ЕЖЕДНЕВНАЯ РАБОТА

Руководство пользователя

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.

Назначение и адрес системы

Руководство предназначено для операторов, аналитиков и администраторов рабочей области. Одинаковые основные сценарии применимы к SaaS и локальному развёртыванию; доступные разделы зависят от роли, состава поставки и настроек рабочей области.

В примерах используется условный адрес https://servername.com. Замените его полным адресом консоли, полученным от администратора или поставщика SaaS. Если при развёртывании выбран префикс приложения, он входит в этот адрес. servername.com не является адресом сервиса СОПКА.Рой. Адрес агента и адрес входа уточняются при установке; их нельзя вычислять по произвольному примеру.

Расчёт на 1000 агентов относится к серверу и заданной нагрузке. Интервалы снимков, массовые выгрузки и сроки хранения согласуют с администратором по «Системным требованиям».

Начало работы

1. Откройте выданный HTTPS-адрес в поддерживаемом браузере и войдите со своей учётной записью.
2. Проверьте выбранную рабочую область и свою роль. Данные разных рабочих областей не объединяются автоматически.
3. Проверьте часовой пояс, период фильтра и наличие нужных прав. Неверный период может создавать впечатление отсутствия событий.
4. При первом вводе согласуйте состав каналов, сроки хранения и ответственных за инциденты. Администратор создаёт регистрационный ключ, устанавливает агент на тестовый компьютер и проверяет связь.

В SaaS серверную инфраструктуру обслуживает поставщик; администратор организации управляет своей рабочей областью, пользователями, устройствами и правилами. В локальном контуре организация дополнительно отвечает за сервер, сертификаты, хранилища, обновления и резервное копирование.

Роли и разделы

Администратор управляет рабочей областью и доступом; редактор выполняет доступные ему операции расследования и настройки; наблюдатель просматривает разрешённые данные. Доступность отдельной команды проверяется отдельно. Если кнопка отсутствует или операция запрещена, обратитесь к администратору, а не используйте другую учётную запись.

Раздел	Задача пользователя
Дашборд	Оценить доступность клиентов, открытые инциденты и активность за выбранный период. Отсутствие событий не доказывает отсутствие нарушений.
Клиенты	Найти компьютер, проверить последнюю связь, версию агента и применённые настройки; открыть карточку и результаты команд.
Группы	Объединить компьютеры для назначения настроек. Один клиент может входить в несколько групп.
Возможности	Разрешить функции клиенту или группе и проверить поддержку, наследование и итоговое состояние.
Политики	Задать условия обнаружения, исключения, реакции и явные действия на компьютере.
События	Отфильтровать наблюдения по времени, клиенту и каналу; изучить совпадения и фактические результаты.
Инциденты	Разобрать значимые срабатывания, назначить ответственного и сохранить ход расследования.
Файлы	Создать задания поиска, запустить их, изучить результаты, маркировки и доступные файловые операции.
Отчёты	Получить доступные отчёты за согласованный период и проверить выбранную область данных.
Установка	Получить пакет агента и регистрационный ключ в рамках своей рабочей области.

Раздел	Задача пользователя
Настройки	Управлять доступными параметрами рабочей области и уведомлениями.

Ежедневный рабочий цикл

1. Проверьте дашборд и время последней связи устройств. Online означает связь агента; готовность пользовательской сессии проверяется отдельно.
2. Откройте критические и новые инциденты. Сопоставьте компьютер, пользователя, канал, время и правило.
3. Посмотрите исходное событие и результат реакции. Срабатывание правила, постановка команды и выполнение действия - разные факты.
4. Назначьте ответственного, оставьте комментарий и выберите статус, соответствующий результату расследования.
5. При ложном срабатывании уточните условие или узкое исключение и повторите тест. Не отключайте все каналы для устранения одного совпадения.

Карточка клиента и команды

В карточке проверяйте идентичность компьютера, последнюю связь, версию, группы, применимость политик и доступные возможности. Вкладки дают сведения о программах, устройствах, сети, событиях, снимках и операциях, если они доступны для данного клиента.

Перед запуском команды проверьте нужный компьютер, полномочия и готовность агента. После запуска дождитесь итогового статуса и изучите результат. Ожидание, выполнение, успех, ошибка и отмена не взаимозаменяемы. Повтор команды при неизвестном результате может повторить действие.

Прямой экран служит для просмотра рабочего стола и не предоставляет управление мышью и клавиатурой. Для снимков, прямого экрана и интерактивной консоли нужен готовый пользовательский процесс агента. Команды питания, отключения устройств и завершения процессов могут прервать работу; заранее определите способ восстановления доступа.

Настройка возможностей и политик

1. В «Возможностях» выберите тестовую группу. Разрешите только нужные функции и проверьте итоговое состояние клиента.
2. В «Политиках» выберите канал, область действия, условия и режим наблюдения. Задайте создание инцидента отдельно.
3. Сверьте поля с документом «Политики и каналы контроля»: режим, приоритет политики и правила, AND/OR, критичность, реакции и исключаемые действия.

4. Включайте явные действия только после проверки наблюдения. Дождитесь получения настроек агентом и подтвердите фактический результат.

Поиск и операции с файлами

Откройте задание по названию; проверьте целевые клиенты, каталоги, фильтры и расписание. Ручной запуск не требует ожидания расписания. История и счётчики относятся к конкретному запуску и компьютеру. Оценка оставшегося времени ориентировочная.

Предпросмотр зависит от формата и размера файла. Скачивание и передача на клиент являются отдельными разрешениями. Найденный файл мог измениться или исчезнуть после поиска. Статус поиска не подтверждает успешное скачивание, а запрос карантина не подтверждает фактическую изоляцию файла.

