Advanced approaches in CyberSecurity

Vatclav Dovnar

whoami

```
{
   speaker_name: “Vatclav Dovnar”
   skills: [appSec, infraSec,  devSecOps,
problem_solving],
   skill_years:  9,
   job_title:  “Head of Product Security”,
   tolk_time:  40,
   hiring_status:  “Looking for cool teammates”

}
```

profile_photo.png

telegram.png

Thanks to

Иван Васильев

Жания Рахметова

Every Security Team is a Software Team Now

DINO DAI ZOVI

Every Security Team is a Software Team Now
DINO DAI ZOVI

Введение

Организации проектируют системы, которые копируют структуру коммуникаций в этой организации

Мелвин Конвей

Введение

Организации проектируют системы, которые копируют структуру коммуникаций в этой организации

Мелвин Конвей

Выводы:

1. Команды будут закреплять зоны ответственности на уровне API интерфейсов

Введение

Организации проектируют системы, которые копируют структуру коммуникаций в этой организации

Мелвин Конвей

Выводы:

1. Команды будут закреплять зоны ответственности на уровне API интерфейсов

2. Необходимо тратить ресурс на кросскомандную коммуникацию

Кто отвечает за безопасность продукта?

Кто отвечает за безопасность продукта?

ИБ

Кто отвечает за безопасность продукта?

ИБ ➡️ не является владельцем актива

Кто отвечает за безопасность продукта?

ИБ ➡️ не является владельцем актива

Команда продукта

Кто отвечает за безопасность продукта?

ИБ ➡️ не является владельцем актива

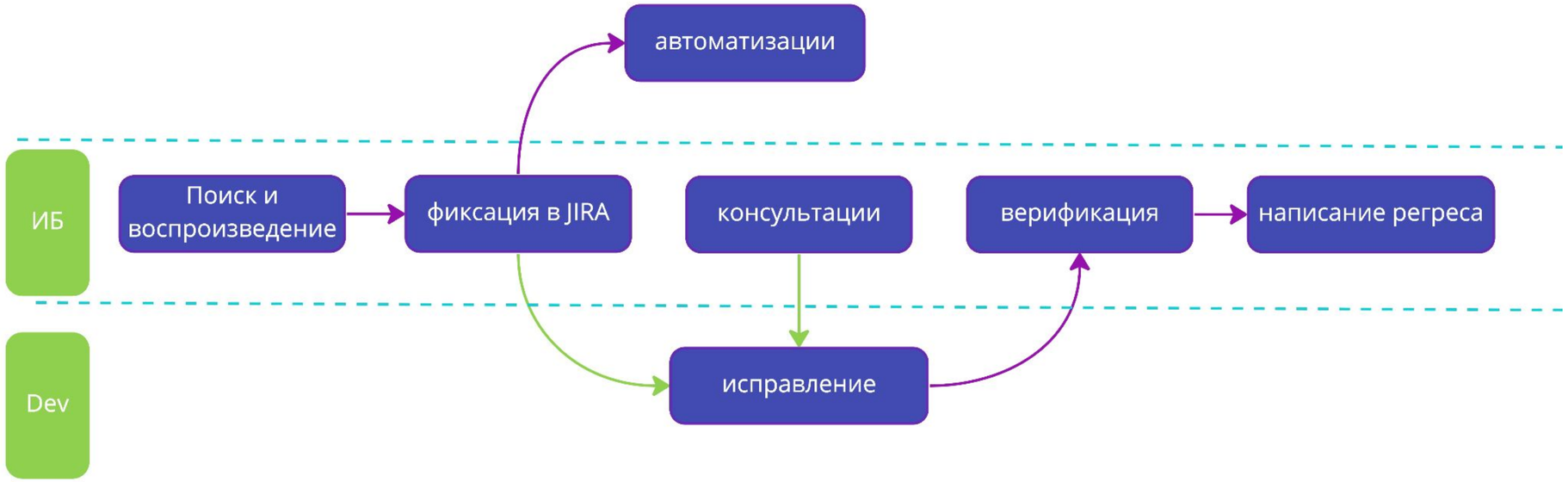
Команда продукта ➡️ не разбирается в ИБ

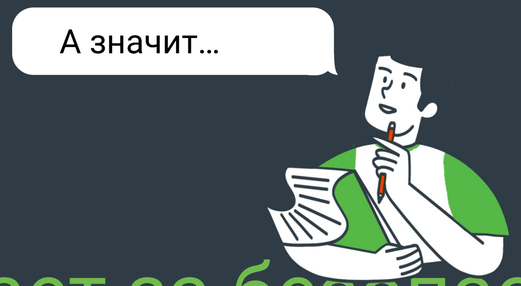
Кто отвечает за безопасность продукта?

ИБ ➡️ не является владельцем актива

Команда продукта ➡️ не разбирается в ИБ

Флоу исправления уязвимостей





Кто отвечает за безопасность продукта?

ИБ	➡️	консультации, инструменты, экосистема
Команда продукта	➡️	ресурсы, вовлечённость

Введение


Dino A. Dai Zovi
@dinodaizovi
Dai Zovi's Law:
The quality of your organization's security will mirror the quality of the communication between its engineering and security functions.

