2 ИЮНЯ 2026, МОСКВА, ЛОФТ ГОЭЛРО

БЕКОН LUNTRY '26

ЕДИНСТВЕННАЯ КОНФЕРЕНЦИЯ ПО БЕЗОПАСНОСТИ КОНТЕЙНЕРОВ И КОНТЕЙНЕРНЫХ СРЕД

SecK8S: от хаоса к системе

Александр Черток | Альфа-Банк

БЕКОН'26

K8SSec:

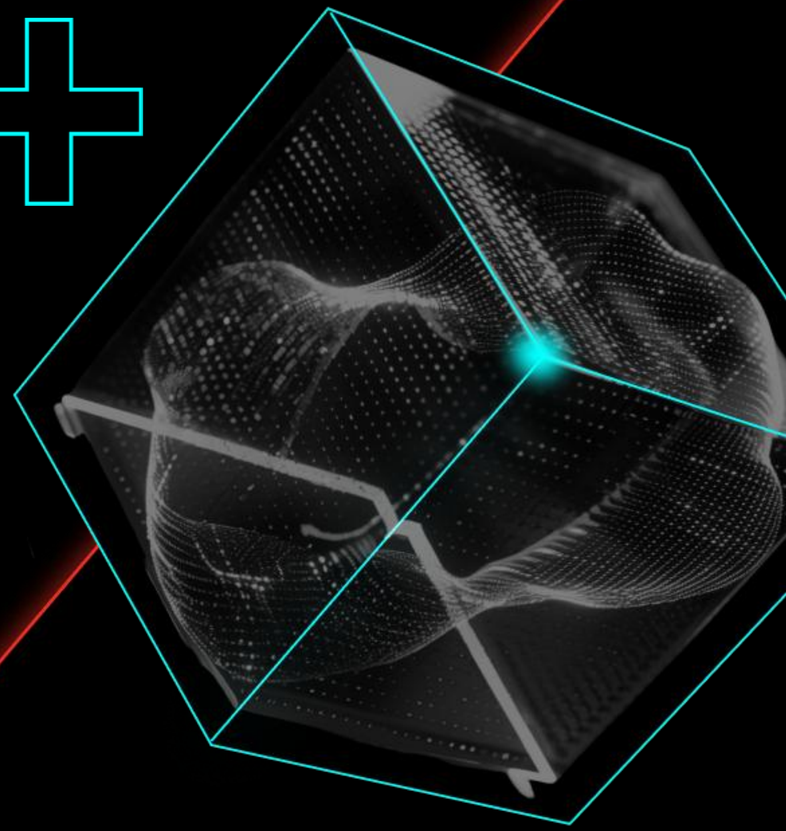
от хаоса к системе

Александр Черток

Руководитель отдела безопасности контейнерных
и облачных технологий, Альфа-Банк

КОНФЕРЕНЦИЯ ПО БЕЗОПАСНОСТИ КОНТЕЙНЕРОВ И КОНТЕЙНЕРНЫХ СРЕД

О себе



- В ИБ – более 10 лет
  И более 4-х лет именно K8S
- Работал в компаниях разного масштаба и специфики
- Сейчас рук. отдела безопасности контейнерных и облачных технологий
- С нуля построил команду, процессы
  и техстэк по ИБ K8S – продолжаю строить

Предисловие

>10 лет

6 июня 2014 года
первый коммит



2-й

Второй крупнейший OpenSource-проект в мире после ...



> 53 %

Более половины компаний в РФ используют ванильный K8S



[1] [2] [3]

Много или мало

Много тулов



100 тулов

И только под Security

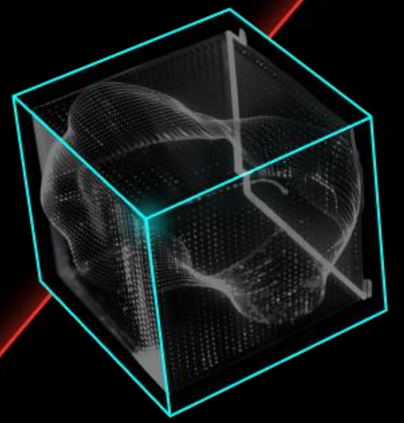
Много взломов

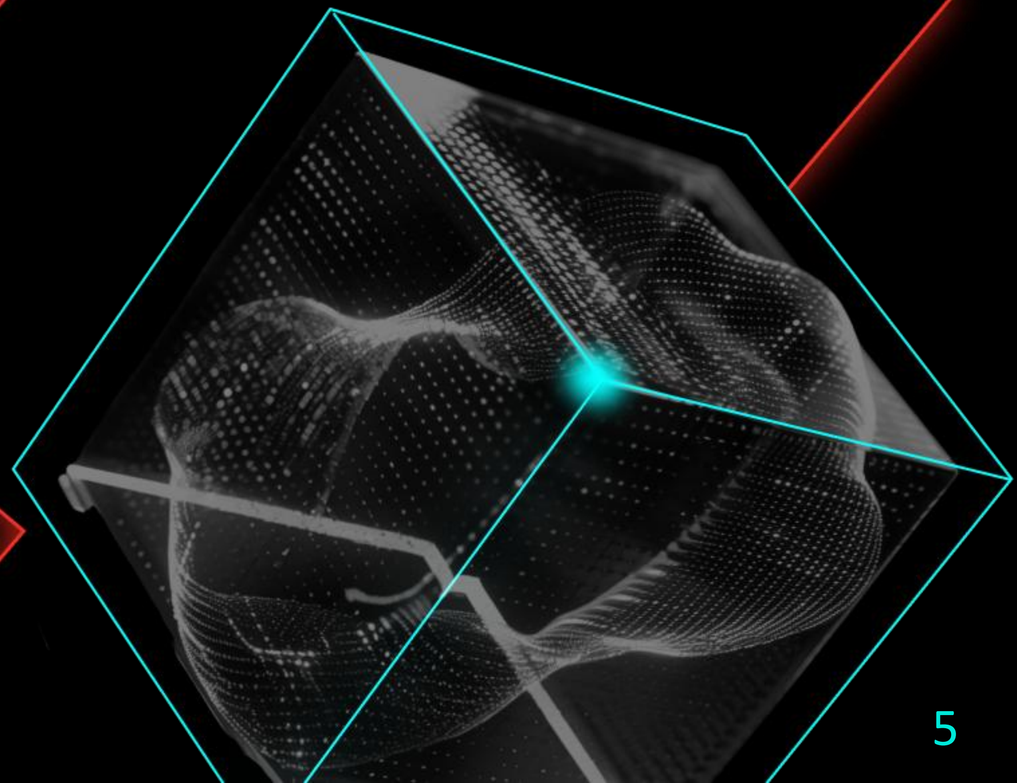
- 90% компаний имели инцидент связанный с K8S
- 46% компаний потеряли прибыль из-за инцидентов ИБ с K8S
- Рост атак +282% за год

[1] [2] [3] [4]

Проблема…

… не в инструментах, а в отсутствии системы





Что было?



