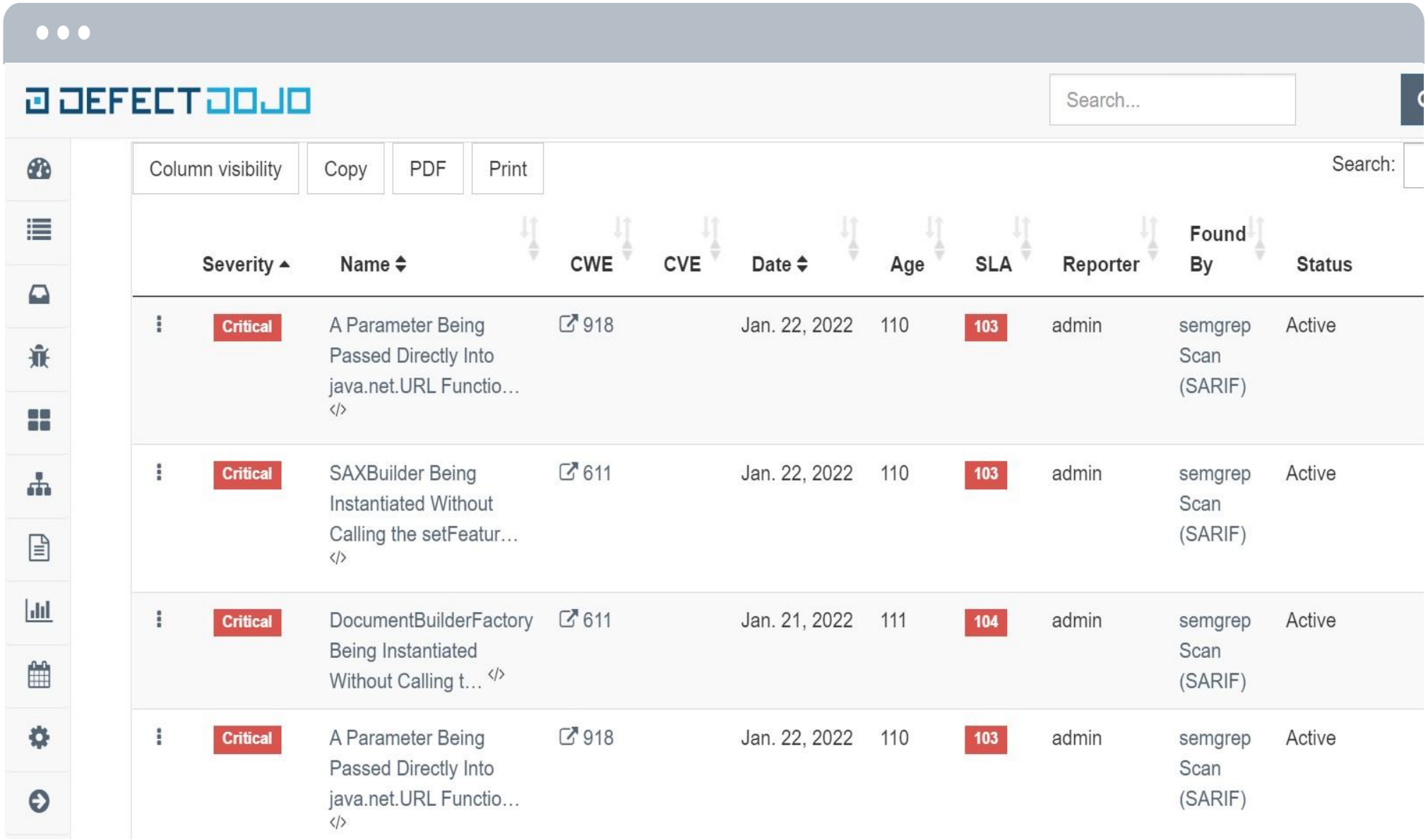
Настройка **профилей** по одной кнопке


TINKOFF
Menu
Search GitLab
21
Projects
New project
Your projects 1,000+
Starred projects 0
Explore projects
Explore topics
Filter by name...
Name
All
Personal
_
Тестовый проект саппорта / _
Reporter
0 1 0
Updated 1 month ago
1
Тестовый проект саппорта / 111111
Reporter
1
0 3 118
Updated 5 days ago
ded-ps / 15cinema
Reporter
CM: Landings: 15cinema
0 1 0
Updated 1 month ago
ded-ps / 15cinema-api
Reporter
CM: Backends: 15cinema
0 0 0
Updated 3 months ago

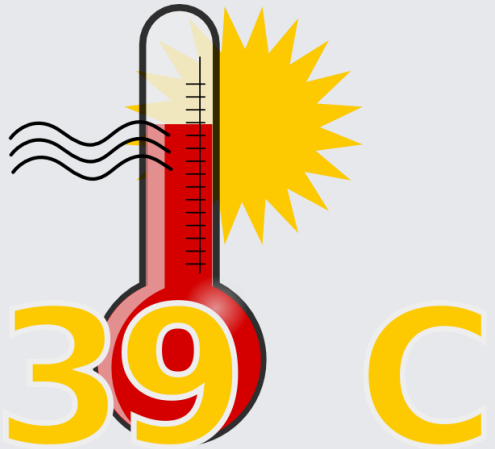
# Complince - CI

```
...
artifacts-upload:
  dependencies:
    - secret-detection-diff
    - sast-semgrep
  extends: .artifacts-upload
  rules:
    - if: $CI_PIPELINE_SOURCE == "parent_pipeline"
  stage: upload
include:
  - secret-detection-diff
  - artifacts-upload
  - metrics-push
  - semgrep
metric-compliance-ci-run:
  extends: .metrics-push
  rules:
    - if: $CI_PIPELINE_SOURCE == "parent_pipeline"
  script:
```