Cyber Strategy

По бумажкам

- Малоэффективно
- Оторвано от реальности

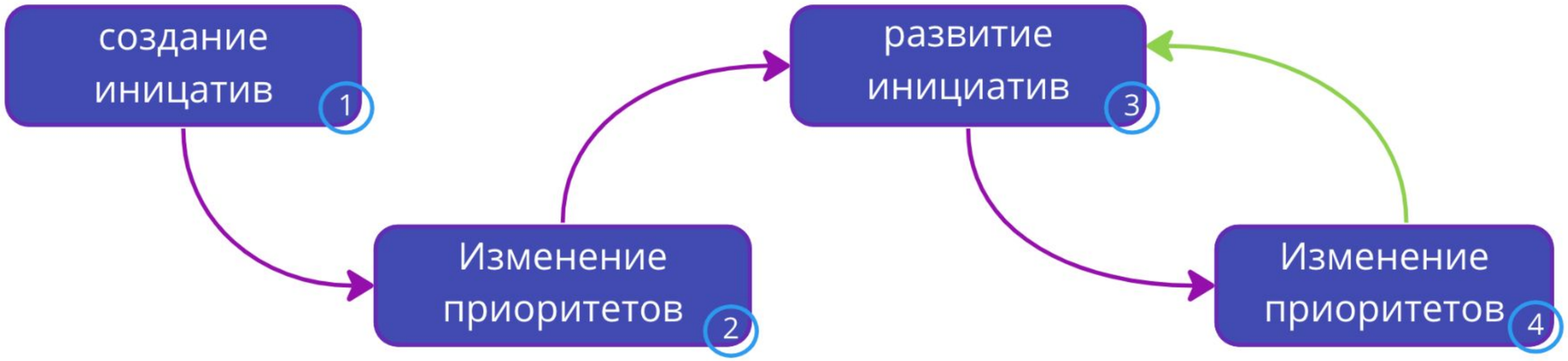
По бумажкам

- Малоэффективно
- Оторвано от реальности

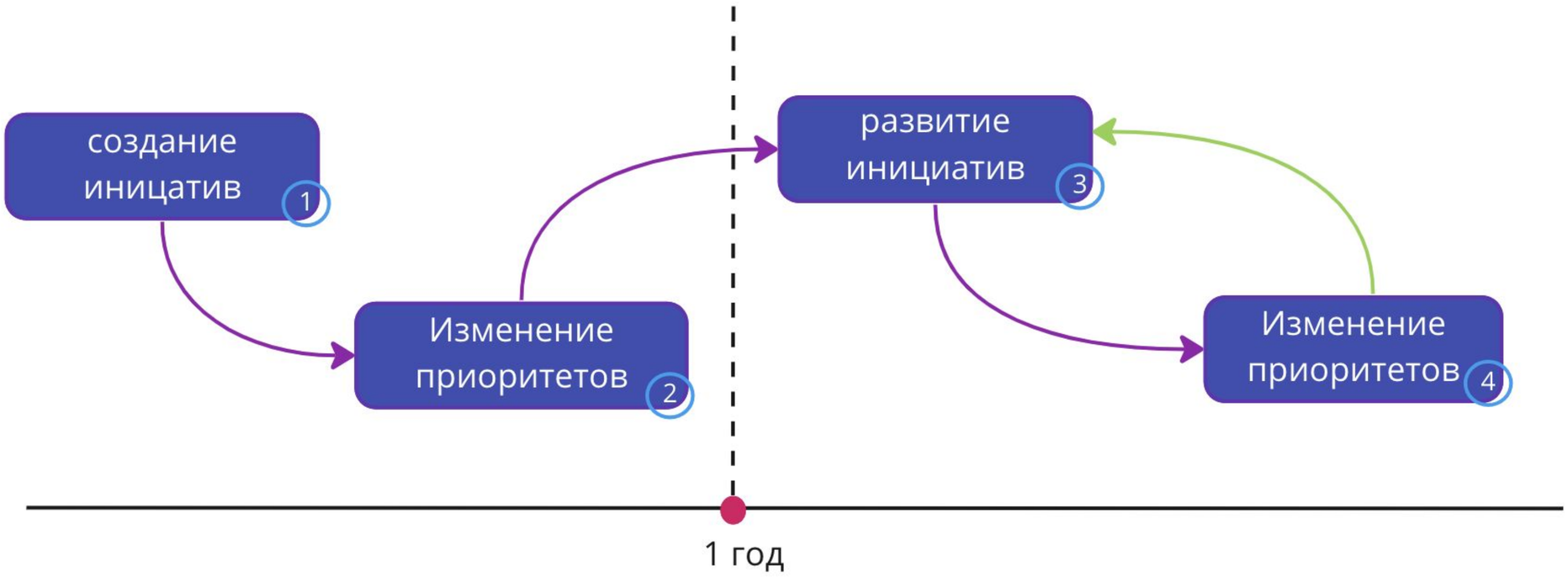
Переоценка рисков

- Раз в год?
- Раз в полгода?
- Раз в квартал?

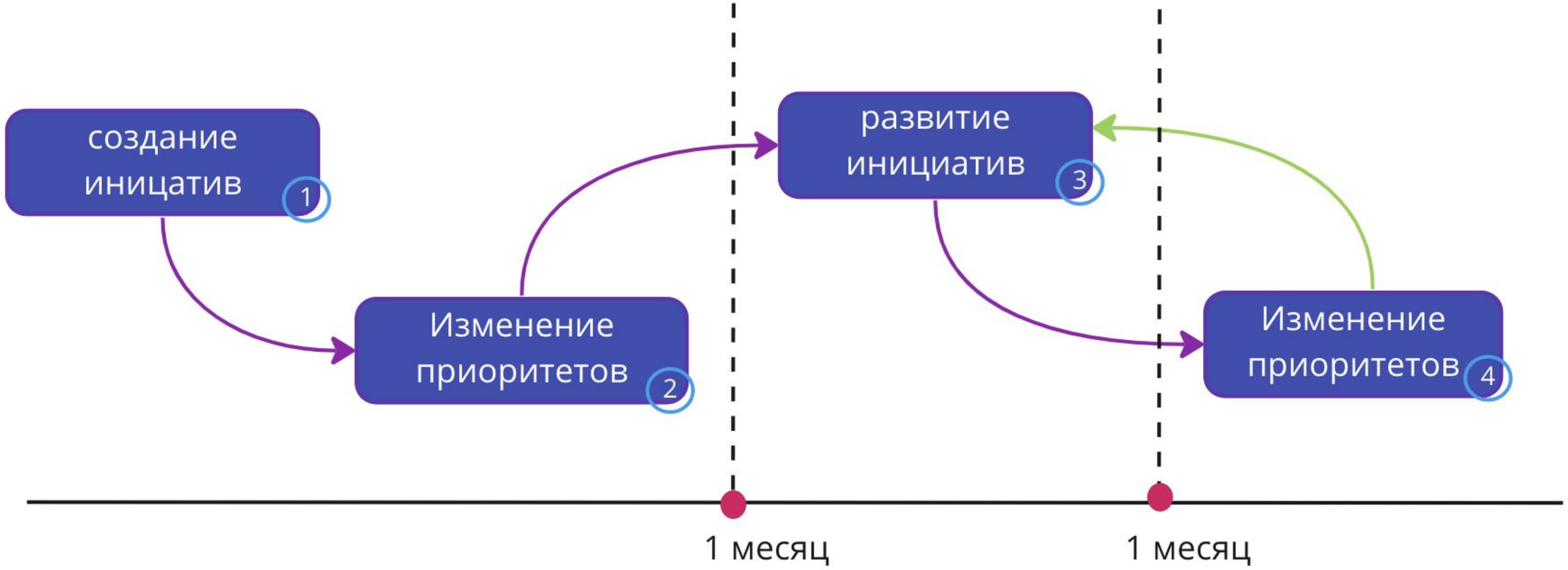
Cyber Strategy



Cyber Strategy



Cyber Strategy



Как ИБ помогает бизнесу?

- Консалтинг по наведению порядка
  (сети, DNS, список активов, expired TLS)
- Мотивация к избавлению от legacy
  (старые сети, сервера, версии API, код)
- Увеличение стабильности
- Экосистема инструментов безопасности в пайплайне сборки
- Помощь в росте сотрудников

Как ИБ помогает бизнесу?

- Консалтинг по наведению порядка
  (сети, DNS, список активов, expired TLS)
- Мотивация к избавлению от legacy
  (старые сети, сервера, версии API, код)
- Увеличение стабильности
- Экосистема инструментов безопасности в пайплайне сборки
- Помощь в росте сотрудников
- Ваш пункт

Как ИБ помогает бизнесу?

Помощь

⬇️

Улучшение коммуникации

⬇️

Долгосрочное улучшение безопасности

Security error budget

Предпосылки

- Процесс исправления уязвимостей превращается в хаос

Предпосылки

- Процесс исправления уязвимостей превращается в хаос
- Нехватка времени в командах

Security error budget

Предпосылки

- Процесс исправления уязвимостей превращается в хаос
- Нехватка времени в командах

Если вам кажется, что мой закон действует против вас

Мелвин Конвей

Security error budget

1

2

3

4

Security error budget

1

Политика исправления уязвимостей

2

3

4

- Crit - 4 hour fix
- High - 2 days fix
- Medium - 2 weeks fix
- Low - half a year fix

Security error budget

1

Политика исправления уязвимостей

- Crit - 4 hour fix
- High - 2 days fix
- Medium - 2 weeks fix
- Low - half a year fix

2

Таблица стоимости уязвимостей

- Crit - 1000$
- High - 500$
- Medium - 200$
- Low - 50$

3

4

Security error budget

1

Политика исправления уязвимостей

- Crit - 4 hour fix
- High - 2 days fix
- Medium - 2 weeks fix
- Low - half a year fix

2

Таблица стоимости уязвимостей

- Crit - 1000$
- High - 500$
- Medium - 200$
- Low - 50$

3

Автоматизация

- установка due date
- подсчет error budget

4

Security error budget

1

Политика исправления уязвимостей

- Crit - 4 hour fix
- High - 2 days fix
- Medium - 2 weeks fix
- Low - half a year fix