- Сотни кластеров и команд – но мы о них не знаем
- Все требования общие, разные, не ясно как переложить на k8s
- Разные команды решали одну проблему по-разному
- Неразбериха с инструментами

Что делать?



- Процессы, которые реально работают
- Четкая зона ответственности
- Команда под задачу, а не «как получилось»
- Платформа вместо набора инструменто

Процессы



Процессы

01

Модель угроз

- Best practices
- Threat Intelligence
- Kill Chain

Процессы

01

Модель угроз

- Best practices
- Threat Intelligence
- Kill Chain

02

Требования

- Спецификации
- Рекомендации
- Паттерны
- Скрипты/Конфиги
- Регуляторика

Процессы

01

Модель угроз

- Best practices
- Threat Intelligence
- Kill Chain

02

Требования

- Спецификации
- Рекомендации
- Паттерны
- Скрипты/Конфиги
- Регуляторика

03

Экспертиза проектов

- Playbooks
- T-Shaped
- FAQ

Процессы

01

Модель угроз

- Best practices
- Threat Intelligence
- Kill Chain

02

Требования

- Спецификации
- Рекомендации
- Паттерны
- Скрипты/Конфиги
- Регуляторика

03

Экспертиза проектов

- Playbooks
- T-Shaped
- FAQ

04

Аудит

- Инвентаризация активов
- Выявление
- Валидация
- Устранение мисконфигов

Процессы

01

Модель угроз

- Best practices
- Threat Intelligence
- Kill Chain

02

Требования

- Спецификации
- Рекомендации
- Паттерны
- Скрипты/Конфиги
- Регуляторика

03

Экспертиза проектов

- Playbooks
- T-Shaped
- FAQ

04

Аудит

- Инвентаризация активов
- Выявление
- Валидация
- Устранение мисконфигов

05

Риски

- Модель оценки
- Модель приоритизации
- Меры митигации

Процессы

01
Модель угроз
- Best practices
- Threat Intelligence
- Kill Chain

02
Требования
- Спецификации
- Рекомендации
- Паттерны
- Скрипты/Конфиги
- Регуляторика

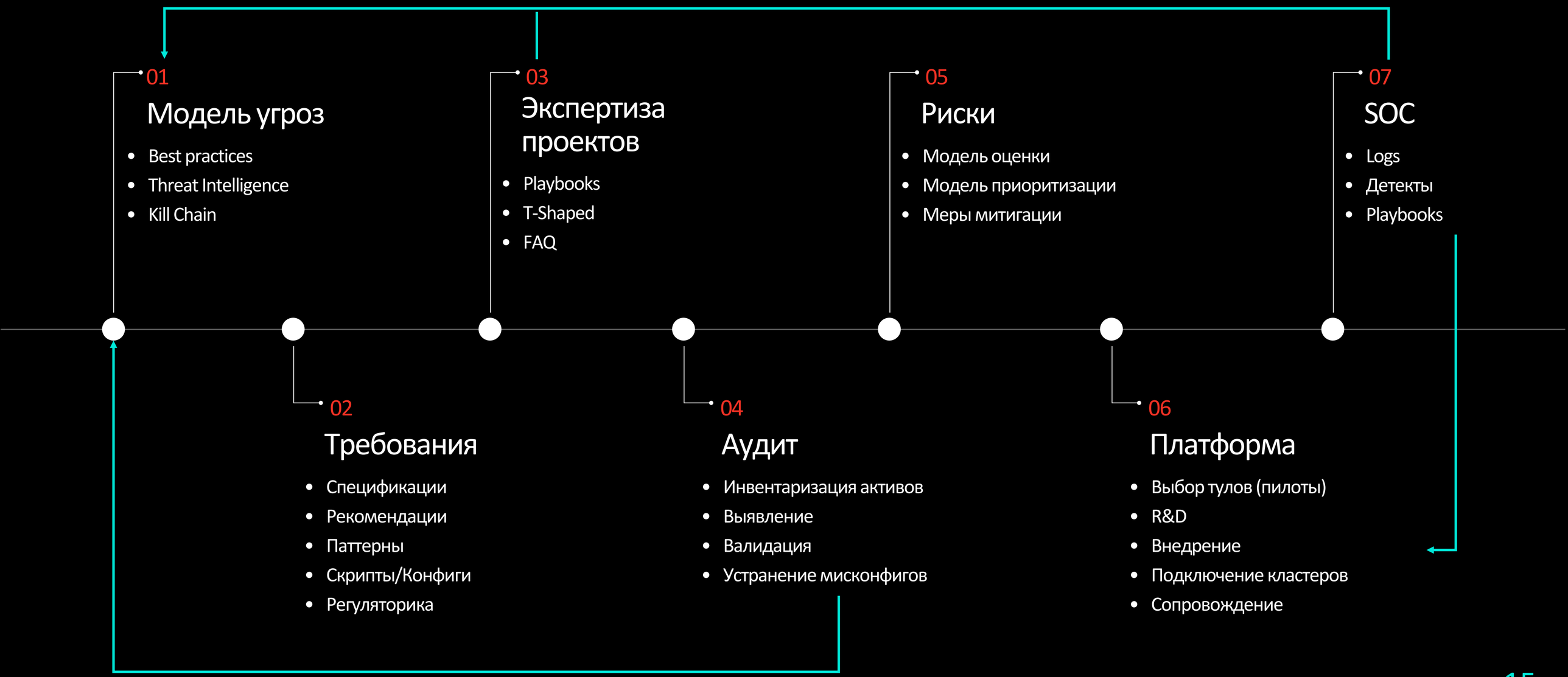
03
Экспертиза проектов
- Playbooks
- T-Shaped
- FAQ

04
Аудит
- Инвентаризация активов
- Выявление
- Валидация
- Устранение мисконфигов

