

Новичку в KUMA

Официальная информация


1. Официальная онлайн-справка — [ссылка](#)
2. Единая страница по продукту KUMA — [ссылка](#)

Начало

1. Что такое SIEM и Приоритет подачи журналов в SIEM — [статья](#)
2. Модель лицензирования KUMA — [статья](#)
3. Схема сетевого взаимодействия KUMA — [статья](#)
4. Подготовка ОС перед установкой и Требования — [статья](#)
5. Обновление / Установка KUMA — [статья](#)
6. Популярные вопросы и ответы FAQ — [статья](#)
7. Траблшутинг по неполадкам — [статья](#)

Работа с системой

1. Работа с системой KUMA (корреляция, поиск, парсинг) — [статья](#)
2. Подключение источников — [статья](#)
3. Модель данных события — [статья](#)
4. Правила корреляции (Описание правил и контент):
 - Community Pack — [ссылка](#)
 - Загрузка Community правил `Community-Pack-RU+MITRE_*` — [ссылка](#), пароль импорта файла в KUMA: `q123123Q!` (Для версий >3.2: `q123123Q!q123123Q!`)
 - Коробочные правила (SOC Content) — [ссылка](#) (более **удобное** представление правил)
 - Загрузка коробочного контента в систему — [статья](#)
 - Добавление маппинга MITRE ATT&CK в правил корреляции — [статья](#) ([Карта покрытия MITRE ATT&CK](#))
5. Описание правил номализации:

- Community Pack — [ссылка](#)
 - Коробочные правила — [ссылка](#)
6. Обновление официального контента в KUMA — [статья](#)
 7. Описание процесса работы с инцидентами в KUMA — [статья](#)
 8. Возможности реагирования KUMA — [статья](#)
 9.  ИИ в KUMA — [статья](#)
 10. Комьюнити скрипты:
 1. Актуальные — [ссылка](#)
 2. Старые (legacy) — [ссылка](#)

Видео материалы:

1. Обзор KUMA ([видео](#))
2. Серия коротких видео по KUMA
 1. YouTube — [ссылка](#)
 2. RUTUBE — [ссылка](#)
3. Работа с Правилами Корреляции ([видео](#))
4. Работа с Нормализаторами ([видео](#))

Revision #24

Created 8 April 2024 08:54:27 by Boris RZR

Updated 21 May 2025 08:09:08 by Boris RZR