Nevel

БЕЗОПАСНОСТЬ

Контроль доступа и аудит

События запросов и администрирования, модель доступа к журналам, SIEM, расследование и проверка полноты.

Облако / В контуре

https://docs.nevel.sh/security/access-audit/

Аудит Nevel связывает действие с проверенной идентичностью, рабочим пространством, объектом, применённой политикой и результатом. Его задача — ответить, кто получил доступ, что было разрешено или запрещено, куда отправился запрос и какие настройки действовали в этот момент. Журнал не должен превращаться во второе неограниченное хранилище корпоративной переписки.

Метаданные события и содержание запроса разделяются. Для расследования часто достаточно идентификатора, времени, типа действия, модели, маршрута, количества найденных сущностей и причины отказа. Полные тела запросов не являются обязательным условием аудита; их дополнительное хранение повышает чувствительность журнала и требует отдельного срока и права доступа.

Какие действия регистрируются

Категория	События	Почему это нужно
Вход и доступ	Успешный и неуспешный вход, отказ проверки, прекращение доступа	Отличить ошибку пользователя от попытки получить чужие полномочия
Пользователи и роли	Приглашение, изменение роли, членство, отзыв	Восстановить, кто обладал правом на момент операции
API-ключи	Создание, изменение ограничений, отзыв, отказ использования	Связать интеграцию с владельцем и обнаружить компрометацию
Модельные запросы	Приём, решение политики, выбранная модель, результат, ошибка	Проверить фактическую цепочку обработки
Guardrail	Режим, типы и число масок, категория, блокировка или смена маршрута	Понять основание отправки или отказа
Файлы и знания	Загрузка, изменение доступа, извлечение, удаление, выдача контекста	Установить происхождение данных и последствия изменения прав
Подключения	Авторизация, изменение области, вызов, отзыв	Установить, какой инструмент получил доступ к источнику
Управление защитой	Изменение политики, получателя, логирования и хранения	Обнаружить попытку ослабить контроль
Эксплуатация	Административный доступ, экспорт, восстановление, удаление	Проследить действия вне обычного пользовательского интерфейса

Не каждый тип события обязан включать содержимое объекта. Например, изменение роли фиксирует прежнее и новое полномочие, но не требует добавления всех диалогов пользователя в запись.

Поля события запроса

Базовая запись содержит идентификатор запроса, время, пользователя или идентификатор ключа, рабочее пространство, модель, периметр обработки, типы и количество замен, статус и описание ошибки безопасного уровня детализации. Для on-prem и облака место платформы отделяется от модельного маршрута: локальная модель, российский провайдер, self-hosted Nevel в РФ или глобальный получатель. Имя модели без endpoint и получателя не объясняет, куда ушёл запрос. Для воспроизводимости решения добавляются версия политики и стадия обработки. При нескольких модельных вызовах одной задачи важно различать родительскую операцию и отдельные обращения.

Ниже — **референсный профиль события** `nevel.audit.reference/1` для проектирования экспортера и проверки нормализатора. Это не контракт существующего Nevel API, не имя готового коннектора и не конфигурация, которую можно импортировать в любую SIEM. Значения синтетические. Адаптер конкретной поставки связывает реальные поля источника с этим профилем; отсутствующее поле отмечается как отсутствующее, а не заполняется догадкой.

```
{
  "schema_version": "nevel.audit.reference/1",
  "source_instance": "example-onprem-01",
  "event_id": "11111111-2222-4333-8444-555555555555",
  "event_type": "model_request_completed",
  "request_id": "example-request-001",
  "operation_id": "example-operation-001",
  "occurred_at": "2026-09-08T09:00:00Z",
  "workspace_id": "example-workspace",
  "actor_type": "service_key",
  "actor_id": "example-key-id",
  "action": "model_request",
  "outcome": "success",
  "policy_version": "example-policy-3",
  "platform_placement": "onprem",
  "route_id": "example-route-ru-01",
  "route_class": "nevel_self_hosted_ru",
  "receiver_host": "model-gateway.example.invalid",
  "processing_country": "RU"
}
```

В событии нет значения API-ключа, банковского счёта, исходных имён или таблицы соответствий. Идентификатор ключа позволяет расследовать действие без раскрытия секрета. Название файла и URL могут содержать персональные сведения, поэтому даже метаданные проходят оценку состава и необходимого объёма.

