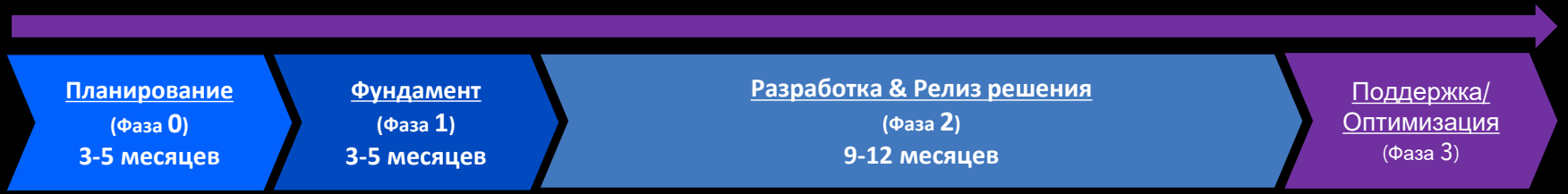
Методология построения Security Operations Center

Дмитрий Ячевский
Руководитель направления IBM Security в странах Средней Азии

SOC как фазовый подход к проекту трансформации

SOC начинается с Фазы 0 ”Основание”, включающей в себя создание стратегии и плана трансформации SOC к заданному совместно с Заказчиком целевому состоянию.



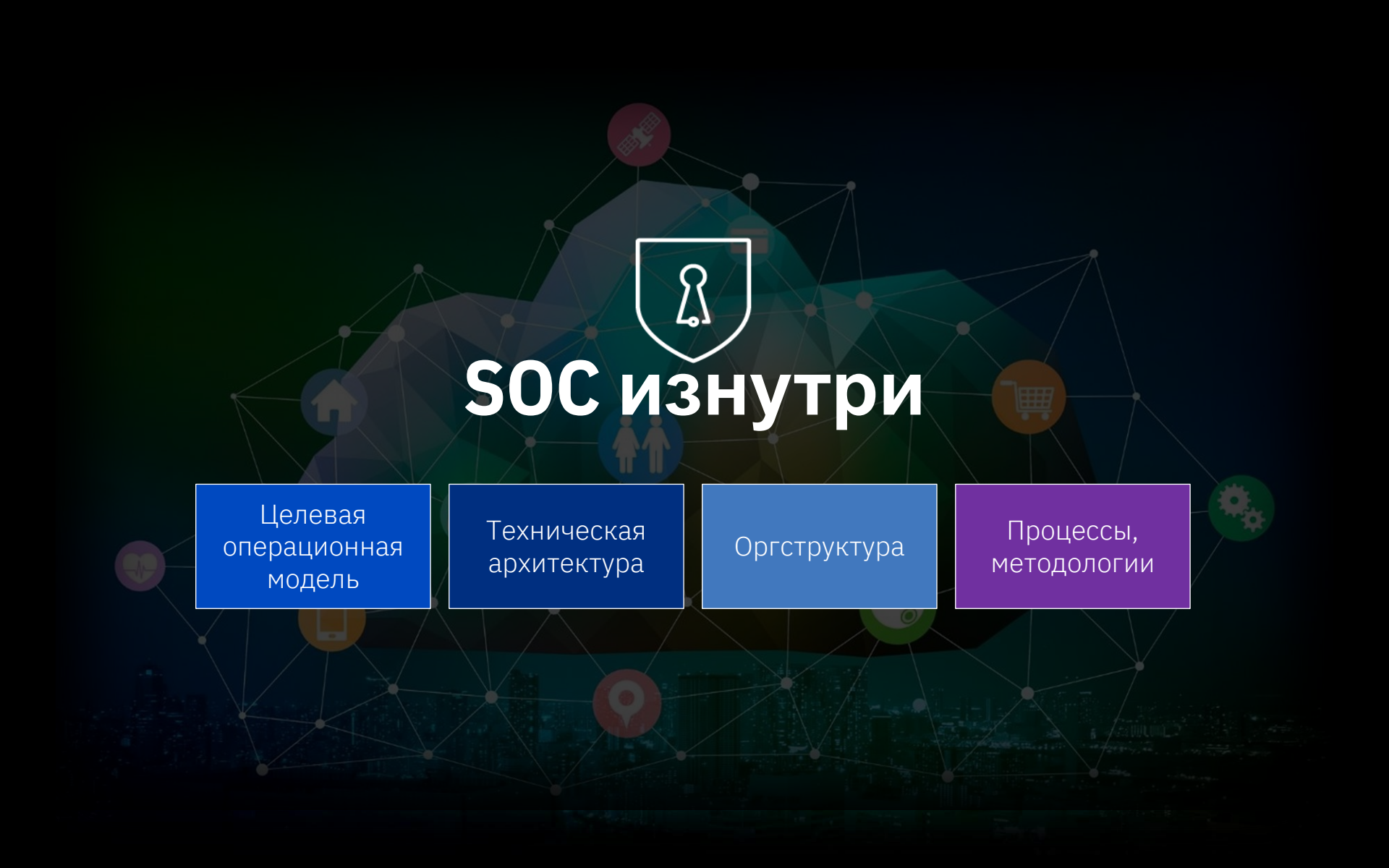
Определение задач SOC
Определение ключевых компонент
Валидация текущей инфраструктуры
Целевая операционная модель
План трансформации SOC и дорожная карта

Внедрение корневых компонентов SOC (SIEM, отчётность, работа с заявками)
Организация работы дежурной смены и базовых процессов мониторинга инцидентов ИБ.

Организация и запуск в работу подразделений инженерной поддержки и аналитики киберугроз. Внедрение новых процессов.
Оптимизация и внедрение новой технической архитектуры SOC, добавление передовых технологий, включая: Forensics, Flow integration, Vulnerability management, BigData Store.
Централизация инцидентов для обеспечения полной готовности
Добавление полного спектра глобальных источников о кибератаках
Использование IBM Use Case Library/Framework

Приоритизация инцидентов
Предиктивная аналитика
Внедрение процессов
Добавление бизнес-контекста
Обучение команды

Предлагаемый проектный подход предполагает, что по окончанию каждой проектной фазы, начиная с фазы 1, Заказчик получает ***функционирующий и выполняющий продуктивные задачи*** SOC различных уровней зрелости.



