

????????????? КАТА 8.0 с MDR

Важно: Информация, приведённая в данной статье, подготовлена командой pre-sales на основании официальной документации Kaspersky Anti Targeted Attack Platform 8.0 и Kaspersky Managed Detection and Response. Материал не заменяет официальную документацию.

“ Для КАТА/KEDR версий 7.x см. отдельную статью: [Интеграция КАТА с MDR](#)

??? ?????????????? ? КАТА 8.0

Ключевые отличия интеграция версии 8.0 от версии 7.x:

- **Новый рекомендованный способ подключения** - авторизация через UIS (uis.kaspersky.com) вместо ручной загрузки конфигурационного файла. Параметры интеграции и сведения о лицензии MDR подтягиваются автоматически.
- **Автоматическая отправка дополнительных данных по запросу Kaspersky SOC.** Аналитики MDR могут запрашивать артефакты, связанные с алертами КАТА (PCAP, отчёты Sandbox, заражённые файлы), напрямую через консоль MDR — без участия заказчика на каждом шаге. Это значительно ускоряет расследование инцидентов.
- Прежний способ с конфигурационным файлом сохранён как **резервный** - для инсталляций без сетевого доступа к uis.kaspersky.com.

“ **ВАЖНО:** При устаревшем способе интеграции (через конфигурационный файл) автоматическая отправка дополнительных данных по запросу SOC **недоступна**.

1. ?????????????????????? ??????????????????

Требование	Комментарий
КАТА Platform	Версия 8.0 или выше (для авто-отправки артефактов)
Лицензия	Действующий лицензионный ключ КАТА
KSN	Обязательно участие в KSN - КАТА передаёт данные в MDR через поток KSN

Требование	Комментарий
Подписка MDR	Активная подписка Kaspersky Managed Detection and Response
Сетевой доступ	С Central Node до <code>uis.kaspersky.com</code> (для рекомендованного способа)
Права в KATA	Учётная запись администратора веб-интерфейса
Права в Консоли MDR	Роль Администратор или Старший сотрудник службы безопасности (для согласия на отправку дополнительных данных)

2. ?????????????????????? ??????????: ?????????????????? ?????? UIS

1. Войдите в веб-интерфейс KATA под учётной записью администратора.
2. Перейдите в раздел **Параметры** → **KSN/KPSN и MDR**.
3. Убедитесь, что участие в KSN активно.
4. В блоке **Интеграция MDR** нажмите кнопку «**Войти в UIS**».

The screenshot shows the Kaspersky Anti Targeted Attack Platform (KATA) interface. On the left is a navigation menu with options like 'Пользователи', 'Общие параметры', 'Политики аутентификации', 'Сертификаты', 'Дата и время', 'Endpoint Agents', 'Проверка трафика ICAP', 'Серверы подключений', 'Коннекторы', 'Секреты', 'KSN/KPSN и MDR', 'Репутационная база KPSN', 'Уведомления', 'SIEM-система', 'Сетевые параметры', and 'Лицензия'. The 'KSN/KPSN и MDR' section is selected.

The main content area is titled 'Участие в KSN/KPSN'. It shows a 'Репутационная база' section with three options: 'Не используется', 'KSN' (selected), and 'KPSN'. Below this is a 'Положение о KSN' section with a text box containing the following text:

ПОЛОЖЕНИЕ О KASPERSKY SECURITY NETWORK (KSN)

Положение о Kaspersky Security Network (далее - Положение о KSN) относится к программному обеспечению Kaspersky Anti Targeted Attack Platform 8.0 (далее - ПО). Положение о KSN совместно с Лицензионным соглашением для ПО, в частности в разделе «Условия обработки данных», определяют условия, ответственность и порядок передачи и обработки данных, указанных в Положении о KSN. Внимательно ознакомьтесь с условиями Положения о KSN, а также со всеми документами, ссылки на которые содержит Положение о KSN, перед тем, как принять его.

Если Пользователь включает использование KSN, Пользователь несет ответственность за обеспечение законности обработки персональных данных Субъектов данных, которая определена в

Below the text box are two radio buttons: 'Я согласен участвовать в KSN' (selected) and 'Я не согласен участвовать в KSN'. There are 'Применить' and 'Отмена' buttons.

Below this is the 'Интеграция MDR' section. It shows 'Источник параметров' as '-'. Below this is a text box: 'Для интеграции с MDR войдите в систему UIS или загрузите конфигурационный файл, полученный с портала MDR.' Below the text box are two buttons: 'Загрузить конфигурационный файл' and 'Войти в UIS' (highlighted with a red box).

