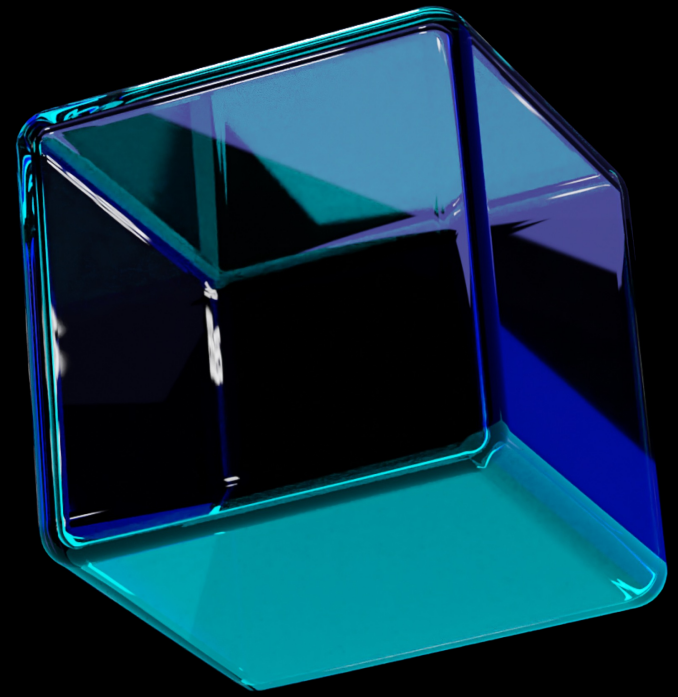


Сервис архитектуры ИБ, который мы заслужили

Роман Панин

Руководитель направления архитектуры ИБ, МТС
Автор Телеграм-канала Пакет Безопасности

Кто я и зачем это всё

>9 лет в ИТ и ИБ

Строил кибербез в финтехе, нефтянке и телекоме

Автор телеграм-канала «Пакет безопасности»

Ментор, автор обучающих курсов по ИБ и просто хороший парень

Про что поговорим

Про крутой и эффективный процесс, а точнее:

- Как всё было «до» и какие были проблемы
- Как с этим связан Security Business Partner
- Как выглядел сервис архитектуры ИБ и какие боли он закрывал
- В какой точке мы находимся сейчас
- Что мы изменили в иерархии и как интегрировались с кластерами
- Что планируем делать дальше

