tech

Как вовлечь разработчиков в фикс уязвимостей.

Рецепт от СберМаркета

tech

“Я триажу по **100** фолсов в день.
И чувствую себя прекрасно”

Кашапов Нияз
AppSec Lead @ Сбермаркет

@niaz.kashapov
niyaz.kashapov@sbermarket.ru

tech

С чего начинается день AppSec?..

...с кофе и триажа файндингов

tech

Надо успеть еще...

Отревьювить архитектуру решений

Проконсультировать команды по вопросам

Нарисовать модель угроз для новых систем

Написать требования по безопасности

Провести аудит нового сервиса

Много чего другого!

Проверить фиксы уязвимостей

Мониторить новости об уязвимостях

Оттриажить bug-bounty

Пересерчить новые практики

Написать статью/выступить на конфе...

tech

Хватит это терпеть!

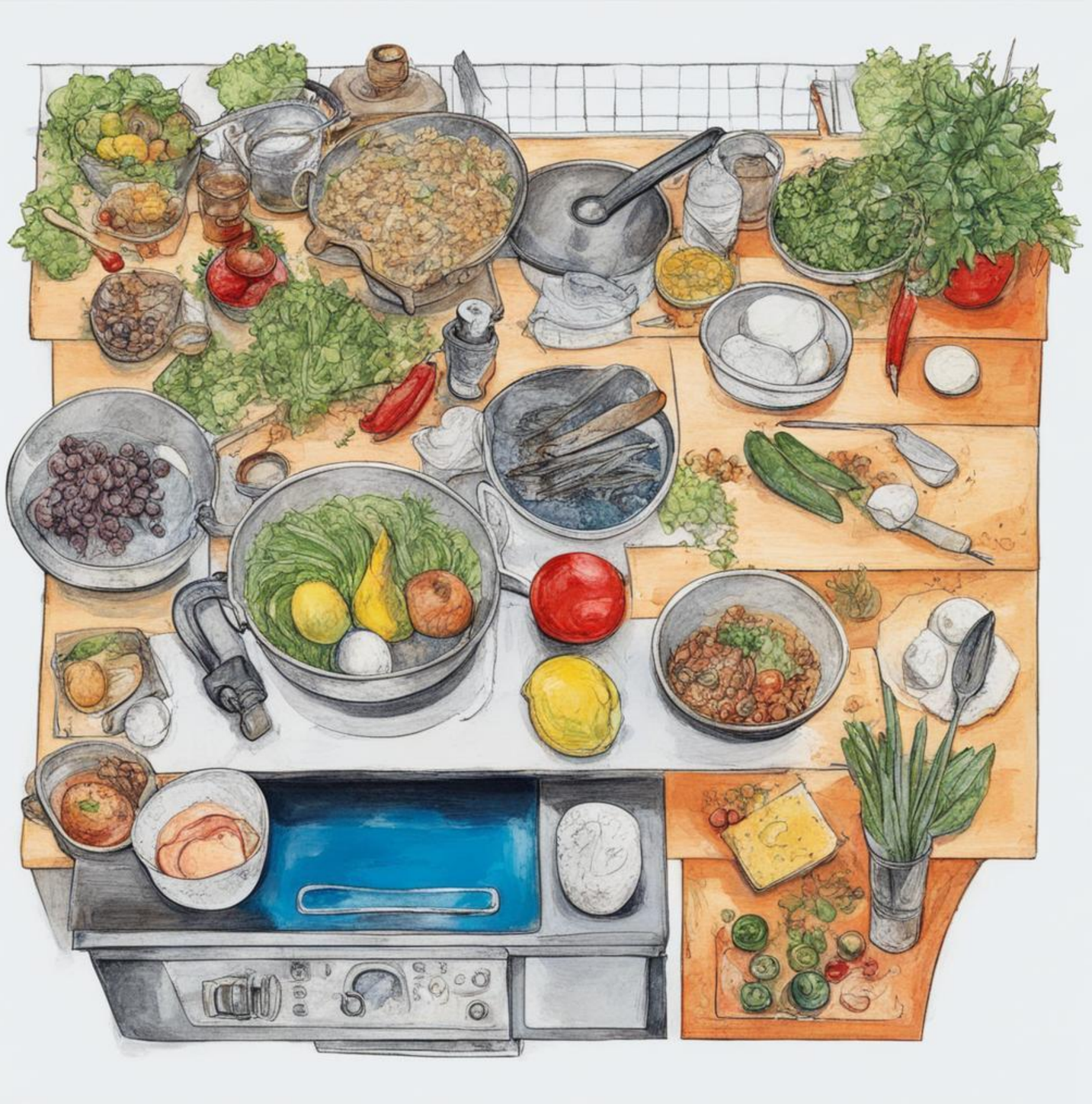
1) Огромное количество файндингов
2) Отсутствие бизнес-контекста
3) Сложный код
4) Игнорирующие команды разработки
5) Вечно растущий техдолг

