SOC
FORUM
2023

Стратегия ИБ в условиях цифровой трансформации

SOC
FORUM
2023

Ложкин Руслан

Абсолют банк

SOC FORUM 2023

Киберпреступность существует благодаря трем составляющим: данные, технологии и люди. Уберите один из элементов и вся киберпреступность сходит на нет, а информационная безопасность становится формальной

Трансформация и кибербезопасность

Аксиома киберпреступности

SOC FORUM 2023

Процессы завязаны на:

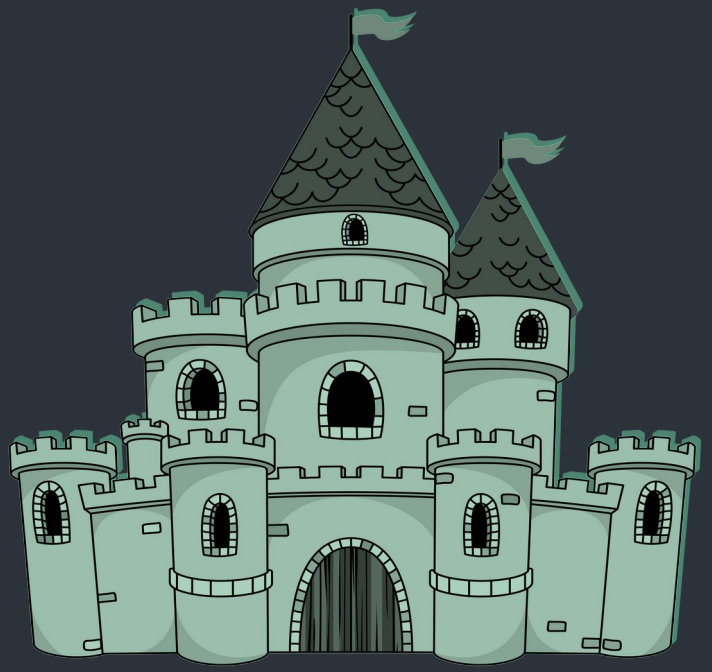
- **Данных**
- **Технологиях**
- **Людях**

Цифровая эпоха 4.0

SOC FORUM 2023

Дистанционные сервисы

Технологии и данные



Организация

Аутсорсинг услуг

Инфраструктура

Кибербезопасность 4.0

SOC FORUM 2023

683-П
719-П
802-П
152-ФЗ
716-П

От регулятора

Risk

От рисков

Учет сверхзависимости от совместных данных и технологий	Противостояние современным техникам и тактикам
Цифровая трансформация учитывает недопустимые события	Помощь в соблюдении обязательств перед клиентами, партнерами

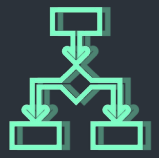
Формальный подход

ALE
ROSI
NPV
VaR

От бизнеса

Доступность сервисов

От ИТ



Искажение данных
Утечка данных
Остановка систем
Кража денег

От недопустимых событий

Detect
incident response
Thread hunting

От качества реагирования

Гибридный подход к стратегии

Учет недопустимых событий

SOC FORUM 2023

Финансовые потери

- Вывод д/с с расчетного счета
- Вывод д/с с корреспондентского счета
- Мошеннические операции
- Мошенничество с прикладным ПО

Искажение или утрата данных

- Информации в базах данных
- Резервных копий
- На официальных ресурсах
- Публикация ложной информации

Прерывание деятельности

- Остановка работы систем
- Перебои внутреннего обслуживания
- Перебои внешнего обслуживания
- Перебои взаимодействия с гос органами

Утечка чувствительных данных

- Утечка баз данных
- Документов организации
- Доступов к системам
- Информации о конфигурациях и уязвимостях систем

Учет требований регуляторов

SOC FORUM 2023

Регуляторы

- Центральный Банк РФ
- ФСБ России
- ФСТЭК России
- Платежные системы (НСПК)
- Минцифры
- Роскомнадзор