2

Таблица стоимости уязвимостей

- Crit - 1000$
- High - 500$
- Medium - 200$
- Low - 50$

3

Автоматизация

- установка due date
- подсчет error budget

4

Контроль метрики

10 000$ / year

Security error budget

1

Политика исправления уязвимостей

- Crit - 4 hour fix
- High - 2 days fix
- Medium - 2 weeks fix
- Low - half a year fix

2

Таблица стоимости уязвимостей

- Crit - 1000$
- High - 500$
- Medium - 200$
- Low - 50$

3

Автоматизация

- установка due date
- подсчет error budget

4

Контроль метрики

10 000$ / year

Дополнительно:
автоматизация, автоматизация, визуализация и автоматизация

Security error budget

$$BaseVulnerabilityPrice = CriticalityPrice * ThreatAssessmentCoefficient$$

Security error budget

$$BaseVulnerabilityPrice = CriticalityPrice * ThreatAssessmentCoefficient$$

$$FinalVulnerabilityPrice = BaseVulnerabilityPrice + \frac{BaseVulnerabilityPrice}{TargetFixPeriod} * DaysOverdue$$

Security error budget

$$BaseVulnerabilityPrice = CriticalityPrice * ThreatAssessmentCoefficient$$

$$FinalVulnerabilityPrice = BaseVulnerabilityPrice + \frac{BaseVulnerabilityPrice}{TargetFixPeriod} * DaysOverdue$$

$$Budget = \sum_{i=1}^{N} FinalVulnerabilityPrice_i$$

Security error budget

Статус OKR	Команда	Приоретет...	Team Type	Взятый OKR / Комментарий
OKR принят	<Redacted>	important	Product	KR 1 Расход error-budget не выше 1000$

Security error budget

AJ

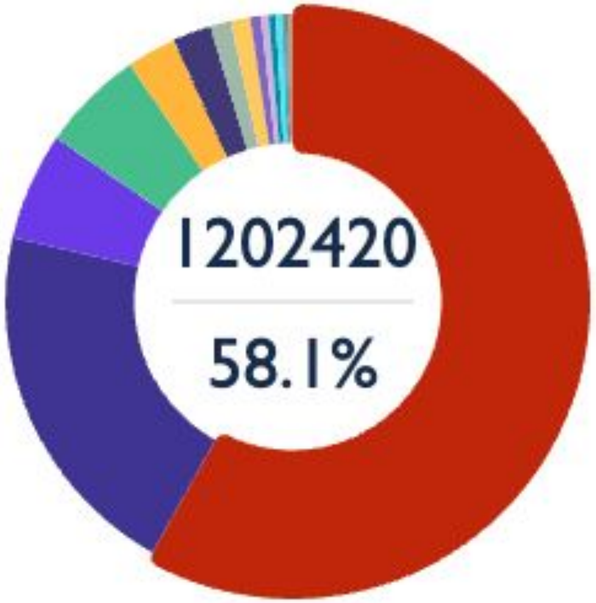
Automation for Jira July 28, 2022 at 4:43 PM

Due Date is set automatically based on Priority and Vulnerability Remediation Policy to 2022-09-26T13:43:07.8+0000

Edit · Delete ·

Security error budget

Error budget consumption by team

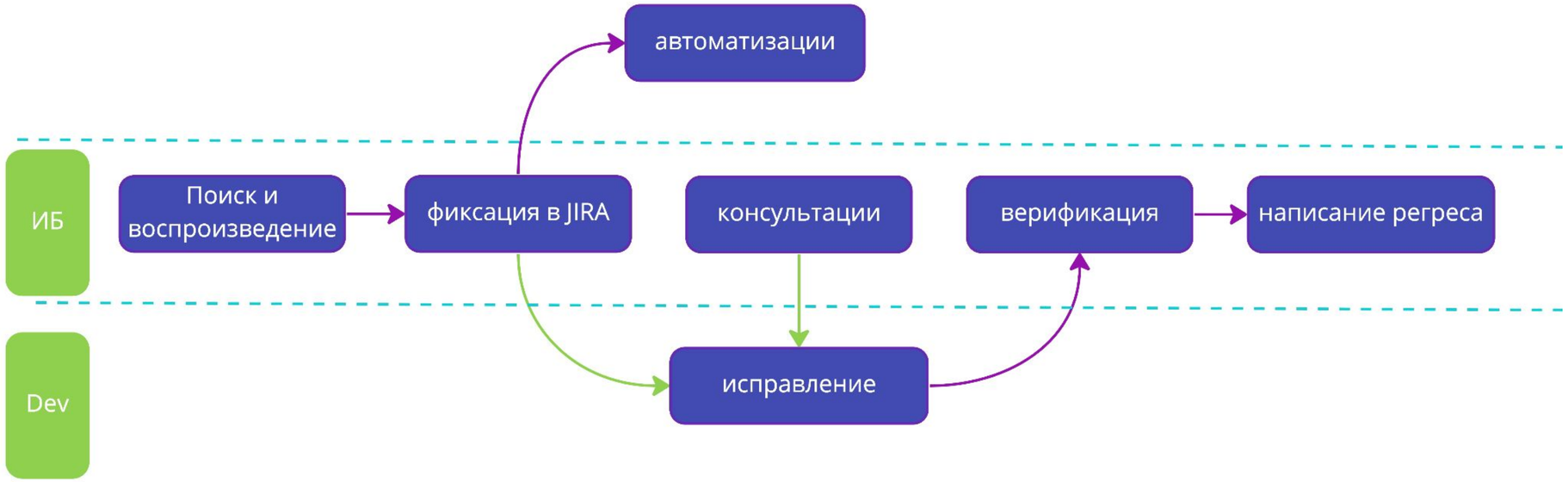


#	Assigned Team	Consupted budget	%
1	Team #4	1202420	58.1%
2	Team #2	423150	20.5%
3	Team #1	125400	6.1%
4	Team #10	119519	5.8%
5	Team #6	57418	2.8%
6 - 19	Show more...	140790	6.8%
Total		2068697	100%

🔎 Референс

- Google SRE Error Budget
- GitLab Error Budget

Флоу исправления уязвимостей



Security error budget + Флоу исправления

📊 Визуализация

— Jira Charts \ Metabase \ Tableau и т.д.

Связь с Конвеем

— Создание чёткой системы разделения зон ответственности

Security error budget + Флоу исправления

📊 Визуализация

— Jira Charts \ Metabase \ Tableau и т.д.

Связь с Конвеем

— Создание чёткой системы разделения зон ответственности

Превращаем “футбол” в конвеер!