# Semgrep / Getleaks



# Чем померить?



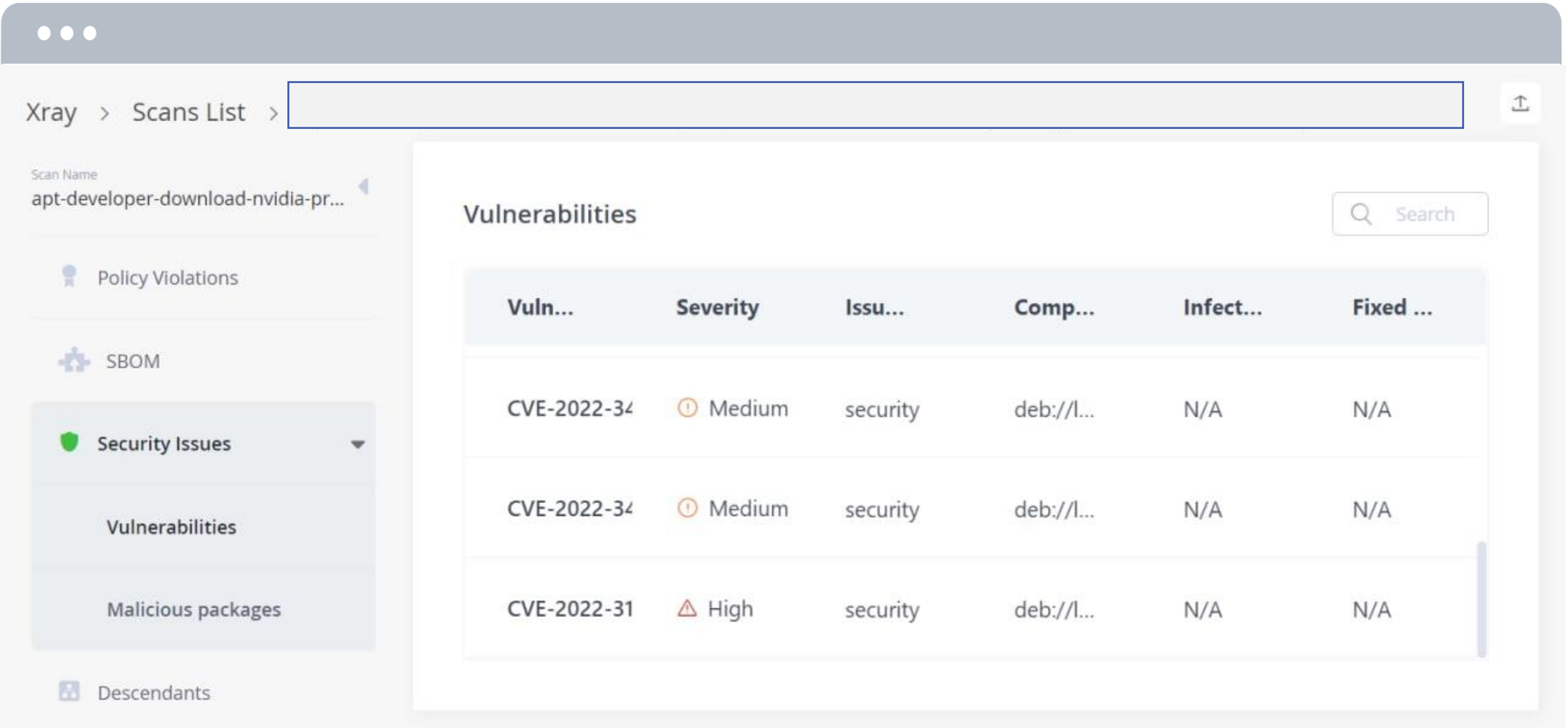

- Количество фолзов/уязвимостям
- Количество обработанных/необработанных
- Количество секретов


да кто такой этот
ваш artifactory

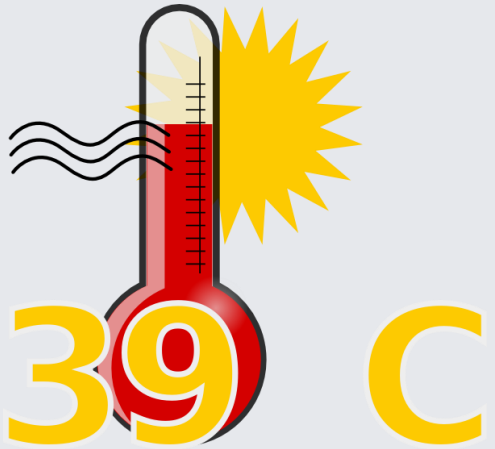
# Безопасность Артефактов

- Конфигурационный скан
- Композитный анализ (SCA)
- Политика базовых образов
- Политика блокировки внешних зависимостей

# SCA


Xray > Scans List >
Scan Name
apt-developer-download-nvidia-pr...
Policy Violations
SBOM
Security Issues
Vulnerabilities
Malicious packages
Descendants
Vulnerabilities
Search
Vuln...
Severity
Issu...
Comp...
Infect...
Fixed ...
CVE-2022-34
Medium
security
deb://l...
N/A
N/A
CVE-2022-34
Medium
security
deb://l...
N/A
N/A
CVE-2022-31
High
security
deb://l...
N/A
N/A