Учет рисков кибербезопасности

SOC FORUM 2023

Риски в ИТ-инфраструктуре

- Мониторинг и анализ уязвимостей, оценка применимости к инфраструктуре
- Оценка и регистрация рисков по выявленным уязвимостям
- Формирование планов мероприятий для снижения рисков
- Контроль устранения путем сканирования на уязвимости

Риски в разработке

- Автоматизированный анализ кода на уязвимости (SAST)
- Формирование планов устранения уязвимостей
- Анализ применимости и возможности эксплуатации уязвимостей
- Устранение уязвимостей для вывода релиза в ПРОМ

Риски в бизнес-процессах

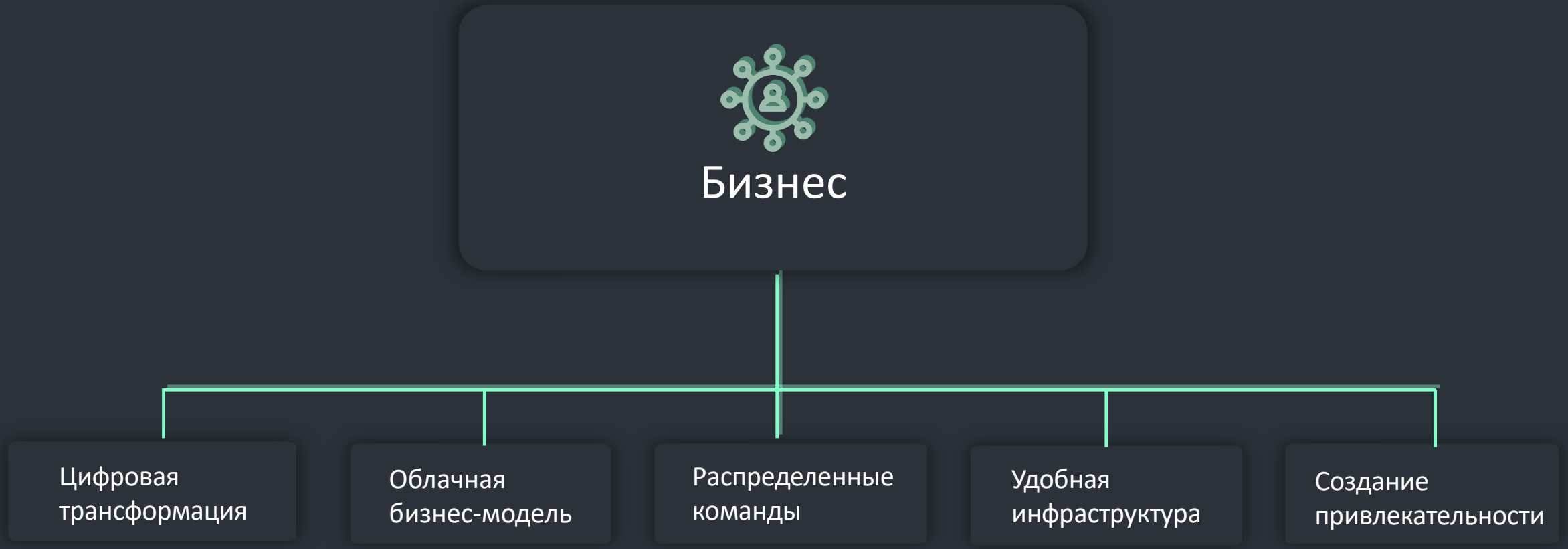
- Экспертиза КБ разрабатываемых продуктов, АС, процессов
- Выставление требований КБ
- Участие экспертов КБ в ПСИ
- Оценка рисков при невыполнении требований КБ
- Обработка оцененных рисков владельцем риска

Риски мошенничества

- Автоматизированный анализ транзакций клиентов
- Выявление и остановка мошеннических операций
- Экспертиза КБ разрабатываемых продуктов и АС
- Оценка рисков при невыполнении требований в части ФМ
- Оценка потерь клиентов от реализаций риска мошенничества