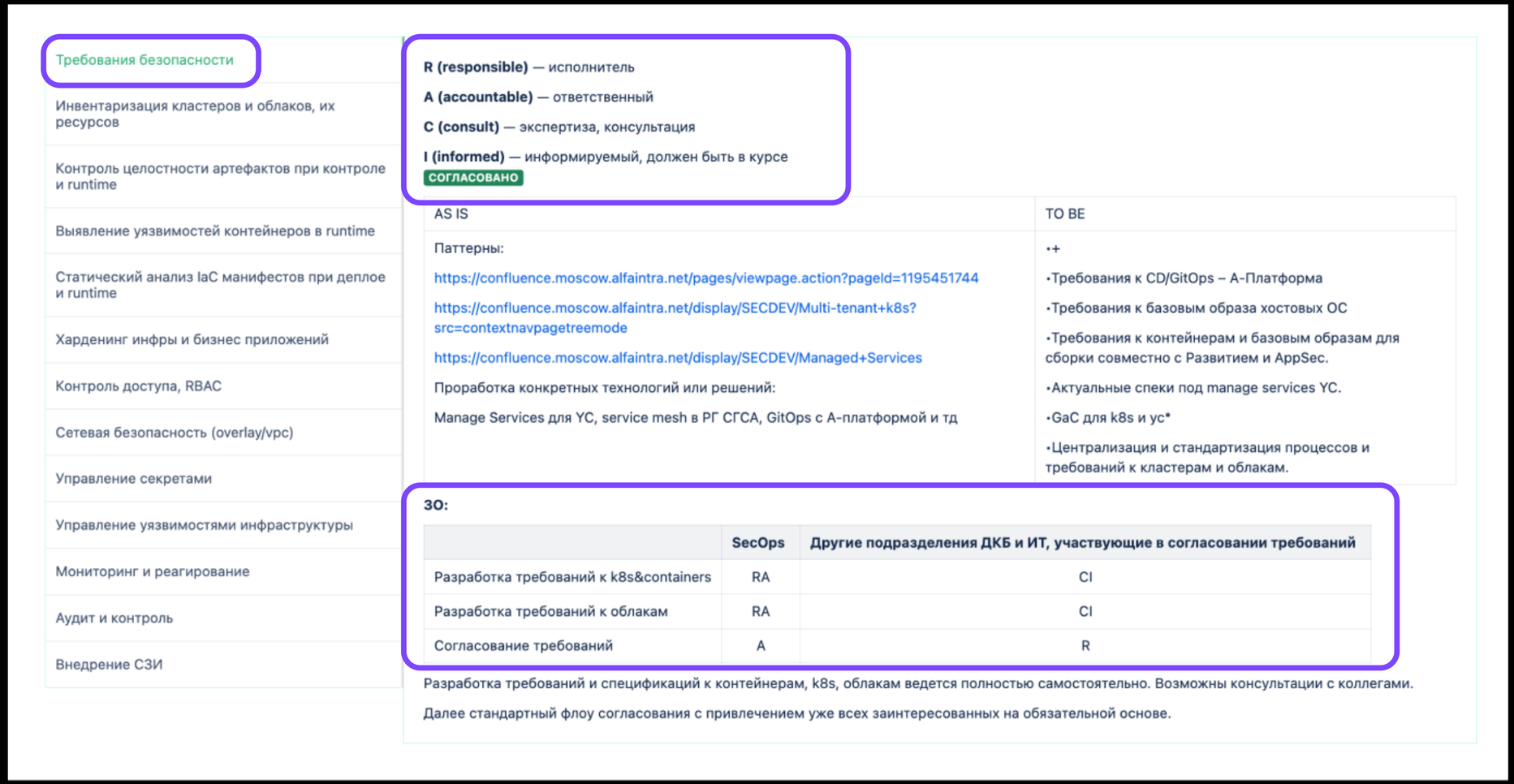
05
Риски
- Модель оценки
- Модель приоритизации
- Меры митигации

06
Платформа
- Выбор тулов (пилоты)
- R&D
- Внедрение
- Подключение кластеров
- Сопровождение

Процессы


01
Модель угроз
Best practices
Threat Intelligence
Kill Chain
02
Требования
Спецификации
Рекомендации
Паттерны
Скрипты/Конфиги
Регуляторика
03
Экспертиза проектов
Playbooks
T-Shaped
FAQ
04
Аудит
Инвентаризация активов
Выявление
Валидация
Устранение мисконфигов
05
Риски
Модель оценки
Модель приоритизации
Меры митигации
06
Платформа
Выбор тулов (пилоты)
R&D
Внедрение
Подключение кластеров
Сопровождение
07
SOC
Logs
Детекты
Playbooks

Зона ответственности



Требования безопасности

- Инвентаризация кластеров и облаков, их ресурсов
- Контроль целостности артефактов при контроле и runtime
- Выявление уязвимостей контейнеров в runtime
- Статический анализ IaC манифестов при деплое и runtime
- Харденинг инфры и бизнес приложений
- Контроль доступа, RBAC
- Сетевая безопасность (overlay/vpc)
- Управление секретами
- Управление уязвимостями инфраструктуры
- Мониторинг и реагирование
- Аудит и контроль
- Внедрение СЗИ

R (responsible) — исполнитель

A (accountable) — ответственный

C (consult) — экспертиза, консультация

I (informed) — информируемый, должен быть в курсе

СОГЛАСОВАНО

AS IS	TO BE
Паттерны:	•+
https://confluence.moscow.alfaintra.net/pages/viewpage.action?pageId=1195451744	•Требования к CD/GitOps – A-Платформа
https://confluence.moscow.alfaintra.net/display/SECDEV/Multi-tenant+k8s?src=contextnavpagetreemode	•Требования к базовым образа хостовых ОС
https://confluence.moscow.alfaintra.net/display/SECDEV/Managed+Services	•Требования к контейнерам и базовым образам для сборки совместно с Развитием и AppSec.
Проработка конкретных технологий или решений:	•Актуальные спеки под manage services YC.
Manage Services для YC, service mesh в РГ СГСА, GitOps с A-платформой и тд	•GaC для k8s и yc*
	•Централизация и стандартизация процессов и требований к кластерам и облакам.

ЗО:

	SecOps	Другие подразделения ДКБ и ИТ, участвующие в согласовании требований
Разработка требований к k8s&containers	RA	CI
Разработка требований к облакам	RA	CI
Согласование требований	A	R

Разработка требований и спецификаций к контейнерам, k8s, облакам ведется полностью самостоятельно. Возможны консультации с коллегами.

Далее стандартный флоу согласования с привлечением уже всех заинтересованных на обязательной основе.

