Nevel

БЕЗОПАСНОСТЬ

Мониторинг и интеграция с SIEM

События Guardrail и Platform, пороги аномалий, доставка в SIEM, диагностика и приёмка мониторинга.

Облако / В контуре

https://docs.nevel.sh/security/monitoring/

Мониторинг Nevel помогает обнаружить изменение поведения запросов, нарушение маршрута, отказ защиты и недоступность сервиса. Он объединяет технические метрики и события безопасности, но сохраняет различие между ними: рост задержки требует диагностики производительности, а передача данных запрещённому получателю — немедленной проверки границы обработки. Оба сигнала могут относиться к одному запросу.

В облаке Nevel наблюдает компоненты своей поставки, а заказчик получает события своей организации и интегрирует их в корпоративный процесс реагирования. В on-prem заказчик наблюдает установленную платформу, внутренние компоненты и доступность разрешённых внешних маршрутов. Адреса сборщиков, SIEM и оповещений задаются отдельно. В изолированном профиле они остаются внутри заданного контура. Экспорт в облачный мониторинг является отдельной передачей служебных данных и не разрешается автоматически местом установки платформы.

Какие сигналы собирать

Наблюдение строится вокруг четырёх вопросов: работает ли запрос, применена ли защита, соблюдён ли разрешённый маршрут и можно ли восстановить цепочку действий. Для каждого сигнала назначаются владелец, источник, интервал расчёта и действие дежурного.

Группа	Сигналы	Первая проверка
Доступность	Успешные запросы, ошибки, тайм-ауты, доступность зависимостей	Какая стадия перестала отвечать и какие организации затронуты
Производительность	Задержка Gateway, DLP и модели по отдельности; очередь обработки	Где возникает ожидание, изменились ли объём и тип входных данных
Маскирование	Доля запросов с заменами, количество и типы сущностей	Не изменились ли поток документов, режим чувствительности или политика
Маршрутизация	Разрешённые, запрещённые и перенаправленные обращения	Соответствует ли фактический получатель категории данных
Идентичность	Ошибки входа, использование отозванных ключей, необычный источник	Есть ли действующая интеграция или признак компрометации
Администрирование	Изменения ролей, правил, получателей и сроков хранения	Кто изменил настройку и какие операции выполнились после изменения
Сам мониторинг	Задержка доставки, пропуски, очередь экспорта, доступность приёмника	Не образовался ли период, за который нет достоверного аудита

Запись запроса связывается с идентификатором операции, временем, пользователем или идентификатором ключа, моделью, периметром обработки, типами и количеством замен, результатом и безопасным описанием ошибки. Состав и пример события приведены в контроле доступа и аудите. Значение ключа, исходные персональные сведения и таблица соответствий в событие не включаются.

Профиль порогов Guardrail

В базовом профиле Guardrail версии 1.2 используются следующие ориентиры. Это начальные правила наблюдения для проверки при внедрении. Они не являются доказательством утечки, гарантией точности распознавания или универсальным SLA любой установки.

Метрика	Ориентир профиля	Что делать при срабатывании
Доля запросов с маскированием	Отклонение от базового уровня более 20%	Сравнить одинаковые сценарии и версии политики; проверить контрольные примеры
Среднее число сущностей в запросе	Аномальный рост более 3σ	Найти изменившуюся группу запросов; исключить пакетную обработку нового типа документов
Распределение типов сущностей	Нетипичный состав	Проверить новый источник данных, обход представлением и изменение классификации
Ложные срабатывания	Порог зависит от режима чувствительности	Разобрать размеченные примеры и обратную связь; проверить влияние на рабочую задачу
Время обработки DLP	p95 более 500 мс	Разделить длину входа, очередь и собственно обработку; проверить ресурсы и зависимости

Базовый уровень нужно считать для сопоставимого потока: одной организации, маршрута, режима и класса задач. Запросы короткого чата и обработка многостраничного файла не должны незаметно попадать в одну выборку. В паспорте правила фиксируются окно, минимальный объём наблюдений, часовой пояс, условия подавления повторов и способ пересчёта базы после изменения политики.

