ЕЖЕДНЕВНАЯ РАБОТА

Руководство пользователя

Продукт: СОПКА.Рой · Версия: 1.0.0 · Агент: 1.0.0 · Протокол: 1 · Редакция: 14.08.2026

1. Назначение руководства

Руководство предназначено для операторов, аналитиков и администраторов рабочей области СОПКА.Рой. В нём описана ежедневная работа в веб-интерфейсе: от входа и выбора рабочей области до расследования инцидента и проверки состояния агента.

2. Вход в систему

1. Откройте адрес продукта с базовым путём `/roy`.
2. На публичной стартовой странице нажмите «Открыть систему».
3. Введите логин и пароль и подтвердите вход.
4. После входа система откроет дашборд либо предложит создать или выбрать рабочую область.

Не передавайте пароль и ссылки-приглашения другим лицам. После работы на чужом компьютере обязательно завершайте сеанс через кнопку выхода.

3. Рабочая область и роли

Все клиенты, политики, события и инциденты принадлежат выбранной рабочей области. Переключение выполняется в верхней панели. Пользователь не должен видеть данные рабочих областей, участником которых он не является.

Роль	Основные действия
Администратор	Управление рабочей областью, приглашениями, агентами, политиками, установочными токенами и чувствительными удалёнными функциями.
Редактор	Работа с событиями, инцидентами, группами, политиками и заданиями поиска в пределах выданных разрешений.
Наблюдатель	Просмотр разрешённых данных без изменения конфигурации.

4. Навигация

Раздел	Назначение
Дашборд	Сводные показатели клиентов, подключений, событий и активных инцидентов.
Клиенты	Список рабочих станций, состояние агента, версия, имя пользователя и переход в карточку клиента.
Группы	Логическое объединение клиентов для назначения и сопровождения политик.
Инциденты	Очередь расследования, поиск, фильтры, статусы и карточка инцидента.
Политики	Создание и редактирование правил контроля по каналам.
Поиск файлов	Задания сканирования, запуски, найденные файлы, метки, watchlist, предпросмотр и загрузка.
Журналы	События агентов и сведения, необходимые для анализа действий.
Установка	Создание временного токена и формирование пакета Windows-агента.
Настройки	Параметры рабочей области, часовой пояс, сроки хранения и разрешение удалённых функций.

5. Дашборд

Дашборд используется для первичной оценки состояния контура. Карточки показывают общее и активное количество клиентов, число инцидентов и объём принятых событий. Графики отражают активность за последние дни, распределение инцидентов по критичности и наиболее частые типы событий.

Рекомендуемый порядок проверки

1. Сравните количество всех и подключённых клиентов.
2. Проверьте рост новых или активных инцидентов.
3. Оцените резкие изменения объёма событий.
4. Перейдите в список клиентов или инцидентов для детализации.

6. Клиенты и группы

В списке клиентов доступны поиск и фильтрация по идентификатору, имени компьютера, пользователю, операционной системе, группе и состоянию. Статус online означает, что сервер недавно получил heartbeat или подтверждённое присутствие Socket.IO. Offline означает отсутствие актуального сигнала.

Типовые действия

• открыть карточку клиента для подробного анализа;

• переименовать клиент понятным служебным именем;

• назначить клиенту группу;

• архивировать, восстановить, отозвать доступ или удалить регистрацию;

• проверить UUID, версию агента, последнее подключение и активную политику.

Удаление и отзыв доступа влияют на возможность дальнейшей связи агента с сервером. Перед действием убедитесь, что выбран правильный компьютер.

7. Карточка клиента

Карточка объединяет сведения конкретной рабочей станции. Набор вкладок зависит от роли и поступивших данных.

Вкладка или блок	Содержание
Обзор	Идентификаторы, имя компьютера, пользователь, ОС, IP, состояние и версия агента.
События	Хронология действий с фильтрами по типу, периоду и содержимому.
Инциденты	Инциденты, связанные с выбранным клиентом.
Приложения и окна	Запущенные процессы, пути, версии, издатели и заголовки окон при наличии соответствующей политики.
USB и сеть	Подключения устройств и состояние контролируемых сетевых интерфейсов.
Файлы	Файловые события и результаты заданий поиска.
Снимки	Разовые и периодические снимки экрана в пределах разрешений рабочей области.
Прямой экран	Ручной сеанс просмотра, доступный только уполномоченному администратору.
Команды и аудит	Отправленные команды, состояние исполнения и журнал действий оператора.

8. События и журналы

Событие фиксирует наблюдаемый факт: запуск приложения, действие с файлом, использование буфера обмена, подключение USB, изменение сетевого интерфейса или другое действие агента. Событие не обязательно является нарушением.

Просмотр события

1. Откройте «Журналы» или вкладку событий клиента.
2. Задайте период и тип события.
3. Проверьте компьютер, пользователя, процесс, путь, время и полезную нагрузку.
4. Сопоставьте событие с политикой и связанным инцидентом.