Семантика референсного профиля

Поля	Значение	Правило нормализации
`schema_version`, `source_instance`	Версия профиля и экземпляр источника	Сохранять для выбора правил разбора и различения установок
`event_id`	Одна неизменная запись о событии	Повторная доставка сохраняет ID; другой этап получает новый ID
`operation_id`, `request_id`	Пользовательская операция и конкретный модельный вызов	Несколько вызовов одной задачи не объединять в один фактический запрос
`occurred_at`	Время действия на источнике	UTC с часовым поясом; время приёма SIEM хранить отдельно
`workspace_id`, `actor_type`, `actor_id`	Организация и инициатор	Идентификатор сервисного ключа не подменять именем сотрудника
`event_type`, `action`, `outcome`	Вид записи, действие и результат	Окончание запроса не смешивать с решением маршрута или успешной доставкой журнала

Поля	Значение	Правило нормализации
`policy_version`, `route_id`	Конфигурация, действовавшая при запросе	Новое имя маршрута не переписывает старую запись
`platform_placement`, `route_class`	Место Platform и класс модельного пути	`onprem` не означает локальную модель
`receiver_host`, `processing_country`	Получатель соединения и география по паспорту маршрута	Не выводить страну обработки из GeoIP relay или имени семейства модели

Ключ повторной доставки в этом профиле — сочетание экземпляра источника, пространства и `event_id`. ID события отличается от ID обращения модели: в одной операции могут быть несколько попыток, а у каждого вызова — отдельные стадии. Точное правило подавления дубликатов реализуется в выбранной цепочке приёма и проверяется контрольной повторной отправкой.

Промежуточный relay добавляет своё время получения и техническое состояние доставки, сохраняя исходное время действия. Адрес relay описывает транспорт журнала; `receiver_host` в приведённом событии описывает модельный маршрут. Перезаписывать одно поле другим нельзя. При нескольких получателях их цепочка хранится в отдельном согласованном расширении или связанной записи; одиночный hostname не выдаётся за всю цепочку.

Если данных для поля нет, применяются отсутствие ключа или согласованное пустое значение. Например, неизвестная страна не становится `RU` из-за российского расположения Platform. Поле с фактом, полученным из конфигурации, различается с сетевым наблюдением. Ошибка типа или длины фиксируется как ошибка преобразования; усечение ID до лимита приёмника может разрушить связь записей.

Пример сопоставления с CEF и KUMA

Таблица ниже — **проект mapping**, а не готовый пакет нормализации. Целевые поля определены в модели событий KUMA 3.0.1. При установленной другой версии проверяется её схема. CEF представляет транспортное содержимое события; собственные строковые поля используются с явными метками назначения. Пример таких расширений опубликован в документации Kaspersky по CEF.

Поле профиля	Представление CEF	Целевое поле KUMA
`event_id`	`externalId`	`ExternalID`
`event_type`	Имя события в заголовке	`Name`
`action`	`act`	`DeviceAction`
`outcome`	`outcome`	`EventOutcome`
`workspace_id`	`cs1` и `cs1Label=workspace_id`	`DeviceCustomString1` и его Label
`request_id`	`cs2` и `cs2Label=request_id`	`DeviceCustomString2` и его Label
`operation_id`	`cs3` и `cs3Label=operation_id`	`DeviceCustomString3` и его Label
`route_id`	`cs4` и `cs4Label=route_id`	`DeviceCustomString4` и его Label
`policy_version`	`cs5` и `cs5Label=policy_version`	`DeviceCustomString5` и его Label
`actor_id` сервисного ключа	`cs6` и `cs6Label=service_key_id`	`DeviceCustomString6` и его Label

Имена `cs1` – `cs6` не являются глобальным словарём Nevel: это выбранное распределение данного профиля. Другой источник может использовать эти позиции иначе. Поэтому нормализатор выбирается по источнику и версии, а не только по наличию строки `CEF`. Для события реального пользователя допускается отдельное сопоставление в `SourceUserID`; ID сервисного ключа не трактуется как пользователь без явной связи.

При прямом JSON-приёме необязательное расширение может сохранять `route_class`, `platform_placement`, получателя и географию отдельно от шести CEF-полей. В KUMA доступно сохранение дополнительных полей в `Extra`; состав задаётся явно. Не направляйте все неизвестные поля туда автоматически, если среди них могут оказаться текст запроса, cookies или авторизация. Настройки парсинга KUMA.

Время требует отдельного преобразования: ISO 8601 из примера переводится в целевой формат времени выбранного поля SIEM с явно заданными единицами. Время приёма устройства не подменяет время завершения операции. При CEF-сериализации проверяются экранирование разделителей, обратного слеша и переносов, ограничения длины, UTF-8 и framing сообщения. Визуально похожая строка ещё не доказывает правильного разбора.

Для MaxPatrol SIEM и других получателей тот же профиль отображается в их собственную модель данных через отдельное правило. Поддержка JSON или Syslog не переносит имена полей KUMA в другую систему. Порядок подготовки такого источника и проверки результата описан в подключении SIEM.

Для рабочей интеграции подтвердите mapping передачей контрольных событий в SIEM выбранной версии. Корректный синтаксис примера не заменяет проверку доставки и разбора.

Как расследуется конкретный запрос

Проверяющий начинает с идентификатора операции и интервала времени. Затем связывает событие аутентификации, доступ к объектам, сборку контекста, решение Guardrail, исходящий вызов и возврат результата. При ошибке устанавливается последняя завершённая стадия: отказ до передачи модели принципиально отличается от ошибки после уже состоявшейся отправки.