# Чем померить?




- Динамика проверенных уязвимостей
- Динамика выявленных в артефактах подтвержденных уязвимостей

# Базовые образа

- Сократить общее число базовых образов
- Правила создание базовых образов

  с зависимостями
- Требование Appsec к базовым образам и аудит
- Публикация и оповещение базовых образов

# Конфигурацио

# нный скан

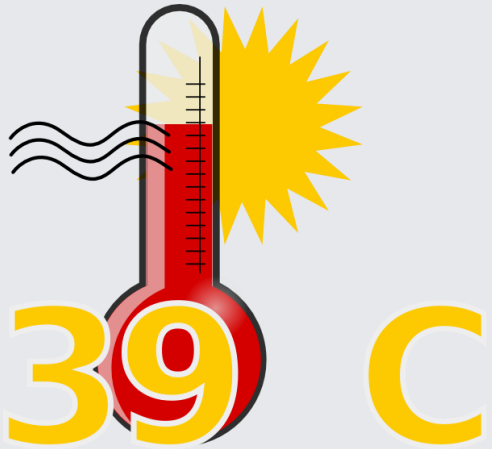
- Завести все Docker – образы и зависимости в Artifactory
- Добавить в Complince – CI сканирование конфигов (Kicks)


ДЕВЕЛОПЕР
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
МАРКЕТИНГОВАЯ ЭФФЕКТИВНОСТЬ

# Обучение

- Организация **внешних** тренингов
- Еженедельные **Digest**
- Проведение конкурсов (**Month of Bugs, CTF**)
- Организация **внутренних** лекций

# Чем померить?




- Количество **обученных**
- Количество **непрошедших** курс
- Количество **уязвимостей** по линиям от **MoB**
- Количество сотрудников **принявших** участие
- Другое


ГОВОРИШЬ МАЛЕНЬКАЯ
ДЫРА В БЕЗОПАСНОСТИ

# Оценка безопасности


- Внутреннее/Внешнее багбаунти
- Внутреннее/Внешнее тестирование
- Контроль публикаций
- Тестирование сценариев SOC

# Внутреннее

- Сотрудники получают T-Money
- Работает круглый год
- Мотивирует приносить уязвимости

# Внешнее

- Сначала в привате
- Потом в паблике
- **Скоро АНОНС**

OFF ONE 2022

# BugBounty vs RedTeam

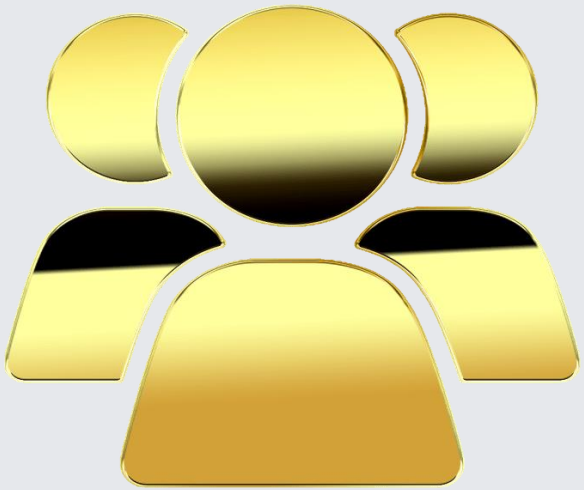
# Внутреннее

- Больше находок
- Более глубокое погружение
- Быстрое реагирование
- Поддержка полного флоу жизни уязвимости

