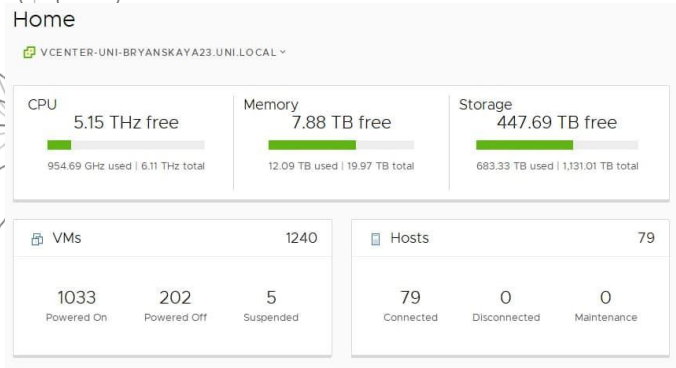
центр информационных технологий Красноярского края

Создание центра мониторинга

на примере кейса КГКУ «ЦИТ»

Предпосылки

Центр информационных технологий Красноярского края



01 **Развитая ИТ инфраструктура**

Количество пользователей ЕСПД и ЕМСПД: около 4000

Количество ВМ: около 1500

02 **Развитый парк СЗИ**

Многокомпонентный парк СЗИ при создании SOC

Регистрационный номер лицензии	Дата предоставления лицензии	Срок действия лицензии	Полное (сокращенное) наименование лицензиата
Поиск	Поиск	Поиск	Поиск
4050	18.02.2022	бессрочно	Краевое государственное казенное учреждение "Центр информационных технологий Красноярского края" (КГКУ ЦИТ)

03 **Получение лицензии ФСТЭК на ТЗКИ**

Один из видов работ - услуги по мониторингу информационной безопасности средств и систем информатизации;

04 **Требования законодательства**

Цель

Создание услуги «Мониторинг ИБ» в интересах государственных учреждений на территории Красноярского края, в интересах повышения уровня информационной безопасности на территории Красноярского края

Задачи

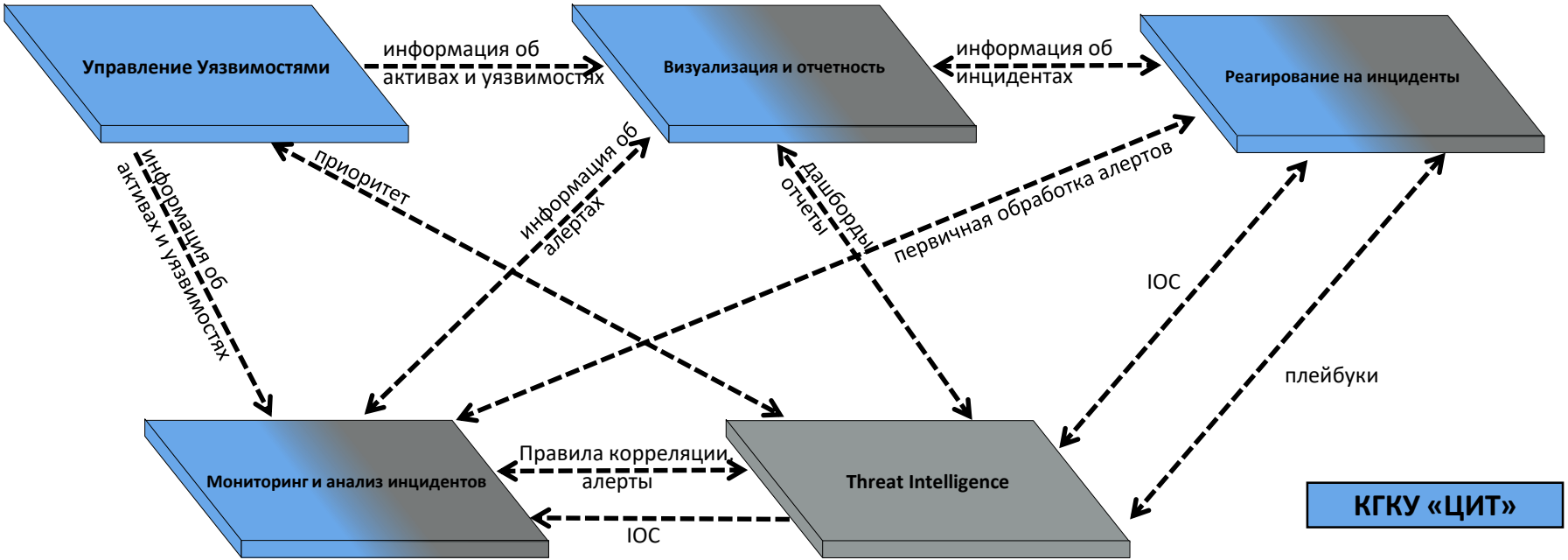
01 Настроить инфраструктуру для хранения и накоплений событий ИБ

