Новичку в KUMA

Официальная документация

1. Официальная онлайн-справка — **ссылка**
2. Полезные статьи — **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. Загрузка коробочного контента в систему — **статья**
3. Описание правил (правила корреляции):
    1. Community Pack — **ссылка**
    2. Коробочные правила (SOC Content) — **ссылка**
4. Подключение источников — **статья**
5. Описание правил номализации — **ссылка**
6. Описание процесса работы с инцидентами в KUMA — **статья**

Видео материалы:

1. Обзор KUMA (**видео**)
2. Серия коротких видео по KUMA YouTube (будет пополняться) — **ссылка**

3. Работа с Правилами Корреляции (**видео**)
4. Работа с Нормализаторами (**видео**)

Revision #12
Created 8 April 2024 08:54:27 by Boris Rzr
Updated 13 September 2024 08:36:34 by Boris Rzr