SOLAR

Подход ГК «Солар» к построению комплексной кибербезопасности

Баскаков Денис
Директор по развитию региональных продаж

НОВОСИБИРСК, 2023

АРХИТЕКТОР КОМПЛЕКСНОЙ КИБЕРБЕЗОПАСНОСТИ

ПАРАДИГМА ИБ SOLAR	ЦЕНТР ИССЛЕДОВАНИЙ КИБЕРУГРОЗ	ЭКОСИСТЕМА ПРОДУКТОВ	ДОМЕНЫ ЭКСПЕРТИЗЫ И КОНСАЛТИНГ
Умеем строить реальную ИБ и развиваем отрасль	Изучаем противника и киберугрозы	Аккумулируем экспертизу в технологиях	Глубоко понимаем задачи клиента

ИНТЕГРАТОР	СЕРВИС-ПРОВАЙДЕР	ВЕНДОР

SOLAR

Сервисы

Solar JSOC

- Мониторинг, реагирование и анализ инцидентов ИБ
- Комплексный контроль защищенности: пентест, RedTeaming, анализ защищенности
- Техническое расследование инцидентов ИБ
- Эксплуатация систем ИБ и реагирование на атаки
- Построение SOC и его частных процессов
- Мониторинг АСУ ТП и объектов КИИ (SOC OT)
- Защита конечных точек (EDR)
- Анализ сетевого трафика (NTA)
- Анализ угроз и внешней обстановки (Aura) New

Solar MSS

- Защита от сетевых угроз (UTM)
- Защита электронной почты (SEG)
- Защита от продвинутых угроз (Sandbox)
- Защита веб-приложений (WAF)
- Защита от DDoS-атак (Anti-DDoS)
- Шифрование каналов связи (ГОСТ VPN)
- Управление навыками ИБ (SA)
- Контроль уязвимостей (VM)

Услуги

- Сервисная поддержка
- Консалтинг
- Импортозамещение
- Солар ТЗИ
- CyberBoost New
- Solar Интеграция
- Киберполигон
- Соответствие требованиям
- Кибербезопасность АСУ ТП

- Безопасная разработка ПО
- Защита корпоративных данных
- Анализ защищенности
- Управление доступом
- Реагирование и восстановление после атак
- Детектирование угроз и хакерских атак

Технологии

- Solar Dozor (DLP)
- Solar appScreener (SAST, DAST, SCA)
- Solar inRight (IdM/IGA)
- Solar webProxy (SWG)
- Solar addVisor (EM)
- Solar Safeinspect (PAM)
- Solar NGFW (FW+IPS+DPI) New
- Solar DAG (Управление доступом к данным) New
- Solar SafeConnect (Защищенный удаленный доступ) New

Домены

SOLAR DAG

SOLAR

- Надежная безопасность данных
- Соблюдение политик и правил
- Предотвращение утечки данных
- Эффективный контроль доступа к информационным активам

Функционал Solar DAG

SOLAR

КОНТРОЛЬ ПРАВ ДОСТУПА К ДАННЫМ	Построение матрицы эффективных прав доступа с отображением категории информации и с поддержкой двунаправленного представления как со стороны учетных записей, так и со стороны ресурсов. Возможность контролировать изменения прав доступа и их состояние на заданный момент времени
КОНТРОЛЬ ПОЛИТИК ХРАНЕНИЯ	Выявление мест хранения конфиденциальных, персональных и прочих данных, подлежащих защите
КОНТРОЛЬ ИСПОЛЬЗОВАНИЯ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ	Журналирование событий, регистрируемых на системах хранения, с целью отслеживания операций, выполняемых над данными, и своевременного обнаружения фактов несанкционированного доступа
ПОЛИТИКИ БЕЗОПАСНОСТИ	Своевременное уведомление об изменениях прав или регистрируемых событий доступа по отношению к критичным данным
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ	Разграничение доступа внутри системы между пользователями на уровне контролируемых систем хранения и каталогов домена, полное журналирование действий пользователей

