Путь новичка в KUMA

Добро пожаловать в базу знаний KUMA SIEM. Эта страница проведёт вас от знакомства с системой до первых алертов — последовательно, шаг за шагом.

Путь изучения □□➡□□➡□□

1. □□ Что такое SIEM и архитектура KUMA

Разберитесь с основами до установки

- Что такое SIEM и приоритет подачи журналов
- О решении Kaspersky Unified Monitoring and Analysis Platform (KUMA)
- Архитектура KUMA
- Схема сетевого взаимодействия компонентов KUMA
- Модель лицензирования KUMA

---

2. ⚙ Подготовка инфраструктуры

Подготовьте инфраструктуру для успешного развертывания KUMA

- Подготовка инфраструктуры для развертывания KUMA
- Настройка портов

> ℹ Настройка сетевых доступов между компонентами требуется в случае использования варианта с распределенной установкой компонентов KUMA.

---

3. □□ Установка и базовая настройка KUMA

Установите KUMA и выполните первоначальные шаги по настройке

- Установка KUMA
- Базовая настройка KUMA
- *(Опционально)* Обновление KUMA и другие варианты установки

---

4. □□ Нормализация, модель данных и хранение событий

Узнайте какая модель данных используется в KUMA, изучите как происходит нормализация (парсинг), обогащение и хранение событий

- Что такое нормализатор
- Модель данных нормализованного события
- Поддерживаемые источники событий
- Создание парсеров в KUMA
- Типы хранения данных в KUMA
- О кластере ClickHouse и сервисе Хранилища

---

5. □□ Подключение источников событий

Подключение источников событий — это ключевой процесс для обеспечения безопасности и мониторинга ИТ-инфраструктуры. KUMA собирает, анализирует и коррелирует данные из различных источников для выявления аномалий, подозрительных действий и потенциальных атак.

В качестве источников могут выступать:

- Сетевые устройства: маршрутизаторы, коммутаторы, межсетевые экраны (например, Cisco ASA, Palo Alto).
- Рабочие станции/серверы под управлением ОС Windows и Linux.
- Инфраструктурные сервисы: Active Directory, DNS, DHCP, почтовые серверы.

- Приложения: веб-серверы (например, Apache, IIS), базы данных (например, MySQL, MSSQL).
- Системы безопасности: антивирусы, IDS/IPS (системы обнаружения и предотвращения вторжений), VPN и другие.
- Облачные сервисы.
- Устройства IoT.
- И другие.

Начните с ключевых и подключайте поэтапно:

- Windows (Какой из вариантов выбрать?)
  - Настройка получения событий Windows с помощью Kaspersky Endpoint Security
  - Настройка получения событий Windows с помощью агента KUMA (WEC)
  - Настройка получения событий Windows с помощью агента KUMA (WMI)
- Linux
  - Настройка auditd в Unix-системах
  - Сбор событий auditd с помощью Rsyslog
  - Сбор событий auditd с помощью Syslog-ng
- Продукты Лаборатории Касперского
- Продукты Microsoft
- NGFW и другое сетевое оборудование
- 1С, веб-серверы, виртуализация и другие типы источников
- Статья онлайн-справки "Настройка источников событий"

---

6. □□ Работа с событиями

События собираются с источников, как с ними работать?

- Работа с событиями
- Создание запросов на практике

---

7. □ □□ Интеграции

Получите дополнительные возможности за счет взаимодействия с другими системами

- Интеграция с Kaspersky Security Center
- Интеграция с Active Directory

- Интеграция с Kaspersky CyberTrace
- Интеграция с Kaspersky Threat Intelligence Portal

---

8. □□ Правила корреляции и детектирование

Загрузите готовый контент — первые алерты появятся без написания правил вручную.

- Где брать официальный контент для KUMA
- Community Pack — готовые правила сообщества KUMA (пароль для импорта: `q123123Q!q123123Q!` или `q123123Q!KLaapt-M4`)
- Оценка покрытия матрицы MITRE ATT&CK правилами корреляции KUMA
- MITRE ATT&CK в SOC — как использовать
- Матрица покрытия MITRE ATT&CK решениями "Лаборатории Касперского"

Узнайте, как написать свои правила.

- Типы правил корреляций
- Cookbook: работа с правилами корреляции

---

9. □□ Работа с алертами и инцидентами

Проведите расследование и выполните действия по реагированию

- Работа с алертами
- Реагирование на алерты и инциденты
- Описание готовых интеграций по реагированию
- Описание процесса работы с инцидентами в KUMA
- Ретроспективная проверка

---

10. □□ Мониторинг и отчетность

Визуализируйте собранные данные

- Панель мониторинга
- Отчеты

---

11. □□ Сервисы ИИ

«Мне нужны твоя одежда, ботинки и ~~мотоцикл~~ алерты» (с)

- Описание сервисов ИИ
- KIRA
- Скоринг активов
- Выявление атак DLL Hijacking

---

12. □□□ Эксплуатация KUMA

Отслеживайте состояние источников и создайте резервную копию

- Отслеживание состояния источников событий
- Резервное копирование и восстановление Ядра KUMA
- Оценка эффективности работы SIEM

---

13. ⚠ Что-то не работает

Мне только спросить...

- FAQ
- Траблшутинг
- TG Сообщество

---

14. □□ Видеоматериалы

Обучающие видео по KUMA:

- Обзор KUMA

- Rutube
- Youtube
- Работа с нормализаторами
- Работа с правилами корреляции

Что нового:

- KUMA 4.2
- KUMA 4.0

KUMA Community Meetup

- Московский планетарий
- Музей криптографии
- Музей космонавтики

---

15. ✍ PoC Чек-лист

У меня пилот, что нужно протестировать?

Чек-лист

☐ Подготовка среды
☐ Установка KUMA
☐ Базовая настройка
☐ Подключение источников
  ☐ Настройка получения событий Windows
  ☐ Настройка получения событий Linux (Auditd)
  ☐ Настройка получения событий Kaspersky Security Center
☐ Работа с событиями
☐ Интеграции
  ☐ Интеграция с Kaspersky Security Center
  ☐ Интеграция с Active Directory
  ☐ Интеграция с Kaspersky CyberTrace
  ☐ Интеграция с Kaspersky Threat Intelligence Portal

- [ ] Правила корреляции
- [ ] Работа с алертами
- [ ] Реагирование на алерты и инциденты
- [ ] Ретроспективная проверка
- [ ] Панель мониторинга
- [ ] Отчеты
- [ ] Сервисы ИИ
  - [ ] KIRA
  - [ ] Скоринг активов
  - [ ] Выявление атак DLL Hijacking
- [ ] Состояние источников событий
- [ ] Резервное копирование Ядра KUMA

16. □□ Полезные ресурсы

- Полезные ссылки по ИБ
- Community-скрипты (GitHub)
- Интерактивный каталог с описанием по GitHub репозиториям KUMA Community
- Интерактивная карта межпродуктовых интеграций

Revision #72
Created 2026-06-09 09:19:47 UTC by Dmitry Borisov
Updated 2026-08-18 15:13:18 UTC by Dmitry Borisov