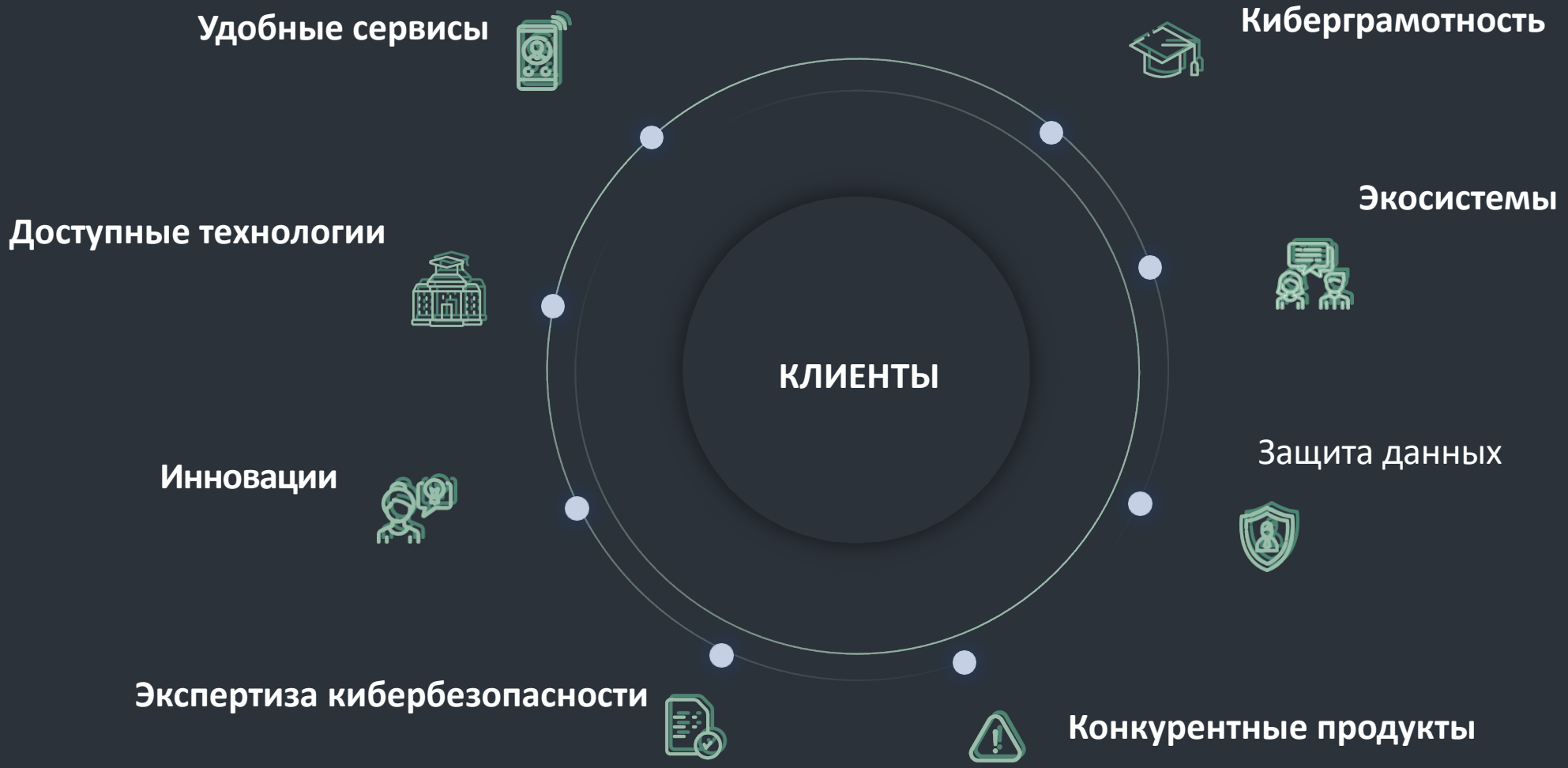
Учет потребностей бизнеса

SOC FORUM 2023



Учет потребностей клиента

SOC FORUM 2023



Концепция противодействия

Гибкий периметр

SOC FORUM 2023

Противодействие атакам

SOC FORUM 2023

SIEM
DLP
WAF
NGFW
Anty-APT
SWG

Threat Detect

Incident Response

IRP
SOAR

SOC – плата за цифровизацию

Threat Hunting

XDR
TI

Собственный

Сервис

Защита данных

SOC FORUM 2023

Статическое обезличивание

Динамическое обезличивание

Контроль утечки данных

Защита неструктурированных данных

Защита баз данных

Усиление конфиденциальности

Основные тренды в цифровой организации

SOC FORUM 2023

От регулятора

Базовая модель

От рисков

1. Сеть кибербезопасности и технологии пограничного доступа
2. Невозможность утечки чувствительных данных
3. Гипераавтоматизация и противодействие атакам
4. Безопасность в публичном облаке
5. Безопасность на стадии жизненного цикла проекта
6. Автоматизация процессов комплаенса
7. Противодействие мошенничеству

Модель стратегии

Пример архитектуры кибербезопасности

SOC FORUM 2023

Противодействие атакам

Детектирование событий(SIEM)	Детектирование уязвимостей (VM)	Детектирование вредоносного кода (anty -APT)	Детектирование конфигураций (CSM)
Менеджер инцидентов (IRP)	Автоматизация реагирования (SOAR)	Управление рисками (SGRC)	Управление активами (assessment)
Поведенческий анализ (behavioral)	Анализ нагрузки хоста (EDR)	Анализ сетевой нагрузки (NTA)	Внешние индикаторы компрометации (TI)
Киберучения	Приманки и ловушки (DDP)	Гибридный SOC	

Сеть кибербезопасности

Anty-d-dos	Защита DNS	Обнаружение вторжений (IPS/IDS)	Потоковый антивирус
Нулевое доверие (ZTNA)	Шлюз веб безопасности (SWG)	Безопасный доступ в облако (CASB)	Межсетевой экран облака (FWaaS)