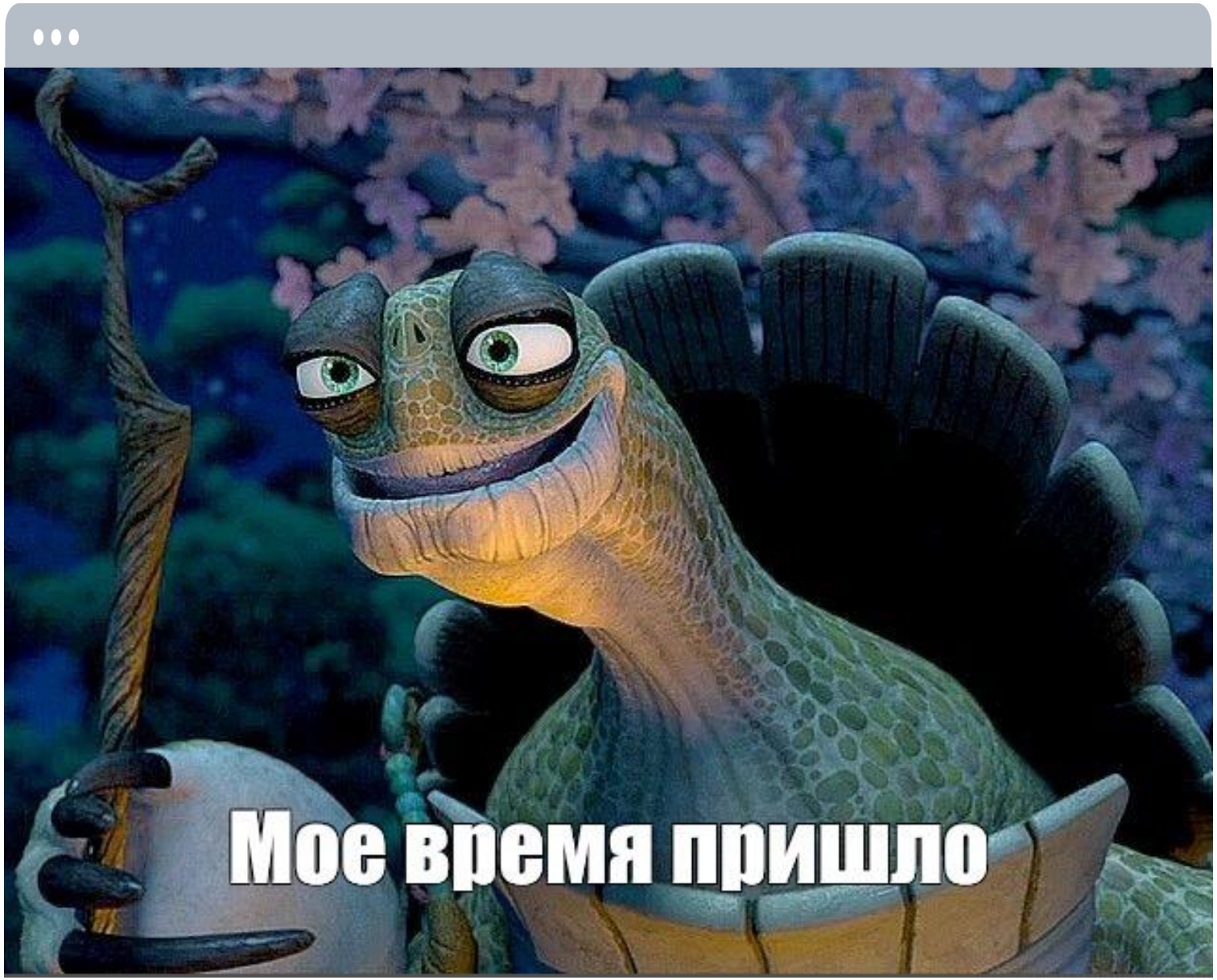
# Внешнее

- Покрывает большой скоуп
- Модель внешнего злоумышленника
- ✗ Приносит меньше уязвимостей
- ✗ Долгая вовлеченность

# Контроль публикаций



- Все **публикации** заносятся в одно место (репозиторий в виде **yaml-конфига**)
- Автоматизированная система **проверяет публикацию** и **ставит задачу** на ручную проверку **требованиям**
- Обязательный **апрув** от безопасности
- Автоматическое разворачивание

