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. Загрузка коробочного контента в систему — **статья**
3. Добавление маппинга MITRE ATT&CK в правил корреляции — **статья**
4. Подключение источников — **статья**
5. Описание правил (правила корреляции):
   - Community Pack — **ссылка**
   - Коробочные правила (SOC Content) — **ссылка**
6. Описание правил номализации:
   - Community Pack — **ссылка**
   - Коробочные правила — **ссылка**
7. Обновление официального контента в KUMA — **статья**
8. Описание процесса работы с инцидентами в KUMA — **статья**

9. Возможности реагирования 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 #18
Created 8 April 2024 08:54:27 by Boris Rzr
Updated 12 November 2024 11:10:47 by Boris Rzr