

KB HOW TO

- DISCLAIMER

DISCLAIMER

Материалы, предоставленные на портале KUMA Community KnowledgeBase (KB), созданы командой российского отдела пресейл ЛК, а также участниками сообщества KUMA для удобства использования инструкций по настройке и работе с системой SIEM ЛК KUMA, а также улучшения общих знаний ИБ по мониторингу и настройке источников.

KB - это не замена документации, а ДОПОЛНЕНИЕ к ней. К KB следует относиться, как к описанию некоторых юзкейсов.

Помните, что все материалы, представленные на портале, не являются официальными, поэтому есть вероятность, что в определенных случаях техническая поддержка может отказать вам в помощи.

Актуальная версия KUMA — **3.4.1.53**, запрос актуального ПО делается через ТП (для систем в эксплуатации)

☐ Актуальная сертифицированная версия (РФ) KUMA — **3.2.1.23** (ссылка ниже в официальных ресурсах)

Предложения по улучшению коробочного (OOTB) контента:

kuma.content.improvement@kaspersky.com

Комьюнити ресурсы:

- Комьюнити KUMA (Телеграм канал) — <https://t.me/kumasiem>
- Legacy инструкции — <https://box.kaspersky.com/d/44309f4fa7184cc79d7c/> (пароль: `kuma-the-best-siem`)
- **Коробочный контент и SOC Package**
- **Интерактивная библиотека по коробочным правилам корреляции**
- **Скачать Community-Pack контент** Пароль импорта: `q123123Q!` (Для версий >3.2: `q123123Q!q123123Q!`)
- **Community-Pack контент на GitHub**
- **GitHub репозиторий Community скриптов**

- Пополнить Community-Pack контент своими наработками Используйте пароль экспорта: q123123Q!
- API коллекция продуктов ЛК (POSTMAN)

Обзорные видео материалы:

- Обзор KUMA (видео)
- Работа с Правилами Корреляции (видео)
- Работа с Нормализаторами (видео)

Официальные ресурсы:

- Единая страница по продукту KUMA — <https://support.kaspersky.ru/kuma/3.2?page=main>
- Официальная документация — <https://support.kaspersky.ru/help/KUMA/3.2/ru-RU/251751.htm>
- Серия коротких видео по KUMA:
 - RUTUBE — <https://rutube.ru/plst/540937/>
 - YouTube — https://www.youtube.com/playlist?list=PL86zv_GQQ5tjv6WyMEF2TNWyF4gFd3WBY
- Обучение и сертификация — <https://support.kaspersky.ru/learning/programs>
- База знаний — <https://support.kaspersky.ru/kuma/3.2?page=kb>
- Карта покрытия MITRE ATT&CK — <https://kuma-mitre.kaspersky.ru/>
- Жизненный цикл поддержки KUMA — <https://support.kaspersky.ru/corporate/lifecycle?type=full,finished&program=kuma>
- Реестр отечественного ПО — <https://reestr.digital.gov.ru/search/?q=%2BMonitoring%2Band%2BAnalysis%2BPlatform>
- Сертификаты ФСТЭК — <https://support.kaspersky.ru/certificates/other-certificates/15810>

© С любовью команда пресейл ЛК ;)

Новичку



Перейти в kb