Защита удаленного доступа	Безопасность ядра сети (NGFW)	Безопасность периметра (NGFW)	Безопасность распределения (NGFW)
Защита wi-fi	Межсетевой экран веб (WAF)	Защита API	Шифрование каналов связи

Безопасность облака

Безопасный доступ в облако (CASB)	Межсетевой экран облака (FWaaS)	Контроль нагрузки облака (CWPP)
Контроль конфигураций облака (CSPM)	Контроль учетных данных в облаке (CIEM)	Антивирус в облаке (AVaaS)

Инфраструктура

Контроль обновлений	Защита от вредоносного кода	Защита виртуальных сред
Контроль целостности	Управление поставщиками	Защита от спама

Безопасная разработка

Статический анализ кода (SAST)	Динамический анализ кода (DAST)	Анализ сторонних артефактов (CSA)
Защита контейнеров	Защита Kubernetes	Тестирование на уязвимости

Защита данных

Контроль утечки (DLP)	Контроль доступа (DCAP)	Защита баз данных (DAM/DBF)
Шифрование данных	Мобильные устройства	Обезличивание данных
Защита конфиденциальных данных (PEC)		

Безопасный доступ

Единый вход (SSO)	Единая аутентификация (IAM)	Привилегированные пользователи (PAM)	Управление сертификатами (PKI)

Антифрод

Внутренний антифрод	Сессионный антифрод

Комплаенсы и аудиты

Автоматизированный пентест (BAS)	Управление комплаенсом	Управление цифровыми рисками (DRP)

Невозможность утечки чувствительных данных (пример)

SOC FORUM 2023

Люди

Ответственный за обработку ПДн

Ответственные владельцы данных на корпоративных ресурсах

Персональная ответственность работника в независимости от формы трудовой деятельности

Организационные меры

- Политика по обработки ПДн
- Регламенты обработки и защиты ПДн
- Стандарты, методики, технологические схемы

- Ответственность за разглашение конфиденциальной информации третьими лицами (NDA)
- Легализация DLP системы в корпоративном контуре банка
- Дополнительная ответственность за утечку данных при удаленной работе