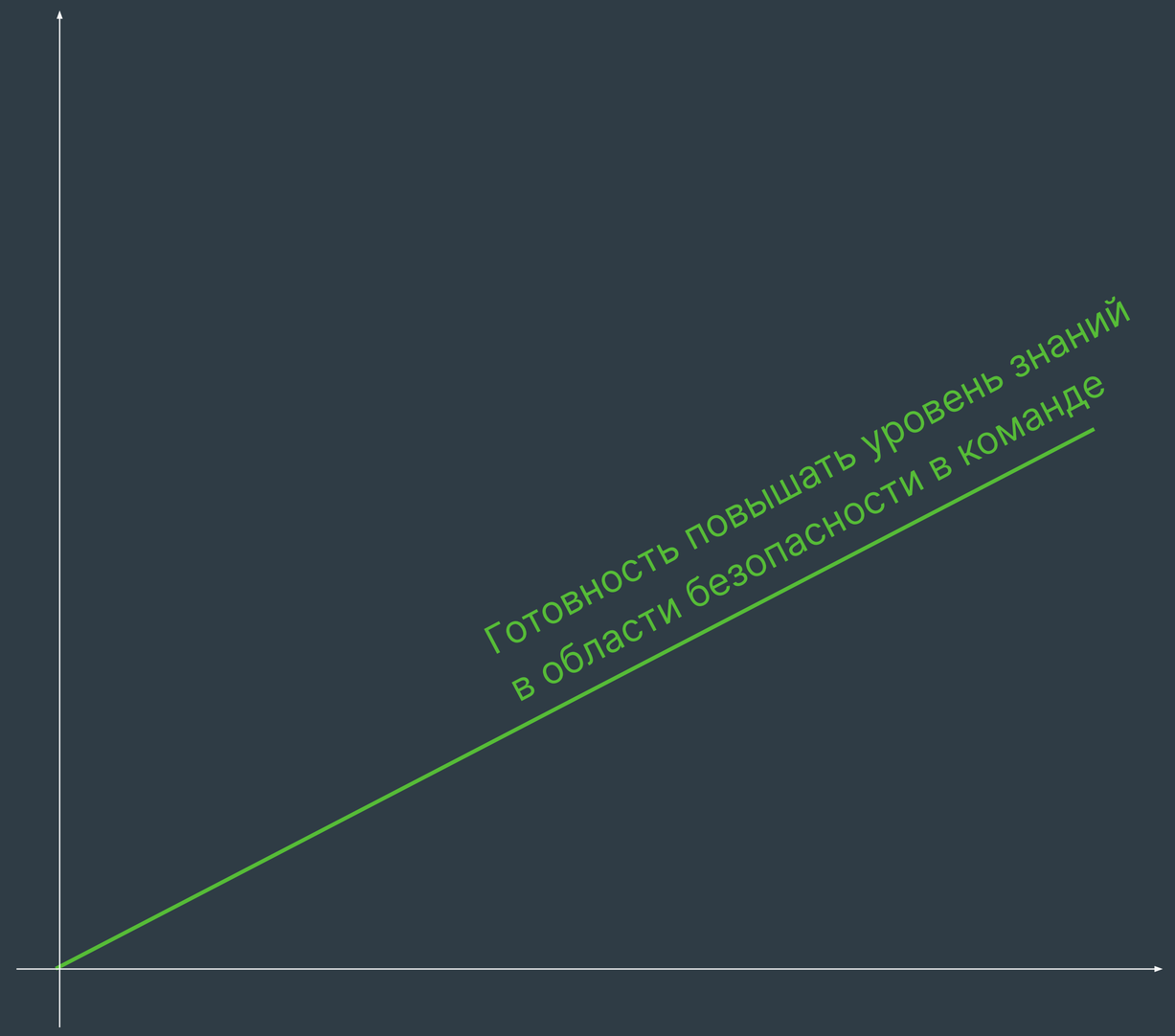
Мелвин Конвей

Security амбасадоры

— не работает для всех команд

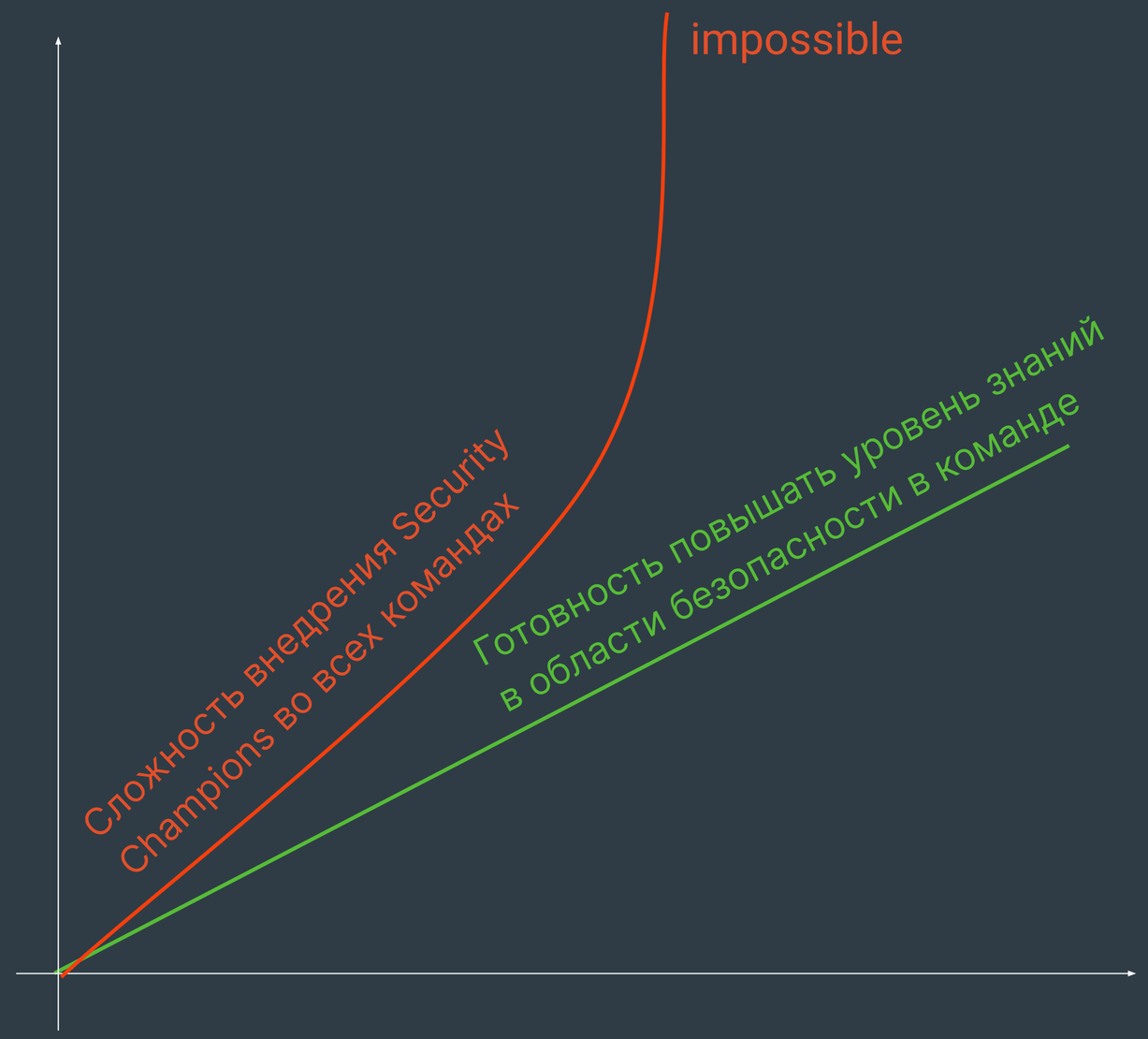
Security Champions

Security-амбассадоры



Security Champions

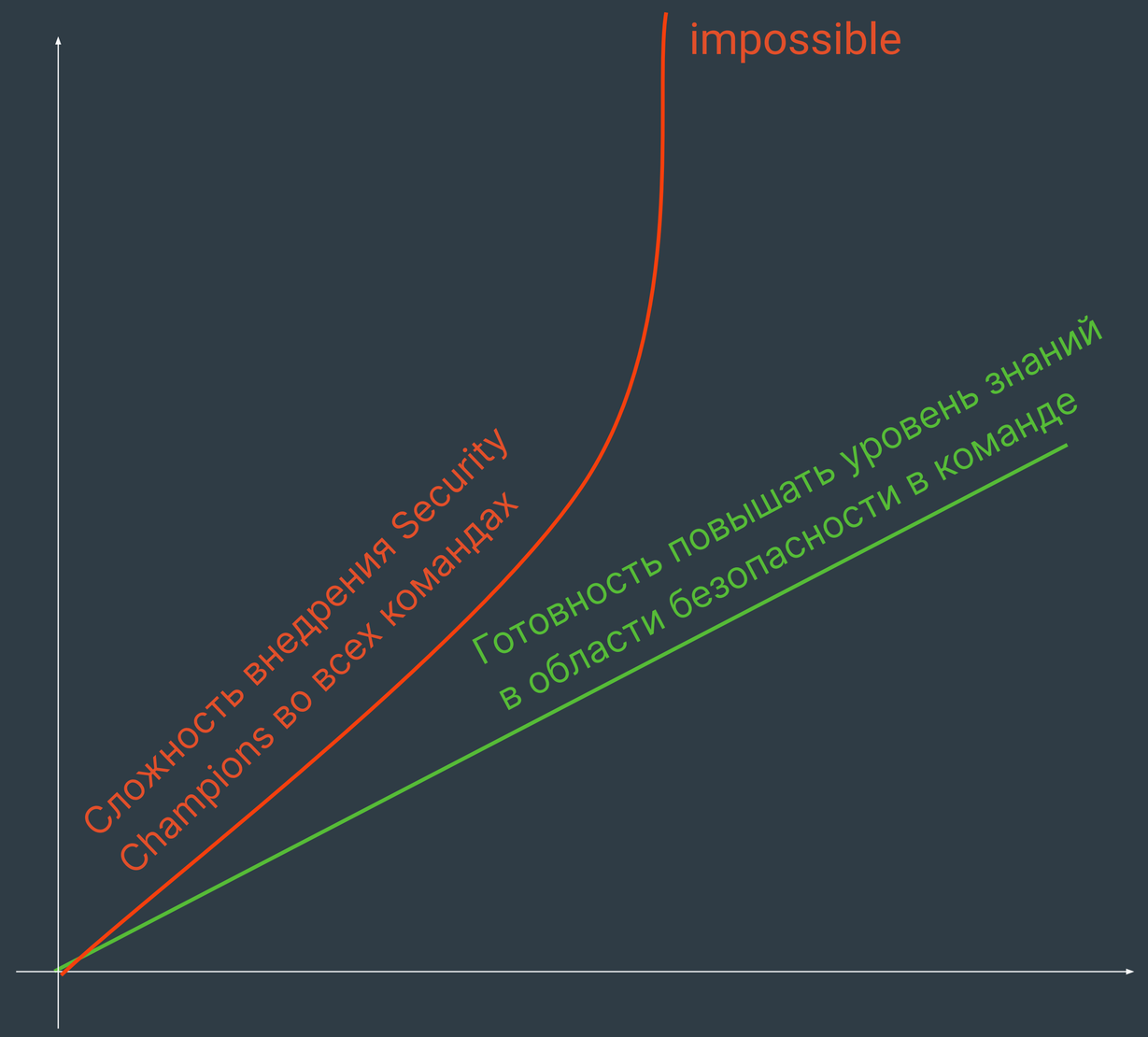
Security-амбассадоры



Security Champions

— Работает не для всех команд

Security-амбассадоры



Security Champions

— Работает не для всех команд

— Чем больше требуется изменений, тем сложнее найти

🎯 Что даёт?

— Решение сложных проблем у сложных команд

— Сокращение расстояния до безопасности

— Уменьшение новых однотипных уязвимостей в команде

Связь с Конвеем

— Способ упрощения коммуникации со сложными командами

Threat Assessment

Threat Assessment

Столбцы имеют краткое наименование. Развернутый текст каждого вопроса и ответы можно найти ниже

▶ ⚠️ 📗 **Описание методов**

2

All Entity | Ready full | 1 more... | Locked | Filter | Sort | Ne

System list

Aa Name	GitHub	∑ Total Risk Assessment
☆ example service	https://github.com/hakluke/how-to-e	60
+ New		

3

1

Threat Assessment

Таблица Threat Assessm
инвентаризация

📢 Опросник для инвентаризации создаваемых и текущих с

- ▶ **Вводная информация по таблице**
- ▶ **Как внести информацию**

Столбцы имеют краткое наименование. Развернутый текст ка
можно найти ниже

- ▼ ⚠️ 📗 **Описание методов**
  1. **Access method** - Тип доступа пользователей
     a. Доступно только с определенных хостов внутри
     b. Доступно сотрудникам только за VPN
     c. Доступно субподрядчикам
     d. Доступно из Интернет
  2. **Number of users** - Количество пользователей
     a. Сервисом пользуется мало людей, число пользо планируют развивать
     b. Сервисом пользуются сотрудники компании
     c. Сервисом пользуется до 70% клиентов/водителе
     d. Сервисом пользуется более 70% клиентов\водит

example service

Description	Сервис-кофеварка, заваривает кофе
GitHub	https://github.com/hakluke/how-to-exit-vim
Status	Active
System manager	Empty
URL	https://github.com/hakluke/how-to-exit-vim
Team	My Team
Documentation li...	Empty
Access method	Available from the Internet [9] ×
Number of users	
Revenue Impact	
Service-off 1 day	
User actions	
Internal integration	The integration allows read access to sensitive data of other systems th
External Integrati...	The integration allows read access to sensitive data of other systems th