Результаты внедрения Solar DAG

SOLAR

ИБ

- Минимизация рисков утечки конфиденциальной информации
- Контроль хранения и доступа к информации
- Минимизация рисков, связанных с действиями вирусов на файловых хранилищах
- Минимизация рисков, связанных с избыточными правами доступа
- Повышение эффективности проведения расследований по фактам инцидентов

РЕГУЛЯТОРЫ

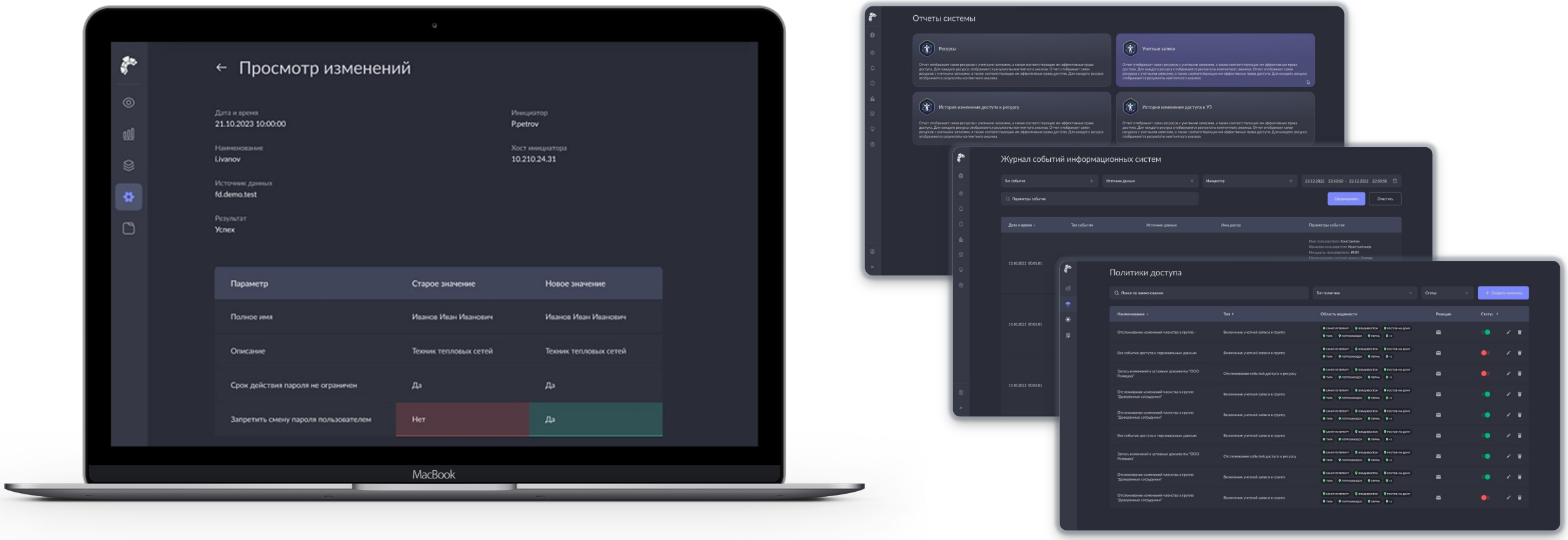
- Предотвращение неправомерного доступа к информации и неправомерных действий в отношении информации на объектах КИИ
- Обнаружение фактов несанкционированного доступа к ПдН, установление правил доступа к ПдН
- Ограничение и мониторинг доступа к ДДК
- Проведение аудита – где хранятся ПдН и кто имеет к ним доступ
- Контроль использования ПдН

ИТ

- Сокращение времени на составление отчетов для внешних и внутренних регуляторов, обнаружение и устранение последствий нарушения политик прав доступа
- Сокращение трудозатрат на инвентаризацию и контроль изменений прав доступа