SOC изнутри

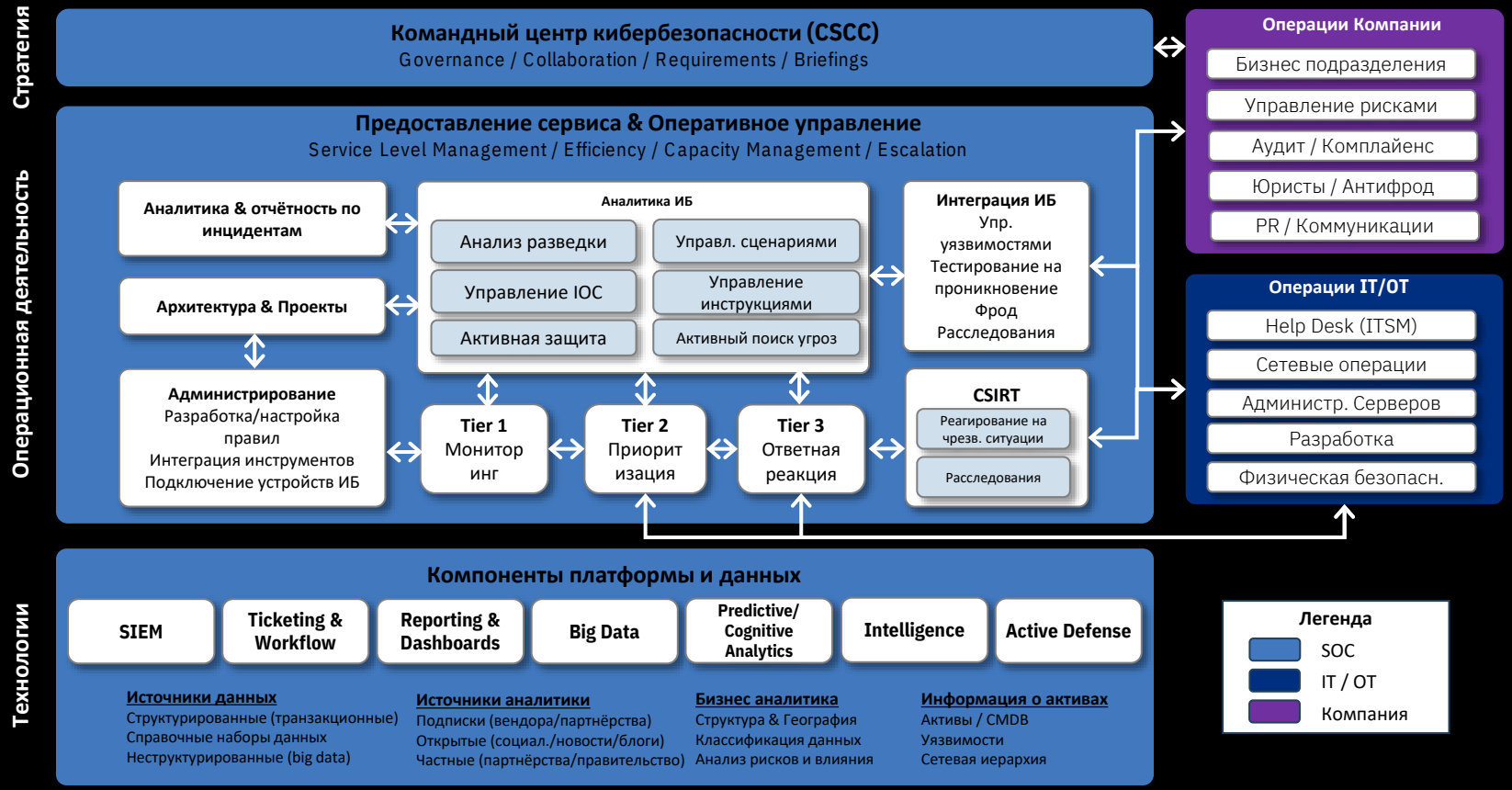
Целевая операционная модель

Техническая архитектура

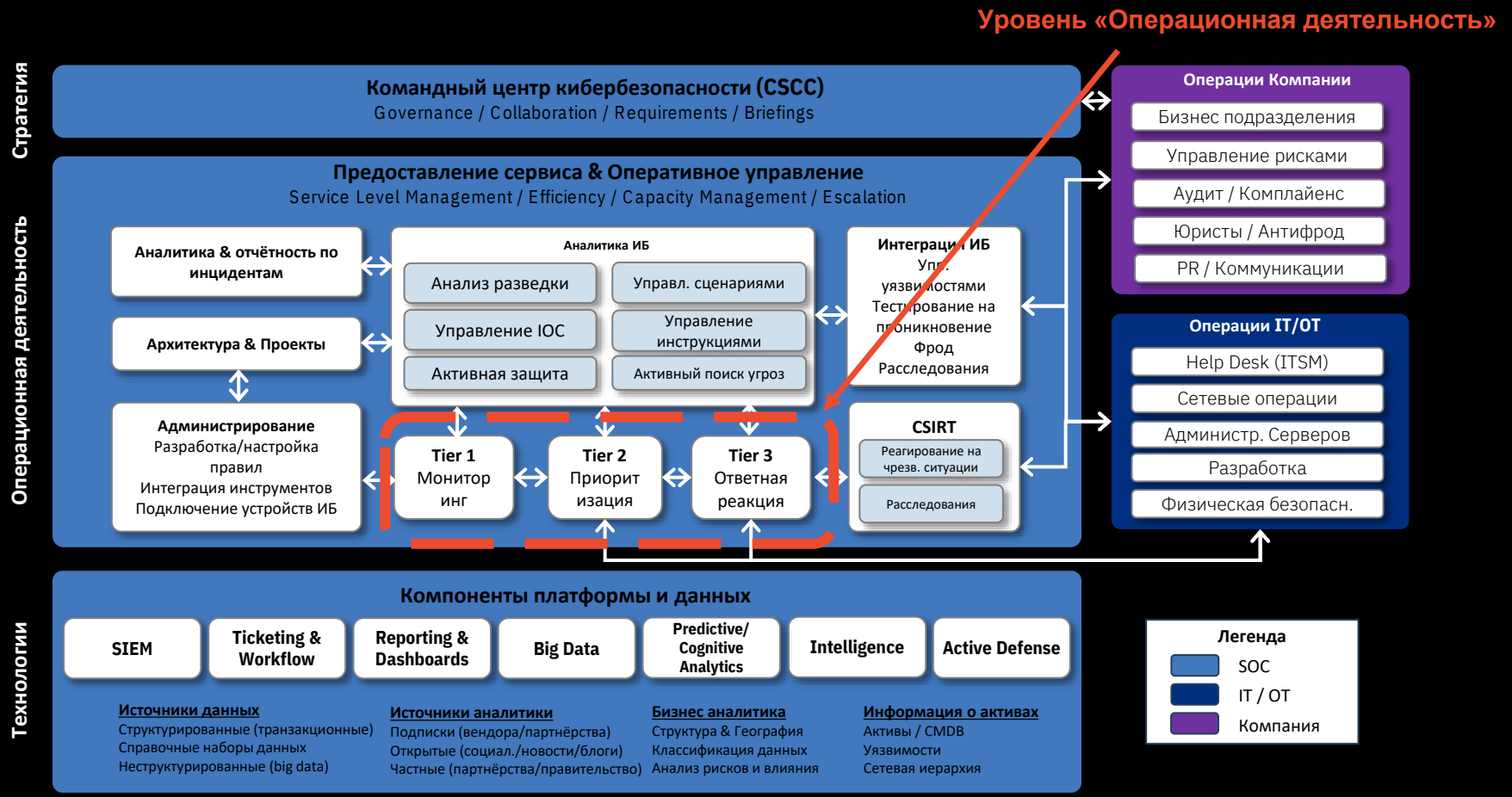
Оргструктура

Процессы, методологии

Целевая модель для построения SOC нового поколения



Целевая модель для построения SOC нового поколения



Целевая модель для построения SOC нового поколения

Целевая модель для построения SOC нового поколения

Методология UseCase - подход «Сверху вниз» при разработке правил реагирования

1. Бизнес определяет релевантные риски и угрозы
2. SOC обеспечивает мониторинг реализации этих угроз **посредством сценариев (Use Case) и правил SIEM**
3. При обнаружении реализации угрозы регистрируется инцидент
4. Инцидент обрабатывается согласно определённым приоритетам

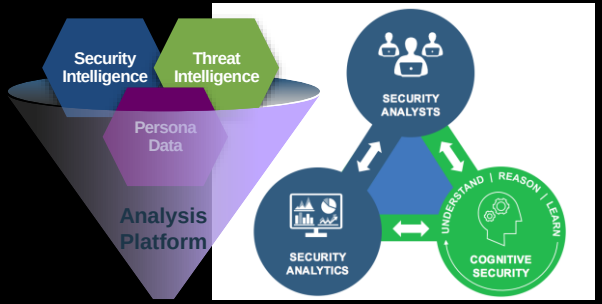
SOC и технологии

- Сбор и анализ логов
- Реагирование на инциденты
- Автоматизация процессов
- Обмен данными

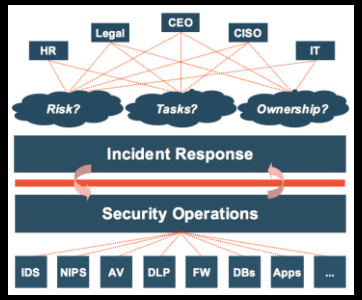
Ключевые технологические компоненты SOC

1 SIEM/Аналитика ИБ

2 Когнитивная аналитика и бизнес аналитика



3 Реакция на инциденты ИБ



4 Киберразведка и аналитика по угрозам ИБ

ИБ в 2021:

Слишком много задач

- ❑ Meet with CIO and stakeholders
- ❑ Nail down third-party risk
- ❑ Manage GDPR program with privacy office
- ❑ Respond to questions from state auditors
- ❑ Update CEO for board meeting
- ❑ Update budget projections
- ❑ Write security language for vendor's contract
- ❑ Make progress on the never-ending identity project
- ❑ Review and updated project list
- ❑ Edit communication calendar
- ❑ Update risk rankings on security roadmap
- ❑ Clarify policies governing external storage devices
- ❑ Provide testing and encryption tool direction
- ❑ Provide data handling best practices
- ❑ Help with new acquisition
- ❑ Meet with senior project manager
- ❑ Send new best practices to development teams
- ❑ Review logs for fraud ongoing investigation
- ❑ Help with insider threat discovery
- ❑ Determine location of sensitive data in the cloud
- ❑ Investigate possible infection on legacy system
- ❑ Continue pen testing of new business mobile app
- ❑ Help architects understand zero-trust
- ❑ Answer security policy emails
- ❑ Format security status report for executives
- ❑ Meet with recruiter to discuss staffing
- ❑ Write test plan requirements for new products
- ❑ Meet regarding improving security of facilities

Слишком много вендоров

Слишком много процессов

Слишком много оповещений

Заказчик в 2021 году:

Ограниченный бюджет

Нехватка сотрудников

Данные разрозненны

Сложно планировать

Свой Cloud Pak для любой задачи:

Cloud Pak for Applications

Build, deploy, and run applications

IBM containerized software

Container platform and operational services Red Hat OpenShift

Cloud Pak for Data

Collect, organize, and analyze data

IBM containerized software

Container platform and operational services Red Hat OpenShift

Cloud Pak for Integration

Integrate applications, data, and APIs

IBM containerized software

Container platform and operational services Red Hat OpenShift

Cloud Pak for Automation

Transform business processes, decisions, and content

IBM containerized software

Container platform and operational services Red Hat OpenShift

Cloud Pak for Multicloud Management

Multicloud visibility, governance, and automation

IBM containerized software

Container platform and operational services Red Hat OpenShift

Cloud Pak for Security

Connect security data, tools and workflows

IBM containerized software

Container platform and operational services Red Hat OpenShift

IBM public cloud

AWS

Microsoft Azure

Google Cloud

Private

IBM **Z**
IBM **LinuxOne**
IBM **Power** Systems

End points

IBM Cloud Pak for Security

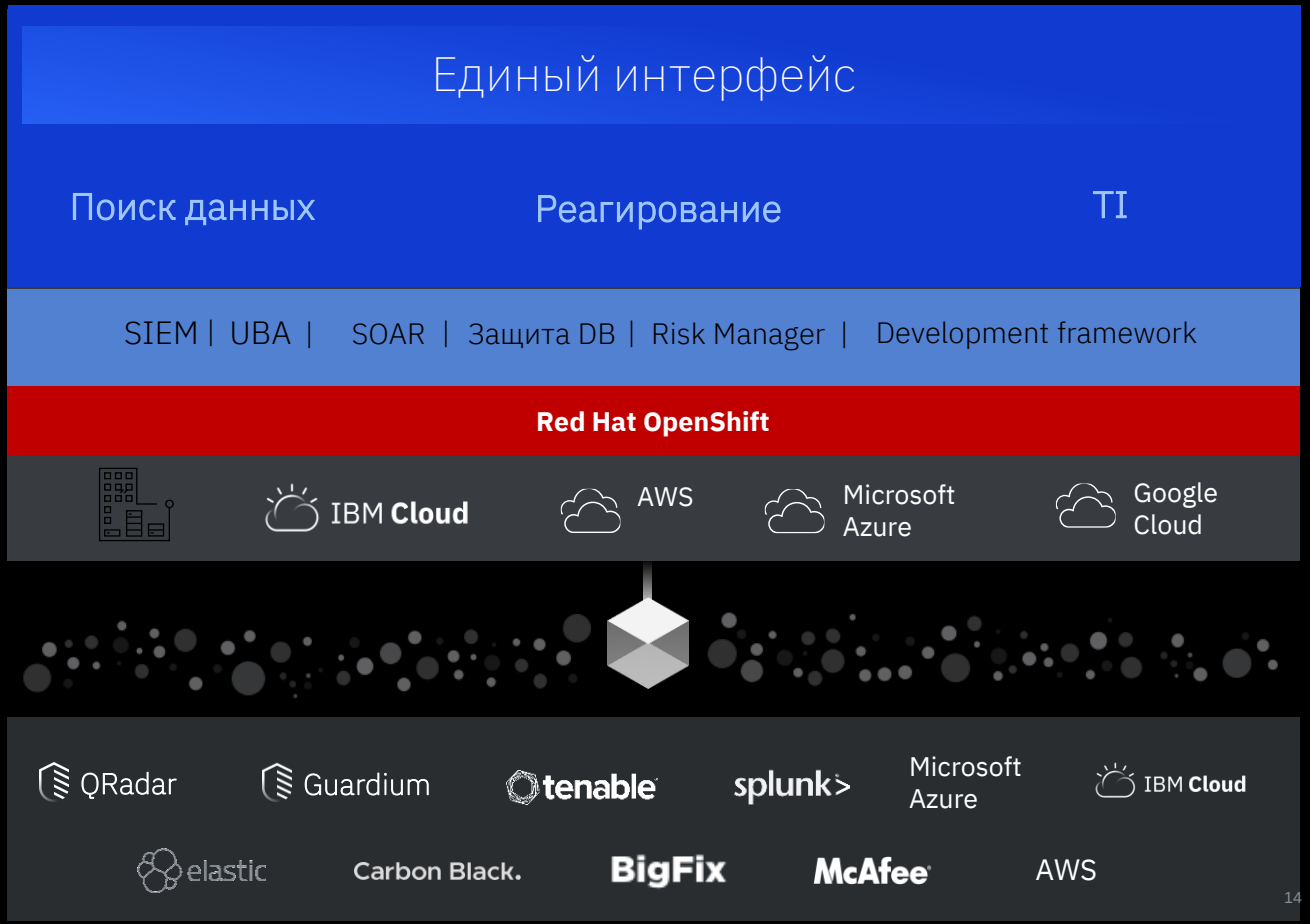
Интеграция с с инфраструктурой

Основные сервисы

Гибридная архитектура

Существующие интеграции

Где угодно | Любые данные | Оперативно



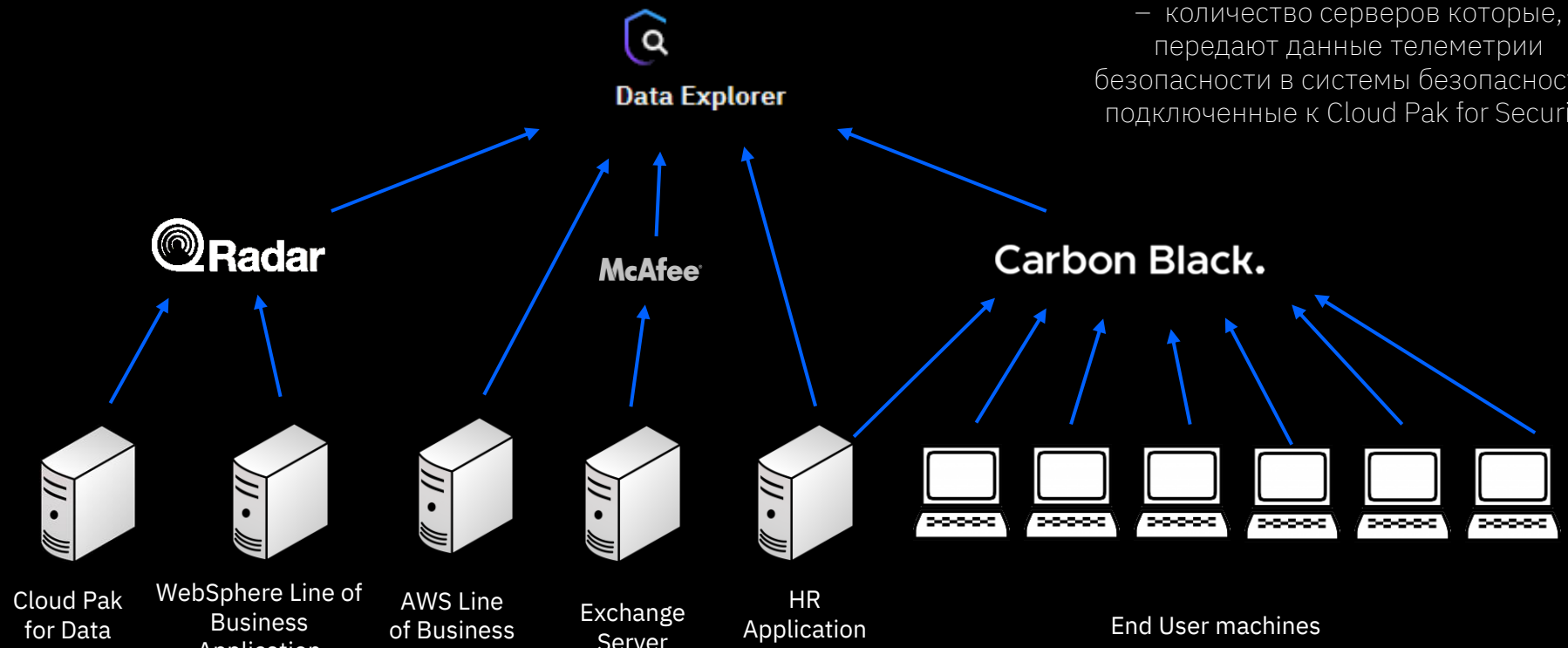
Заказчик в 2021 году:

Ограниченный бюджет

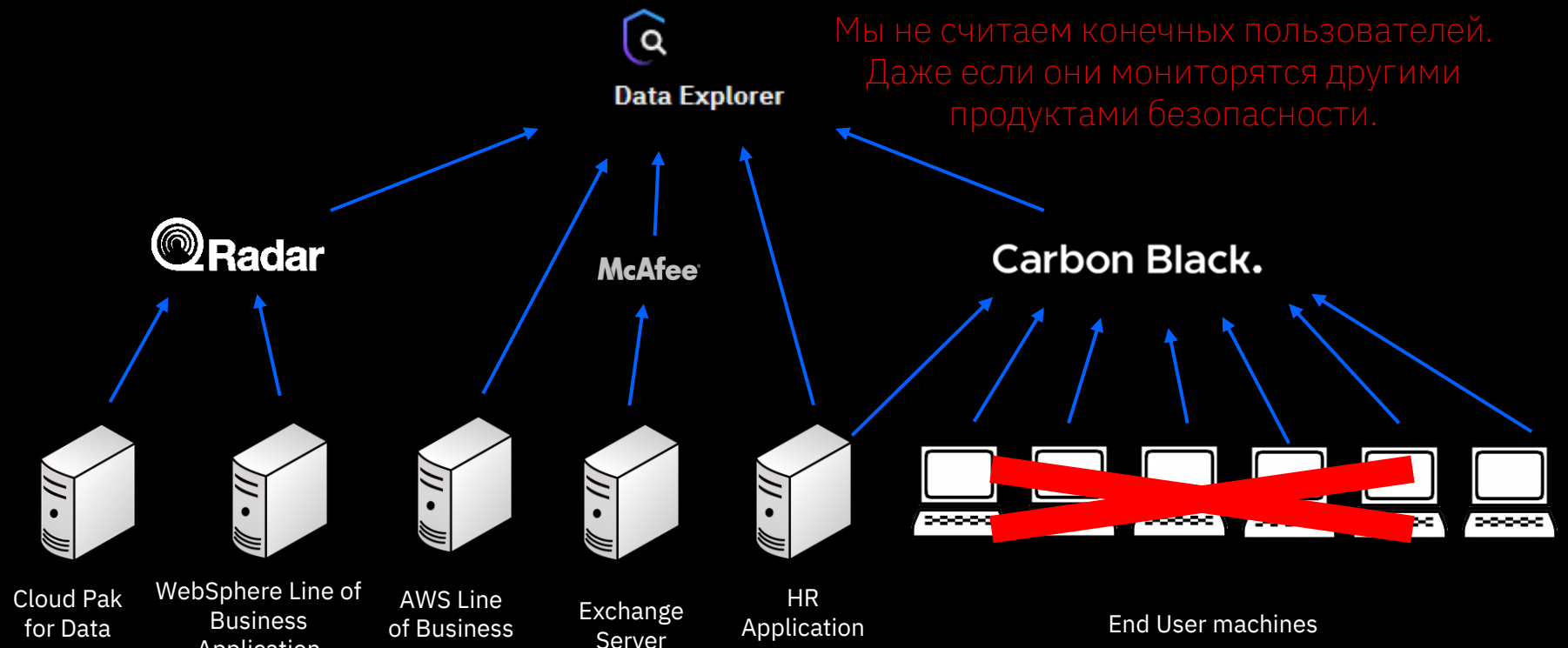
1. Платформа SOC из коробки с необходимым функционалом
2. Лицензирование по серверам источника (только Win/Unix) вместо лицензирования по EPS, объема данных, количества аналитиков и т.п.

Как лицензируется Cloud Pak for Security?

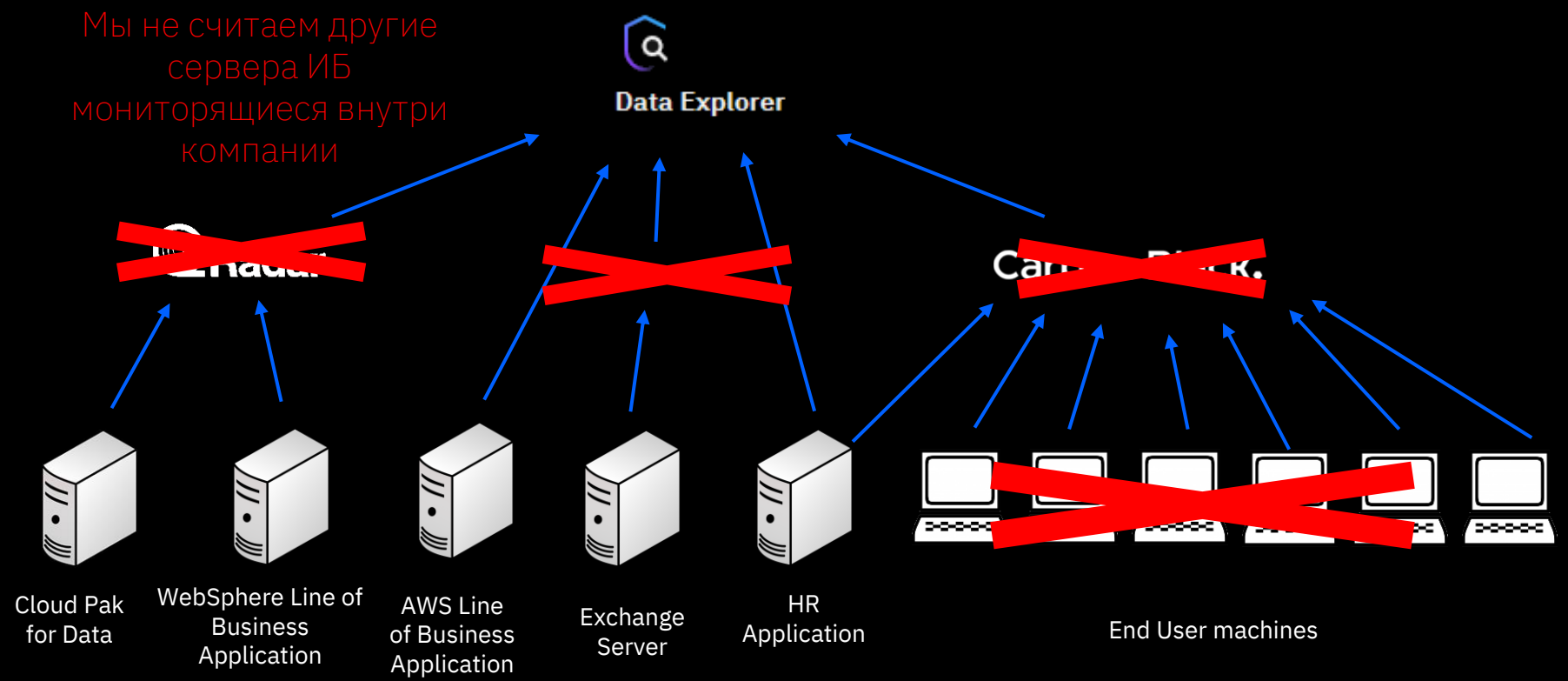
Мы считаем управляемые серверы – количество серверов которые, передают данные телеметрии безопасности в системы безопасности, подключенные к Cloud Pak for Security