Число «20%» требует явно выбранной формулы. Например, в **иллюстративном правиле с относительным отклонением** базовая доля равна 40%, текущая — 30%. Отклонение составляет `abs(30 - 40) / 40 = 25%`, поэтому порог превышен. Разница при этом равна 10 процентным пунктам. Эти две шкалы нельзя смешивать. При нулевой базе относительная формула неприменима: правило должно использовать абсолютное количество, отдельное условие появления события или другую определённую метрику.

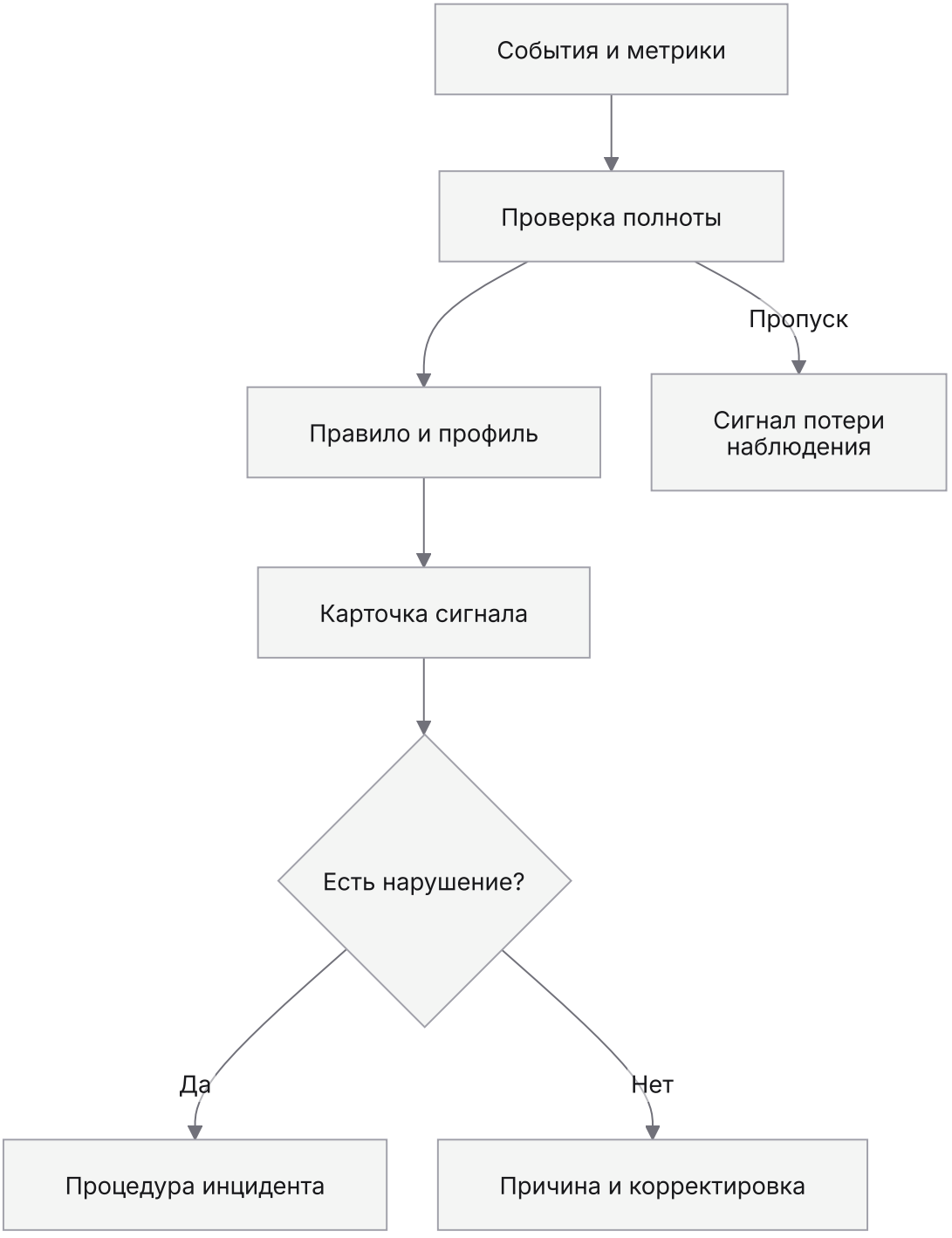
Порог 3σ сравнивает наблюдение с историческим разбросом, а не устанавливает вероятность утечки. Небольшая выборка, сезонность и резкое изменение нагрузки делают такое сравнение ненадёжным. Поэтому карточка сигнала показывает период, число запросов, среднее, разброс и изменившийся сегмент. После массовой загрузки нового класса файлов сначала выясняется причина сдвига, затем принимается решение о новой базе; автоматическое обучение на подозрительном периоде может скрыть проблему.

