

ДЛЯ РУКОВОДИТЕЛЯ SOC, CISO И АРХИТЕКТОРА ИБ

Готовность SOC к ИИ-аналитике

Пять блоков самопроверки: что измерить до пилота, годится ли журнал инцидентов, что спросить у вендора и как сформулировать критерии успеха, пока проект ещё не начался.

Замеры до старта

Журнал инцидентов

Источники и данные

Контур и эксплуатация

Вопросы вендору

Критерии пилота

Числовых нормативов в документе нет: «нормальной доли ложных срабатываний» в отрасли не существует, а эффект зависит от качества правил корреляции, состава источников и того, как в организации считают шум. Лист даёт методику счёта и вопросы, а не отраслевые величины.

Как пользоваться

СОДЕРЖАНИЕ

- | | |
|-------------------------------------|----------------------------------|
| 1. Как пользоваться | 7. Блок 4. Контур и эксплуатация |
| 2. Кому и когда этот чек-лист нужен | 8. Блок 5. Люди и процесс |
| 3. Блок 1. Замеры до пилота | 9. Что спросить у вендора |
| 4. Чего мерить не нужно | 10. Критерии успеха пилота |
| 5. Блок 2. Журнал инцидентов | 11. Итоговая самооценка |
| 6. Блок 3. Источники и данные | 12. Если нужна помощь |

На выходе у вас будет зафиксированная база измерений собственного SOC и понимание, какие из пяти блоков готовности провалены. С этим можно предметно спорить о результате пилота через квартал — и предметно отказаться от него сейчас.

По срокам. Замеры первого блока идут фоном около трёх недель, проверка журнала занимает час, блоки про источники и людей заполняются за пару рабочих сессий. Отдельной строкой — согласования: доступ к контексту DLP, состав передаваемых полей, использование истории разборов. Эти вопросы упираются во владельцев данных и живут по своему календарю, который вы не контролируете. Начинайте их первыми, параллельно с замерами.

Если после заполнения станет ясно, что пилот сейчас не нужен, — это нормальный результат, ради которого чек-лист тоже написан.

Для заполнения от руки используйте печатную версию: светлый фон и увеличенные поля для заметок.



Кому и когда этот чек-лист нужен

Чек-лист написан для того, кто отвечает за поток: руководителя SOC, CISO, архитектора ИБ. Он нужен в момент, когда разговор об ИИ-надстройке над средствами защиты уже начался — своей инициативой, запросом от руководства или письмом вендора, — но никто ещё не назвал цифры, от которых можно оттолкнуться.

Когда заполнять рано

SIEM внедрён меньше полугода назад и правила корреляции ещё переписываются каждую неделю — сначала нужно, чтобы поток стабилизировался, иначе не с чем сравнивать.

Значительная часть первой линии отдана на аутсорс и у вас нет доступа к журналу разборов — оценивать придётся вместе с сервис-провайдером, и это другой разговор.

Основные источники событий подключены частично, и вы это знаете. ИИ-слой над неполной картиной даёт уверенные ответы на неполных данных, что хуже, чем отсутствие ответов.

Когда пора

Когда аналитик первой линии физически не успевает разобрать смену и вы это видите по времени закрытия, а не по жалобам. Когда одинаковые инциденты разные смены закрывают по-разному и никто не может сказать, какая версия правильная. Когда L2 регулярно дёргают не за экспертизой, а за справкой — посмотреть, чей это хост и что за учётка.

1 Что мерить до разговора о пилоте

Это главный блок. Если пропустить его и перейти сразу к демонстрациям, через квартал вы не сможете доказать ни эффект, ни его отсутствие: у вендора найдётся выгодная выборка, у вас — ощущения. Базу фиксируют до того, как что-либо включено, и методику счёта записывают письменно — в документе, который подписывают обе стороны.

Поток алертов на аналитика в смену

Что считаем. Количество срабатываний, доходящих до первой линии, делённое на число аналитиков в смене.

Источник. Выгрузка SIEM за период, график смен.

Формула. Алерты за период ÷ число смен ÷ число аналитиков в смене.

Типовая ошибка. Считать по среднему за календарный месяц вместе с выходными. Выходной день размывает картину буднего пика. Рабочие дни и ночные смены считайте отдельно — это разные режимы.

