

Чек-лист для пре-пилотной встречи

Готовы ли вы к пилоту?

Инфраструктура и производительность

- Конфигурация серверов/BM проверена не только по CPU/RAM, но и по реальной производительности дисков (IOPS, чтение/запись) под целевой EPS?
- Проведено тестирование под нагрузкой, близкой к фактической, без роста очередей и задержек корреляции/обогащения?
- Настроены лимиты использования ресурсов для микросервисов под фактический поток событий?

Сценарии и контент

- В план пилота заложено время на прогон демонстрационных сценариев вендора и 1–2 критичных сценариев клиента?
- Проверена полная цепочка по сценариям: подключение источников → детекция → обогащение → реакция (авто/полуавто)?
- Определено, какие сценарии готовы к промышленному запуску, а какие требуют доработки?

Команда клиента и самостоятельность

- Предусмотрено задача «руками» для специалиста клиента (изменить правило/адаптировать сценарий/подключить источник)?
- Оценено время на выполнение задачи без постоянной помощи вендора?
- Запланировано обучение/сопровождение, если команда пока не готова самостоятельно развивать контент?

Инциденты, связанные с утечками и компрометацией

- Вы сталкивались с публикацией конфиденциальных данных вашей компании в интернете или даркнете
- Вы получали информацию о продажах доступов к корпоративным ресурсам или обсуждении уязвимостей вашей инфраструктуры на хакерских форумах
- Были кейсы использования реквизитов, платежных форм и интернет-эквайринга вашей компании мошенниками

Источники данных и коллекторы

- Выбраны основные источники событий на пилот (БД, NGFW, критичные приложения) для заказчика?
- Выбраны существующие СЗИ для интеграций по API с целью оркестрации (получение информации о пользователях, изоляция хостов, блокировка соединений)
- Используется встроенная диагностика коннекторов (сеть, права, запрос, формат данных)?
- Оценено время на адаптацию нормализации и контента под инфраструктуру клиента?

Организационная готовность

- Инфраструктура (серверы/BM, хранилища) выделена и доступна для команды внедрения?
- Сетевые доступы (порты, маршруты, firewall) настроены до старта пилота?
- Согласованы окна для совместных сессий и подтверждены ключевые специалисты клиента?

Результаты и план промышленного запуска

- Понятно, какую конфигурацию ресурсов закладывать для продакшена?
- Определён приоритетный список источников для первого этапа промышленного запуска?
- Есть утверждённый перечень сценариев, готовых к работе, и план доработки остальных?
- Оценена отказоустойчивость инсталляции?
- Понятен ли дальнейший формат взаимодействия с вендоров?