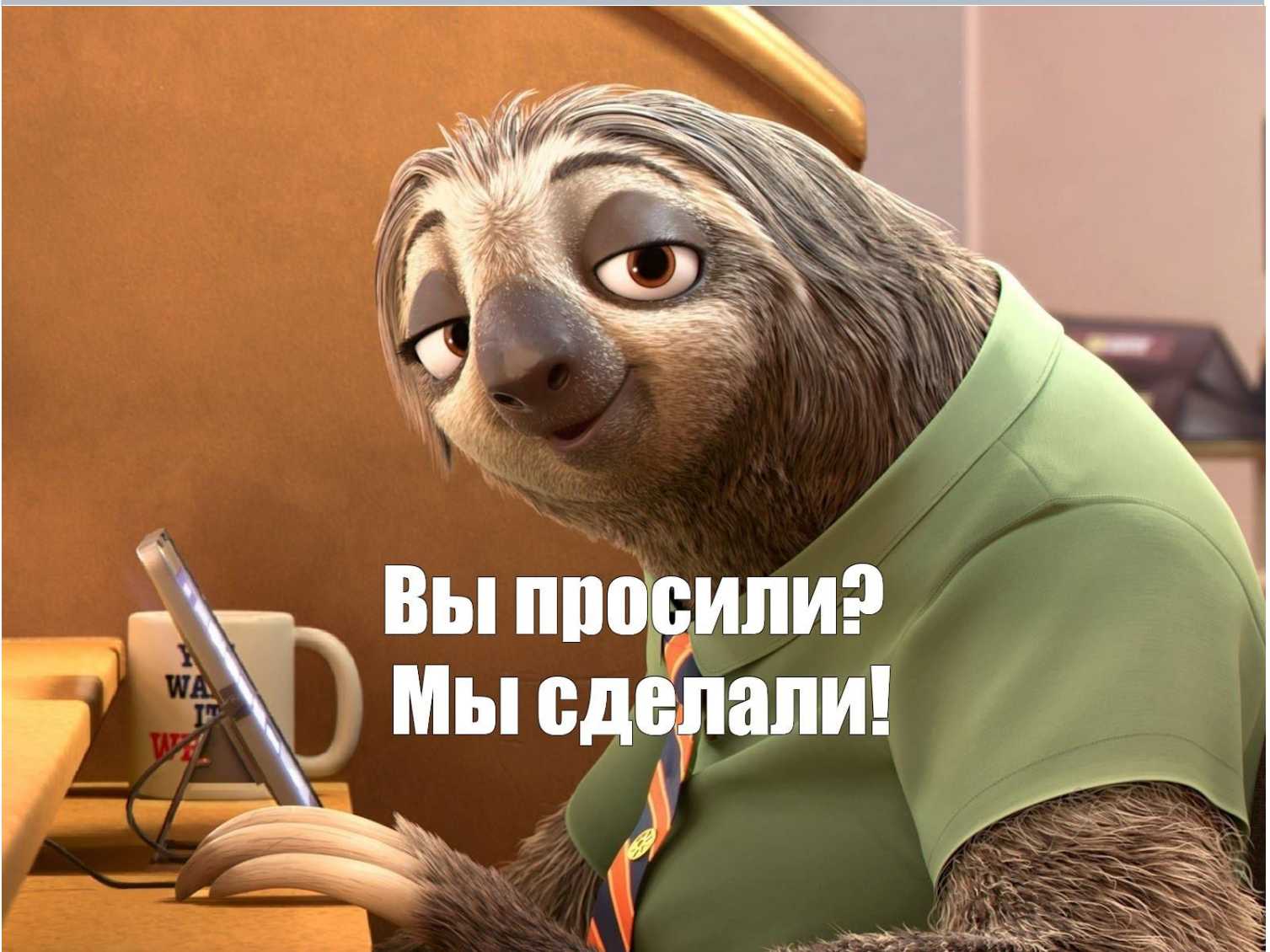

Мое время пришло

# AppSec BP

- Глубокая интеграция в бизнес
- Поддержка и внедрение процессов AppSec в бизнес
- Создание AppSec FrameWork
- Контроль релизов

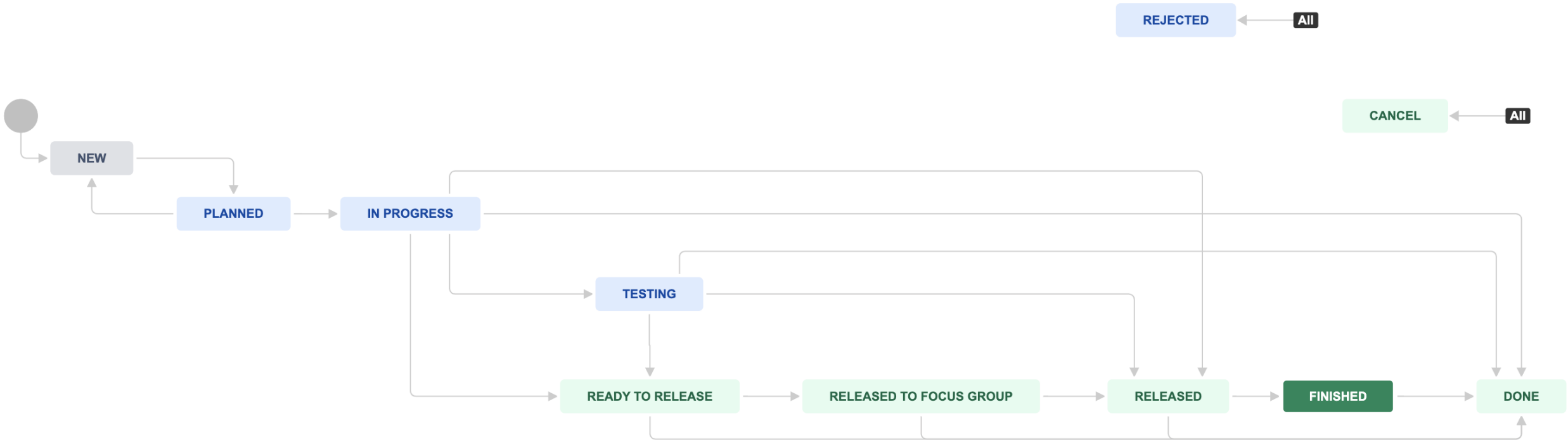
# Процессы

- **Подключение** линий и **создание метрик** к общим **процессам** банка
- **Архитектурное** и **бизнес** планирование
- **Релизная** политика
- Устранение **уязвимостей** и обслуживание **систем** автоматического **сканирования**
- Создание **Defensive Framework**


Вы просили?
Мы сделали!

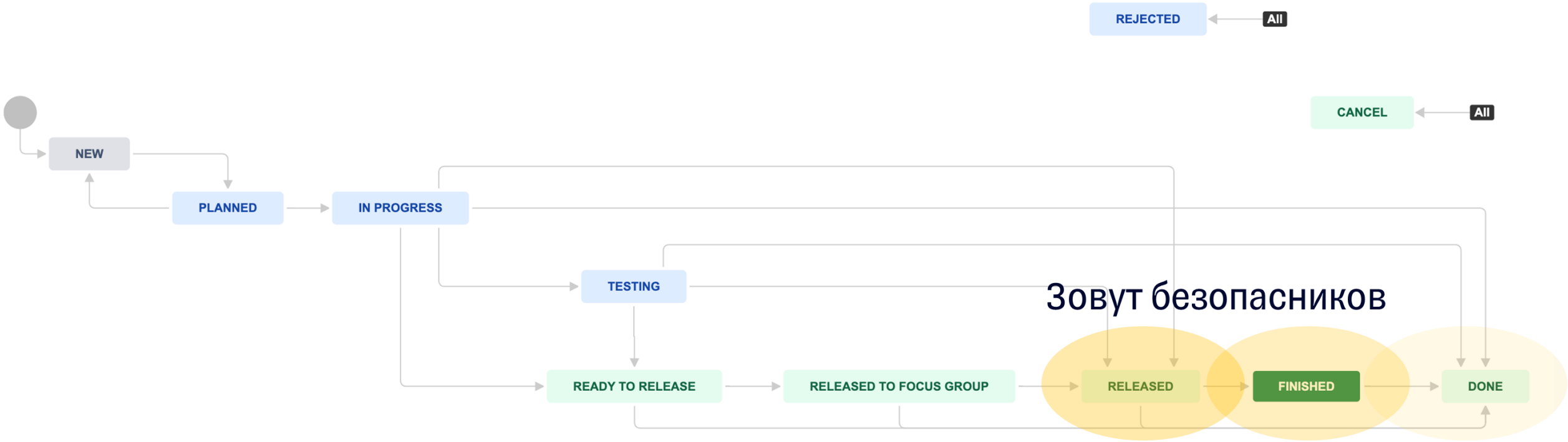
# Релизная политика

Это процесс появления безопасности на ранних этапах выполнения проекта или задачи.



