?????????? KATA 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 KATA/KEDR версий 7.x см. отдельную статью: Интеграция KATA с MDR

??? ?????????? ? KATA 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 KATA (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**.

---

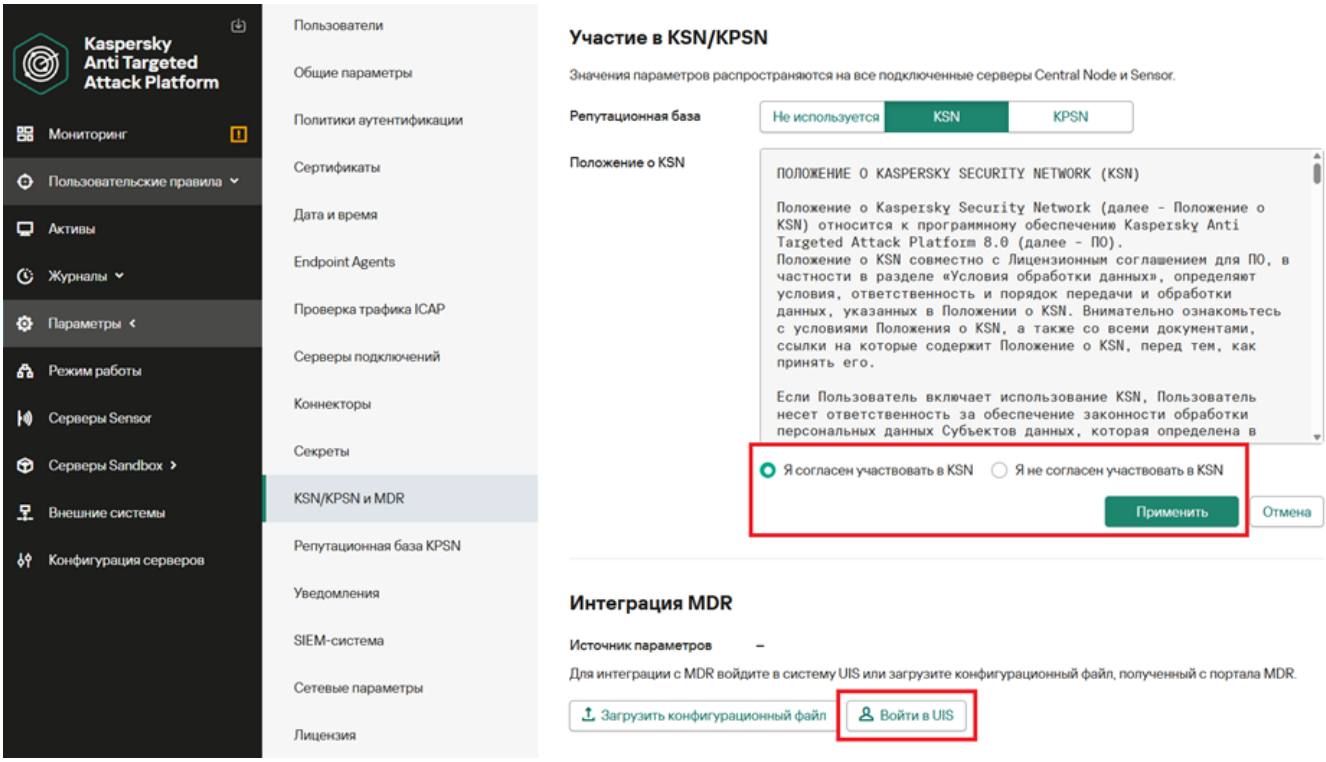
1. ?????????????? ??????????

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

Требование	Комментарий
Подписка MDR	Активная подписка Kaspersky Managed Detection and Response
Сетевой доступ	С Central Node до `uis.kaspersky.com` (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)

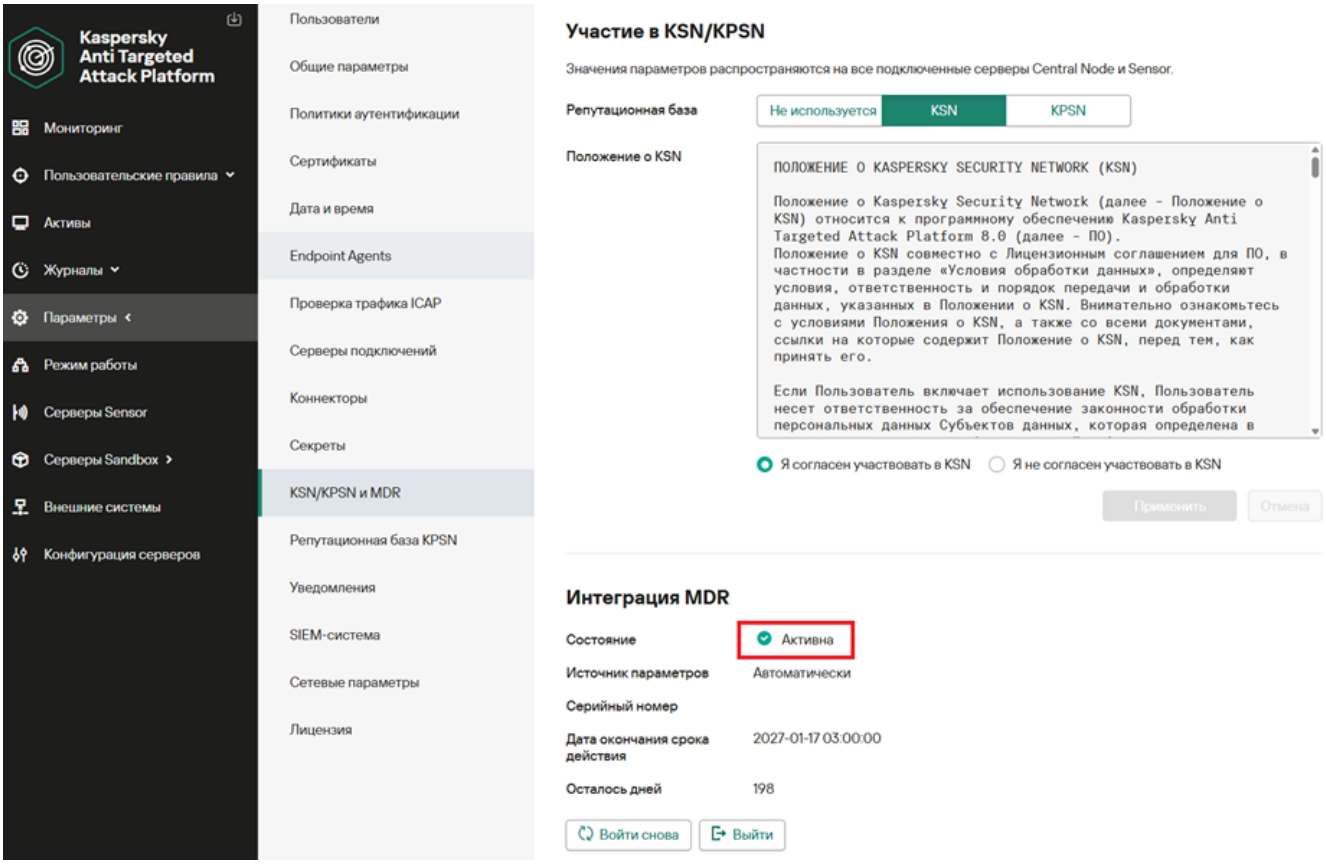
2. ?????????????? ??????: ??????????? ????? UIS

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»**.



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**



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