*Устаревшая для примера

ЗО. Модель угроз

K8S Sec

Threat Intellegence Intellegence

Помимо внешних источников используйте внутренние

- Pentests
- Аномалии

K8S Sec

Связка с требованиями и тулами

Покрытие требованиями

Покрытие тулами

K8S Sec

Kill Chain

Сценарии реализации угроз

*ЗО – Зона Ответственности

ЗО. Модель угроз

	K8S Sec	Смежные команды ИБ	ИТ
TI	RA	C	I
Покрытие тулами	RA	CI	I
Сценарии	RA	CI	CI

*ЗО – Зона Ответственности

ЗО. Требования

K8S Sec

Спецификации и рекомендации

Важно не только что, но и как

K8S Sec

+ Arch

Паттерны

Single-Tenant Cluster

Multi-Tenant Cluster

K8S Sec

+ DevOps

Скрипты/ Конфиги

Раскатка – роли

Политики

Чарты

Методо-логи

Регуляторика

ФСТЭК

ЦБ

*ЗО – Зона Ответственности

ЗО. Требования

	K8S Sec	Архи-тектура	Dev Ops	Методо-логи
Спецификации и рекомендации	RA	C	I	CI
Паттерны	R	A	CI	CI
Скрипты/ Конфиги	RA		CI	
Регуляторика	CI			RA

*ЗО – Зона Ответственности

ЗО. Экспертиза проектов

K8S Sec

+ BP

Playbooks + сама экспертиза экспертиза

Что можно согласовать без вас
и как это сделать

Консультации с BP

K8S Sec

T-shaped

Чтобы представлять полный контекст

K8S Sec

FAQ

Меньше созвонов и переписок —больше времени

*ЗО – Зона Ответственности

ЗО. Экспертиза проектов



*ЗО – Зона Ответственности

ЗО. Аудит

K8S Sec

Выявление мисконфигов

Автоматизированно

В ручном режиме

K8S Sec

+ BP + DevOps

Валидация

Дедупликация

Выявление false positive

Исключения

K8S Sec

+ BP + DevOps

Устранение

Рекомендации/ меры митигации

SLA

Ретесты

DevOps

+ K8S Sec

Инвентаризация активов

Сколько кластеров

Мониторинг новых кластеров

Что внутри кластера

*ЗО – Зона Ответственности

ЗО. Аудит

	K8S Sec	BP	DevOps
Выявление мисконфигов	RA	I	I
Валидация	ACI	I	R
Устранение	ACI	CI	R
Инвентаризация активов	CI		RA

*ЗО – Зона Ответственности

ЗО. Риски

Риски

Модель оценки

Качественная и кол-ая оценка рисков

K8S Sec

Меры митигации

*ЗО – Зона Ответственности

ЗО. Риски



*ЗО – Зона Ответственности

ЗО. Платформа

K8S Sec

R&D/Пилоты

- Инструменты
- Подходы
- Меры
- Варианты реализации

K8S Sec

Внедрение

- Согласование проекта
- Разворачивание инфры
- Разворачивание решения
- Согласование процесса

K8S Sec

Подпроцессы

- Подключение кластеров
- Дебаг
- Интеграции

K8S Sec

Сопровождение

- Системное
- Функциональное
- Процессное
- Консультативное

*ЗО – Зона Ответственности

ЗО. Платформа

	K8S Sec	ИТ	Смежные команды ИБ
R&D/Пилоты	RA	C	I
Внедрение	RA	C	CI
Подпроцессы	RA	I	CI
Сопровождение	RA	C	

*ЗО – Зона Ответственности

ЗО. SOC

K8S Sec

+ DevOps

Logs

Требования

Политика (AuditPolicy)

Инструкции

Сборка

K8S Sec

Детекты

Сигнатуры

Playbooks

SOC

+ K8SSec

Реагирование

Фактическая регистрация

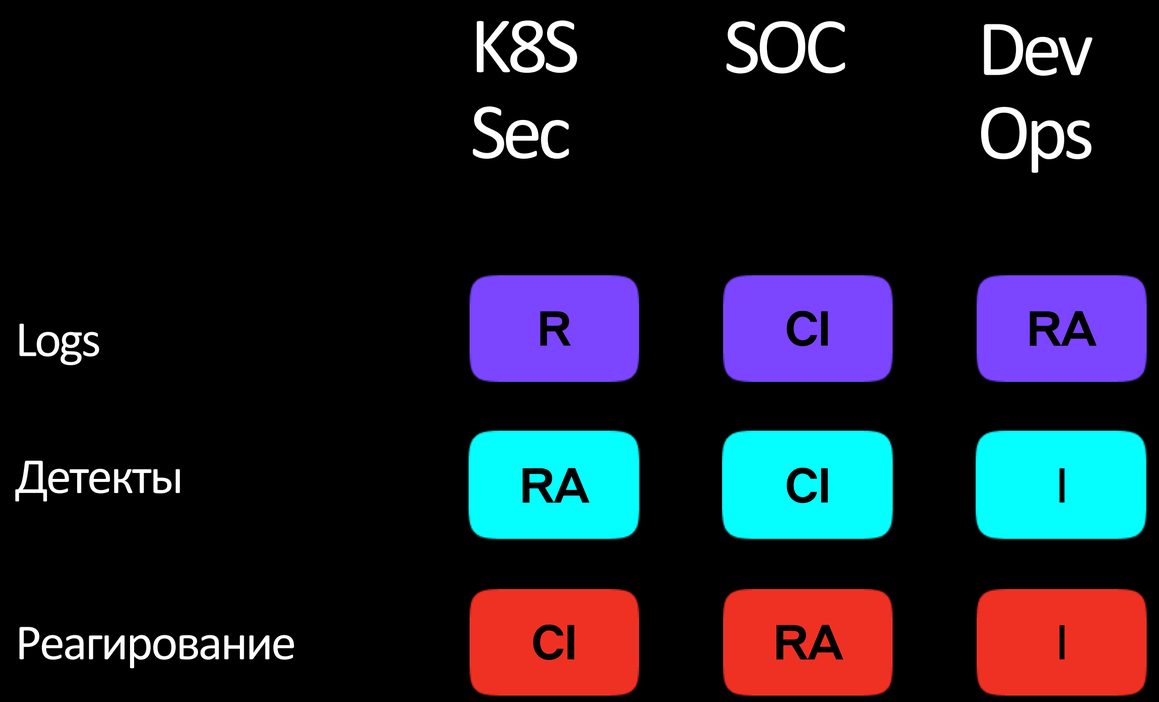
Обработка

Реагирование

Расследование

*ЗО – Зона Ответственности

ЗО. SOC



*ЗО – Зона Ответственности

Компетенции. K8S Sec

Security

Моделирование угроз

Требования

Риски

Soft Skills



Dev

Автоматизация (аудит)