Как мы доварились то такого?

Невкусный рецепт двухлетней давности

tech

Начинаем готовить!

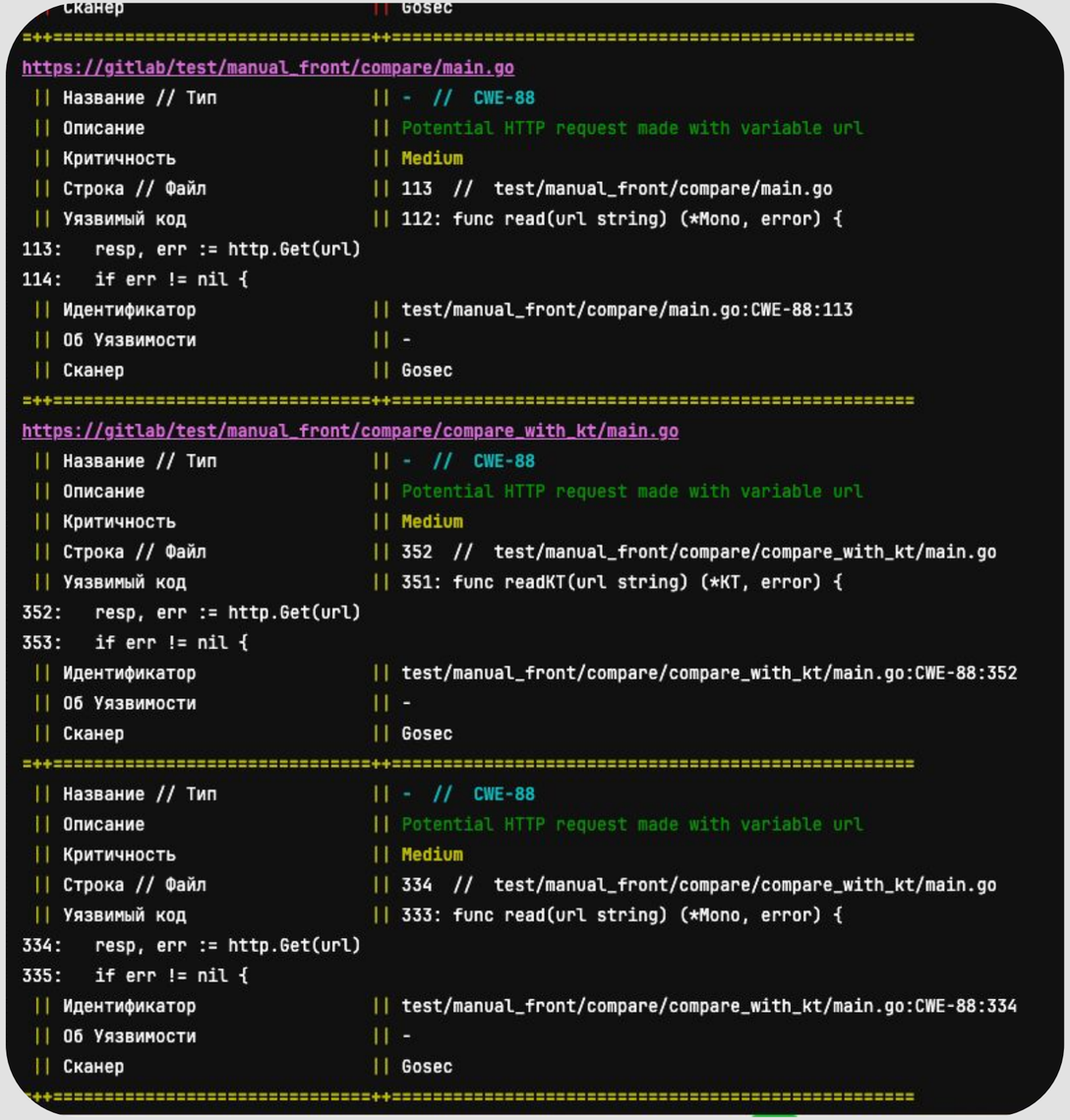


tech

Начинаем с *технического* мяса!

tech

Отказываемся от defect dojo в пользу... ничего!



tech

Плюсы в отказе от DefectDojo

Как для appsec, так и для Dev-команд

01

скорость получения результатов (непосредственно в пайплайне)

02

отсутствие дополнительного инструмента, работа в “едином” окне

03

нет необходимости управлять учетными записями (доступ по-умолчанию)