02 Реализовать возможность оперативного подключения источников событий ОГВ

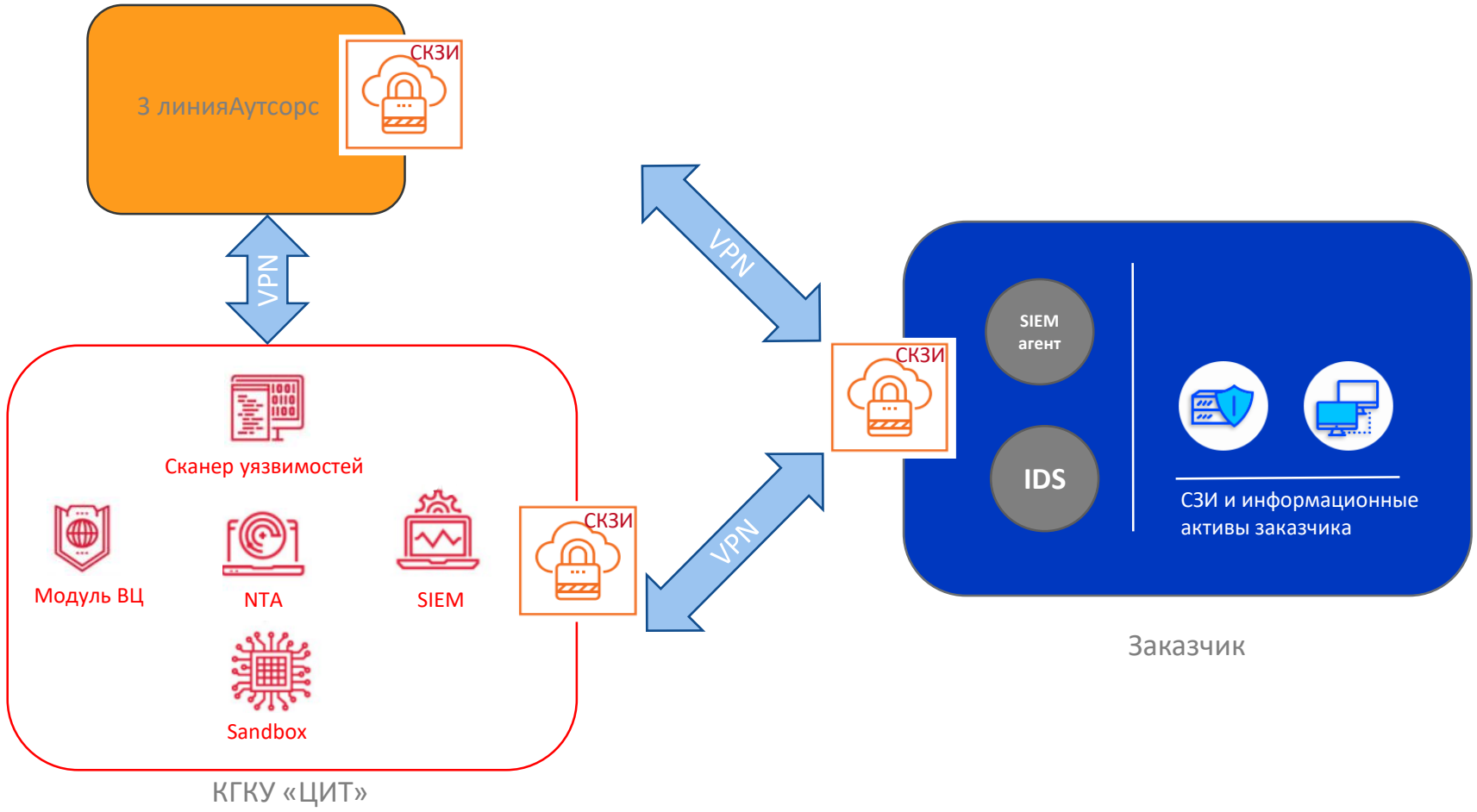
03 Предоставить инфраструктуру и доступ к данным для анализа и выявления корреляций для сотрудников КГКУ «ЦИТ» и 3 линии Аутсорс