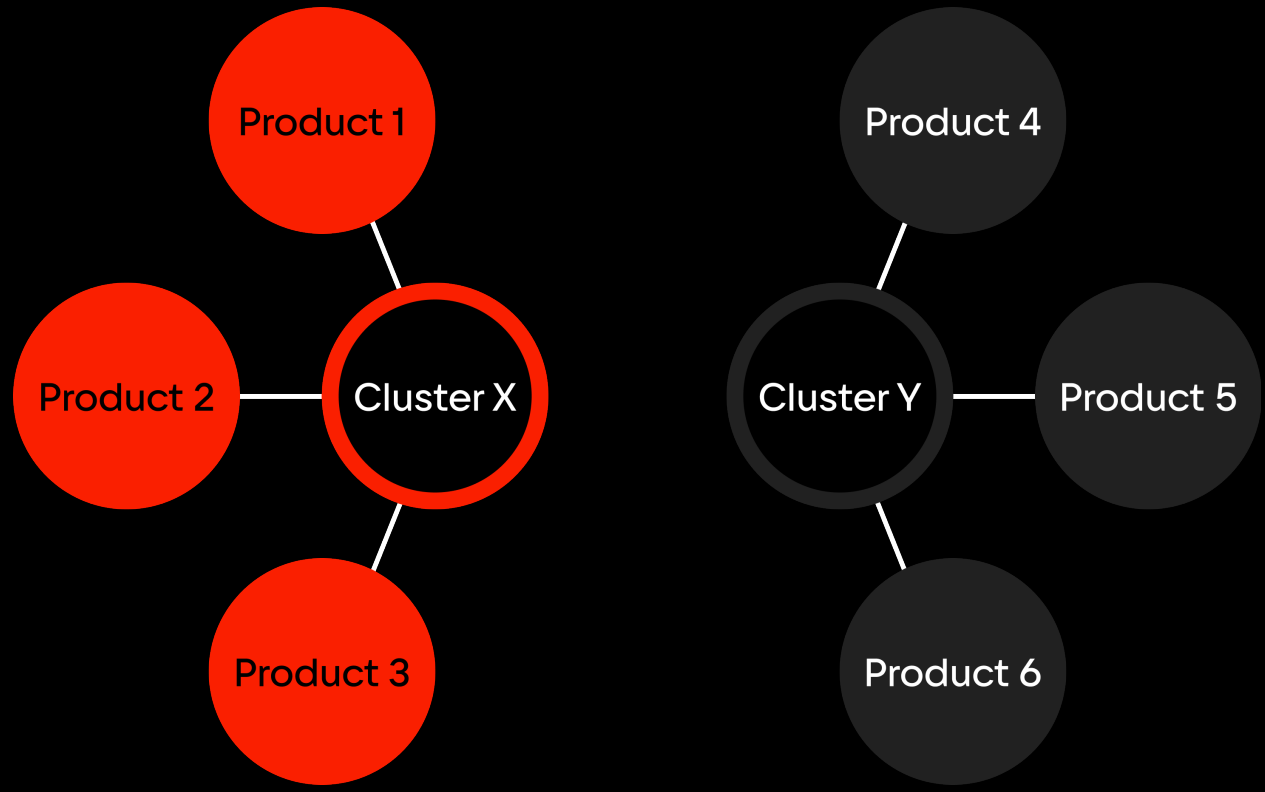
Структура кластеров и лидеров практик

Принципы формирования кластеров

СТО и лидеры практик

ЦК и ЦП

Преимущества этой модели для ИБ



Как выглядел сервис архитектуры ИБ

Продуктовая команда

Описывает сервис
и формирует HLD

Пытается понять,
что произошло,
и живет дальше

Архитектура ИБ

Дорабатывает HLD
и формирует
требования по ИБ

До

Поточный сервис архитектуры ИБ

+ Сервис работает

— Отсутствие понимания бизнес-контекста

— Отсутствие коннекта с продуктовыми командами

— Отсутствие доступа к бэклогу команд

— Отсутствие достаточных компетенций в нишевых технологиях

— Сложности при подсчете ресурсов во время масштабирования

— Несвоевременное включение в жизненный цикл ПО

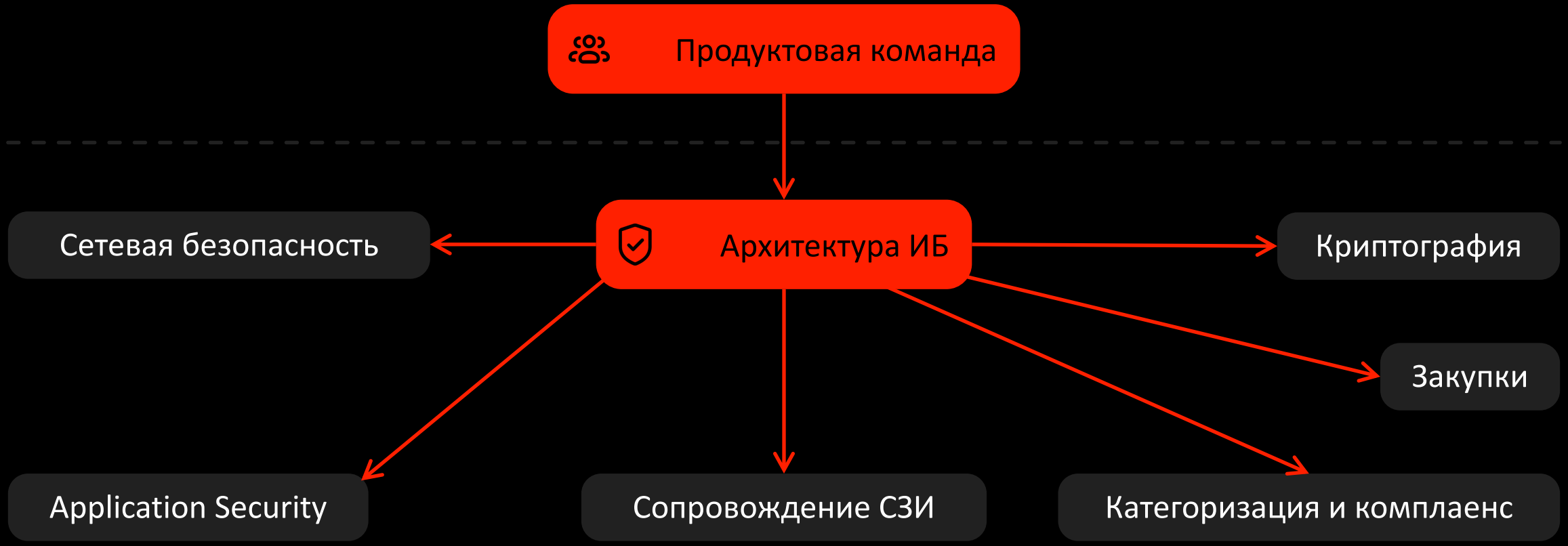
После

Единое входное окно по вопросам ИБ

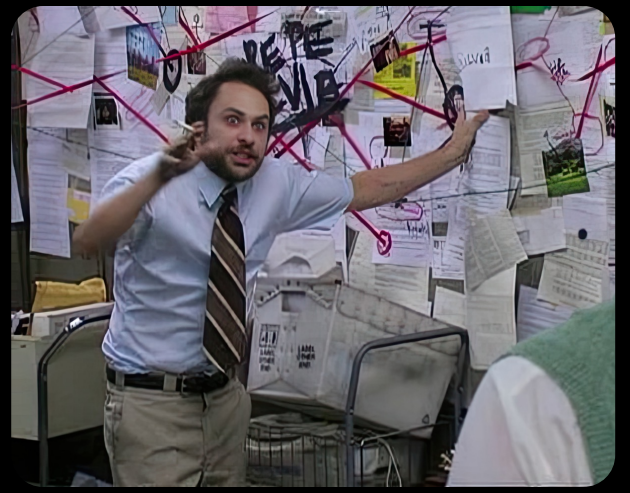
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

— [illegible]

Функции архитекторов ИБ
Роутинг



Функции архитекторов ИБ
Прикладные функции

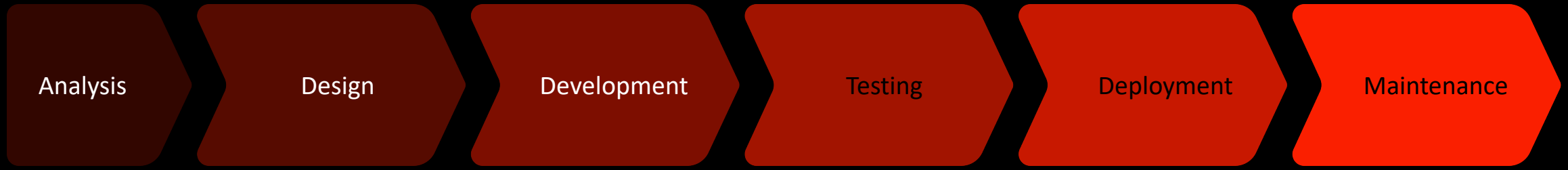


Интеграция в кластеры и процессы

- Выход на уровень лидеров практик
- Фиксация перечня продуктов за каждым из архитекторов ИБ
- Знакомство с СТО и членами команд продуктовой разработки
- Погружение в бизнес-контекст

Индивидуальный подход

- Единое входное окно
- Тесный контакт с командами и гибкий подход при формировании требований (относительно бэклога и статуса продукта)
- Security Business Partner, которого мы заслужили
- Широкий охват Secure SDLC (от планирования до продакшена)
- Ключевые компетенции под каждый кластер (mobile, IoT, etc.)
- Пресловутый Shift Left Security



До

Поточный сервис архитектуры ИБ

+ Сервис работает

— Отсутствие понимания бизнес-контекста