Значение	Период выборки	Кто считал	Дата
----------	----------------	------------	------

Доля срабатываний, закрытых как ложные или незначимые

Что считаем. Отношение закрытий со статусами «ложное срабатывание», «не подтвердилось», «легитимная активность» к общему числу закрытых инцидентов.

Источник. Журнал IRP или система учёта инцидентов.

Важная оговорка. Единого определения ложного срабатывания не существует. Легитимная активность, которую правило корректно поймало, — это ложное срабатывание или корректная работа системы? Ответ у каждого SOC свой, и его нужно зафиксировать письменно до начала замеров. Иначе через квартал спор пойдёт не о результате, а о том, что считать шумом.

Типовая ошибка. Смешивать в одну корзину закрытия «ложное» и «дубликат». Дубликаты — отдельная величина, и именно она обычно уходит первой при внедрении дедупликации.

Ваше определение ложного срабатывания:

Значение	Период выборки	Кто считал	Дата
----------	----------------	------------	------

Медианное время до первого действия аналитика

Что считаем. Интервал от появления алерта до первой отметки аналитика в карточке.

Источник. Таймстемпы IRP.

Почему медиана. Среднее по времени реакции легко «улучшить» спокойным ночным дежурством с тремя алертами и испортить одним забытым инцидентом, провисевшим сутки. Медиана показывает типичный день, а не арифметику хвостов. Средним при желании считайте дополнительно, но решения принимайте по медиане.

Типовая ошибка. Брать время смены статуса вместо времени первого действия: статус часто меняют пакетом в конце смены.

Значение	Период выборки	Кто считал	Дата
----------	----------------	------------	------

Доля разборов с ручным походом за контекстом

Что считаем. Долю инцидентов, для разбора которых аналитик открывал две и более смежные системы — каталог учётных записей, CMDB, инвентаризацию, историю по пользователю.

Источник. Автоматически из логов не достаётся. Нужна контрольная выборка — столько инцидентов, сколько команда успевает разобрать за один рабочий день, — по которым аналитик отмечает, ходил ли он за контекстом и куда.

Типовая ошибка. Оценить на глаз. Руководитель SOC и аналитик первой линии нередко называют разные величины, и разброс между ними больше, чем ожидают оба.

Значение	Размер выборки	Кто считал	Дата
----------	----------------	------------	------

Соотношение эскалаций «за справкой» и содержательных

Что считаем. Долю передач на L2, которые нужны были только для получения контекста, а не для экспертизы.

Источник. Журнал эскалаций плюс разметка силами L2 за две недели: закрывая переданный инцидент, аналитик второй линии отмечает, требовалась ли его квалификация.

Зачем. Самый чувствительный к ИИ-надстройке показатель и одновременно самый честный. Если эскалаций «за справкой» заметная часть потока, эффект вы увидите быстро. Если их почти нет — ИИ-слой даст меньше, чем обещает презентация, и лучше узнать это заранее.

Значение	Период выборки	Кто считал	Дата
----------	----------------	------------	------

Чего мерить не нужно

Отдельно про показатели, которые вам предложат и которые ничего не решают.

Точность модели, полнота, F-мера

Внутренние метрики разработчика. Они говорят о том, насколько система воспроизводит решения, принятые в исторических данных, и ничего не говорят о том, стало ли вашей смене легче. Просить их можно, принимать решение по ним — нет.

Количество обработанных событий в единицу времени

Величина растёт от объёма инфраструктуры, а не от качества работы, и в презентациях выглядит внушительно именно поэтому.

Удовлетворённость аналитиков в первый месяц

Она будет низкой у всех и у всех по разным причинам. Спрашивать имеет смысл через квартал, и лучше разговором со сменой, чем анкетой.

2 Годится ли ваш журнал инцидентов

Если система приоритизации опирается на вашу историю разборов — а так устроены не все решения, и это прямой вопрос к вендору из раздела ниже, — журнал, который вёлся небрежно, воспроизводится в подсказках вместе со всеми привычками смен. Проверка занимает час и полезна сама по себе, независимо от исхода проекта.

Возьмите тридцать закрытых инцидентов за последние три месяца, отобранных случайно, а не по памяти. Пройдите по ним и посчитайте, сколько карточек проходит по каждому критерию.