Owners fears	Application data breach [5]
Data types	Non-sensitive data [5]
Financial logic	No [0]

Select an option
- Available only from certain hosts within the infrastructure [0]
- Only available via VPN [4]
- Available to subcontractors [7]
- Available from the Internet [9]

1 2 3 4

Threat Assessment

9. **Data types -** Какие типы данных хранятся в сервисе / системе?
    a. Не хранятся
    b. Данные для работы приложения
    c. Не конфиденциальные данные
    d. Конфиденциальные данные
    e. Множество типов конфиденциальных данных
10. **Financial logic -** Связан ли сервис / система с какой-либо финансовой логикой?
    a. Нет
    b. Да
11. **Money loss -** Денежные потери\Потери иных материальных активов
    a. Нельзя потерять деньги
    b. Возможность непрямых денежных потерь
    c. Возможность прямых денежных/материальных потерь
12. **Business critical data -** Количество и качество обрабатываемых данных (бизнес-критичность данных)
    a. Не содержит
    b. Персональные данные водителей / сотрудников (частично) / частичные данные по внутренним процессам
    c. Персональные данные клиентов (не относящиеся к бизнес-критичным) / полные данные по внутренним процессам
    d. Персональные данные водителей или клиентов (содержащие бизнес критичные данные)
13. **Count roles -** Количество ролей пользователей

Documentation li...	Empty
Access method	Available from the Internet [9]
Number of users	The service is used by more than 70% of clients [9
Revenue Impact	Does not affect [0]
Service-off 1 day	Company will not suffer or the processes of a sma
User actions	Read sensitive data [8]
Internal integration	The integration allows read access to sensitive dat
External Integrati...	The integration allows read access to sensitive dat
Owners fears	Application data breach [5]
Data types	Non-sensitive data [5]
Financial logic	No [0]
Money loss	Possibility of indirect money losses [5]
Business critical ...	Personal data of drivers / employees (partly) / part
Count roles	Not required. No roles [0]
Total Risk Asses...	60
TA ready	☑
Full document re...	☐

Threat Assessment

1

Направляем
анкеты лидам

2

Выделяем ТА
заполненные
без безопасника

3

Проводим интервью
со всеми, кто
не выслал в срок

4

Делаем переоценку
не реже, чем раз в год

Threat Assessment

🎯 Что даёт?