Интеграции

DevOps

Платформа

Спеки/конфиги

CI/CD

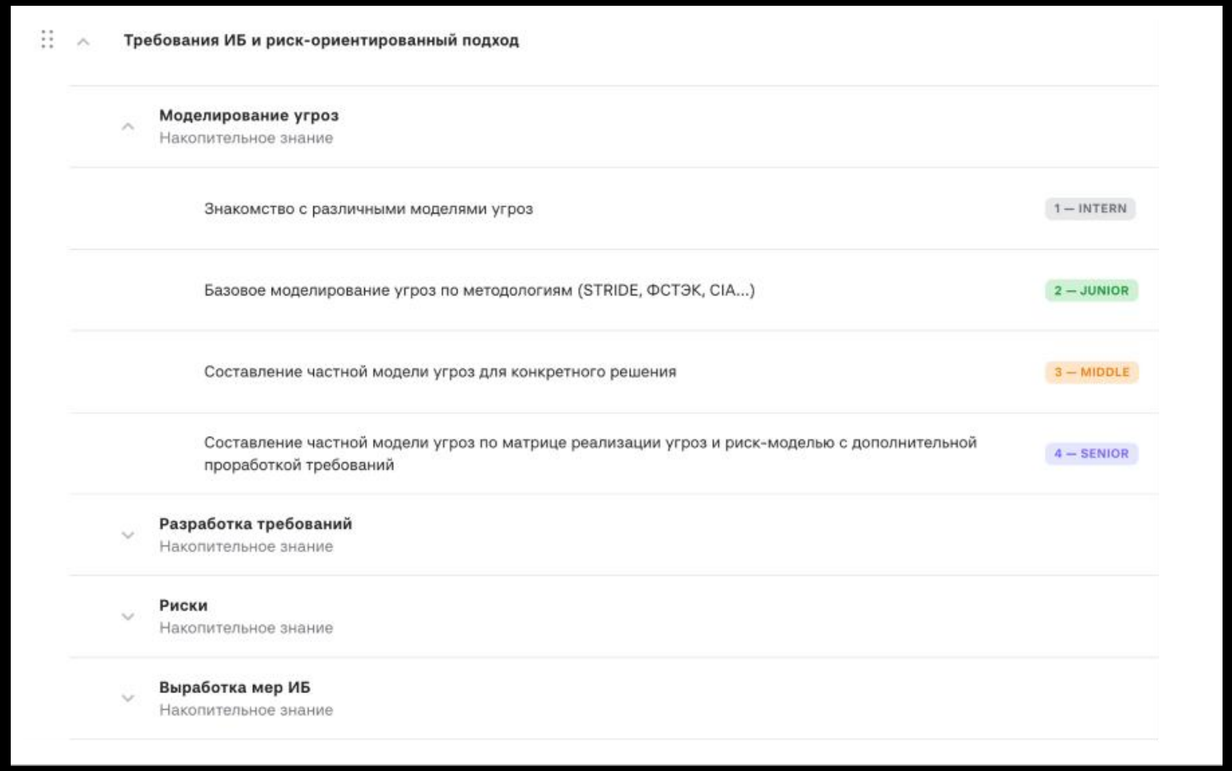
Архитектура

Паттерны

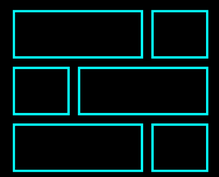
Картинка взята из фильма «Doctor Strange», 2016 г.

Компетенции. Пример

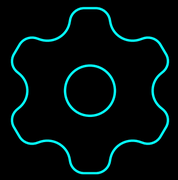
- Soft skills
- Hard skills
- Специфика



Процессы + Компетенции = Роли



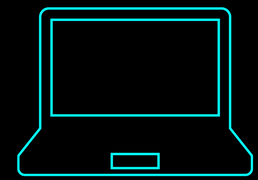
K8S Security Architect
Architect



K8S Security
Analyst/Engineer



K8S Auditor



DevOps

K8S Security Architect



Проработка, внедрение и развитие процессов



Проектирование решений под процессы/Паттерны



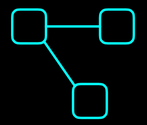
Формирование требований



Сопровождение команд / Анализ проектов



Участие в оценке рисков



Сопровождение совместных проектов со смежными подразделениями и ИТ

K8S Security Architect

01

Модель угроз

- Best practices
- Threat Intelligence
- Kill Chain

02

Требования

- Спецификации
- Рекомендации
- Паттерны
- Скрипты/Конфиги
- Регуляторика

03

Экспертиза проектов

- Playbooks
- T-Shaped
- FAQ

05

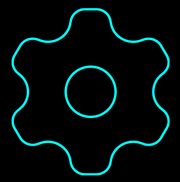
Риски

- Модель оценки

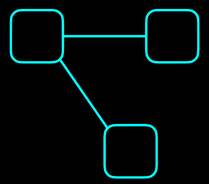
K8S Security Analyst/Engineer



Актуальность политик набора инструментов



Тестирование, выявление аномалий



Сопровождение и развитие процесса подключения кластеров к Платформе



Взаимодействие с SOC



Пилоты/R&D

K8S Security Analyst/Engineer

07

SOC

- Logs
- Детекты
- Playbooks

02

Требования

- Спецификации
- Рекомендации
- Скрипты/Конфиги

06

Платформа

- Выбор тулов (пилоты)
- R&D
- Внедрение
- Подключение кластеров

K8S Auditor



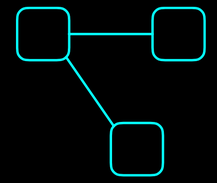
Развивает методы и инструменты выявления уязвимостей



Сопровождает процесс валидации и устранения



Прорабатывает меры митигации



Взаимодействие со смежными командами (BP)

Процессы

01

Модель угроз

- Best practices
- Threat Intelligence
- Kill Chain

02

Требования

- Спецификации
- Рекомендации
- Регуляторика

04

Аудит

- Инвентаризация активов
- Выявление
- Валидация
- Устранение мисконфигов

05

Риски

- Меры митигации

06

Платформа

- Выбор тулов (пилоты)