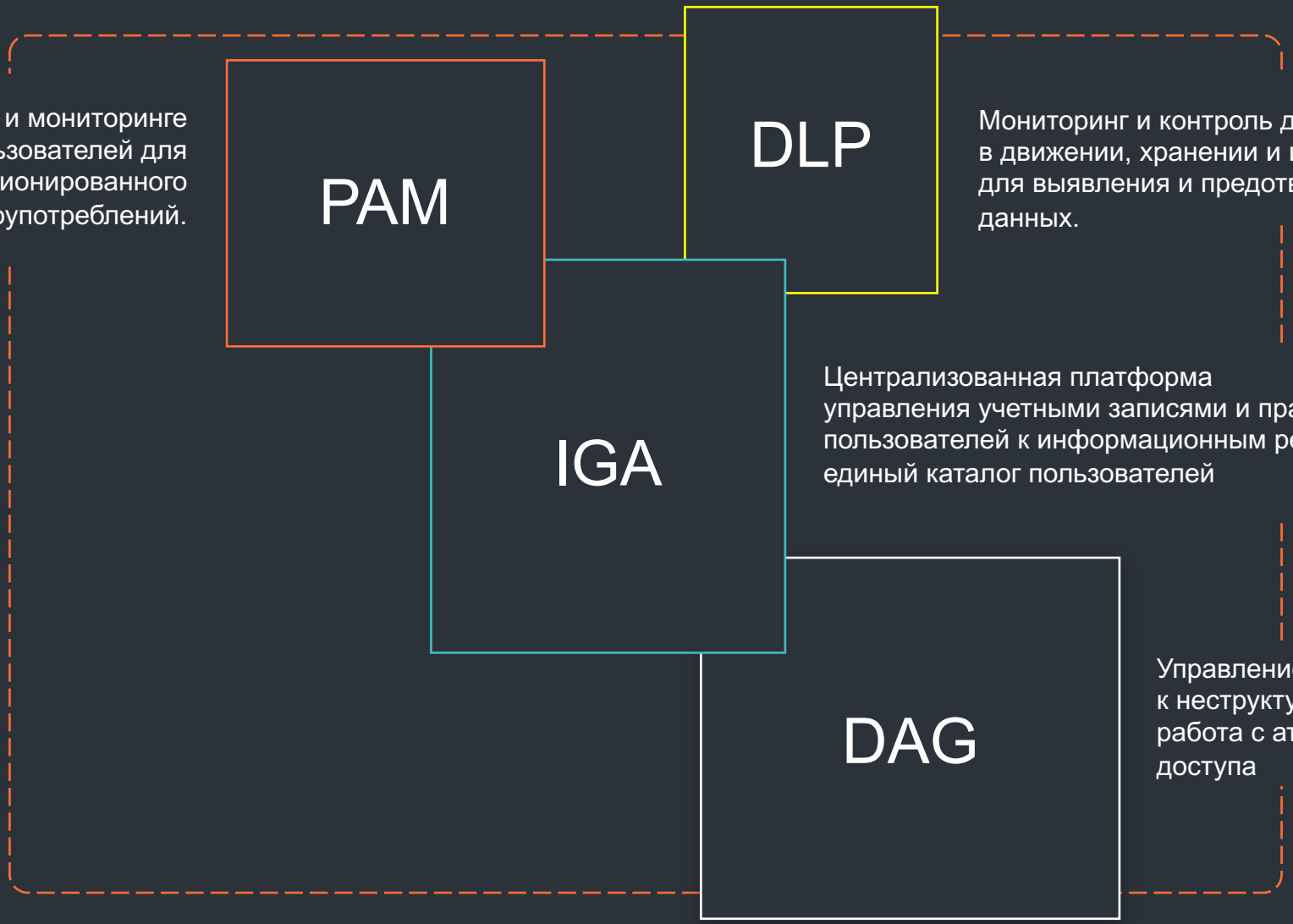
Интуитивно понятный и дружелюбный интерфейс

Разработан на прогрессивной санкционно независимой технологии Vue.js и является динамически конфигурируемым инструментом, который адаптируется под пользователя, легко масштабируется и настраивается.