- Возможность считать метрики
  (WRT, DRW, Error Budget)
- Приоритеты на основе данных
- Выполнение требований ISO 27001

Связь с Конвеем

- Позволяет
  команде осознать
  ответственность

Security Architecture

Security Architecture

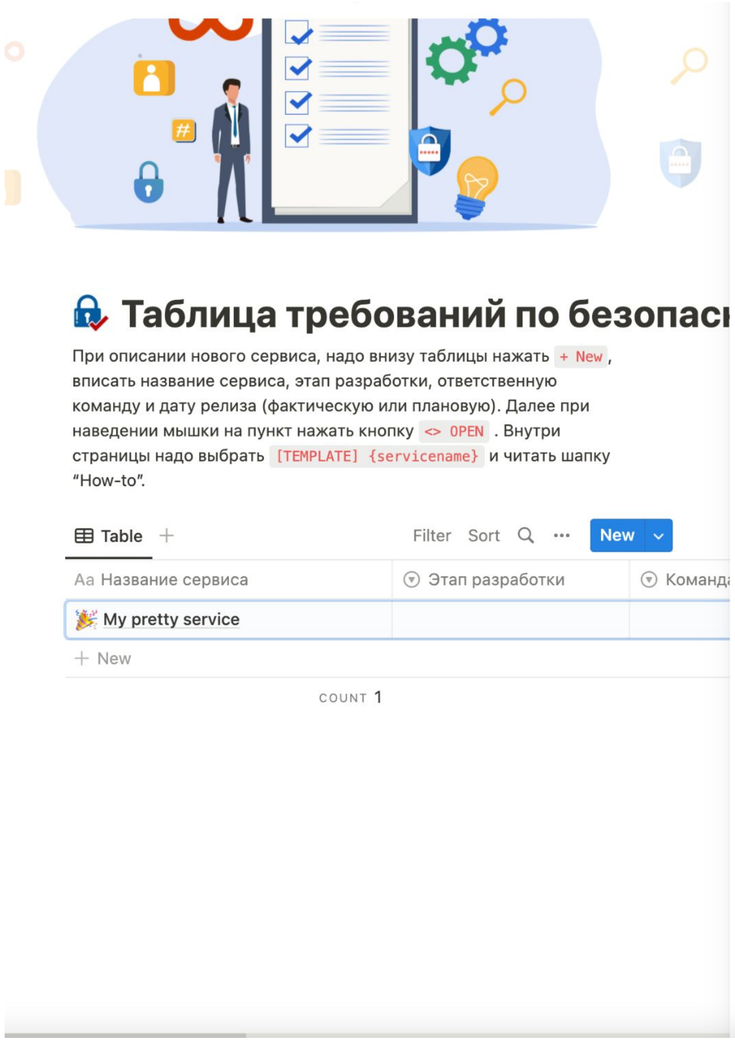


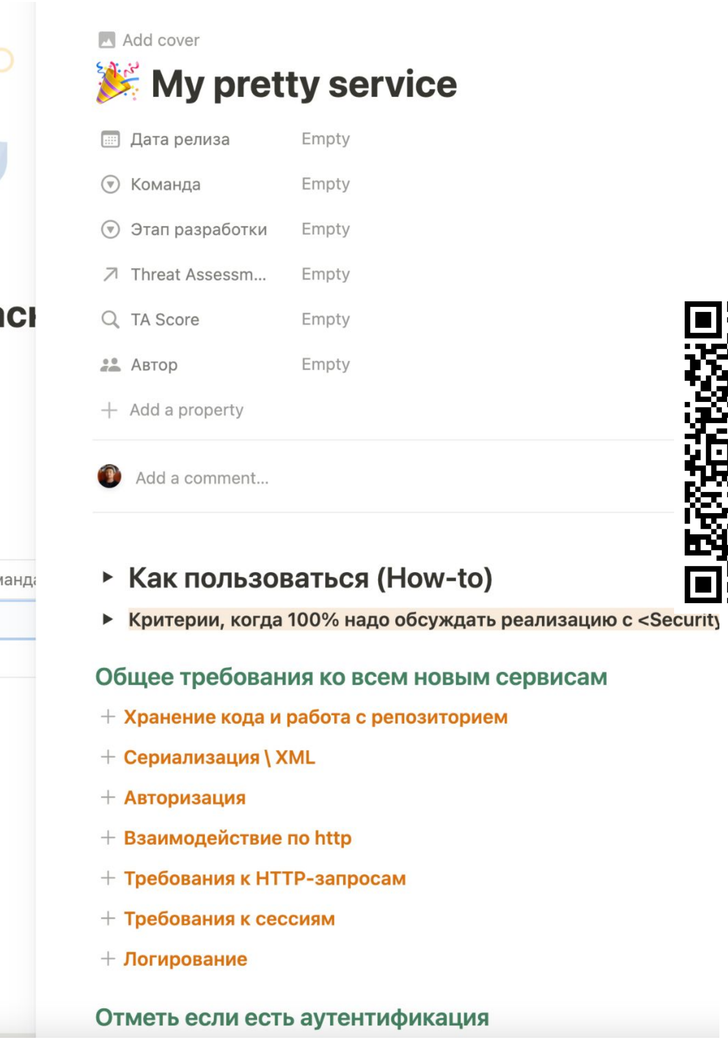
Таблица требований по безопасн

При описании нового сервиса, надо внизу таблицы нажать `+ New`, вписать название сервиса, этап разработки, ответственную команду и дату релиза (фактическую или плановую). Далее при наведении мышки на пункт нажать кнопку `<> OPEN`. Внутри страницы надо выбрать `[TEMPLATE] {servicename}` и читать шапку "How-to".

Table + | Filter | Sort | New

Aa Название сервиса	Этап разработки	Команда
My pretty service		
+ New		

COUNT 1



Add cover

My pretty service

Дата релиза	Empty
Команда	Empty
Этап разработки	Empty
Threat Assessm...	Empty
TA Score	Empty
Автор	Empty

+ Add a property

Add a comment...