Фильтры, таблицы и экспорт

Перед сравнением данных сверяйте период, часовой пояс, рабочую область, клиента и канал. Меню таблицы «…» позволяет выбрать от 1 до 50 записей либо исходное значение; Ctrl+клик используется для выбора строк там, где это поддерживается. Экспортируйте только необходимый объём, проверяйте содержимое файла и передавайте его согласованным способом.

Если данные или функция недоступны

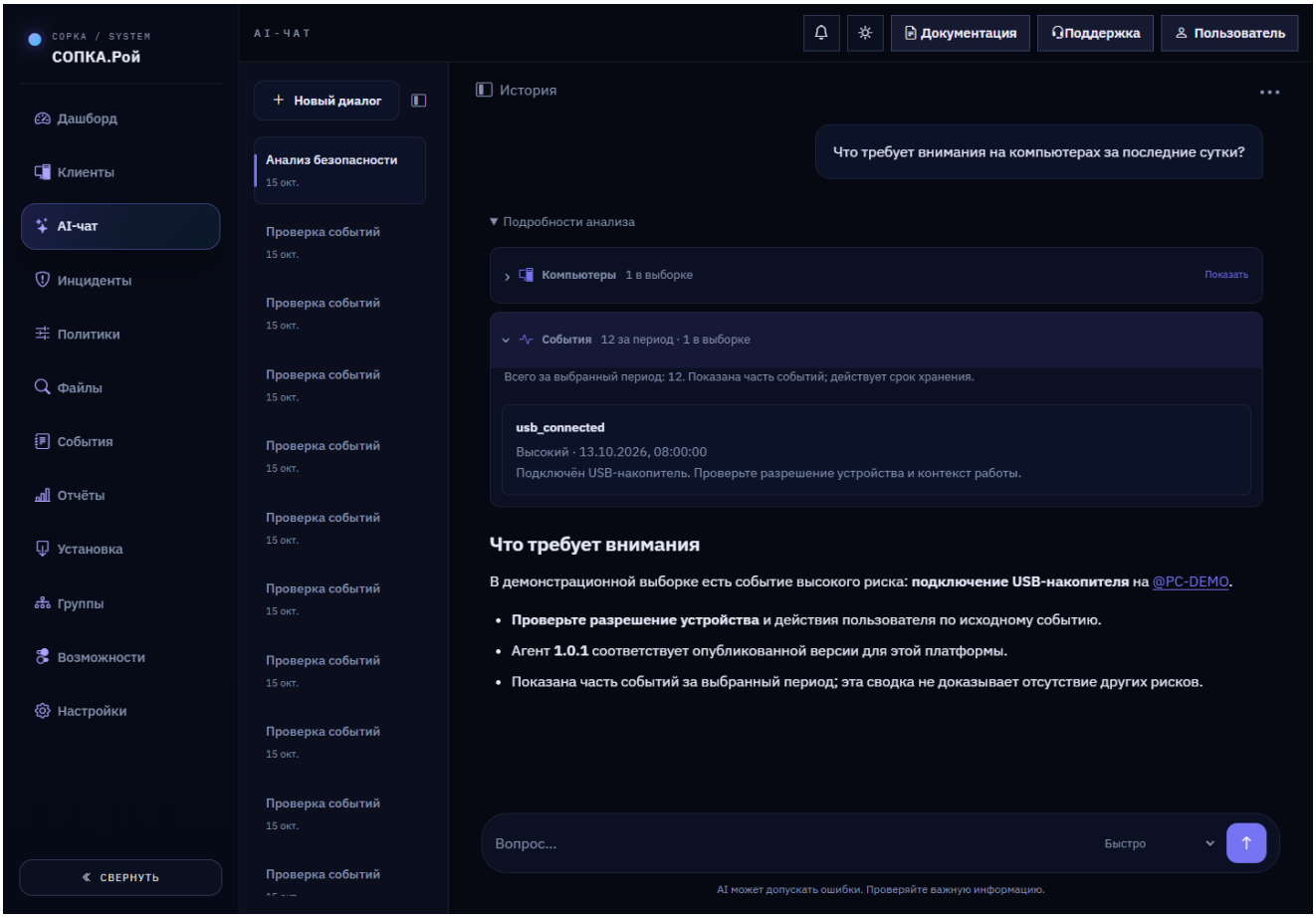
- Нет клиентов: проверьте рабочую область, регистрацию и фильтры.
- Клиент offline: уточните питание компьютера и сетевую доступность у ответственного администратора.
- Нет событий: проверьте период, разрешение канала, поддержку агента и применимость правил.
- Нет снимка или сеанса: проверьте пользовательскую сессию, разрешение функции и итоговую ошибку команды.
- Не сработало действие: изучите совпадение, исключения, конфликт приоритетов, полномочия и результат исполнения.
- Нет уведомления: создание инцидента, уведомление пользователя и доставка административного уведомления настраиваются отдельно.

Обращение в поддержку и завершение работы

Укажите версию, время с часовым поясом, раздел, ожидаемый и полученный результат и обезличенный пример. Не прикладывайте пароли, ключи регистрации, токены, cookies и полные конфигурации. Завершайте интерактивные сеансы и выходите из консоли на общем компьютере.

Работа с AI-чатом

Откройте AI-чат, укажите компьютер или период и цель. Диалоги личные; результаты инструментов раскрываются по клику. Единый выбор глубины анализа влияет на подготовку ответа. Для объектов используйте @; подтверждения команд находятся под ответом. Ограничения квот действуют независимо от создания нового чата.



Подробнее: AI-чат: анализ безопасности.

PDF через AI

Попросите создать отчёт: помощник использует шаблон раздела «Отчёты» и выдаёт ссылку «Скачать PDF». Серверная копия доступна автору 24 часа, затем удаляется фоновой очисткой.