Время агента передаётся в UTC и отображается в часовом поясе пользователя. При сравнении с внешними журналами учитывайте выбранный часовой пояс.

9. Работа с инцидентами

Инцидент создаётся, когда решение политики требует отдельного расследования. Он содержит описание, критичность, источник, доказательства и историю обработки.

Рекомендуемый цикл расследования

1. Откройте новый или активный инцидент.
2. Проверьте рабочую область, клиента, пользователя, время и канал.
3. Изучите исходное событие, процесс, файл, устройство или сетевое назначение.
4. Проверьте сработавшее правило и его приоритет.
5. Назначьте ответственного и измените статус на рабочий.
6. Добавьте комментарий с результатами проверки.
7. Подтвердите нарушение, отклоните срабатывание либо отметьте его как ложное.
8. При необходимости скорректируйте политику, сохранив историю инцидента.

Не удаляйте доказательства до завершения расследования и истечения установленного срока хранения.

10. Политики контроля

Политика определяет канал, условия совпадения, приоритет и решение. Правила одного канала проверяются от большего приоритета к меньшему; первое подходящее правило определяет результат.

Создание правила

1. Откройте «Политики» и нажмите добавление.
2. Выберите канал: файлы, буфер обмена, приложения, USB, сеть или другой доступный модуль.
3. Задайте область действия: все клиенты, группа, компьютер или пользователь.
4. Добавьте условия по процессу, пути, расширению, ключевым словам, регулярному выражению, устройству или назначению.
5. Выберите решение: разрешить, запретить, наблюдать или игнорировать.
6. Укажите дополнительные действия: записать событие, создать инцидент, уведомить или выполнить поддерживаемое блокирование.
7. Сохраните правило и проверьте его на тестовом клиенте.

Сначала используйте режим наблюдения. После проверки точности переводите правило в блокирующий режим.

11. Поиск файлов

Поиск файлов используется для централизованного обнаружения документов по имени, расширению, пути, размеру, хэшу и признакам содержимого.

Создание задания

1. Откройте «Поиск файлов» и создайте новое задание.
2. Выберите целевые клиенты или группы.
3. Укажите разрешённые каталоги и исключения.
4. Задайте маски имён, расширения, размер и условия анализа содержимого.
5. Настройте разовый запуск или расписание.
6. Сохраните задание и запустите его.

Разбор результатов

• следите за состоянием запуска и количеством обработанных клиентов;

• откройте карточку найденного файла и проверьте путь, размер, время и хэши;

• используйте метки и статусы проверки для совместной работы;

• добавляйте важные файлы в watchlist для отслеживания изменений;

• предпросмотр и загрузку выполняйте только при наличии полномочий и служебной необходимости.

12. Снимки и прямой экран

Разовый снимок запрашивается из карточки клиента. Прямой экран запускается вручную и должен быть остановлен сразу после выполнения задачи. Доступ ограничивается ролью администратора и настройками рабочей области.

1. Убедитесь, что клиент online.
2. Проверьте правовое основание и служебную необходимость.
3. Запустите снимок или сеанс просмотра.
4. Дождитесь подтверждения агента.
5. После проверки остановите прямой экран и убедитесь, что команда завершена.

13. Установка и повторная регистрация агента

В разделе «Установка» администратор создаёт временный токен и скачивает пакет, привязанный к рабочей области. На целевой станции пакет запускается с правами администратора. После установки клиент должен появиться в списке, передать heartbeat и получить подписанную политику.

При повторной установке сначала определите, нужно восстановить существующую регистрацию или отозвать старую и создать новую. Один и тот же экземпляр ключа не должен использоваться для несанкционированного клонирования агента на другой компьютер.

14. Настройки и хранение

Администратор задаёт часовой пояс, сроки хранения событий, инцидентов и снимков, а также разрешает или запрещает чувствительные функции. Изменения должны соответствовать локальным нормативным актам организации.

15. Типовые проблемы

Симптом	Что проверить
Клиент offline	Службу Windows, адрес сервера, DNS, TLS, локальный firewall, токен и журнал агента.
Политика не применяется	Область действия, включённость правила, приоритет, версию bundle, подпись и совместимость протокола.
Нет события	Включён ли канал, попадает ли процесс в исключения, работает ли пользовательский агент и нет ли лимита размера пакета.
Команда долго выполняется	Состояние клиента, очередь Redis, Socket.IO/WebSocket и журнал команд.
Не открывается предпросмотр	Доступность клиента, существование файла, лимит размера, права роли и состояние защищённой сессии.

16. Завершение работы

Закройте открытые сеансы прямого экрана, сохраните комментарии по расследованиям и выполните выход из системы. Не оставляйте интерфейс открытым на общедоступном рабочем месте.