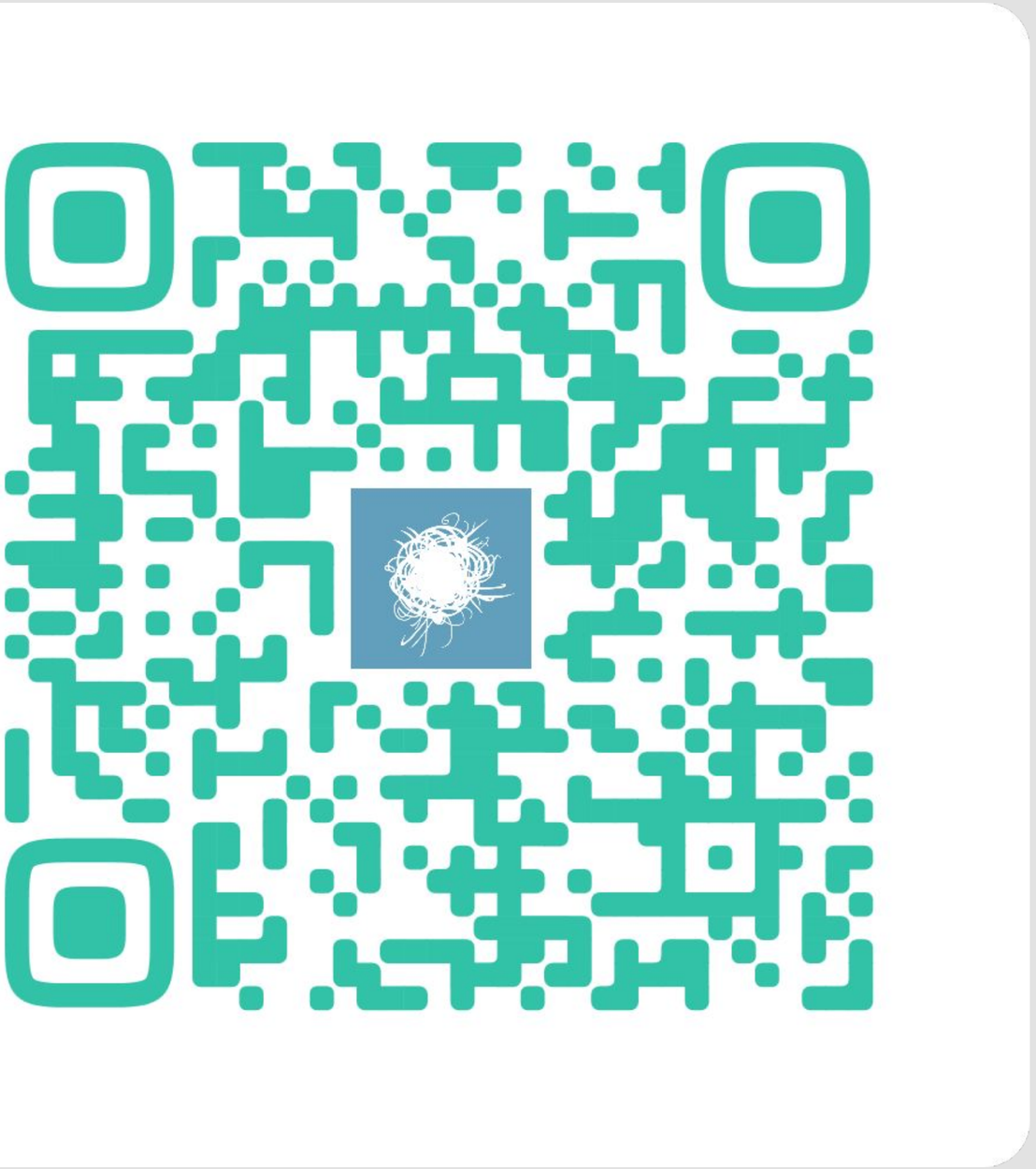
04

Пайплайны можно валить при обнаружении критичных уязвимостей

tech

Пайплайны и сканеры

Подробности в статье на Хабре



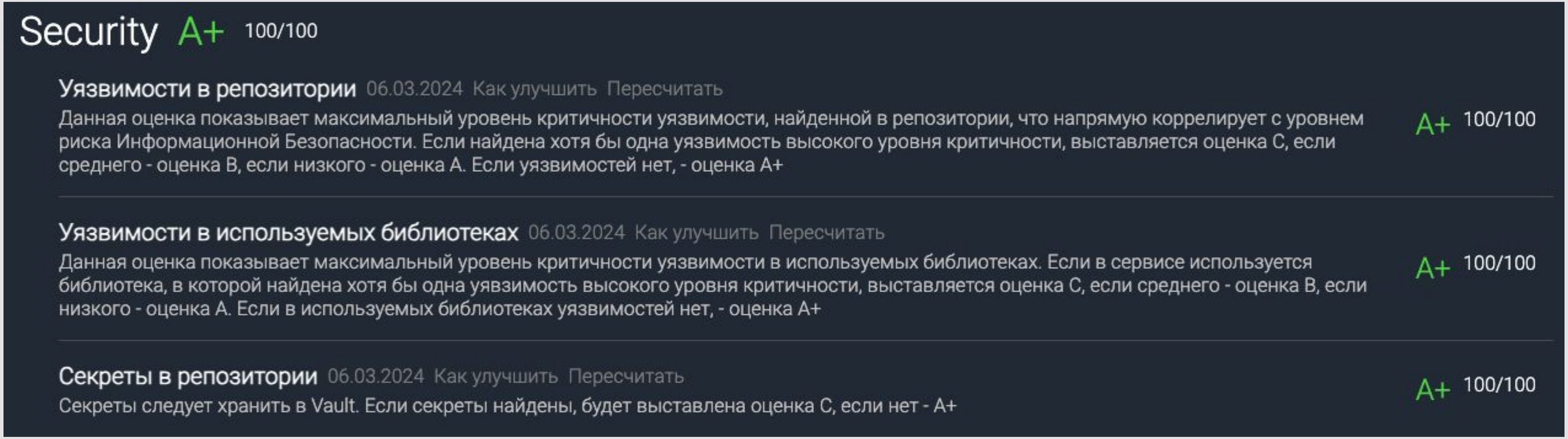
tech

Как устроен наш пайплайн

Шашлычок из джобов

Ставим оценки за результаты прохождения пайплайнов

Оцениваем прохождение SAST, SCA, Secret Detection



tech

Мерим общее состояние дел по всей компании

Это уже метрика для AppSec

tech

Переходим к основе)

tech

План кодера на день:

1) Код писат
2) MP делать
3) Код Пушит
4) Ждать (обед)
5) Ошибки видит
6) Бежат от AppSec

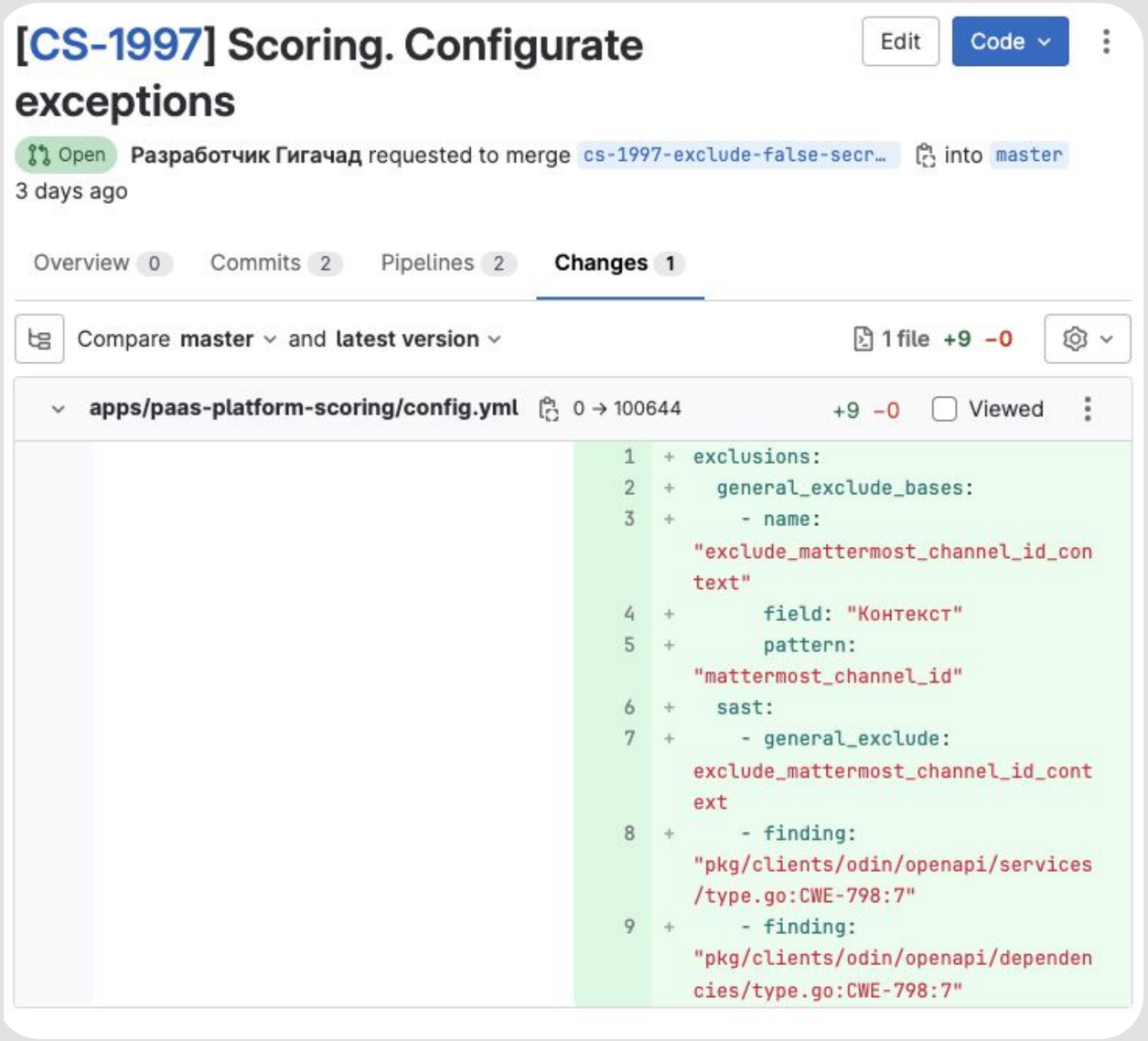
tech

План разработчика на день:

1) Код качественный писать
2) MP создать, отдать на ревью
3) Посмотреть результаты сканов в пайплайне
4) Проанализировать на false positive
5) Добавить исключения в репозиторий

tech

Exclusions as a Code



tech

Способ готовки: экспресс-курс

tech

до обучения

обычный разработчик скорее всего не очень сильно разбирается в безопасности, и понять false positive это или нет не сможет
это не бро для AppSec

после обучения

после проведения обучения, разработчик будет знать про типовые уязвимости, будет уметь писать исключения для файндингов, понимать тестировать сервисы на безопасность

Способ готовки: специализированный-курс

tech

А где мотивация?

Ставим оценку сервисам за качество

Ставим минимальный уровень для команд, чтобы точно понимали что надо работать над безопасностью

Ставим OKR для тимлидов для поднятия и поддержки уровня

Делаем премию зависимой от OKR

Переходим к процессам

tech

Оцениваем как обучились разработчики

Оценка Security Education & Culture

Уровень 1

- Указан состав команды в описании в Story команды
- Командой пройден онбординг курс по безопасности и сдан финальный тест

Дата назначения	Срок выполнения	Статус
18 мар. 2021 г.	–	Не начат
20 февр. 2023 г.	–	Завершен
7 мая 2021 г.	–	Не начат
19 мар. 2021 г.	–	Не начат