Падение доли маскирования не обязательно означает улучшение защиты: могли исчезнуть персональные данные, измениться документы или перестать работать детектор. Рост не доказывает атаку. Для оценки качества нужен размеченный контрольный набор с ожидаемыми заменами и проверка пропусков. Методика связана с работой Guardrail, а не выводится из одного графика.

От сигнала до действия

СХЕМА 1

Обработка сигнала мониторинга



Карточка включает время, правило, затронутую область, наблюдаемое и базовое значение, идентификаторы примеров, текущую версию политики и назначенного ответственного. Ссылка ведёт в защищённый интерфейс аудита. Копировать тело запроса в тему письма или корпоративный мессенджер не требуется.

Для подозрения на обход проверяются транслитерация, разделение символов, необычное кодирование и повторные попытки после блокировки. Для аномалии API сопоставляются интенсивность, время, источник, владелец ключа и ожидаемая задача. Работа новой пакетной интеграции может объяснить всплеск; использование отозванного ключа требует отдельной проверки даже

при низкой частоте. Автоматическое отключение всей организации по одному статистическому сигналу не является обязательным действием этого профиля.

Нарушение маршрута разбирается по фактическим стадиям: запрос заблокирован до отправки, перенаправлен разрешённой политикой или уже передан получателю. Только последний случай означает состоявшуюся передачу. Порядок локализации и оценки последствий описан в реагировании на инциденты.

Доставка в SIEM и оповещения

Профиль предусматривает панели метрик, email, webhook в корпоративную систему инцидентов и экспорт в SIEM через Syslog/CEF. Конкретный транспорт, поля расширения CEF, адрес приёмника, аутентификация и ограничения размера являются контрактом подключения. Название формата само по себе не подтверждает шифрование или гарантированную доставку.

Для подключения используются три разных объекта: реальный источник событий Nevel, согласованный профиль преобразования и принимающая SIEM. Референсный профиль аудита помогает спроектировать mapping. Он не объявляется уже существующим API или поставляемым по умолчанию нормализатором.

Шаг 1. Определить источник и область экспорта

Владелец интеграции фиксирует организацию, установки Platform, типы событий и необходимые поля. События пользователя, модельного запроса, администрирования и самой доставки различаются по типу. Отправлять весь журнал операционной системы вместо событий приложения недостаточно: он может не содержать исходный ID запроса и решение маршрута.

Для cloud-установки экспорт ограничивается организацией заказчика. Для on-prem источник относится к установленным компонентам; события внешнего провайдера автоматически не появляются в локальном журнале. Каждый добавленный источник имеет собственные версию, область доступа и способ получения.