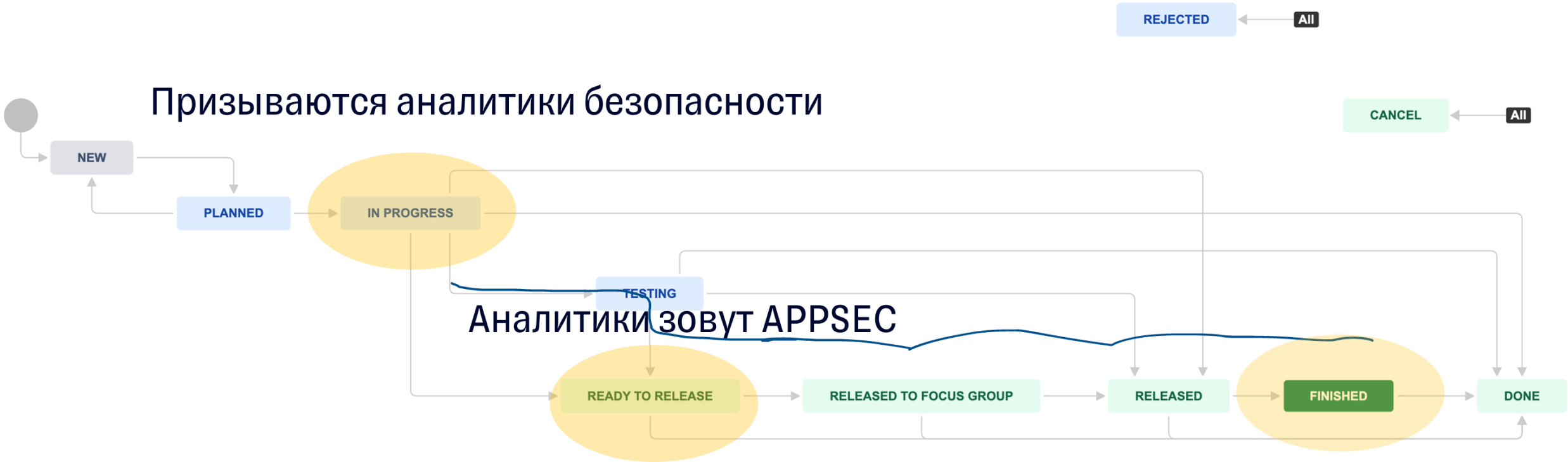
# Релизная политика

Это процесс появления безопасности на ранних этапах выполнения проекта или задачи.



# Релизная политика

Это процесс появления безопасности на ранних этапах выполнения проекта или задачи.



Security Analytics / ASEC-277

# TWork проверка безопасности IAPI-9883

Edit | Add comment | Assign | More | Trashed | Todo | Cancel

## Details

| | | | |
|---|---|---|---|
| Type: | Task | Status: | NEW (View Workflow) |
| Component/s: | None | Resolution: | Unresolved |
| Labels: | None | | |

## Description

TWork проверка безопасности IAPI-9883

## Attachments

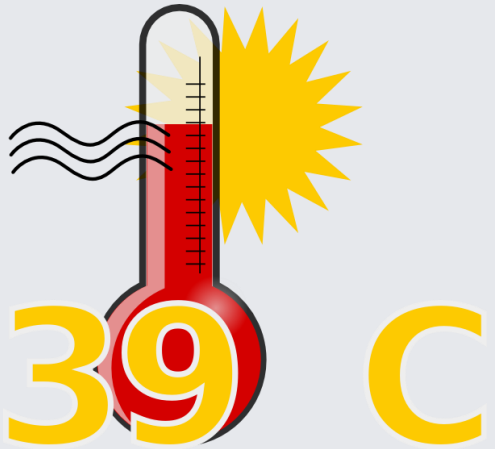
Drop files to attach, or browse.

## Issue Links

# Зачем?

- Соответствие общепринятому **уровню безопасности** в компании
- **Снижение стоимости** разработки через **оптимизацию** работы с командой безопасности
- **Абстрагироваться** от знания **контактов** безопасности и форм аудита
- Избавиться от **человеческого фактора** «надо потом как – нибудь позвать»

# Чем померить?




- Количество **обработанных задач**
- Общее количество тикетов
- Процент покрытия
- Скорость обработки в неделю

