РЕЗЮМЕ БИЗНЕС-ПРОЕКТА

«Услуги в области корпоративной кибербезопасности, противодействия сетевым атакам и мониторинга информационной безопасности».

1. **Опишите ваш продукт/ услугу.**

• Разработка собственного программного продукта – SOC-сервиса (Security Operations Center) с применением самообучающихся систем и нейронной сети, эвристический и сигнатурный анализ сетевых потоков на предмет выявления угроз. Применение моделей искусственного интеллекта и технология Big-data для обучения сервиса реагировать на новые угрозы, локализовать их и предотвратить возможный ущерб.
• Проектирование объектов ИТ-инфраструктуры в защищенном исполнении (оценка рисков и актуальность угроз, модель вероятного нарушителя);
Мониторинг ИБ компании (оптимизация и поддержание работоспособности, сбор информации, реагирование и нейтрализация угроз, анализ показателей эффективности защиты, отчеты)
• Защита конфиденциальной информации (аудит с рекомендациями по устранению угроз, установка, настройка, сопровождение систем защиты информации, подготовка концепций и дорожных карт по развитию ИБ)
• Защита критической информационной инфраструктуры (КИИ) (разработка и реализация требований, мер по обеспечению безопасности КИИ, реализация мер по организации системы безопасности значимых объектов КИИ (СБЗОКИИ).
• Инженерная и ИТ-инфраструктура компании (поставка, настройка и запуск защищенных корпоративных сетей, серверного оборудования, обслуживание средств криптографической защиты информации).

2. **Кто ваш покупатель/ заказчик?**

– 1 января 2018 г. вступил в силу Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры (КИИ) Российской Федерации». Закон направлен на обеспечение устойчивого и бесперебойного функционирования критической информационной инфраструктуры, а также для правового регулирования в сфере обеспечения информационной безопасности.

В связи с тем, что требования ФЗ № 187 необходимо выполнить всем субъектам КИИ, которыми являются организации, которым на законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления и функционирующие в определенных сферах экономической деятельности, то потенциальными покупателями услуг Центра являются практически все государственные организации, все крупные промышленные и ресурсоснабжающие компании, объекты здравоохранения, образования. Кроме в услугах Центра заинтересованы частные компании, желающие провести аудит и защитить свои информационные ресурсы от внешних и внутренних угроз. Клиенты аутсорсинга информационной безопасности – небольшие компании у которых отсутствует возможность содержать свой штат специалистов. Услуги SOC-центра рассчитаны на компании, имеющим филиальную и распределенную сеть и нуждающихся в бесперебойной ее работе.

3. **Почему они будут покупать (покупают) именно у вас? (Существенные конкурентные преимущества)**

– В связи с вводимыми санкциями в отношении Российской Федерации обеспечение безопасности объектов КИИ является крайне актуальной задачей. Нехватка отечественных специалистов в этой области и сложность технологий создает определенные сложности российским компаниям.

Наличие высококвалифицированных специалистов в области компьютерных сетей, информационной безопасности и разработки программного обеспечения любой сложности со стажем работы более 20 лет, имеющих в том числе непосредственный опыт работы со специфическим оборудованием и документацией. Обладание ими всеми необходимыми навыками для реализации и развития проекта.

4. **Объём привлекаемых инвестиций (кредит, займ): 2,46 млн. €**