СХЕМА 1

Связь событий расследования



После этого проверяется не только пользовательский запрос, но и административная история. Изменение списка разрешённых моделей за минуту до спорной отправки может объяснить результат лучше, чем текст диалога. События должны сохранять прежнюю версию решения, чтобы новая политика не переписывала историю задним числом.

Время приводится к единой шкале; рассинхронизация часов фиксируется как проблема качества доказательств. При распределённой обработке порядок доставки в SIEM может отличаться от порядка выполнения, поэтому используются время события, время поступления и идентификаторы связи.

Доступ к аудитным данным

Пользовательский доступ, администрирование платформы и чтение журнала разделяются. ИБ получает нужную область расследования; эксплуатация видит технические ошибки; владелец интеграции — события её использования. Право выгрузить данные отдельно от права их просмотреть, поскольку экспорт создаёт новую копию вне основного контроля приложения.

Фильтрация по организации применяется на сервере и к поиску, и к выгрузке. Пользователь не может расширить область журналов передачей другого идентификатора пространства. Просмотр чувствительных событий и экспорт также регистрируются. Доступ поддержки ограничивается задачей, периодом и необходимыми данными.

Полные тела запросов, если их хранение включено, получают более строгий доступ, чем общие метрики. Даже замаскированный текст может содержать коммерческую тайну или косвенно идентифицировать человека. Таблица соответствий не добавляется в аудит для удобства расследования: это создало бы объединённую копию исходных данных.

Интеграция с SIEM

События используются для централизованного мониторинга через предусмотренные поставкой каналы, включая Syslog/CEF и Webhook. Отображение полей, адрес получателя, транспортная защита и правила повторной доставки определяются конфигурацией интеграции. Наличие формата CEF не доказывает готовность конкретного корреляционного правила во всех SIEM.

При настройке проверяются идентификатор источника, время, код события, критичность, организация, инициатор, решение, причина и связь с запросом. Тестовый отказ запрещённой модели должен появиться в SIEM с тем же идентификатором, который видит расследующий в Nevel. Повторная доставка не должна создавать ложную картину нескольких фактических запросов; потеря связи должна давать наблюдаемую проблему доставки.

Содержание тела Webhook, заголовки и сведения о получателе не должны раскрывать секреты. Сам endpoint SIEM — разрешённый получатель служебных данных. В on-prem журнал установленной платформы и разрешённый экспорт описываются отдельно; внешняя SIEM не разрешается автоматически. Для изолированного профиля журнал и его доставка остаются внутри заданного контура. И облачный экспорт в корпоративную SIEM, и экспорт из on-prem учитываются как отдельные потоки метаданных.

Для интеграции с российскими продуктами используйте карту корпоративной среды и пошаговый процесс доставки и нормализации. Технический профиль содержит источник, версию схемы, mapping, приёмник и тестовые события. Реальные значения адресов, сертификаты и секреты хранятся в конфигурации установки.

Полнота, хранение и ограничения

Аудит должен сохранять и успешные, и запрещённые операции. Только успешные ответы не показывают попытку обхода. Только ошибки приложения не показывают изменение роли или политики. Проверка полноты сопоставляет контрольный набор действий с ожидаемыми событиями, а не просто проверяет наличие файла журнала.

В базовом профиле Guardrail версии 1.2 срок хранения аудита составляет 90 дней с диапазоном настройки от 30 дней до 3 лет. Хранение замаскированных тел по умолчанию выключено. Сроки не являются универсальным требованием российского закона и не устанавливаются одинаково для всех данных. Подробная таблица и удаления — в жизненном цикле.

Защита журнала от изменения включает ограничение прав записи и удаления, отдельный доступ к выгрузкам и контроль административных операций. Криптографическая неизменяемость или квалифицированная электронная подпись каждой записи требуют отдельного механизма в поставке. Для доказательства неизменности конкретной выгрузки можно фиксировать контрольную сумму, время получения и цепочку хранения в процедуре расследования.

Негативные проверки

Выполните разрешённый запрос, запрещённый маршрут, обращение с отозванным ключом, попытку чужого файла и изменение политики. У каждого события должны быть правильные организация, инициатор и результат. Повторите часть действий при временной недоступности SIEM и проверьте наблюдаемость сбоя и последующую доставку в рамках настроенного механизма.

Затем попробуйте выгрузить аудит соседнего пространства и получить полные тела без соответствующего права. Проверьте журнал на точное значение синтетического секрета, cookie и исходного значения маски. Наконец, удалите тестовый объект и убедитесь, что сохраняемый след удаления объясняет операцию, но не сохраняет удалённое содержимое целиком.

Пороговые правила и оповещения описываются в мониторинге, процедура реакции — в инцидентах. Правовые основания хранения и сроков уведомлений рассматриваются в 152-ФЗ.