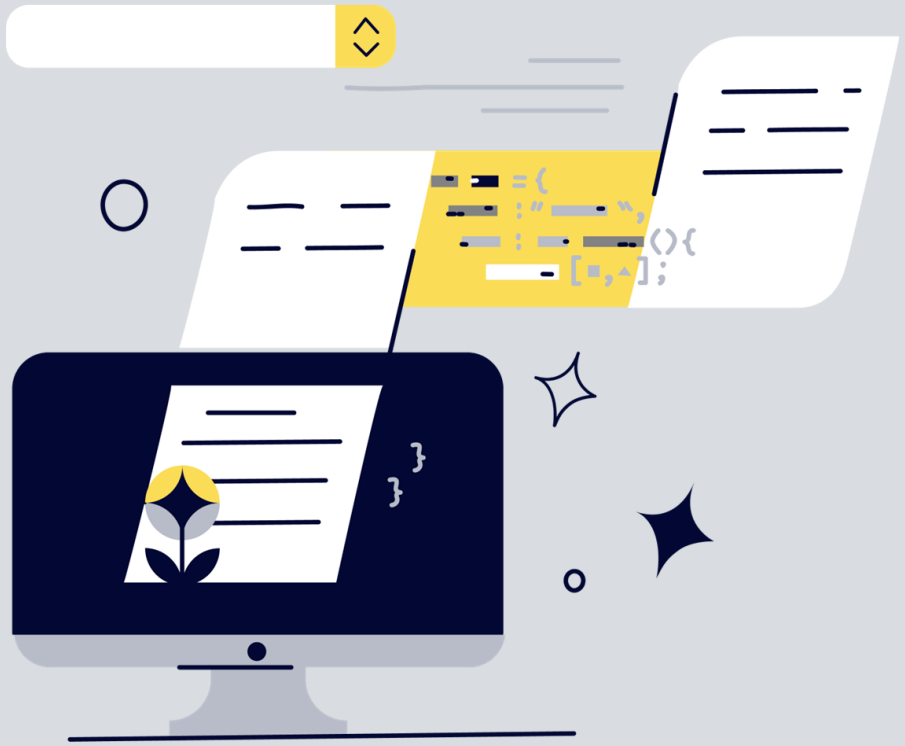
# Development

Создание системы внешнего сканирования

Внедрение системы контроля публикаций

Развитие DevPlatform

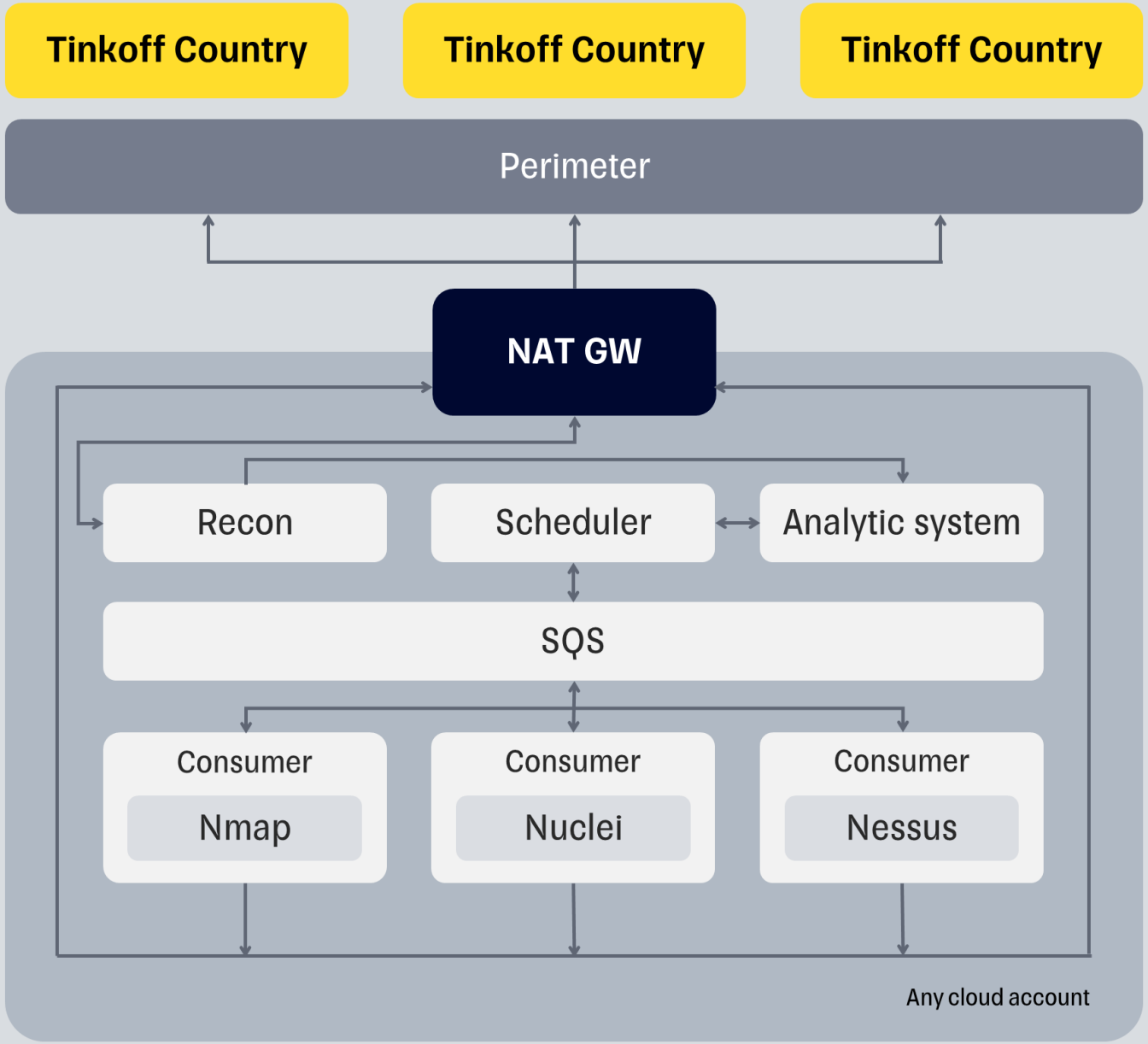
Развитие систем сканирования библиотек



# Scan

- Регулярный сбор доменов, IP адресов
- Сканирование средствами Nmap, Nuclei
- Масштабируемость и поддержка Docker
- Система очередей, многопоточность