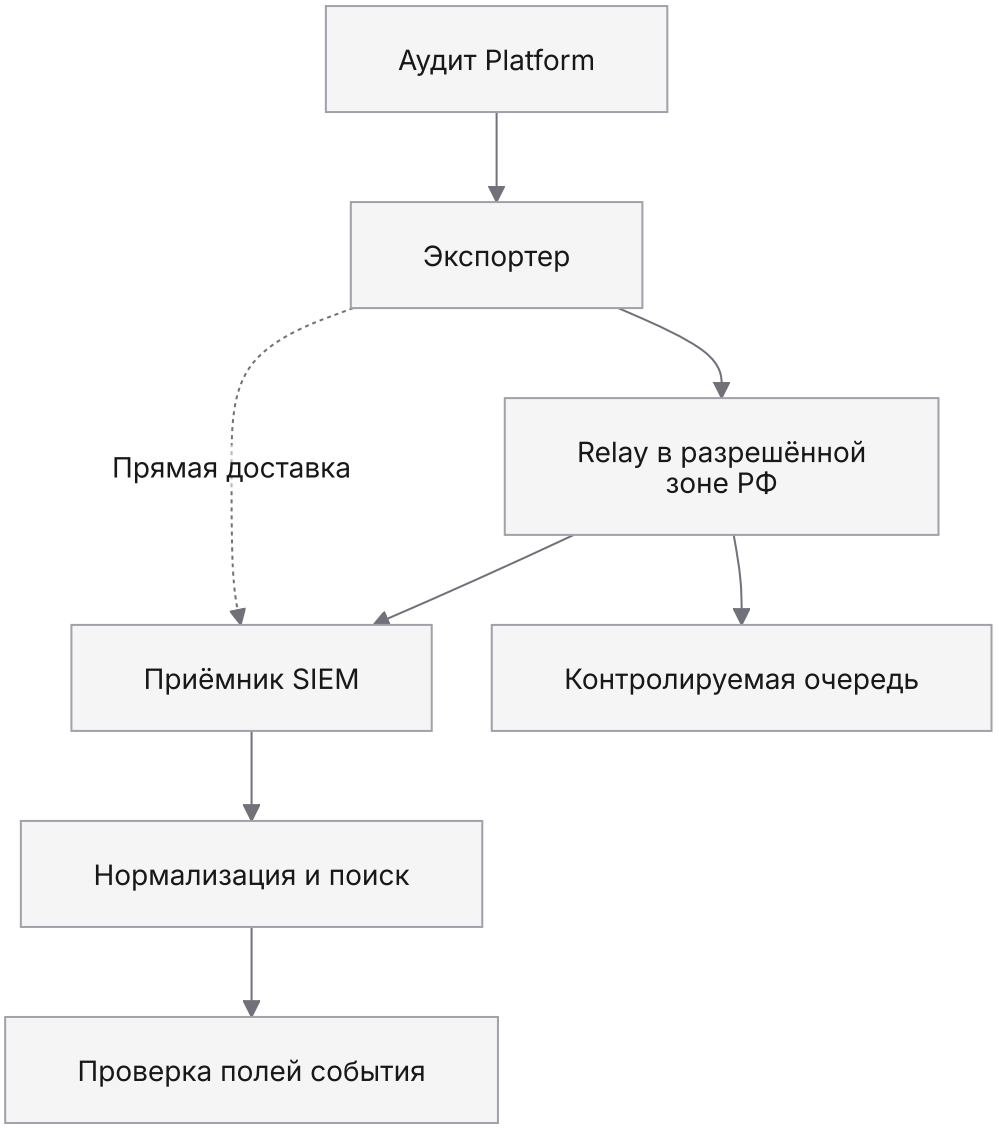
Минимальный комплект: пример реального обезличенного события, описание его полей, версия источника, перечень включённых категорий и ожидаемый результат для каждого контрольного действия. Идентификаторы и служебные коды сохраняются; секреты и тела рабочих запросов не добавляются ради удобства настройки.

Шаг 2. Выбрать прямую доставку или relay

Прямое соединение используется, когда экспортер и SIEM поддерживают один согласованный формат, транспорт и доверие. Relay — отдельный промежуточный узел для приёма, преобразования и повторной доставки — нужен, когда требуется разделить сетевые зоны, адаптировать формат или разместить очередь в контролируемой инфраструктуре. Его наличие и функции являются частью проекта поставки, а не неявной возможностью любой инсталляции.

СХЕМА 2

Путь события в корпоративную SIEM



Для relay указываются площадка, оператор, дисковая очередь, диагностические файлы, доступ администраторов и очистка. Облачный Nevel может отправлять события на разрешённый relay в РФ, откуда они поступают во внутреннюю SIEM по подготовленному соединению. Внутренний адрес SIEM не становится доступным облаку автоматически. Приёмник в DMZ предоставляет сервис событий, а не административную консоль SIEM.

В изолированном профиле вся цепочка, включая relay и резерв очереди, остаётся внутри контура. При обычном on-prem допускается разрешённая внешняя доставка событий. Российское расположение промежуточного узла не заменяет проверку его получателей и не определяет маршрут запроса к модели. Примеры продуктов и точки контроля раскрыты в корпоративной среде.