▸ **Как пользоваться (How-to)**

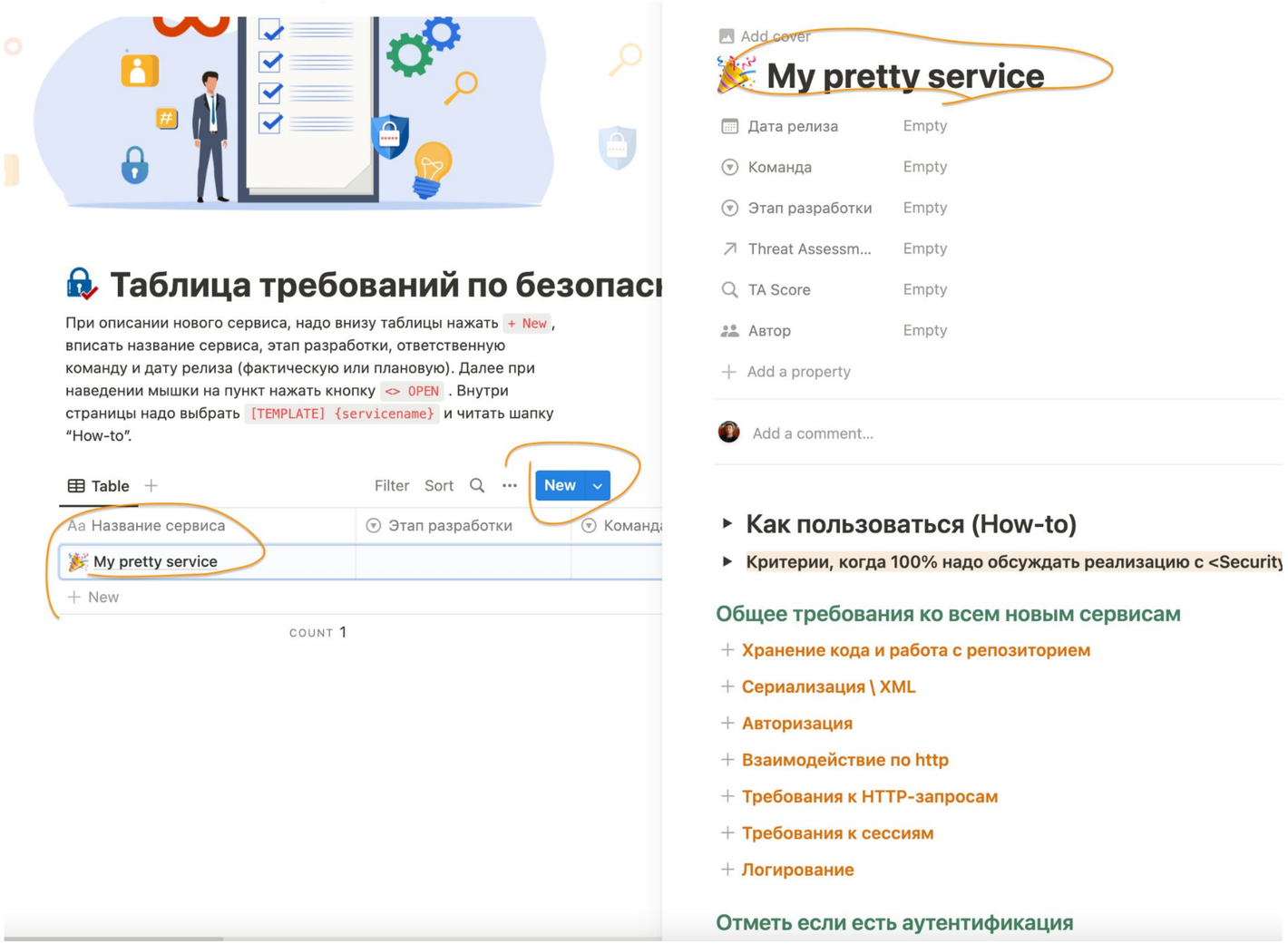
▸ **Критерии, когда 100% надо обсуждать реализацию с <Security**

Общее требования ко всем новым сервисам

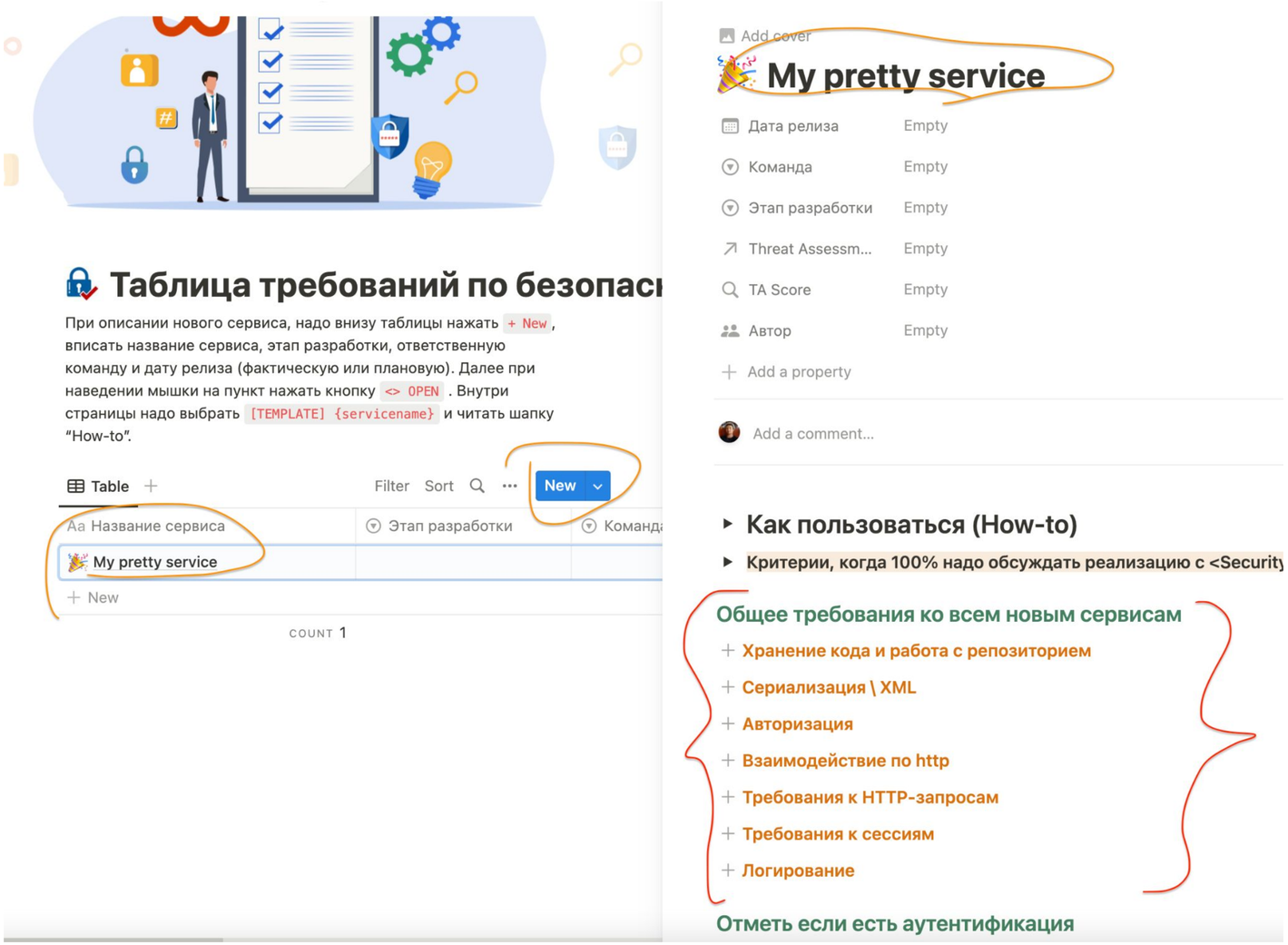
+ Хранение кода и работа с репозиторием
+ Сериализация \ XML
+ Авторизация
+ Взаимодействие по http
+ Требования к HTTP-запросам
+ Требования к сессиям
+ Логирование

