

RULE ENGINE

Политики и каналы контроля

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

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

Модель правила

Каждая политика имеет канал, приоритет, область действия и решение. Включённые правила выбранного канала проверяются от большего приоритета к меньшему. Первое совпавшее правило определяет результат.

Группа условий	Примеры
Субъект	Пользователь, группа, компьютер.
Процесс	Все процессы, allowlist, denylist или исключения.
Содержимое	Ключевые слова, регулярные выражения, расширения, имя и путь файла.
Устройство	Тип, серийный номер, доверенные и запрещённые накопители.
Сеть	Интерфейс, домен, адрес назначения и категория канала.

Решения

- allow - разрешить и при необходимости записать событие;
- deny - запросить блокирование, если модуль канала это поддерживает;
- monitor - наблюдать без блокирования;
- ignore - не обрабатывать совпавшее событие.

Дополнительные действия: запись события, создание инцидента, уведомление администратора, очистка буфера, карантин и блокирование.

Основные каналы

Канал	Что контролируется
clipboard	Копирование и вставка, процесс и окно, хэш/маскированный фрагмент, совпавшие правила.
files	Создание, изменение, копирование, перенос, удаление и восстановление файлов.
usb	Подключения, отключения и идентификаторы внешних устройств.
applications	Процессы, пути, окна и признаки запрещённых приложений.
network_interfaces	Wi-Fi, Ethernet, VPN, Bluetooth и виртуальные интерфейсы.
browser/messengers	События загрузки, передачи файлов и контролируемые приложения.
keylogger	Только при явном разрешении; по умолчанию минимизированные и аудируемые данные.

Пример минимального правила

```
{
  "name": "Контроль ключевых файлов на USB",
  "enabled": true,
  "priority": 100,
  "channel": "files",
  "content_rules": {"extensions": [".pem", ".key"]},
  "device_rules": {"target": "usb"},
  "decision": {
    "effect": "deny",
    "action": "create_incident",
    "severity": "high",
    "store_full_content": false
  }
}
```

Принцип минимизации

Для clipboard и клавиатурных событий полный текст не следует отправлять на сервер без отдельного обоснованного правила. Предпочтительны хэш, маскированный фрагмент и список совпавших признаков.