Критерий	Сколько из 30
Категория проставлена осмысленно, а не значением по умолчанию	
Комментарий о причине закрытия содержательный, не шаблон в одну строку	
По карточке спустя три месяца понятно, что произошло, без вопросов к автору	
Инцидент закрыт так же, как закрыли бы его другие смены	

Последняя строка считается иначе: найдите в выборке пары одинаковых по сути инцидентов и проверьте, совпадают ли категории. Если пар нет — выборка слишком мала или поток слишком разнообразный, отметьте это словами.

Как читать результат. Ориентируйтесь на худшую из четырёх строк — именно она определяет качество истории в целом. Если шаблонных комментариев или разнобоя между сменами набирается заметная часть выборки, историю разборов придётся приводить к единому виду, и это работа вашей команды. Делегировать её подрядчику целиком нельзя: категоризацию инцидентов в вашей инфраструктуре знаете только вы. Закладывайте её отдельным этапом до пилота, а не внутрь него.

Вывод по блоку — годится / нужна чистка:

3 Источники и данные

ИИ-слой связывает события по общим сущностям. Если сущности не совпадают, связывать нечего — карточка не соберётся, и вместо одной понятной картины аналитик получит те же разрозненные алерты, но с лишним интерфейсом.

- ☐ Подключены и стабильно отдают события: межсетевой экран, прокси, DLP, EDR, каталог учётных записей.
- ☐ В событиях присутствует идентификатор учётной записи в едином формате между источниками.
- ☐ Имена хостов совпадают между EDR, инвентаризацией и журналами прикладных систем.
- ☐ Сетевые адреса сопоставимы с активами — есть актуальная инвентаризация или CMDB.
- ☐ Все источники синхронизированы по времени, часовой пояс в событиях явный.
- ☐ Известна задержка доставки событий от каждого источника и она укладывается в приемлемое окно.
- ☐ Проверено, какой объём контекста реально отдаёт DLP: факт срабатывания политики или ещё и фрагмент, на котором она сработала.
- ☐ Определено, кто владелец каждого источника данных и с кем согласовывать расширение состава полей.
- ☐ Есть тестовый контур или возможность проверять изменения не на бое.

Про время. Единая временная база кажется мелочью до тех пор, пока связывание по временному окну не начнёт разносить события одного инцидента по разным карточкам. Расхождение в минуты между источниками ломает логику связывания целиком, и чинится это на стороне источников, а не в аналитическом слое. Проверьте до пилота — дешевле.

Про DLP. Это место, где переговоры занимают больше времени, чем доработка. Владелец данных обычно не готов отдавать содержимое срабатывания в смежную систему, и вопрос решается ролевой моделью или выборочной передачей. Начинайте обсуждение заранее.

Про правила корреляции. Аналитический слой работает поверх того, что уже сформировал SIEM. Правило, которое срабатывает на легитимную активность несколько сотен раз в сутки, после внедрения будет срабатывать столько же — изменится лишь то, что аналитик увидит эти срабатывания одной карточкой. Это разгрузка, но не исправление правила. Если у вас есть известные генераторы шума, которые давно пора переписать, — перепишите их до пилота. Иначе эффект от этой работы припишут ИИ-слою, и вы сами не поймёте, что сработало.

4 Контур и эксплуатация

Эти вопросы определяют способ поставки раньше, чем выбор продукта. Ответьте на них до демонстраций — половина вариантов отсеется сама.

- ☐ Граница защищённого сегмента, в котором живёт мониторинг, известна и зафиксирована документом.
- ☐ Понятно, что происходит при изменении границ сегмента: состав работ, чьими силами, в какие сроки.
- ☐ Решено, допускается ли исходящий канал наружу; если нет — описан порядок переноса обновлений и тот, кто его согласует.
- ☐ Описана диагностика без удалённого доступа вендора: кто выгружает журналы, в каком объёме, с какой периодичностью.
- ☐ Сроки реакции поставщика в этой схеме оценены реалистично и согласованы с тем, что пойдёт в SLA.
- ☐ Оценён дополнительный объём журналов аудита и определено место хранения.
- ☐ Определено, требуется ли журналировать каждое действие системы и каждую реакцию аналитика, и есть ли на это ресурсы.