DevOps

Системное и функциональное сопровождение Платформы

Построение CI/CD Платформы

Мониторинг

Сопровождение пилотов

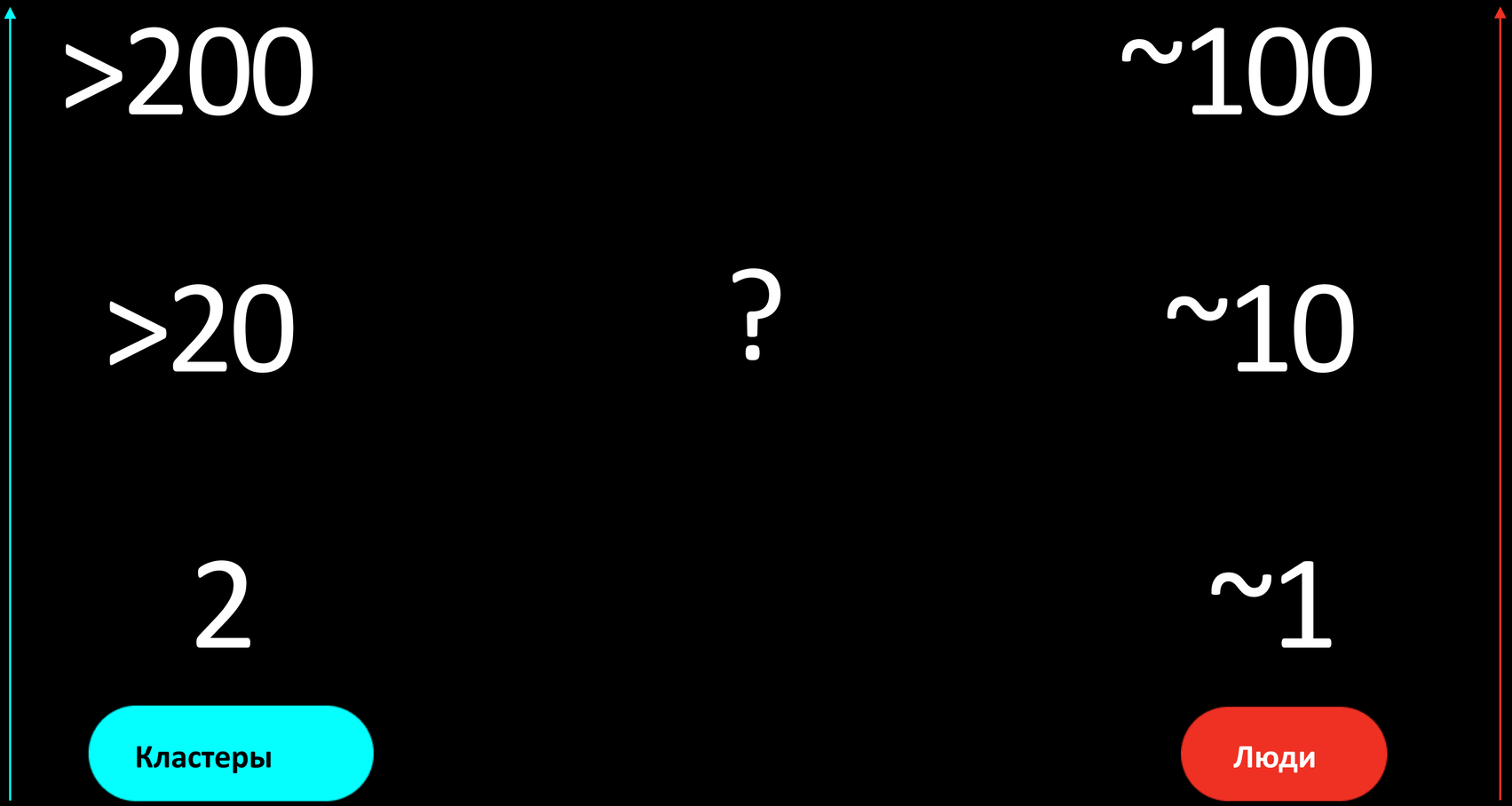
Процессы

06

Платформа

- Выбор тулов (пилоты)
- R&D
- Внедрение
- Подключение кластеров
- Сопровождение

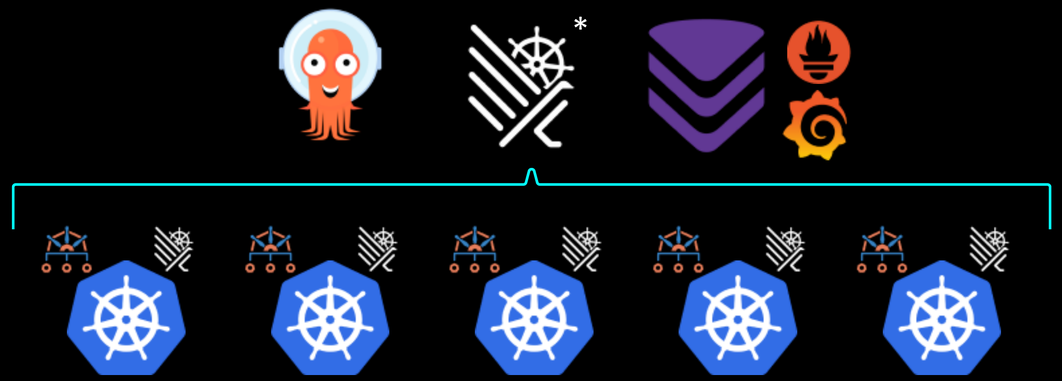
Много или мало



Платформа

Jira

CI/CD-platform





ASOC

SIEM
SOC

В каждый кластер ставится только
агент CSP, который автоматически подключается к единому центру управления

Плюсы

1. Мониторинг и контроль (реагирование на инциденты везде)
2. Управляемость (можем управлять нашими агентами)
3. Централизация
4. Масштабируемость (подключение любого кол-ва кластеров и/или инструментов
5. Скорость
6. Интеграции
7. И др.