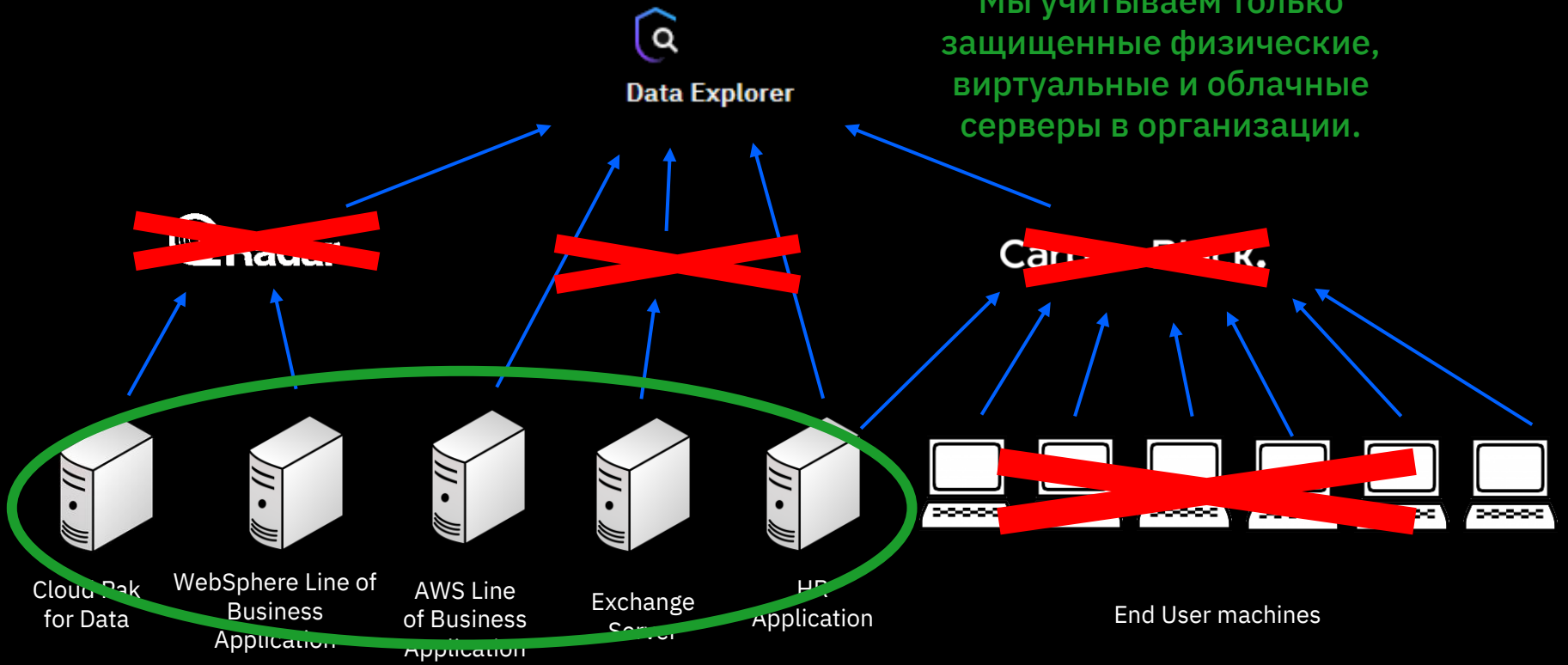
Как лицензируется Cloud Pak for Security?



Как лицензируется Cloud Pak for Security?



Как лицензируется Cloud Pak for Security?



Заказчик в 2021 году:

Ограниченный бюджет

1. Платформа SOC из коробки с необходимым функционалом
2. Лицензирование по серверам источника (только Win/Unix) вместо лицензирования по EPS, объема данных, количества аналитиков и т.п.
3. Нет необходимости дополнительных вложений при росте EPS, объема данных, количества аналитиков и т.п.

Заказчик в 2021 году:

Ограниченный бюджет

Нехватка сотрудников

Данные разрозненны

Сложно планировать

Заказчик в 2021 году:

Нехватка сотрудников

1. Повышение компетенции через возможность проводить симуляцию инцидентов, отслеживая ключевые KPI
2. Автоматизация процессов
3. Watson AI
4. Threat Intelligence Insights
   Отчеты
   Приоритетная аналитика с адаптивной оценкой
   Идентификация и проактивный поиск угроз, которые можно запускать вручную и по расписанию

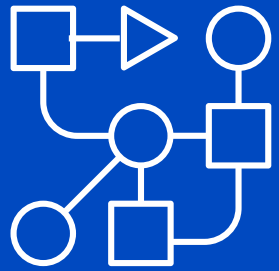
Заказчик в 2021 году:

Данные
разрозненны

Заказчик в 2021 году:

Данные разрозненны

Интегрировать



✗ Тяжело управлять

✗ Нет координации

✓ Подходит, когда средств не много

Интеграция чаще всего рушится из-за обновлений (персонал, процессы, апдейты ПО)

Консолидировать

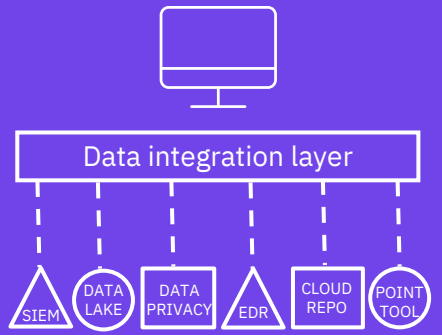
✗ Дорого

✗ Не все данные

✓ Эффективно для конкретных сценариев работы (например SIEM)

Озера данных превращаются в болота устаревших данных

Унификация



✓ Всеобъемлющий

✓ Минимальные расходы

✓ Способствует сотрудничеству между инструментами и командами

Open Cybersecurity Alliance (OCA):
Создан при участии IBM для продвижения и поддержки открытой безопасности

Кто

Глобальные единомышленники-поставщики кибербезопасности, конечные пользователи, идейные лидеры и отдельные лица

Видение

Открытая экосистема кибербезопасности: Продукты свободно обмениваются информацией, идеями, аналитикой и согласованным ответом

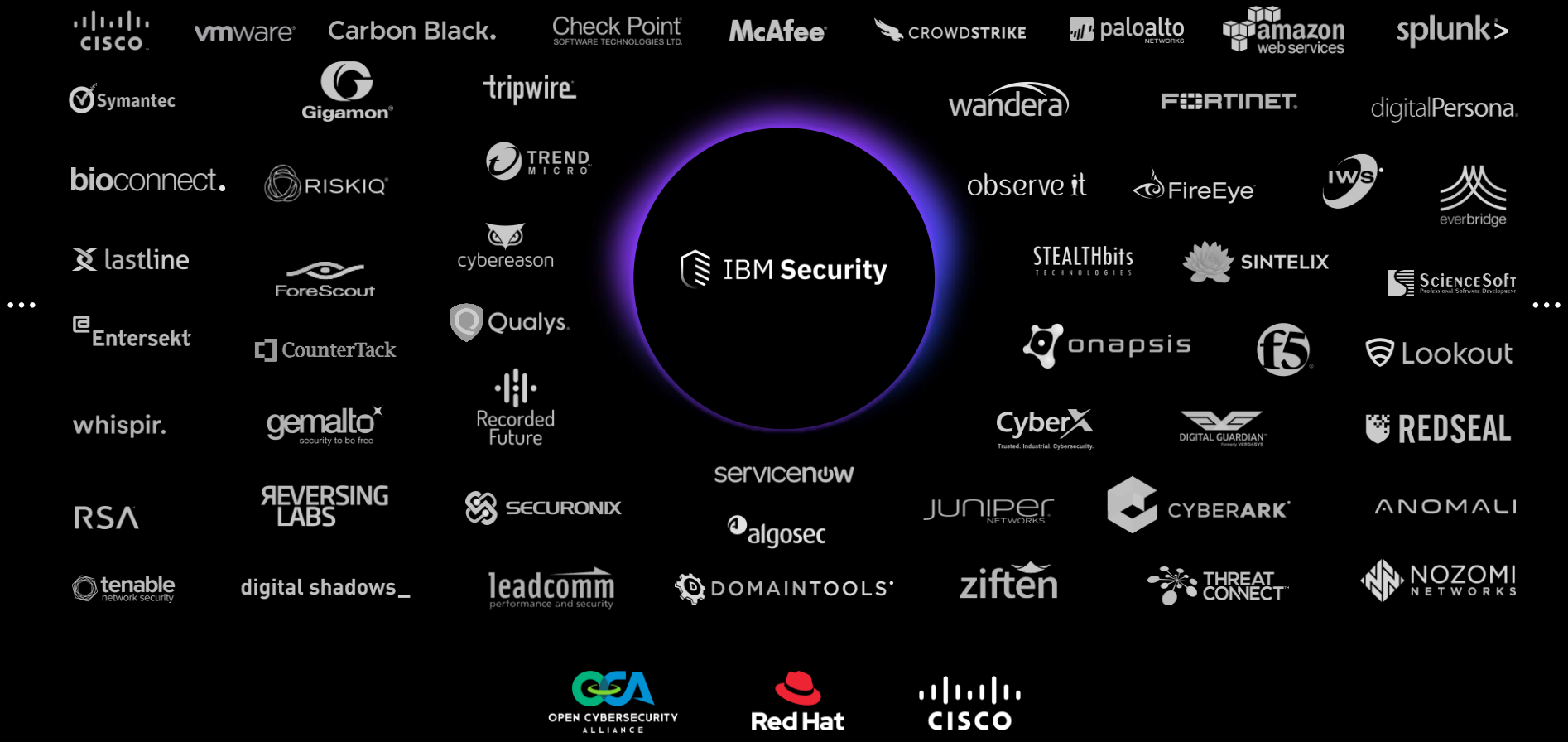
Как

Открыто
Общеразрабатываемый код и инструменты
Взаимно согласованные технологии, стандарты и процедуры

Первоначально совершенные проекты - Stix Shifter и Open DXL Ontology теперь на Github

Вовлеченность в OCA - количество участников увеличено с 16 до 24

IBM Security



Заказчик в 2021 году:

Сложно планировать

Заказчик в 2021 году:

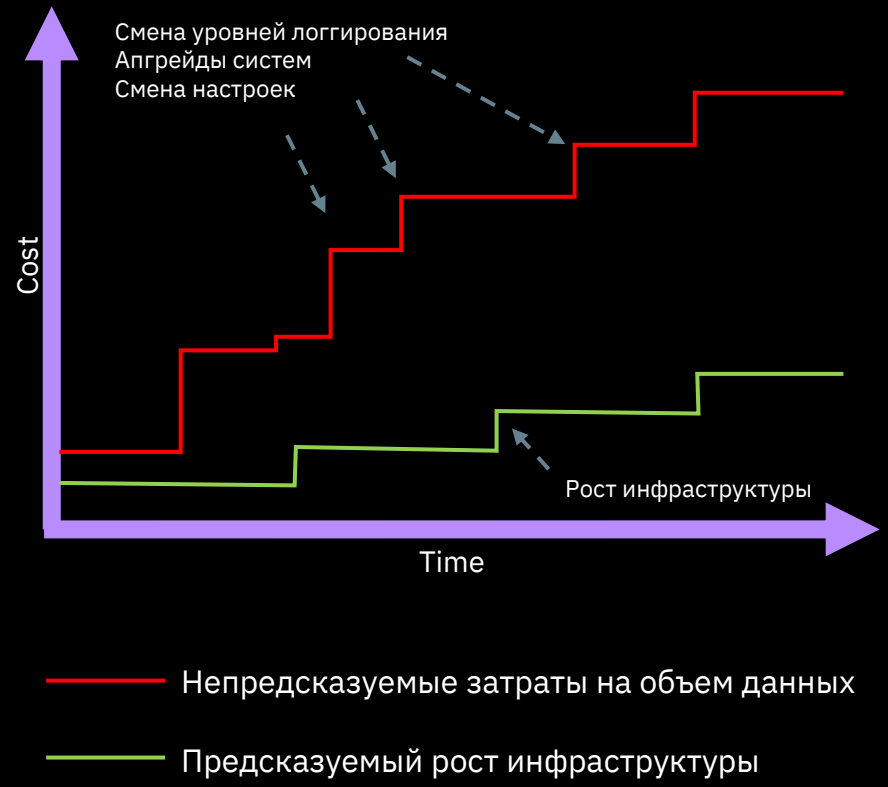
Сложно планировать

1. Заказчик самостоятельно активирует/деактивирует необходимый для своих задач функционал в рамках приобретенных лицензий на сервера источники без дополнительных финансовых вложений

2. Подключение новых инструментов и функционала по мере плавного перехода по фазам проекта

Простая и прогнозируемая модель лицензирования Cloud Pak for Security позволяет использовать все лог данные

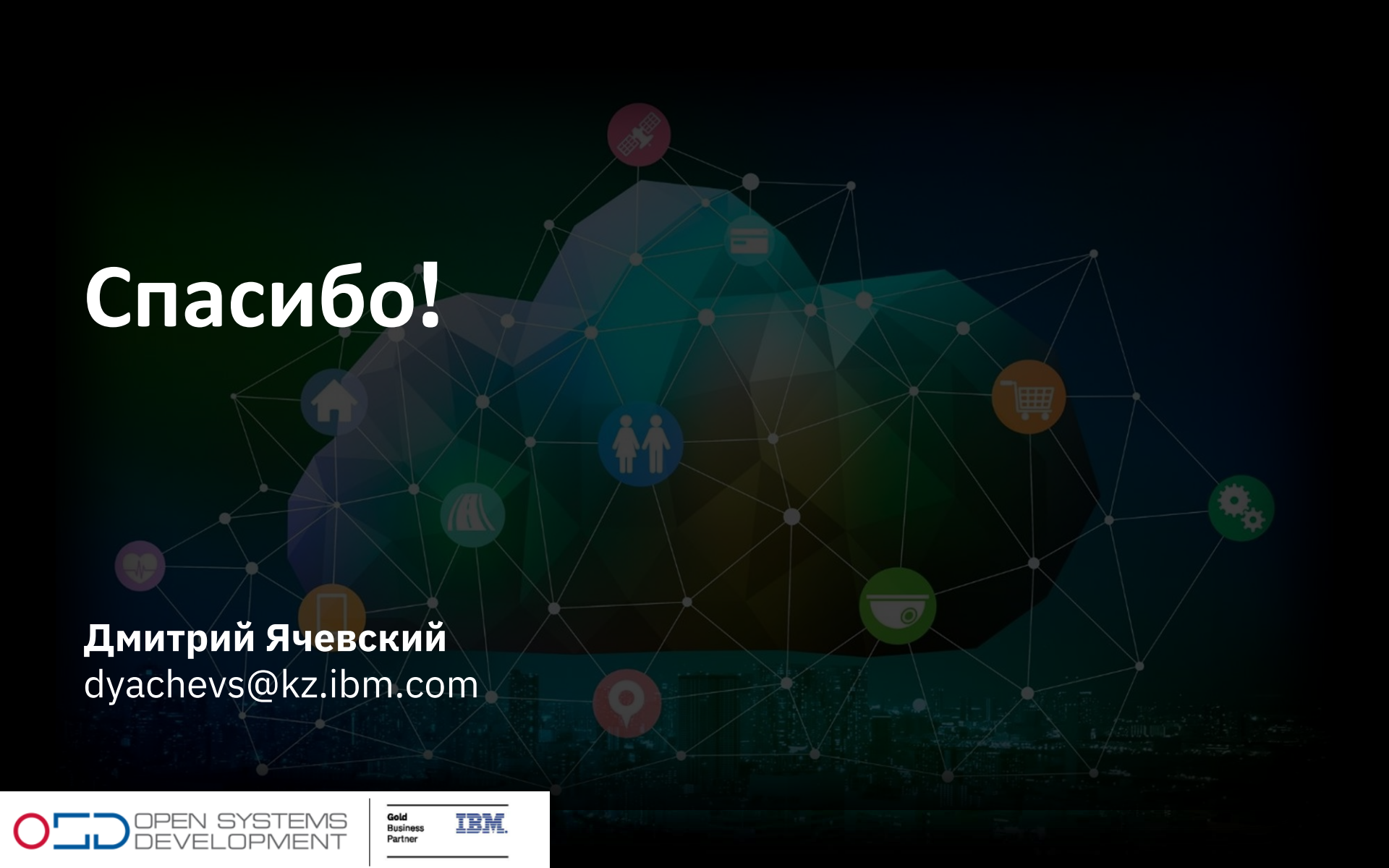
- Модель лицензирования не накладывает штрафов на использование и не основана на объемах данных
- Модель ценообразования Cloud Pak for Security основана на управляемых серверах и не требует дополнительных затрат на данные, журналы, потоки, действия событий или пользователей



IBM Cloud Pak for Security

Платформа, позволяющая объединить существующие решения и процессы

- Развёртывание в любом облаке и локально
- Открытая платформа
- Data Explorer
- SOAR (Resilient)
- TI Feed
- Qradar Events & Flows
- Qradar Network Insights
- DataLake
- DB Protection (Guardium)
- Risk Manager



Спасибо!

Дмитрий Ячевский
dyachevs@kz.ibm.com