4 июн. 2021 г.	–	Завершен
10 мар. 2022 г.	–	Завершен

tech

Оцениваем как обучились разработчики

Оценка Security Education & Culture

Уровень 2

- Выбран Security Champion, который прошел курс по своей специальности Backend или Frontend/Mobile for React Native

Domain	Team	Security champion	Team lead	Stack	
Demand	Odin	@Разработчик Гошник Секчемповец	@Тимлид Секчемпа Крутовец	js, java tester	QA
Demand	Odin	@Бэкендер Секчемп Бэкендеровец	@Тимлидов Бэкенд Разработчикович	ruby	Back

tech

Оцениваем как обучились разработчики

Оценка Security Education & Culture

Уровень 3

- Security Champion провел встречу со своей командой, по изученным им материалам по безопасности и приложил материалы или запись проведенного семинара

или

- Все члены команды прошли курсы Backend или Frontend/Mobile for React Native в зависимости от специальности

Оцениваем как разработчики взаимодействуют

Оценка Secure Development

Уровень 1

- Прочитали статью по взаимодействию с командой AppSec (Взаимодействие с AppSec)
- Связались с командой AppSec и запросили аудит безопасности
- Получили список требований после аудита и согласовали с бизнес партнером AppSec

tech

Оцениваем как разработчики взаимодействуют

Оценка Secure Development

Уровень 2

- Исправили/реализовали все замечания/предложения после аудита безопасности и получили апрув у бизнес партнера AppSec
- Прочитали статьи и следуете безопасными паттернами при разработке