04 Настроить отчетность и ее дистрибуцию

Формирование ключевых процессов



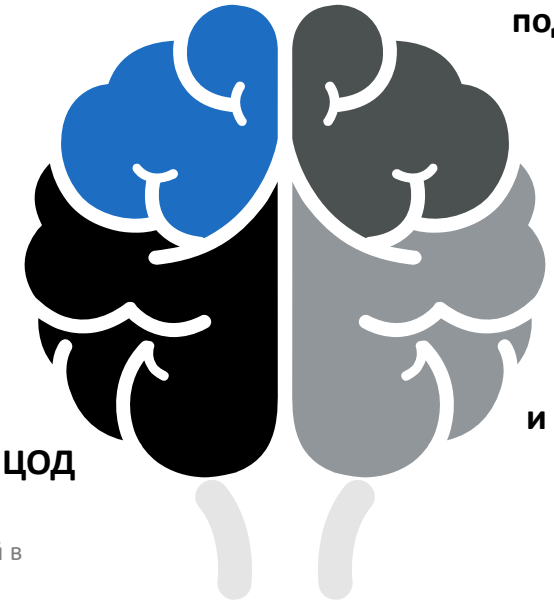
Техническое обеспечение



Промежуточные результаты

Сформировано понимание ключевых процессов

Сформирован единый подход подключения инфраструктуры заказчика к мониторингу



Заведены в источники событий ключевые ИС ОГВ, а также СЗИ и сетевое оборудование ЦОД

Количество активов – 1400 активов;
Текущий поток событий в секунду- 21 тыс. событий в секунду;
Объем траффика – 1.7 Гбит/сек

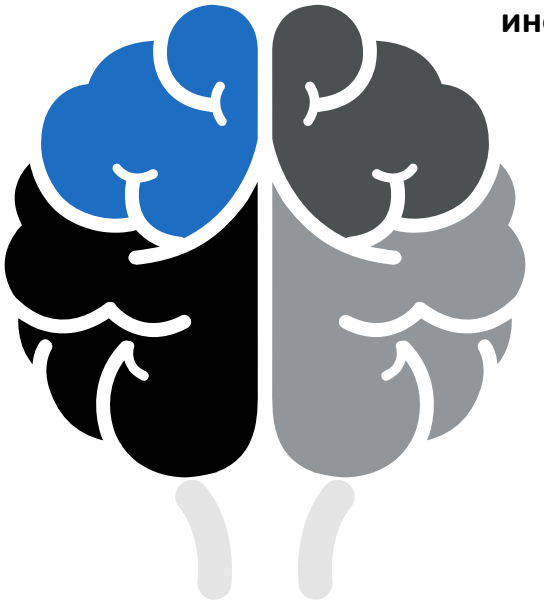
Сформирована потребность и направленность обучения сотрудников

Дальнейшее развитие

Центр информационных технологий Красноярского края

Стандартизация и регламентирование всех процессов

Реализация единого подхода подключения инфраструктуры заказчика к мониторингу



Заведены в источники событий ключевые ИС ОГВ, а также СЗИ и сетевое оборудование ЦОД

Повышение компетенций сотрудников

центр информационных технологий Красноярского края

Благодарю за внимание!