5. Авторизуйтесь в UIS с учётными данными вашей организации.
6. После успешной авторизации платформа автоматически получит параметры интеграции. В блоке **Интеграция MDR** отобразится:
 - **Состояние:** Активна
 - **Источник параметров:** Автоматически
 - **Серийный номер** лицензии MDR

• Дата окончания срока действия и количество оставшихся дней

The screenshot shows the Kaspersky Anti Targeted Attack Platform (KATA) interface. The left sidebar contains navigation options: Мониторинг, Пользовательские правила, Активы, Журналы, Параметры, Режим работы, Серверы Sensor, Серверы Sandbox, Внешние системы, and Конфигурация серверов. The main menu on the right lists: Пользователи, Общие параметры, Политики аутентификации, Сертификаты, Дата и время, Endpoint Agents, Проверка трафика ICAP, Серверы подключений, Коннекторы, Секреты, KSN/KPSN и MDR (highlighted), Репутационная база KPSN, Уведомления, SIEM-система, Сетевые параметры, and Лицензия. The 'Участие в KSN/KPSN' section shows 'Репутационная база' set to 'KSN' and 'Положение о KSN' with a detailed text box explaining the Kaspersky Security Network (KSN) terms. Below this, there are radio buttons for 'Я согласен участвовать в KSN' (selected) and 'Я не согласен участвовать в KSN'. The 'Интеграция MDR' section shows 'Состояние' as 'Активна' (highlighted with a red box), 'Источник параметров' as 'Автоматически', 'Серийный номер', 'Дата окончания срока действия' as '2027-01-17 03:00:00', and 'Осталось дней' as '198'. Buttons for 'Войти снова' and 'Выйти' are at the bottom.

На этом подключение завершено.

“ **Преимущество способа:** при продлении подписки MDR ничего перезагружать вручную не нужно - параметры и сведения о лицензии обновляются автоматически.

3. ?????????? ???????: ?????????????????????? ?????

Используйте этот способ **только** если рекомендованный недоступен - например, при отсутствии сетевого доступа с Central Node к uis.kaspersky.com.

1. На портале MDR получите архив с конфигурационным файлом (Консоль MDR → раздел лицензирования → скачать архив; распаковывать его не нужно).
2. В веб-интерфейсе KATA перейдите в **Параметры → KSN/KPSN и MDR**.
3. В блоке **Интеграция MDR** нажмите «**Загрузить конфигурационный файл**» и выберите скачанный архив.
4. После загрузки отобразятся сведения о лицензии MDR: серийный номер, дата окончания и количество оставшихся дней.

Два существенных недостатка этого способа:

1. Не работает автоматическая отправка артефактов по запросу SOC - интеграция лишается одного из главных преимуществ версии 8.0.
2. Конфигурационный файл нужно вручную обновлять при каждом продлении лицензии (ежегодно).

4. ?????????? ?????????????????????? ?????????? ?? ?????????? ??????????????? MDR

??? ??? ???????????

При расследовании аналитикам MDR часто нужен дополнительный контекст. В KATA 8.0 платформа может передавать его автоматически по запросу - это один из типов действий по реагированию в MDR.

Данные передаются **только после согласия** пользователя с ролью **Администратор** или **Старший сотрудник службы безопасности** в Консоли MDR. Без выданного согласия автоматическая передача не выполняется.

?????? ?????????? ?????????????????

Категория	Содержимое
PCAP и Payload	Файлы, связанные с алертом IDS
Отчёт Sandbox	Результаты проверки файлов: скриншоты выполнения объекта, журнал активности и другие данные проверки
Заражённый файл	Архив с файлом, при проверке которого был создан файловый алерт (файл, отправленный в Sandbox)
Данные алерта	Файл в формате JSON с информацией об алерте

При запросе указываются идентификатор узла KATA, идентификатор алерта и категории файлов для копирования.

“ **Персональные данные:** передаваемые файлы могут содержать персональные и конфиденциальные данные. Согласуйте выдачу согласия на отправку с ИБ- и комплаенс-подразделениями организации до включения функции.

???????? ???? ?

- [Справка KATA 8.0: отправка дополнительных данных для анализа в MDR](#)
- [Интеграция KATA с MDR \(версии 7.x\)](#)

Revision #2

Created 2 July 2026 07:46:52 by Анна

Updated 2 July 2026 11:52:46 by Анна