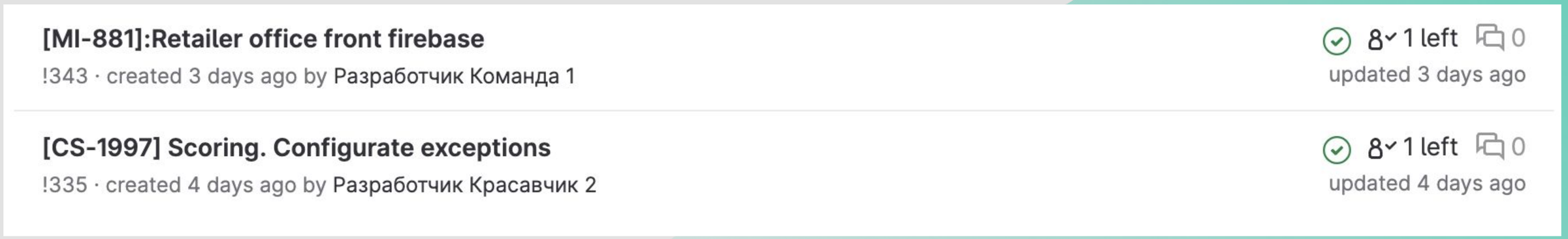
tech

Оцениваем как разработчики взаимодействуют

Оценка Secure Development

Уровень 3

- Достигли и поддерживаете уровень метрик на уровне A+ (SAST/SCA/Secrets)
- Добавляете самостоятельно исключения в **https://gitlab/information-security/devsecops-configs** при возникновении фолсов



tech

Что такое TMM?

“Модель зрелости команд (Team Maturity Model TMM) – это список инженерных практик с описанием базового уровня для всех команд разработки в СберМаркете.
Цель внедрения TMM — сильная инженерная культура.“

Зачем TMM для команд?

- понимать, что такое "базовый уровень" в компании и как его достичь;
- диалог с экспертами – куда идет компания, что нужно делать командам, почему именно так;
- инструмент для самодиагностики и ретроспективы, чтобы найти зоны роста и создать план развития.

20.	[3 уровень] Внедрить предиктивную аналитику или способы отслеживания отклонений/аномалий в работе сервисов	TMM-1649	Observability		OPEN
21.	[2 уровень] Выбрать участника команды и назначить его Security Champion и внести в таблицу	TMM-1650	Security Ed&Culture		OPEN
22.	[2 уровень] Security Champion должен назначить себе курс самостоятельно по своей специальности и пройти его	TMM-1651	Security Ed&Culture		OPEN
23.	[3 уровень] Security Champions назначает встречу со своей командой, проводит семинар/лекцию по изученным им материалам	TMM-1652	Security Ed&Culture		OPEN
24.	[3 уровень] Подтвердить знания прохождением тестирования всеми членами команды	TMM-1653	Security Ed&Culture		OPEN
25.	[2 уровень] Исправить/реализовать все замечания/ предложения после аудита безопасности и получить апрув у бизнес партнера AppSec	TMM-1654	Secure Development		CLOSED
26.	[2 уровень] Изучить и следовать безопасными паттернами	TMM-1655	Secure Development		CLOSED
27.	[3 уровень] Самостоятельно поддержать скоринг A+ для своего сервиса (если есть)	TMM-1656	Secure Development		OPEN
28.	[3 уровень] Договориться с юнит лидом/хэдом домена о максимальном значении Lead time по PROJ для вашей команды	TMM-1657	Delivery metrics		OPEN
29.	[3 уровень] Связать задачи команды (через эпик команды или через конкретные задачи) с задачами в PROJ и делать это на регулярной основе	TMM-1658	Delivery metrics		OPEN
30.	[3 уровень] Проводить регулярные ретроспективы/ обзоры потока по улучшению метрик на основании командных задач и задач из проекта PROJ	TMM-1659	Delivery metrics		OPEN
31.	[3 уровень] Попасть в согласованный лид тайм по PROJ с юнит лидом/хэдом домена	TMM-1660	Delivery metrics		OPEN
32.	[3 уровень] Достигнуть определенного значения Velocity/Throughput и для Kanban команд подготовить расчет SLA по командным типам задач	TMM-1661	Delivery metrics		OPEN

Зачем TMM для команд?