Граница сегмента и документ, которым она закреплена:

Порядок переноса обновлений:

Схема диагностики и сроки реакции:

Что обычно недооценивают. Архитектуру продумывают все; спотыкаются на поддержке. В закрытом контуре вендор не видит вашу телеметрию и не может подключиться, чтобы посмотреть. Любая диагностика превращается в переписку с выгрузками, а значит, идёт медленнее. Это не повод отказываться от контура, но это повод описать сроки реакции честно, до подписания, а не выяснять их на первом инциденте.

Второе — объём аудита. Требование фиксировать действия системы предсказуемо, но в первоначальную оценку ресурсов попадает редко.

5 Люди и процесс

Между датой, когда система заработала, и датой, когда ею начали пользоваться, обычно проходят месяцы. Эта разница и есть главный риск проекта — технических причин у неё нет ни одной.

- ☐ Назван владелец качества подсказок — конкретный человек, а не подразделение.
- ☐ У него есть выделенное время на эту работу, и оно защищено от текучки.
- ☐ Работа с подсказками попадёт в регламент смены и в чек-лист приёма-передачи.
- ☐ Продумана обратная связь: как аналитик отмечает согласие или несогласие с предложенным приоритетом.
- ☐ Определено, кто и с какой периодичностью разбирает расхождения между решением человека и предложением системы.
- ☐ Зафиксировано письменно, что решение по инциденту принимает аналитик, а система готовит вход для этого решения.

Про владельца. Без этой роли система деградирует тихо. Точность подсказок уплывает вслед за изменениями в инфраструктуре, аналитики постепенно перестают на них смотреть, использование сходит на нет — и никто не может назвать момент, когда это произошло. Роль без выделенного ресурса не работает: если владелец совмещает её с полной загрузкой по правилам корреляции, считайте, что владельца нет.

Про разговор со сменой. Первая линия слышит про ИИ-проект раньше, чем вы успеваете его объяснить, и трактует однозначно: нас готовят к сокращению. Дальше система получает ровно то отношение, которого заслуживает угроза. Разговор стоит провести до включения, и говорить в нём про то, что изменится в смене: какие задачи уйдут, что появится взамен, кто принимает решения по инцидентам. Если сокращение действительно планируется — тем более скажите прямо; узнают всё равно, но к тому моменту обратной связи от аналитиков вы уже не получите, а без неё настройка не работает.

Про свободное время. Решите заранее, куда пойдёт высвобожденный ресурс. Разбор накопившихся низкоприоритетных срабатываний, актуализация правил, ретроспективный анализ — то, что откладывается годами. Если ответа нет, освободившееся время растворится и эффект проекта окажется невидимым для руководства.

? Что спросить у вендора

Вопросы намеренно неудобные. Уверенный ответ на каждый из них — не гарантия, но уклончивый ответ на любой — повод насторожиться.

Как система ведёт себя на инцидентах, не похожих на исторические?

Тревожный ответ: «модель обобщает». Ожидаемый: такие случаи помечаются как требующие ручного разбора, и это часть дизайна.

На какой базе измерялся заявленный эффект?

Спрашивайте про определение ложного срабатывания у того заказчика, период, размер выборки и кто считал. Процент без методики не значит ничего.

Что происходит в первый месяц после включения?

Если вам обещают эффект с первой недели без периода настройки — это продажа, а не проект.

Опирается ли система на нашу историю разборов, и если да, то как именно?

От ответа зависит объём согласований с ИБ по использованию исторических инцидентов.

Как работает решение без исходящего канала наружу?

Уточните по отдельности: обновления, лицензирование, телеметрия, диагностика.

Журналируются ли действия системы и в каком виде?

Для объекта КИИ спрашивайте, восстановима ли по журналам логика конкретной подсказки спустя месяцы.

Что нужно от нашей команды и сколько человеко-часов?

Если ответ «ничего не нужно», разговор можно заканчивать.

Кто отвечает за качество подсказок после сдачи проекта?

И что произойдёт, когда изменится состав источников.

Как измеряется деградация и кто её отслеживает?

Ответ должен содержать периодичность и ответственного, а не описание технологии.

Что система точно не умеет?

