

Модель лицензирования KUMA

Проверить поддержку версии продукта
<https://support.kaspersky.com/corporate/lifecycle#b2b.block13.kuma>

Лицензирование продукта Kaspersky Unified Monitoring and Analysis Platform (KUMA) происходит по **среднему** количеству обрабатываемых событий в секунду (EPS) за 24 часа.

Минимально возможное количество EPS к приобретению = **500**.

Подсчет событий идет после процесса их обработки, то есть после фильтрации, агрегации и обогащения.

Если от коллектора событие отправляется в несколько точек назначения, то оно учитывается как одно событие.

В случае, если среднее значение превышает ограничение по EPS, указанное в лицензионном ключе, KUMA уведомляет о данном событии в интерфейсе. А также, если за 7 дней работы KUMA среднее значение EPS превышало ограничение 30% времени и более, KUMA дополнительно отправляет на email-адрес администратора уведомление о превышении количества полученных событий и продолжает далее подсчет среднего значения EPS, не блокируя функционал.

Лицензии срочные, выписываются на 1, 2 или 3 года, если необходимо больше, то цена складывается из цен за ранее указанные периоды.

По истечении лицензии + **7 дней** блокируются все функции (создание и / или изменение контента SIEM, обработка новых событий, корреляция, а также создание или изменение правил корреляции, нормализации, дашбордов, отчетов и пр.), за исключением просмотра информации по ранее собранным событиям.

Описание модулей лицензирования

Решение класса SIEM (Security Information and Event Management), предназначенное для централизованного сбора, анализа и корреляции событий информационной безопасности с различных источников данных. Решение обеспечивает единую консоль мониторинга, анализа и реагирования на угрозы ИБ, объединяя как решения «Лаборатории Касперского», так и сторонних производителей. Начиная с версии 2.1 поддерживается развёртывание в режиме отказоустойчивости, при котором отказ одного или нескольких узлов не приводит к нарушению потоковой обработки событий и выявления инцидентов. Отказоустойчивость системы достигается за счёт встроенных механизмов маршрутизации данных. Дополнительных лицензии и лицензионного ключа для отказоустойчивости не требуется. Отдельный модуль High Availability доступен только до версии 2.0 (включительно).

Каждый из модулей решения KUMA включает в себя возможность сделать **50 запросов в Kaspersky Threat Lookup** для получения дополнительного контекста в ходе проведения расследования. Чтобы активировать эту функцию, отправьте запрос с указанием номера заказа на адрес intelligence@kaspersky.com.

Netflow Support (Netflow)

События телеметрии о трафике, которые помогают в обнаружении аномалий на сетевом уровне и расследовании инцидентов. KUMA выполняет приём и обработку Netflow событий без ограничений, при этом данные Netflow не учитываются в счётчике EPS. Следует учитывать дополнительную нагрузку на мощности машины при анализе Netflow.

Почему это может быть полезно

Netflow собирает данные о потоках, а не о каждом отдельном пакете, что делает его более эффективным с точки зрения производительности.

Основные данные, содержащиеся в трафике Netflow, (**Netflow v5**): IP-адрес источника (Source IP), IP-адрес назначения (Destination IP), Порт источника (Source Port), Порт назначения (Destination Port), Номер протокола (Protocol Number, например, TCP, UDP), Количество пакетов (Packets), Количество байтов (Bytes), Время начала потока (Flow Start Time), Время окончания потока (Flow End Time), Номер интерфейса (Interface Index).

Другие параметры: Тип сервиса (Type of Service, TOS), Флаги TCP (TCP Flags), Входящий и исходящий VLAN ID (VLAN ID), Направление потока (Ingress/Egress Interface)

Netflow v9: Более гибкая и расширяемая версия, чем Netflow v5, поддерживающая шаблоны полей, что позволяет собирать дополнительные данные, такие как: MAC-адреса источника и назначения, Имена приложений, Уровень MPLS, Информация о VPN.

Netflow позволяет (целесообразность с точки зрения ИБ):

- отслеживать объемы, типы и направления трафика, что помогает выявлять аномальные паттерны, которые могут указывать на кибератаки, такие как DDoS, сканирование портов, попытки взлома и т.д.;
- отслеживать попытки несанкционированного доступа к сетевым ресурсам;
- предоставляет информацию о том, какие приложения и пользователи потребляют больше всего сетевых ресурсов, что помогает выявить потенциальные уязвимости и оптимизировать сетевую инфраструктуру;
- реконструировать последовательность событий, которые привели к инциденту, что помогает в расследовании и выявлении причин.

GosSOPKA (ГосСОПКА)

Модуль, обеспечивающий возможность интеграции с технической инфраструктурой НКЦКИ (Национальный координационный центр по компьютерным инцидентам). Модуль ГосСОПКА позволит передавать инциденты, выявленные SIEM «по требованию» (т. е. по явному указанию пользователя), в техническую инфраструктуру НКЦКИ через API и получать рекомендации по реагированию на эти инциденты. Модуль ГосСОПКА регулирует только взаимодействие с НКЦКИ по инцидентам.