- понимать, что такое "базовый уровень" в компании и как его достичь;
- диалог с экспертами – куда идет компания, что нужно делать командам, почему именно так;
- инструмент для самодиагностики и ретроспективы, чтобы найти зоны роста и создать план развития.

20.	[3 уровень] Внедрить предиктивную аналитику или способы отслеживания отклонений/аномалий в работе сервисов	TMM-1649	Observability		OPEN
21.	[2 уровень] Выбрать участника команды и назначить его Security Champion и внести в таблицу	TMM-1650	Security Ed&Culture		OPEN
22.	[2 уровень] Security Champion должен назначить себе курс самостоятельно по своей специальности и пройти его	TMM-1651	Security Ed&Culture		OPEN
23.	[3 уровень] Security Champions назначает встречу со своей командой, проводит семинар/лекцию по изученным им материалам	TMM-1652	Security Ed&Culture		OPEN
24.	[3 уровень] Подтвердить знания прохождением тестирования всеми членами команды	TMM-1653	Security Ed&Culture		OPEN
25.	[2 уровень] Исправить/реализовать все замечания/ предложения после аудита безопасности и получить апрув у бизнес партнера AppSec	TMM-1654	Secure Development		CLOSED
26.	[2 уровень] Изучить и следовать безопасными паттернами	TMM-1655	Secure Development		CLOSED
27.	[3 уровень] Самостоятельно поддержать скоринг A+ для своего сервиса (если есть)	TMM-1656	Secure Development		OPEN
28.	[3 уровень] Договориться с юнит лидом/хэдом домена о максимальном значении Lead time по PROJ для вашей команды	TMM-1657	Delivery metrics		OPEN
29.	[3 уровень] Связать задачи команды (через эпик команды или через конкретные задачи) с задачами в PROJ и делать это на регулярной основе	TMM-1658	Delivery metrics		OPEN
30.	[3 уровень] Проводить регулярные ретроспективы/ обзоры потока по улучшению метрик на основании командных задач и задач из проекта PROJ	TMM-1659	Delivery metrics		OPEN
31.	[3 уровень] Попасть в согласованный лид тайм по PROJ с юнит лидом/хэдом домена	TMM-1660	Delivery metrics		OPEN
32.	[3 уровень] Достигнуть определенного значения Velocity/Throughput и для Kanban команд подготовить расчет SLA по командным типам задач	TMM-1661	Delivery metrics		OPEN

Зачем TMM для AppSec?

Картина мира и метрики!

Secure Development level	Count	Percentage
0	38	37%
1	17	16%
2	32	31%
3	17	16%
Total	**104**	

tech

Что в итоге?

tech

Рецепт:

1) Результаты пайплайнов безопасности вынесим в job-output
2) Исключения пишем в виде кода в git
3) Добавляем Security Quality Gate для остановки пайплайна
4) Внедряем оценки по Secure Development и Security Education в процесс ревью команд

Что имеем после внедрения?

46

контрибьюторов в репозиторий с исключениями

85

Security Champion в разных командах разработки

65%

команд активно работают с AppSec BP

80%+

сервисов проходят security quality gate без проблем

tech

Что изменилось для AppSec-команды

1) Стало легче отслеживать команды в которых нужно внимание (консультация или аудит)
2) Разработчики сами триажат файндинги сканеров
3) Сразу видно сервисы где нужно внимание (оценка B или C)
4) Разработчики начали проходить курсы по безопасной разработке
5) Есть сформированный и актуальный список Security Champion

спасибо за внимание

tech

Кашапов Нияз
AppSec Lead @ Сбермаркет

@niaz.kashapov
niyaz.kashapov@sbermarket.ru

tech