# Scan




**Local Team:**

1. triage and fix vulnerabilities

- Detect new ip, fqdns
- Detect open ports
- Continuously detect vulnerabilities
- Detect illegal publications

**Global Team:**

1. write detection rules
2. support system

# Scan

## Grasper

Смотрит в yaml-конфиги, в которых описание путей до днсов, затем обходит все ресурсы и собирает хосты/порты/доменты  и загружает в Faradey

## Invoker

Вытаскивает из Faradey хосты/домены/порты, создаёт задачи на сканирование и пихает их в очередь, которую слушает scandozer

# Scan

## Scandozer

Получает задачи, вызывает nmap/ nuclei, получает данные об уязвимостях и добавляет в результирующую очередь, которую слушает invoker

## Invoker

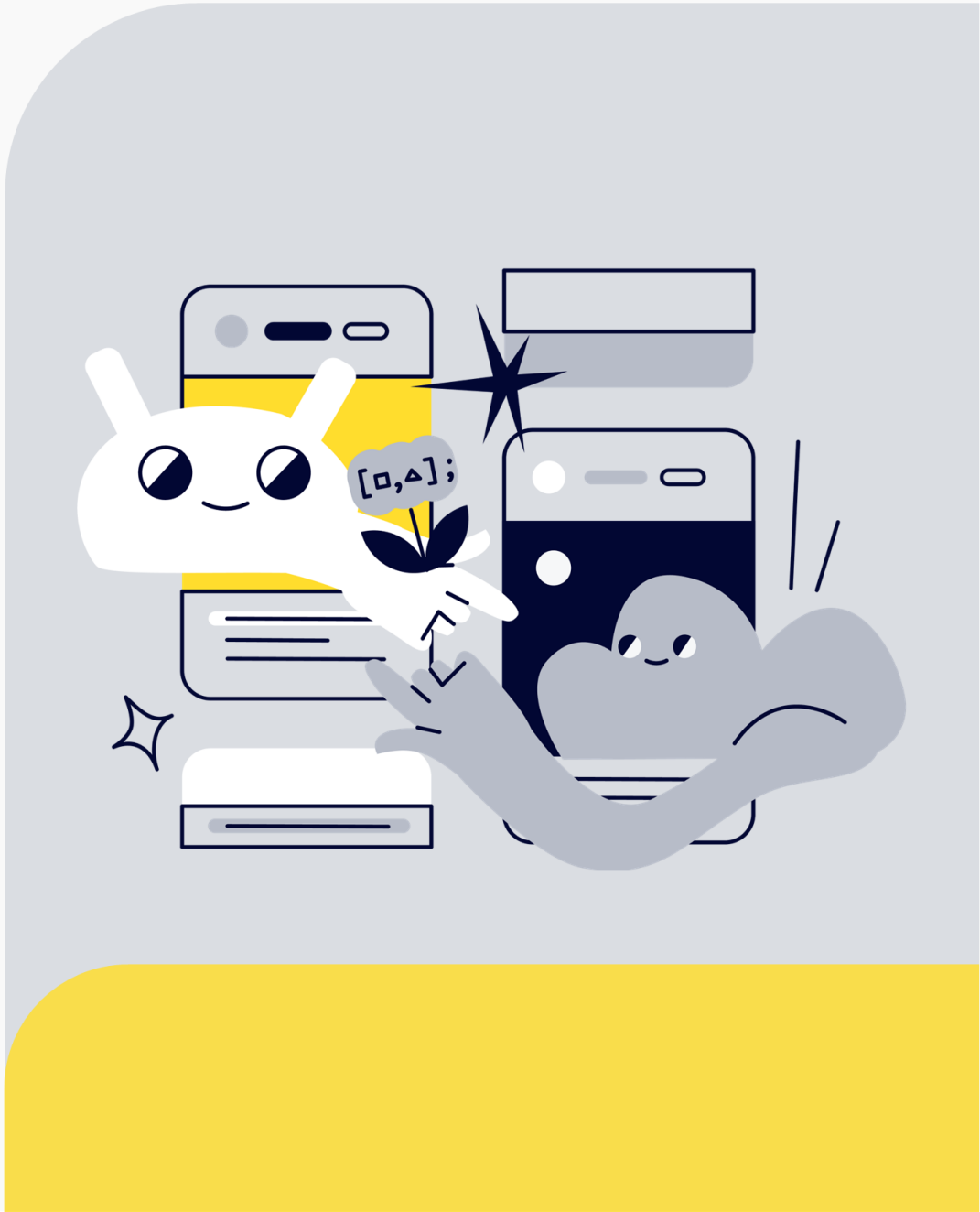
Получает данные об уязвимостях и обогащает ими то, что лежит в Faraday

# Log4Shell


- Поиск всех зависимостей по Artifactory
- Внедрение X-RAY
- Поиск по Run-Time и файловой системы
- Блокировка на уровне WAF и LB

# Недавние события

- Удаление публикаций с периметра
- Импортозамещение средств безопасности Усиление мер контролей
- Замещение BugBounty



# Оргструктура

Appsec (21 чел)

- Offensive
- AppSec BP
- DevSecOps
- Development
- Awareness
- Architecture

# Помните

- Безопасность - это процесс, а не цель
- Учимся на чужих ошибках
- Хороший AppSec – гибкий AppSec
- Trend is your friend

# Спасибо за внимание!

Будьте в безопасности!


al.d.morozov@tinkoff.ru

@SooLFaa