Минусы

1. Технологически сложно

* Другие коммерческие/OS решения

Сканер



[redacted]yrfd

Параметры | Уязвимости | Связанные активы | Сканирования

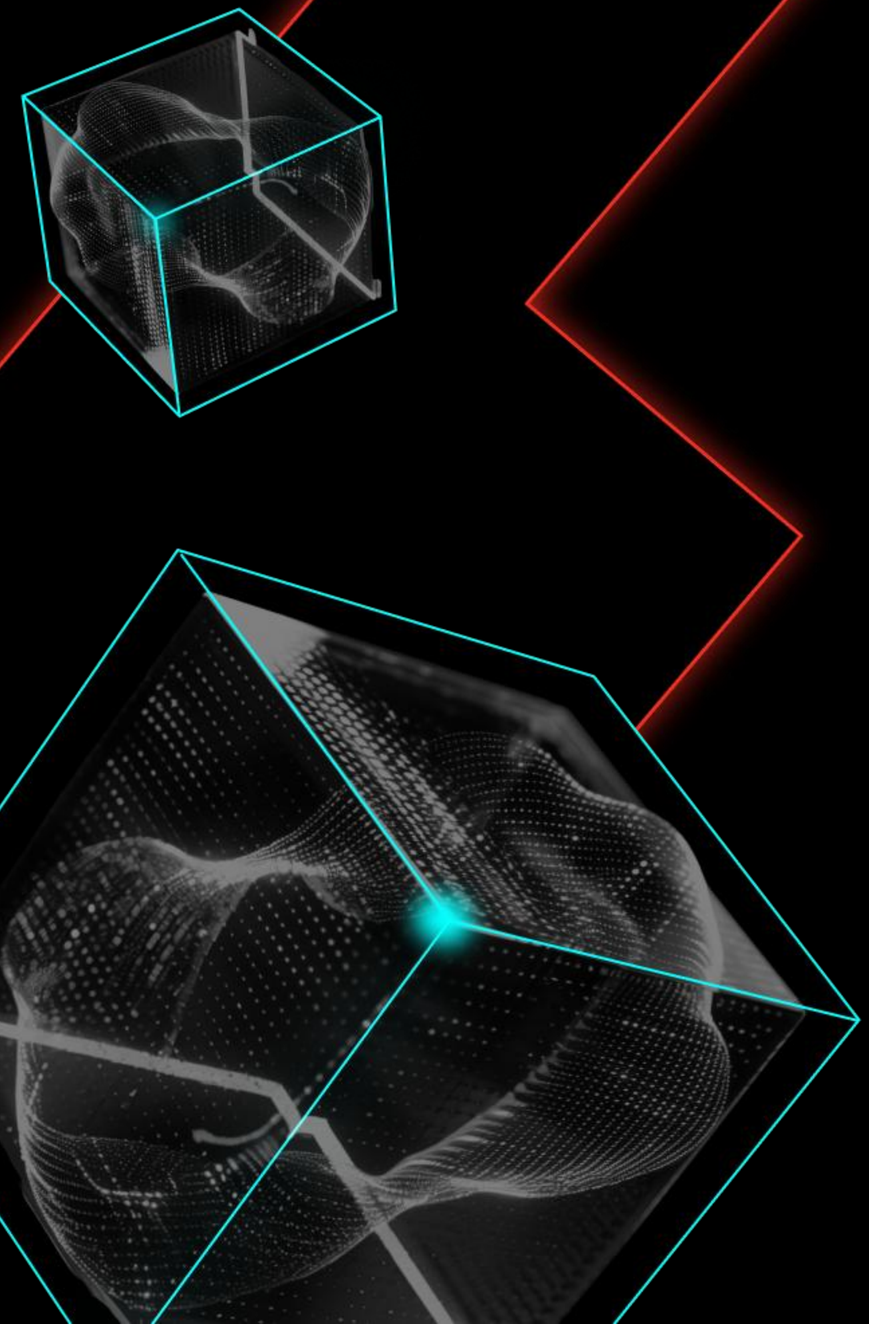
Типы активов: **Выбрано 5** | Активы: [redacted]yrfd

Выбрано 0 из 40

НАЗВАНИЕ УЯЗВИМОСТИ	УР. КРИТИЧ.	ПУТЬ	ТИП		ИСП.
Сетевые политики Kubernetes	Высокий	undefined (-)	НАРУ...	0	ЧА
CIS Kubernetes Benchmark: конфигурация кластера	Высокий	undefined (-)	НАРУ...	0	ЧА
ServiceAccount в namespace бизнес-сервисов	Высокий	undefined (-)	НАРУ...	0	ЧА
3.1.8. Привязка к роли cluster-admin на уровне пространства имен	Высокий	undefined (-)	НАРУ...	0	ЧА

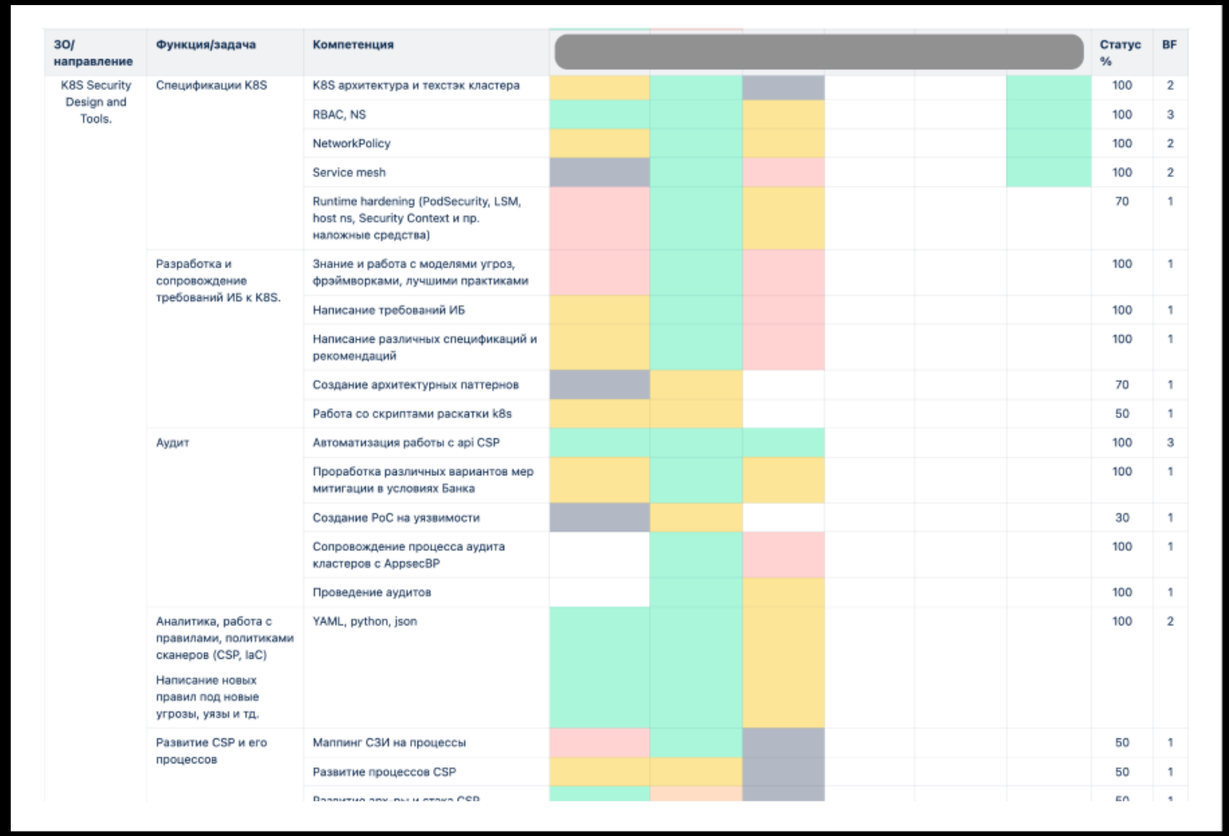
Масштабируемся
не ~~людьми~~ линейно

- Процессы
- Зоны ответственности
- Платформа / автоматизация



К чему пришли?