Шаг 3. Зафиксировать сетевой и транспортный профиль

Параметр	Что указать	Что проверить
Приёмник	DNS-имя, порт, владелец и зона	Это адрес сервиса приёма, а не web UI
Транспорт	Поддерживаемый обеими сторонами Syslog/TLS или HTTPS-приёмник	Формат внутри транспорта и границы одного сообщения

Параметр	Что указать	Что проверить
Доверие	CA, имя сертификата, срок, клиентская аутентификация при её использовании	Неверный сертификат не приводит к отключению проверки
Отправители	Источники или relay, разрешённые сети	Случайный внешний узел не может писать в источник Nevel
Формат	JSONL, CEF либо иной согласованный профиль	UTF-8, переносы, escaping, максимальная длина
Область	Организации и категории событий	События другой организации не попадают в поток
Повтор	Подтверждение приёма, очередь, ID и предел попыток	Дубликат отличим от нового события

Syslog — способ передачи и оформления сообщения, CEF — структура его содержимого. TCP сам по себе не шифрует соединение. Успешная запись байтов в сокет не доказывает, что SIEM разобрала и проиндексировала событие. Для HTTPS-контракта отдельно определяется, что означает успешный ответ приёмника: приём в очередь, сохранение или завершённая обработка. Не приписывайте ответу `2xx` более сильную гарантию, чем даёт конкретный сервис.

Следующий YAML — **референсная карточка подключения**, а не файл настройки Nevel или конкретного производителя. Порт выбран для примера и не является обязательным портом продукта.

```
profile: nevel-siem-reference-1
source_instance: example-onprem-01
workspace: example-workspace
receiver_host: siem-relay.example.invalid
receiver_port: 6514
transport: syslog-over-tls
payload_profile: nevel.audit.reference/1
serialization: cef
tls_server_name: siem-relay.example.invalid
deduplication_fields:
  - source_instance
  - workspace_id
  - event_id
include_request_body: false
```

В рабочую конфигурацию переносят смысл полей с использованием действительного синтаксиса выбранных компонентов. Сертификаты, секреты и размер очереди задаются отдельно. Структура карточки не обещает, что любой экспортер понимает приведённые ключи.

Шаг 4. Подготовить нормализацию для выбранной SIEM

Kaspersky KUMA. Для профиля JSON приёмник передаёт один JSON-объект на строку в UTF-8; многострочный JSON перед отправкой сериализуется в JSONL. В нормализаторе выбирают метод `json` или `cef`, добавляют примеры и таблицу сопоставления. Для JSON доступны пути к вложенным полям через точку; для CEF — исходное сопоставление с последующей проверкой. Указанные параметры относятся к KUMA 3.0.1. Параметры парсинга KUMA.

В таблице mapping показан пример назначения ID, результата и пользовательских строковых полей. Сохраняйте исходный ID события отдельно от внутреннего ID, который присваивает SIEM. Поля времени, адресов и чисел проверяются контрольными значениями; появление события в общем списке ещё не подтверждает, что каждое поле прошло преобразование.

MaxPatrol SIEM. Правило нормализации выбирается с учётом формата события. В версии 8.1 различаются текстовый и структурированные варианты, включая JSON; совпадение с правилом определяет создание нормализованной записи. Поэтому отдельному источнику Nevel нужны образцы входных событий, правило разбора и проверка целевых полей. Профиль KUMA не загружается сюда как готовое правило. Принцип нормализации MaxPatrol SIEM.

Для установленной версии владелец SIEM выбирает поддерживаемый механизм получения событий, регистрирует источник и добавляет собственный проверенный профиль. Контрольная выборка содержит несколько типов записей и необязательные поля. Успешный разбор только одного примера не подтверждает покрытие всех событий приложения.

UserGate SIEM. В версии 7.x приёмник настраивается в разделе **Настройки → Сборщик логов → Syslog**. Для TCP указываются порт и число сессий; защищённое соединение включает TLS и сертификаты, а разрешённые соседи ограничивают отправителей. После изменения выполняется сохранение и перезапуск. Настройка Syslog-сервера UserGate.