Системы защиты

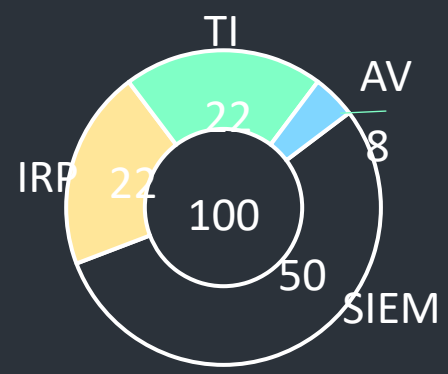
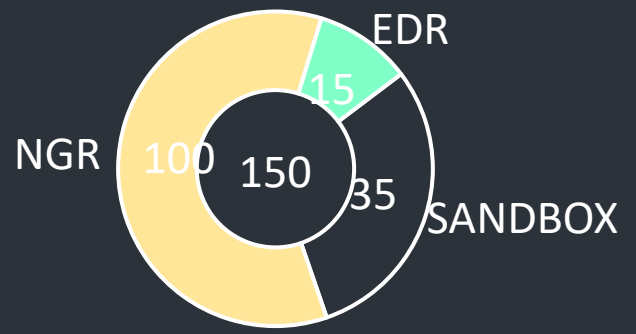
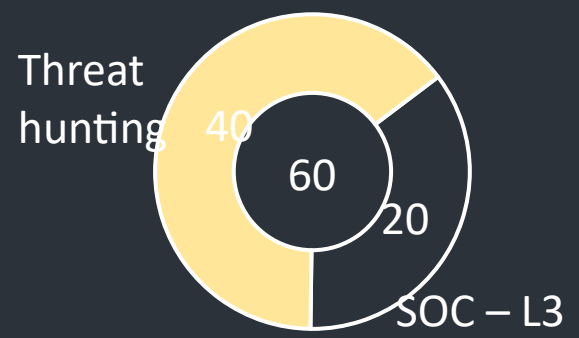
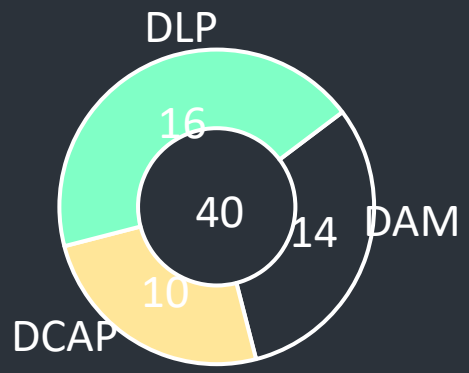
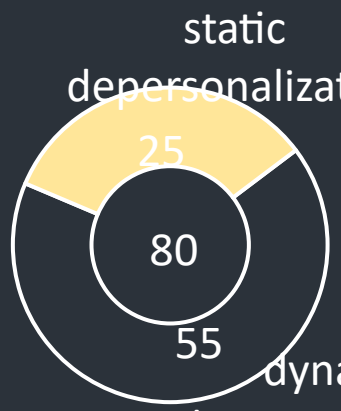
- Контроль утечки конфиденциальной информации (DLP)
- Контроль и управление доступом к неструктурированным данным (DCAP)
- Управление доступом и защита баз данных (DAM)
- Защита данных на мобильных устройствах (MDM)
- Контроль и управление доступом к сервисной инфраструктуре (CASB)
- Контроль и управление доступом к данным для привилегированных и удаленных работников
- Системы контентного и поведенческого ан

Процессы

- Маскирование баз данных при работе с партнерскими сервисами
- Шифрование баз данных при их обработке в неконтролируемой инфраструктуре
- Разделение продуктивных контуров и сегмента разработки
- Реализация требований по защите данных при проектировании инфраструктуры
- Реализация требований по защите данных при проведении пилотов и взаимодействию с партнерами
- Защита данных от искажения/ утраты

Пример финансовой модели

SOC FORUM 2023

	Операционная часть	Проектная часть	Сервисная часть
1 Противодействие атакам			
310			
2 Защита данных			
120			
430	140	230	60

+74957777171
r.lozhkin@absolutbank.ru

Москва, Цветной Бульвар 18

SOC FORUM 2023

+74957777171
r.lozhkin@absolutbank.ru

Москва, Цветной Бульвар 18