— Отсутствие коннекта с продуктовыми командами

— Отсутствие доступа к бэклогу команд

— Отсутствие достаточных компетенций в нишевых технологиях

— Сложности при подсчете ресурсов во время масштабирования

— Несвоевременное включение в жизненный цикл ПО

После

Единое входное окно по вопросам ИБ

+ Понимание бизнес-контекста

+ Тесный контакт с продуктовыми командами

+ Доступ к бэклогу команд

+ Проще подбирать релевантные компетенции под специфику продуктов

+ Легко считать ресурсы специалистов под каждый кластер

+ Своевременное включение в процесс

— Нужно время на полномасштабное масштабирование

Что нам и всем это дало

- Минимизация боли при взаимодействии с ИБ
- Упрощение жизни продуктовых команд
- Ускорение процессов согласований, решения вопросов и проблем
- Контроль всех процессов, связанных с безопасностью, и сроков
- Подстройка под бизнес-контекст
- Понимание ценности ИБ со стороны бизнеса/разработки
- Своевременное и централизованное подключение ИБ

На каком мы сейчас этапе

- Гибрид поточного сервиса и индивидуального подхода
- Построение своего ЦК
- Внедрение входного окна со стороны продукта — Security Champion
- Масштабирование архитектуры ИБ внутри кластеров

На каком мы сейчас этапе

- Освоение всех продуктовых кластеров
- Полноценное включение в стратегию компании со стороны архитектуры ИБ
- Создание гильдии Security Champion
- Оптимизация того, что уже есть

Какие были трудности

- Продажа идеи и донесение ценности до лидеров кластеров
- Налаживание контакта с командами разработки/эксплуатации
- Выделение зон ответственности внутри ИБ и описание ключевых процессов
- Своевременное масштабирование внутри кластеров

Вопросы и ответы

@ROMANPNN

«Пакет безопасности»
https://t.me/package_security