ЧАСТЫЕ ВОПРОСЫ

FAQ

Продукт: СОПКА.Рой · Версия: 1.0.0 · Агент: 1.0.1 · Протокол: 1 · Редакция: 15.10.2026

Правообладатель ПО: Общество с ограниченной ответственностью «Каннам». ИНН 2543020645, ОГРН 1132543001502. Реквизиты приведены в отдельном разделе документации.

Что считается подключённым клиентом?

Клиент считается online, когда сервер недавно получил heartbeat или подтверждённое присутствие через Socket.IO. При длительном отсутствии сигнала клиент отображается offline.

Событие всегда становится инцидентом?

Нет. Событие фиксирует наблюдаемый факт. Инцидент создаётся только тогда, когда сработавшая политика требует отдельного расследования.

Можно контролировать любой компьютер сотрудника?

Контроль выполняется только на законных основаниях, в пределах полномочий организации, локальных нормативных актов и информирования работников. Наличие технической функции само по себе не является правовым основанием.

Где хранится история?

Прикладные сущности находятся в PostgreSQL, история DLP-событий - в ClickHouse, бинарные материалы - в RustFS/S3. PostgreSQL outbox временно хранит принятые, но ещё не подтверждённые ClickHouse события. Временные состояния обрабатывает сервер.

Почему клиент не появляется после установки?

Проверьте службу Windows, адрес сервера, DNS, TLS, доступ к порту 443, срок действия регистрационного ключа, его рабочую область и журнал агента.

Почему клиент online, но время последнего heartbeat старое?

Оперативный статус может обновляться через серверные уведомления быстрее, чем поле `last_seen` записывается в PostgreSQL. При диагностике учитывайте оба источника.

Почему политика не применилась?

Проверьте включённость политики и правила, платформу, область, условия AND/OR, поддержку и разрешение функции, получение актуальной конфигурации. Затем сопоставьте приоритет политики и правила, исключаемые действия и результат выполнения. Критичность не задаёт порядок оценки; совпадение не доказывает успешное действие.

Почему нет нужного события?

Проверьте период и фильтры, разрешение функции в возможностях, поддержку и работу модуля агента, доставку локальной очереди и перенос принятых событий в историю. Правило задаёт условия и реакции, а не заменяет разрешение функции. Отсутствие совпадения правила и отсутствие самого события - разные ситуации.

Можно использовать один установочный ключ на нескольких ПК?

Только в пределах предусмотренного режима массовой регистрации и срока действия токена. Сервер проверяет UUID и параметры регистрации; копирование готовой папки агента не должно создавать рабочий клон на другом компьютере.

Какие данные передаёт контроль буфера обмена?

В событии могут присутствовать тип данных, контекст процесса и окна, доступные сведения о содержимом и совпадении. Фактический состав зависит от агента и обработки события. В текущем редакторе правил нет переключателя передачи полного содержимого; поля ключевых слов и регулярных выражений задают сопоставление, а не разрешение хранить полный текст.

Можно держать прямой экран включённым постоянно?

Нет. Рекомендуемый режим - ручной запуск уполномоченным администратором, аудит действия и обязательное завершение сеанса сразу после выполнения задачи.

Почему не открывается предпросмотр файла?

Проверьте доступность клиента, существование файла, лимит размера, права роли, разрешённость пути и состояние защищённой preview-сессии.

Что делать, если часть функций временно недоступна?

Проверьте подключение, выбранную область, права и состояние агента. Если проблема сохраняется, сообщите оператору время и сообщение об ошибке.

Где задаются сроки хранения?

В настройках рабочей области. Значения выбираются с учётом локальных актов, расследований, доступного диска и резервного копирования.

Поддерживается ли Linux?

В версии 1.0.0 агент поддерживает Windows x64. Linux пока не поддерживается.

Как получить демонстрацию?

Направьте запрос на office@kannam.pro.

Почему событие принято, но его ещё нет в журнале?

Проверьте период и фильтры, доставку очереди в ClickHouse и состояние task-worker. Приём и доступность в основном журнале могут происходить в разное время. Некоторые экраны, включая снимки, могут показать только что принятый материал до переноса; это не подтверждает готовность всей истории. Не очищайте очередь до выяснения причины.

Почему online-клиент не отдаёт экран или PowerShell?

Служба может быть на связи, когда пользовательский агент не работает в нужном интерактивном сеансе. Проверьте вход пользователя, capabilities, роль и результат команды. Прямой экран не является удалённым вводом мыши и клавиатуры.

Достаточно ли сохранить дамп PostgreSQL?

Нет. Для полного восстановления нужны также история ClickHouse, объекты S3, конфигурация и ключи. Проверяйте восстановление на отдельном стенде.

Почему приглашение не пришло по почте?

Проверьте адрес получателя, состояние приглашения, настройки SMTP, доступность почтового сервера и его журнал доставки. Не передавайте SMTP-пароль вместе с диагностикой.

Почему в истории только 1.0.0?

Документация описывает единственный текущий выпуск продукта 1.0.0. Технический каталог установочных пакетов не подменяет историю опубликованной документации.

Какая конфигурация нужна на 1000 агентов?

В «Системных требованиях» приведён начальный бюджет умеренного профиля и отдельные расчёты снимков и событий. Он относится к заданным частотам, сроку хранения и операциям пользователей. 1000 активных устройств не равны 1000 одновременным прямым экранам. Фактическую ёмкость подтверждают нагрузочным испытанием; увеличение числа потоков приложения само по себе её не гарантирует.

Почему AI-чат не отвечает на обычные вопросы?

Область ограничена DLP и информационной безопасностью. Посторонний запрос получает стандартный отказ.

Почему исчез интернет-переключатель?

Аналитик сам выбирает публичный поиск при необходимости и наличии настроенного сервиса.

Кто видит мои чаты?

В интерфейсе — только вы в соответствующей рабочей области. История сохраняется в рабочей области и доступна после повторного входа. Удаление чата не сбрасывает квоту.

Можно ли поручить AI удалить сертификат или запустить команду?

Сертификаты и политики AI не изменяет. Разрешённые команды обслуживания и питания можно подготовить для компьютера, группы или всей области; отправка требует кнопки «Выполнить». Отключённые компьютеры пропускаются.

Подробнее: AI-чат: анализ безопасности.