Threat Intelligence (TI)

В рамках данного модуля поставляются платформа для управления данными об угрозах Kaspersky CyberTrace и потоки данных об угрозах Kaspersky Threat Data Feeds. Наличие лицензии упрощает интеграцию потоков данных с KUMA для дальнейшего использования аналитики угроз в повседневной работе ИБ-служб. KUMA собирает журналы с различных устройств, ИТ-систем и ИБ-инструментов и отправляет данные о событиях с URL, IP-адресами и хешами в Kaspersky CyberTrace на анализ, который сопоставляет поступающие события с потоками данных об угрозах и отправляет данные об обнаруженных угрозах в обратно в KUMA и Kaspersky CyberTrace Web. Аналитик ИБ получает оповещения об обнаруженных угрозах с дополнительным контекстом и может провести первоначальное расследование и инициировать процесс реагирования на основе полученного контекста. Платформа взаимодействует с любыми типами потоков аналитических данных об угрозах («Лаборатории Касперского», других поставщиков, из открытых источников или иных каналов) в форматах JSON, STIX/TAXII, XML и CSV и поддерживает интеграции с рассылками НКЦКИ и бюллетенями ФинЦЕРТ. В рамках данного модуля доступны следующие **потоки данных об угрозах: Malicious URL, BotnetCnC URL и Phishing URL, IP reputation и Ransomware URL.**

Использовать фиды и Kaspersky CyberTrace, приобретённые в рамках данного модуля, можно **только для обогащения событий**, получаемых KUMA (использовать с другими SIEM системами, а также для интеграции с системами других классов

недопустимо).

При приобретении KUMA (любых модулей) также предоставляется доступ к Kaspersky Threat Intelligence Portal (до 100 запросов в Kaspersky Threat Lookup и до 10 запросов в Kaspersky Threat Analysis) в период действия лицензии. Портал позволяет получить дополнительный контекст в ходе проведения расследований. Чтобы активировать эту функцию,

отправьте запрос с указанием номера заказа на адрес intelligence@kaspersky.com

KUMA Integration Add-on (отправка логов ОС с помощью KES)

(*Дополнение к любой лицензии KUMA)

В KES для Windows, начиная с версии 12.6, есть возможность отправлять события из журналов Windows в коллектор KUMA. Это позволяет получить в KUMA события из журналов Windows со всех хостов, на которых установлен KES для Windows версии 12.6, без установки агентов KUMA на эти хосты. Подробнее тут: <https://support.kaspersky.com/KUMA/3.4/ru-RU/280730.htm> Ограничений на количество хостов нет.

В KES для Linux, начиная с версии 12.2, есть возможность отправлять события ОС Linux в коллектор KUMA. Поддерживаемые типы событий: ProcessCreate, ProcessTerminate, FileChange, EventLog (ServiceStart, LinuxSessionStart, ServiceStop, LinuxSessionEnd, SuccessfulLogin, NewUserCreated, ...).

Отправка событий из журналов начинается с самой начальной записи

Модуль AI (Artificial intelligence)

Kaspersky Investigation & Response Assistant (KIRA) - облачный ИИ ассистент, который позволяет в карточке события или карточке корреляционного события проанализировать с подробным анализом и с кратким содержанием командной строки (Windows или Linux) с деобфускацией для помощи в расследовании и приоритезации алертов. Для работы модуля помимо лицензии KUMA необходим еще сертификат для выполнения запросов.

Использование KIRA [подробнее](#).

Блочная деобфускация: извлекает фрагменты текста и представляет их как деобфусцированные части:

- Кодировка: `base64`, `base32`
- Кодировка символов: `Binary`, `ASCII`, `Octal`, `Hex`
- Сжатие `Gzip` и `deflate` внутри `b64 /b32`

Встроенная деобфускация: заменяет распространенные встроенные обфускации:

- Диакритические знаки: `Äutömátíõn` → `Automation`
- Объединение строк: `"ha"+"ck"` → `"hack"`
- Кодировка символов Powershell: `[cHAr](70*34/34)` → `F`
- Удаление управляющего символа: `cm`d`.ex^e` → `cmd.exe`

Сервис AI (on-prem) по рейтингу и статусу активов - получает корреляционные события со «связанными активами», выстраивает ожидаемую последовательность событий и обучает модель AI. На основании цепочки срабатываний корреляционных правил AI-сервис высчитывает, является ли последовательность срабатываний не типичной для в этой инфраструктуры, затем повышает рейтинг / критичность (числовое значение от 0 до 1) AI и изменяют статус (`critical`, `high`, `middle`, `low`) актива. Это позволяет снизить нагрузку на специалистов ИБ и повысить время реакции – в первую очередь будут обрабатываться реальные инциденты, а не ложные срабатывания. Переобучение модели раз в сутки, а переоценка рейтинга активов происходит раз в час для всех активов, которые были в событиях за последние 24 часа. [Инструкция](#) по настройке.

Предлагаемая техническая поддержка

<https://support.kaspersky.ru/corporate/msa#tab2> по KUMA см. документ "Поддержка для Premium и Premium Plus"

Каналы связи

	Premium	Premium Plus
Company account (веб-портал, уведомления через почту)	✓	✓
Телефон	✓	✓

Время реакции в зависимости от уровня критичности

	Premium	Premium Plus
Критический (24 / 7)	2 часа	0,5 часа

Высокий (в рабочие часы)	6 часов	4 часа
Средний (в рабочие часы)	8 часов	6 часов
Низкий (в рабочие часы)	10 часов	8 часов

Доступные услуги

Программные исправления	Premium	Premium Plus
Удаленное подключение для диагностики проблем	✓	✓
Постпроектная поддержка*	✓	✓
Частные исправления	✓	✓
Рекомендации по оптимизации	✓	✓
Персональный технический аккаунт менеджер (ТАМ)	□	✓
Регулярные статус-встречи с ТАМ для анализа зарегистрированных инцидентов, связанных с ТП	□	Ежеквартальный отчет
Разработка нормализаторов для нестандартных источников событий	10 шт.	20 шт.

* Консультации по донастройке в среде заказчика проводятся только по продукту KUMA и при наличии информации о инфраструктуре и схеме развёртывания продукта.