Отметь если есть аутентификация

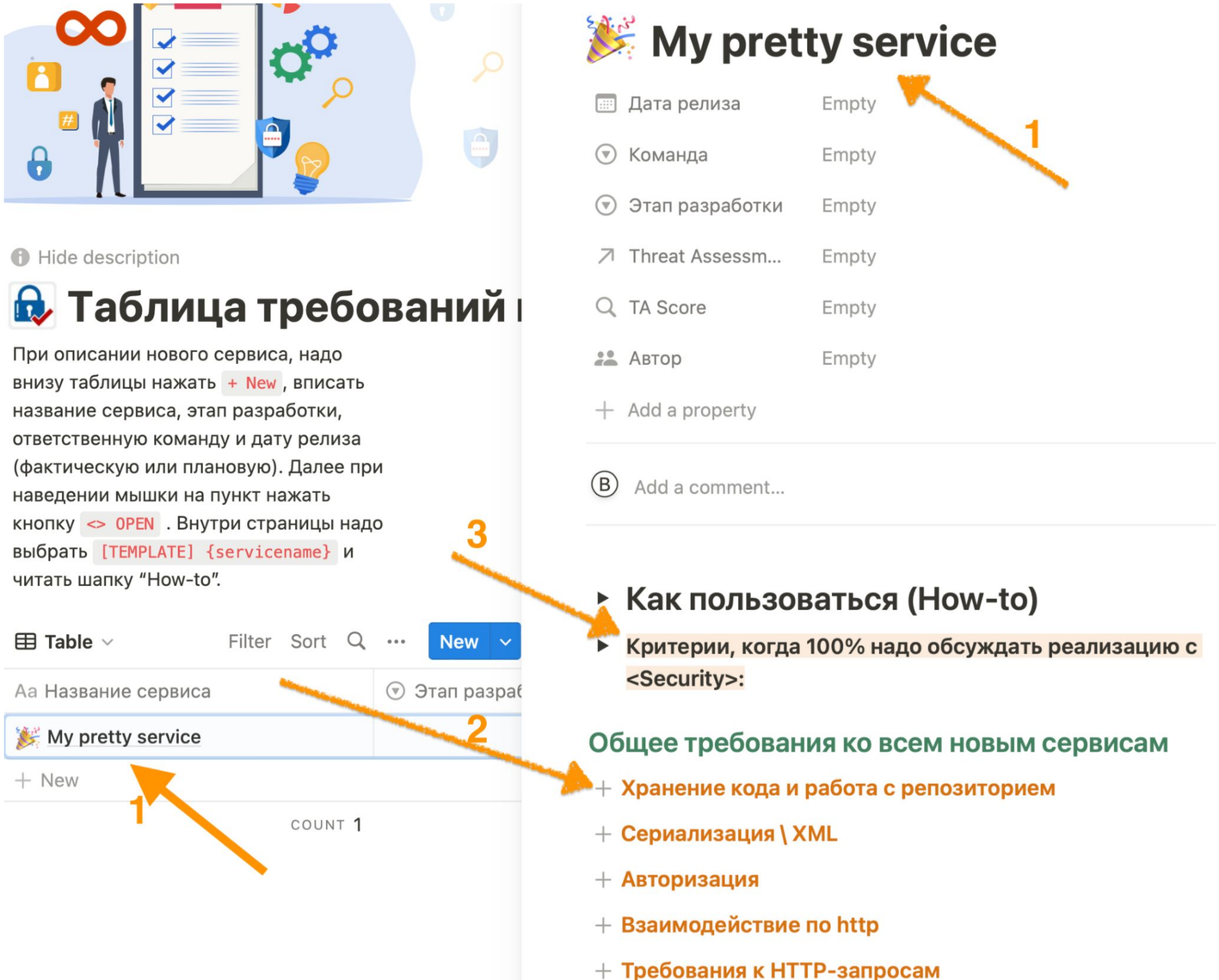
Security Architecture



Security Architecture



Security Architecture



Security Architecture

Отметь если есть аутентификация

+ **Базовые требования**

- [ ] При реализации механизмов аутентификации убедись что ты не строишь свой велосипед, когда есть уже готовый
- [ ] Любые внутренние “ручки” (эндпоинты) приложения должны проверять наличие сессии и права на выполнение данного действия у пользователя.

+ **Аутентификация с помощью паролей**

- [ ] Не используй аутентификацию по паролям не обсудим это с <Security>
- [ ] Для хеширования паролей используется алгоритм bcrypt
- [ ] Обдумай сценарий инвалидации сессий при смене пароля или предложи альетрнативы
- [ ] Ссылка для сброса пароля с токеном, должно жить не более 24ч.

+ **Общие требования по аутентифкации пользователей**
+ **Общие требования по аутентификации через OTP**

Секреты, токены

+ **Хранение**
+ **Валидация**

Отметь если используются файлы

Security Checklist

Security Checklist

🎯 Что даёт?

— Учёт регрессов по архитектуре

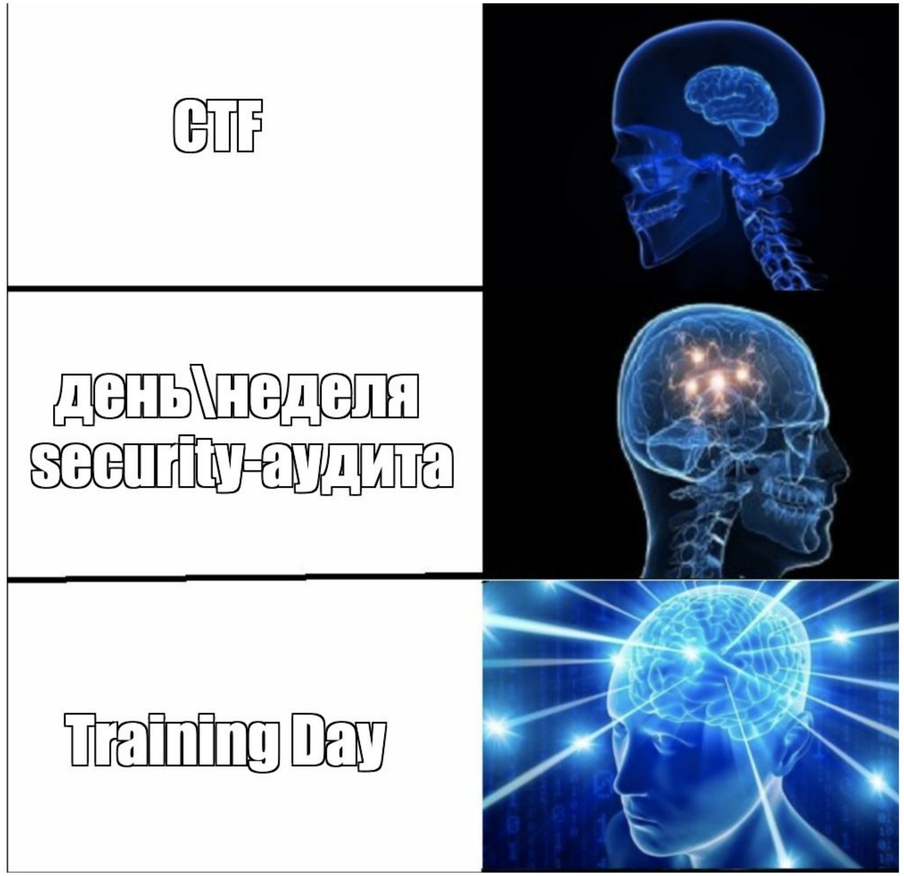
— Чек-лист для проверки реализации

Связь с Конвеем

— Делаем архитектурный комитет комфортным для ИТ

Training days

Training days



Training days

🎯 Состав

— Тренировка BlueTeam

— Аудит сервиса

— Шеринг экспертизы

🎯 Что даёт?

— Тренировка BlueTeam

— Шаринг экспертизы

— Выход за пределы повседневных задач

Как измерить?

— Найден хотя бы один инсайт

— Экспертиза пошарена на N человек

— Выявлены новые уязвимости

— Положительный фидбек

🎯 Что даёт?

— Тренировка BlueTeam

— Шаринг экспертизы

— Выход за пределы повседневных задач

Как измерить?

— Найден хотя бы один инсайт

— Экспертиза пошарена на N человек

— Выявлены новые уязвимости

— Положительный фидбек

Связь с Конвеем

— Решение проблемы межкомандного взаимодействия

Вопросы?

- Проекция закона Конвея на ИБ
- Cyber Strategy
- Security error budget
- Security-амбассадоры
- Threat Assessment
- Security Architecture
- Training Days

```
{
  telegram: “t.me/edgesec”,
  github: “edgesecc”
}
```

profile_photo.png

telegram.png