Эта настройка поднимает транспортный приёмник. Отдельно проверяются распознавание структуры Nevel, извлечение исходных ID и поиск по организации и маршруту. Приём строки в журнал без нужных полей не считается завершённой интеграцией.

Шаг 5. Проверить очередь, повторы и ошибки разбора

В проекте фиксируется точка подтверждения: когда источник может считать запись принятой следующим звеном. Если используется дисковая очередь, описываются её предел, сохранность после перезапуска, действия при заполнении и порядок удаления доставленных записей. Точное число часов и размер очереди задаются выбранной конфигурацией, а не универсальным обещанием Nevel.

Потеря подтверждения может вызвать повтор уже принятого события. Поэтому тест выполняется с тем же `event_id`, а не с новой записью, похожей по содержанию. После нормализации проверяется выбранная обработка дубликата. При нескольких источниках одинаковый локальный ID не должен смешивать разные организации и установки.

Невалидное событие не удаляется бесследно и не считается успешно разобранным. Для него нужен контролируемый путь диагностики: причина ошибки, источник, время и безопасный исходный образец в пределах политики хранения. Этот путь не должен бесконечно повторять одну ошибочную запись и останавливать остальные события.

Контрольный пример	Ожидаемый результат
Корректная запись из reference-профиля	Совпадают ID, пространство, действие, результат и маршрут
Повтор той же записи	Отличим от нового модельного вызова; действует правило дубликатов
Новая запись той же операции	Сохраняется отдельный ID события и связь с общей операцией
Поле времени с неверным форматом	Видна ошибка или оговорённый результат преобразования
Запись с неизвестной версией схемы	Не разбирается молча по несовместимому старому правилу
Недоступный приёмник и перезапуск relay	Подтверждены очередь, восстановление и фактическая полнота
Текст с кириллицей, переносом и разделителем CEF	Значения сохраняются после разбора, не создают ложные поля

Часы компонентов синхронизируются; время события сохраняет часовой пояс или передаётся в UTC. Время приёма, задержка доставки и время самого действия остаются отдельными величинами. Это позволяет отличить задержанную запись от нового действия.

Шаг 6. Зафиксировать результат подключения

Итоговый профиль содержит версии компонентов, сетевую схему, mapping, тестовые события, результат поиска по исходным ID и проверку восстановления доставки. Состояние отражается предметно: транспорт проверен, нормализация проверена, полнота категорий проверена либо ограничена перечисленными типами. Это точнее общего ярлыка «SIEM интегрирована».

Развёртывание в другой организации требует замены адресов, доверия и области событий. Обновление версии экспортера или SIEM требует повторения затронутого набора примеров. Срок хранения и повторная выгрузка связываются с политикой хранения; подключение средств контроля — с сетевой защитой.

Приёмка и регулярная проверка

Приёмка проходит на синтетических данных. Выполняются успешный запрос, блокировка политикой, попытка с отозванным ключом, разрешённое перенаправление, изменение правила и кратковременный отказ приёмника SIEM. Для каждого случая проверяются запись, корреляция, правило оповещения, получатель и понятное действие дежурного.

Отдельно проверяется конфиденциальность: исходное значение и секрет отсутствуют в журнале, письме, webhook и диагностике обработчика. В изолированном профиле контроль сетевых соединений подтверждает внутренний адрес SIEM и отсутствие внешнего канала мониторинга. В обычном on-prem проверяется соответствие каждого исходящего канала разрешённому списку.

Результат приёмки — перечень активных правил с владельцами, измеренные задержки доставки, проверенные каналы и известные ограничения. После изменения политики, формата событий или маршрута повторяются затронутые сценарии. Зелёная панель без контрольного события не доказывает, что мониторинг обнаружит реальную проблему.

Версии и совместимость

Параметры Kaspersky, Positive Technologies и UserGate относятся к версиям, указанным в ссылках. YAML, таблицы mapping и контрольные примеры — референс для настройки, а не готовый пакет интеграции. Совместимость конкретных версий Nevel и SIEM подтверждается протоколом испытаний.