- Определили
  Что необходимо делать —
  Процессы
- Определили Как именно делать —
  подпроцессы/
  задачи/зо
- Определили Что требуется для этого
  — компетенция
- Определили Роли
- Сформировали
  и оценили команду



ЗО/ направление	Функция/задача	Компетенция	Статус %	BF
K8S Security Design and Tools.	Спецификации K8S	K8S архитектура и техстэк кластера	100	2
		RBAC, NS	100	3
		NetworkPolicy	100	2
		Service mesh	100	2
		Runtime hardening (PodSecurity, LSM, host ns, Security Context и пр. наложные средства)	70	1
	Разработка и сопровождение требований ИБ к K8S.	Знание и работа с моделями угроз, фрэймворками, лучшими практиками	100	1
		Написание требований ИБ	100	1
		Написание различных спецификаций и рекомендаций	100	1
		Создание архитектурных паттернов	70	1
		Работа со скриптами раскатки k8s	50	1
	Аудит	Автоматизация работы с api CSP	100	3
		Проработка различных вариантов мер митигации в условиях Банка	100	1
		Создание PoC на уязвимости	30	1
		Сопровождение процесса аудита кластеров с AppsecBP	100	1
		Проведение аудитов	100	1
	Аналитика, работа с правилами, политиками сканеров (CSP, IaC) Написание новых правил под новые угрозы, уязы и тд.	YAML, python, json	100	2
	Развитие CSP и его процессов	Маппинг СЗИ на процессы	50	1
		Развитие процессов CSP	50	1

Метрики успеха

Сотни кластеров, и мы всех знаем - покрытие инструментами 90+%

На каждую проблему у нас есть решение – мы видим каждый новый проект, который едет в кластер

1 тикет – 1 пайплайн автоматизации – пара команд в kubectl – 5 минут и кластер у нас. А с платформой автоматически.

Аудит кластера - это нажатие пары кнопок

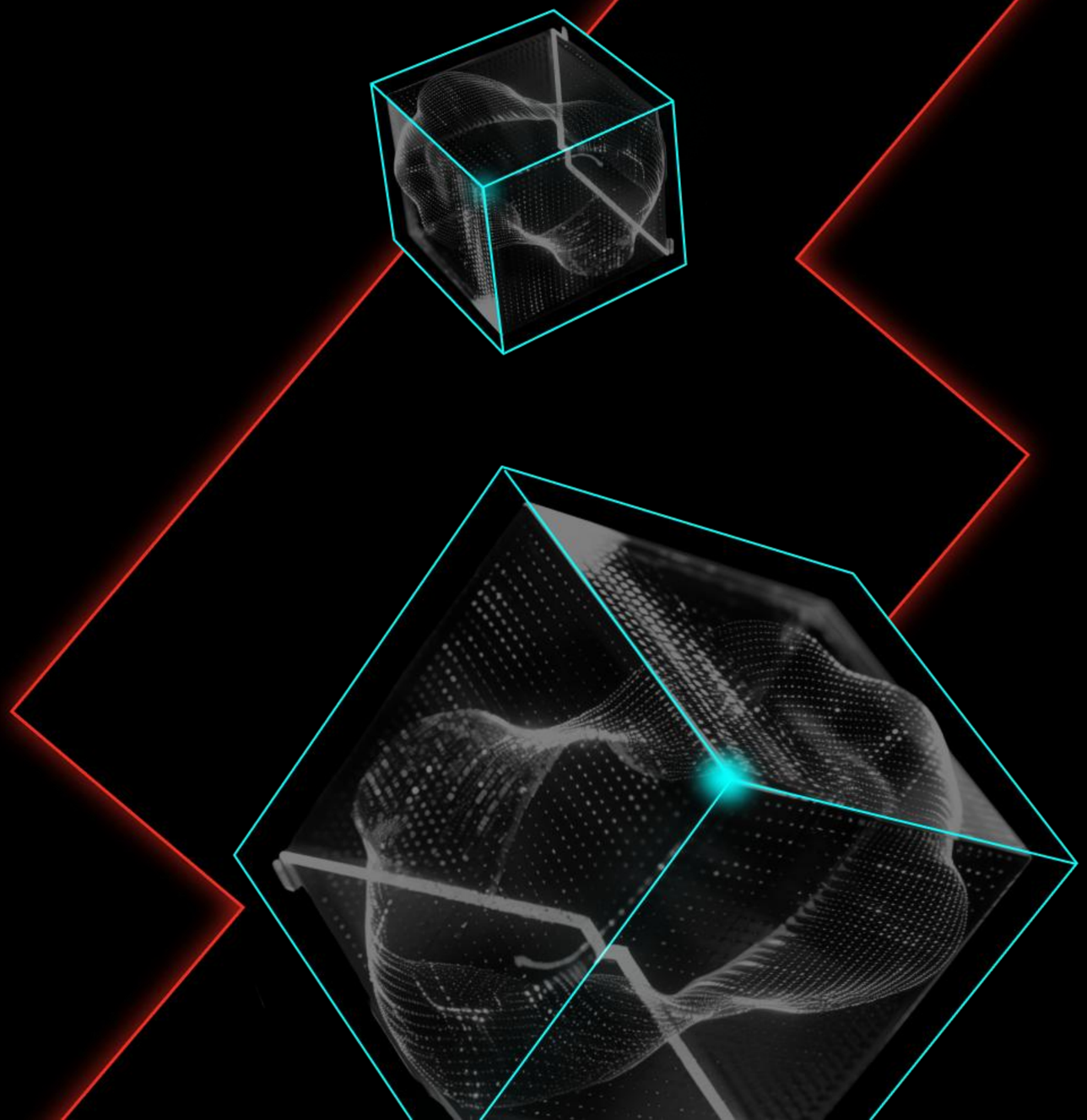
Знаем что делать, если какое-то требование не выполнимо (риски)

Знаем, где у нас узко, а где у нас уже отлично

Какие были факапы

Так делать не надо

- Думать, что вот мы один кластер причешем и сразу ко второму перейдем — так всё и успеем
- Готовить коммерческий продукт легко, open-source возьму просто и запущу
- Всё сами сделаем, напишем скрипты, затриажим кластера
- Всё автоматизируем



БЕКОН'26

КОНФЕРНЦИЯ ПО БЕЗОПАСНОСТИ КОНТЕЙНЕРОВ И КОНТЕЙНЕРНЫХ СРЕД

Про BP

bekon.luntry.ru

@ARTDEEPITECH

Про Multi-tenant