Мы строим архитектуру комплексной безопасности в управлении доступом

SOLAR



Фокус на управлении и мониторинге привилегированных пользователей для предотвращения несанкционированного доступа и злоупотреблений.

Мониторинг и контроль данных в движении, хранении и использовании для выявления и предотвращения утечек данных.

Централизованная платформа управления учетными записями и правами пользователей к информационным ресурсам, единый каталог пользователей

Управление доступом к неструктурированным данным, работа с атрибутивной моделью доступа

Киберполигон сегодня

SOLAR

КИБЕРУЧЕНИЯ

- Практические киберучения на платформе «Солар Кибермир»
  - Стандартные сценарии
  - Кастомные сценарии
- Командно-штабные тренировки для организационной отработки сценариев реагирования
- Командные соревнования в формате CTF

ПОСТРОЕНИЕ КИБЕРПОЛИГОНОВ

- Построение киберполигонов на базе инфраструктуры заказчика с использованием платформы «Солар Кибермир»
- Создание цифровых двойников сегментов ИТ-инфраструктуры заказчика на базе мощностей киберполигона ГК «Солар»

СОЛАР КИБЕРБУСТ New

- Модульный образовательный киберинтенсив для получения ключевых знаний и навыков ИБ
- Комплексная образовательная программа развития навыков киберзащиты для Blue Team, практическая отработка на киберполигоне

ОСНОВНАЯ ЗАДАЧА

Повышение компетенций и отработка практических навыков по кибербезопасности

Программа развития навыков

Солар КиберБуст

SOLAR

РАЗВИТИЕ НАВЫКОВ

Учебный план составляется из модулей, необходимых каждому специалисту. Обучение сопровождается большим количеством практических заданий различных типов

КЛЮЧЕВЫЕ ЗНАНИЯ ПО КИБЕРБЕЗОПАСНОСТИ

Получение ключевых знаний и навыков по информационной безопасности

НАВЫКИ ОБРАБОТКИ ИНЦИДЕНТОВ

Практико-ориентированное обучение специалистов для результативной обработки инцидентов и предотвращения потерь от кибератак

ПОЛЬЗОВАНИЕ ИБ-ПРОДУКТАМИ

Обучение по ИБ-продуктам с возможностью проверить работу СЗИ на киберполигоне

Вектор кибератак

ЦЕЛЬ ЗЛОУМЫШЛЕННИКОВ №1

Разрушение критической информационной инфраструктуры

ЦЕЛЬ ЗЛОУМЫШЛЕННИКОВ №2

Воздействие на медиа-инфраструктуру и встраивание антироссийской политической пропаганды

Статистика атак

170

атак ежедневно фиксируется на российские ресурсы в 2023 г.

65%

атак имеют целенаправленный характер

445 млн

строк конфиденциальных сведений попало в сеть с начала 2023 г.

91,8 ТБ

составил общий объем размещенных данных российских компаний

4RAYS by SOLAR

Центр исследований Solar 4RAYS

SOLAR

Всегда актуальные знания об угрозах

24 ЧАСА

на гарантированное создание мер противодействия (хостовых или сетевых сигнатур)

КРУПНЕЙШАЯ БАЗА ЗНАНИЙ ОБ УГРОЗАХ И ПОНИМАНИЕ РЕАЛИЙ РОССИЙСКОГО КИБЕРЛАНДШАФТА

180+ МЛРД

событий в сутки регистрируют автоматизированные сенсоры

3+ МЛН

алертов в сутки на автоматизированных сенсорах

1+ МЛН

фактических действий злоумышленников фиксирует сеть ханипотов

Узнать первым о запуске страницы и блоге центра Solar 4RAYS

Домены экспертизы

Передаем богатый опыт ГК «Солар» по построению систем безопасности уровня Enterprise

Обучаем специалистов по кибербезопасности и даем им практические навыки

Команда ГК «Солар» - единое окно, обеспечивающее своевременную поддержку по всем вопросам

ГК «Солар» полностью управляет построением и развитием ИБ инфраструктуры, как генеральный конструктор