Отсутствие внятного ответа — самый надёжный признак того, что перед вами презентация, а не продукт.

Критерии успеха пилота

Сформулируйте их до старта и запишите в протокол. После — поздно: любой результат будет казаться либо победой, либо провалом в зависимости от настроения комитета.

Горизонт. Один месяц не показывает ничего, кроме просадки. Разумный горизонт оценки — квартал, из которого первые недели уходят на настройку.

База сравнения. Значения из первого блока, зафиксированные до включения, с записанной методикой счёта.

Показатели. Не больше трёх, иначе обсуждение расплывётся. Разумный набор: доля ложных срабатываний в потоке первой линии, медианное время до первого действия, доля эскалаций «за справкой».

Правило остановки. Условие, при котором пилот прекращается досрочно. Например: если через месяц после того, как настройка завершена и показатели перестали скакать, ни один из трёх не сдвинулся — проект закрывается без продолжения. Срок правила должен помещаться внутрь выбранного горизонта, иначе оно не работает ни разу.

Кто подписывает. Протокол с критериями должен быть подписан теми, кто через квартал будет оценивать результат. Если решение о продолжении принимает ИТ-директор или финансовый блок, они должны видеть критерии на старте: смена состава оценивающих в середине пилота меняет и оценку.

Предупреждение о просадке. Первые недели показатели, скорее всего, ухудшатся: дедупликация схлопнет лишнее, приоритеты поедут, отчётность станет читаться некорректно. Это ожидаемая фаза. Занесите её в протокол заранее — иначе на первом же управляющем комитете проект получит ярлык неудачного ровно тогда, когда до результата останется несколько недель.

Показатель	Значение до старта	Целевое изменение

Правило остановки и срок его проверки:

✓ Итоговая самооценка

Перенесите сюда результат по каждому блоку.

Блок	Готово	Требуется работы	Не выполнено
Замеры зафиксированы, методика записана	☐	☐	☐
Журнал инцидентов пригоден как опора	☐	☐	☐
Источники и данные подключены и сопоставимы	☐	☐	☐
Контур и эксплуатация проработаны	☐	☐	☐
Люди и процесс: владелец, регламент, обратная связь	☐	☐	☐

Вывод:

Следующий шаг и срок:

Ответственный:

Если провален любой из первых двух блоков, начинать нужно с него, а не с выбора продукта. Если провален пятый — пилот технически состоится, а организационно нет.

Если нужна помощь

Заполнить этот чек-лист можно без подрядчика — методика выложена целиком именно поэтому. Но если нужно сверить замеры с тем, что реально даёт ИИ-слой на вашем потоке, или собрать архитектуру пилота под закрытый контур, этот путь мы проходим вместе с командой заказчика.

AZONE-AI — направление корпоративных ИИ-решений компании «Азон», российского ИТ-интегратора с лицензиями ФСТЭК, ФСБ и Минобороны. Специализация — ИИ в закрытых и защищённых контурах: там, где данные не могут покинуть периметр, а любое изменение границ сегмента стоит отдельных работ.

Экспресс-оценка SOC: состав источников, качество журнала инцидентов, текущие показатели потока и оценка реалистичного эффекта — включая вариант «сейчас не нужно». Дальше, если оценка положительная, — архитектура пилота в закрытом контуре, оценка ресурсов и работы по защищённому сегменту силами лицензиата.

Обсудить пилот в вашем SOC

Подробный разбор: статья «ИИ-аналитика в SOC: что ломается в первые три месяца и как к этому подготовиться» на сайте AZONE-AI

azoneai.ru/services/ii-dlya-kii/ · ContentGuard — ИБ-аналитика поверх SIEM, DLP, NGFW и EDR · лицензии ФСТЭК, ФСБ, МО РФ · статья: azoneai.ru/blog/34-ii-analitika-v-soc-pervye-tri-mesyaca/

Документ подготовлен в сентябре 2026 года. Числовых нормативов он намеренно не содержит: доля ложных срабатываний, эффект от внедрения и сроки зависят от качества правил корреляции, состава источников и принятого в организации определения шума. Приведённые методики счёта и вопросы — рабочие ориентиры, а не отраслевая статистика. Документ не заменяет предпроектное обследование и не является техническим заданием.