МОДЕЛЬ ЗАЩИТЫ

Безопасность

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.

Контур эксплуатации

СОПКА.Рой используется как SaaS либо развёртывается в инфраструктуре организации или в выделенном контуре. Сервер размещается в инфраструктуре заказчика или в согласованном защищённом контуре. Доступ пользователей, состав включённых модулей контроля, сроки хранения и порядок реагирования определяются договором, локальными актами и ролями рабочей области.

Сервер приложения публикуется через reverse proxy по HTTPS. PostgreSQL, серверные службы и служебные endpoints не предназначены для прямой публикации в Интернет. Проверки `/roy/api/health/live` и `/roy/api/health/ready` используются для локального мониторинга контейнера и reverse proxy.

Разграничение доступа

Данные клиентов, событий, инцидентов, политик и заданий относятся к рабочей области. Пользователь получает доступ только к тем рабочим областям, где он является участником. Роли `admin`, `editor` и `viewer` ограничивают управление пользователями, политиками, клиентами, расследованиями и настройками.

Проверка рабочей области выполняется на сервере. Идентификаторы, переданные из формы или JSON, не считаются основанием доступа без проверки роли пользователя или валидного агентского секрета.

Регистрация агента

Windows-агент регистрируется по регистрационному ключу. Ключ привязан к рабочей области, действует ограниченное время и после создания показывается полностью только один раз. В дальнейшем интерфейс отображает preview, чтобы администратор мог сверить начало и конец ключа без раскрытия полного секрета.

После регистрации агент получает device-токен. Этот токен используется для heartbeat, получения политик, отправки событий, статусов команд и запросов обновления. При отзыве регистрации сервер прекращает принимать новые запросы от соответствующего клиента.

Подпись политик и обновлений

Bundle политик подписывается Ed25519. Агент проверяет подпись и версию протокола до применения правил. Это защищает клиент от применения неподписанного или несовместимого набора политик.

В основном EXE-сценарии агент проверяет SHA-256 пакета, полученного по защищённому grant, и запускает штатный установщик. Подписанный Ed25519 манифест и CopkaRoyUpdater.exe относятся к legacy ZIP-сценарию. Не подменяйте проверенные пакеты произвольным EXE и не отключайте проверки для обхода ошибки обновления.

Интерактивные каналы

Прямой экран и удалённый PowerShell являются интерактивными функциями и запускаются только по явной команде пользователя с соответствующей ролью. Их нельзя считать фоновым постоянным мониторингом: сеанс должен быть инициирован, завершён и отражён в журнале действий.

Интерактивный обмен использует временные сессионные ключи и аутентифицированное шифрование. Детали криптографического формата относятся к внутренней документации сопровождения.

Ввод и вывод удалённой консоли защищаются в рамках сеанса. При невозможности согласовать защиту операция завершается ошибкой. Корректность работы зависит также от оперативного состояния серверной инфраструктуры.

Хранение и журналы

PostgreSQL хранит прикладные сущности, ClickHouse - историю событий, S3 - бинарные материалы. Доступ к каждому хранилищу и резервным копиям ограничивается отдельно. Журналы и экспорт могут содержать чувствительные данные; исключайте токены и секреты из обращений в поддержку.

Снимки экрана, прямой экран, клавиатурные события, буфер обмена и загрузка файлов относятся к чувствительным функциям. Их использование должно быть разрешено политикой организации, отражено в локальных документах и ограничено кругом уполномоченных пользователей.

Сетевой периметр

- публикуется HTTPS reverse proxy по согласованному адресу; `/roy` - пример префикса приложения;
- служебные проверки готовности доступны из локальной сети или с reverse proxy;
- PostgreSQL и серверные службы остаются во внутренней Docker-сети;
- WebSocket upgrade разрешается только для маршрутов продукта;
- резервное копирование и восстановление проверяются до ввода в эксплуатацию.

Секреты и эксплуатационные границы

Тестовые значения .env.example нельзя оставлять в рабочем контуре. Разделяйте учётные записи приложения, мигратора, резервного копирования и аналитики. Приватные ключи, device-токены, SMTP-пароли и ключи S3 не должны попадать в общедоступные логи, скриншоты и HAR.

Шифрование интерактивного потока не означает одинаковую модель защиты всех функций: сервер принимает и обрабатывает телеметрию и отдельные файловые операции. Не обещайте недоступность данных серверу там, где конкретный протокол этого не обеспечивает.

Проверка доступа

Проверяйте операции не только под admin, но и под ограниченной ролью и пользователем другого workspace. Скрытая кнопка не заменяет серверную проверку. Browser API требуют сессию, same-origin контекст и внутренний токен; изменяющие запросы защищаются CSRF. Отдельный контур Owner API не следует использовать как пользовательскую интеграцию.

Политики, права и восстановление

Приоритет политики и правила, критичность результата и полномочия оператора имеют разные назначения. Исключение отменяет выбранные действия с учётом приоритетов; разрешение возможности не выдаёт административную роль. Отключение политики не восстанавливает автоматически учётную запись, устройство или сетевой доступ после выполненного действия. Для таких операций предусматривают разрешённый способ возврата доступа. Увеличение нагрузки и объёма хранения не расширяет права доступа к материалам.

Граница доверия AI-аналитика

Ответы модели, тексты событий и публичные источники не являются инструкциями безопасности. Проверки прав, изоляция областей, схемы инструментов и серверные квоты действуют независимо от модели. Очевидные попытки переопределения роли блокируются; семантический фильтр не гарантирует защиту от всех инъекций. Вопрос и ограниченные метаданные передаются внешнему сервису генерации; поисковый API получает только фиксированные публичные темы.

Подробнее: AI-чат: анализ безопасности.