Глубокая, лидирующая на рынке экспертиза в выбранной тематике кибербезопасности

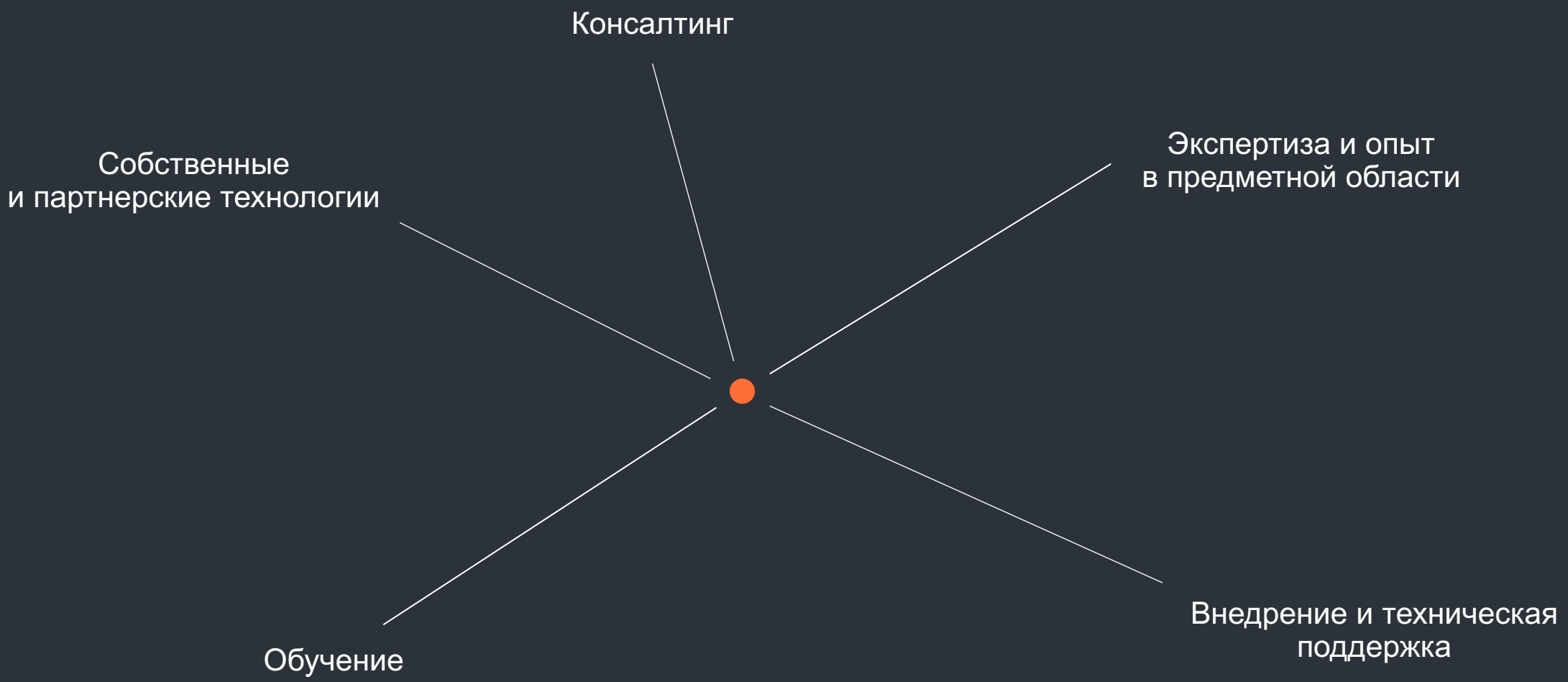
Собственные технологии основанные на огромном опыте проектов по тематике домена

Предоставление технологий по сервисной модели в ходе построения рабочей системы

Сплав собственных технологий, экспертизы внедрений, консалтинга и сервиса в едином предложении

Состав домена

SOLAR



SOLAR

Баскаков Денис
Директор по развитию
региональных продаж

+7 (914) 707-67-87
d.baskakov@rt-solar.ru