Kaspersky Unified Monitoring and Analysis Platform

Руководство администратора



Уважаемый пользователь!

Спасибо, что доверяете нам. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Внимание! Права на этот документ являются собственностью АО "Лаборатория Касперского" (далее также "Лаборатория Касперского") и защищены законодательством Российской Федерации об авторском праве и международными договорами. За незаконное копирование и распространение документа и его отдельных частей нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с применимым законодательством.

Копирование в любой форме, распространение, в том числе в переводе, любых материалов возможны только с письменного разрешения "Лаборатории Касперского".

Документ и связанные с ним графические изображения могут быть использованы только в информационных, некоммерческих или личных целях.

Документ может быть изменен без предварительного уведомления.

За содержание, качество, актуальность и достоверность используемых в документе материалов, права на которые принадлежат другим правообладателям, а также за возможный ущерб, связанный с использованием этих материалов, "Лаборатория Касперского" ответственности не несет.

Дата редакции документа: 25.09.2020

© 2020 АО "Лаборатория Касперского"

https://www.kaspersky.ru https://support.kaspersky.ru

О "Лаборатории Касперского" https://www.kaspersky.ru/about/company

Содержание

О программе Kaspersky Unified Monitoring and Analysis Platform	4
Комплект поставки	4
Аппаратные и программные требования	5
Архитектура программы	7
Ядро	8
Коллектор	8
Коррелятор	10
Хранилище	11
Установка КUMA	12
Подготовка к установке программы	13
О лицензионном соглашении	14
Работа с инцидентами	15
Работа с событиями	15
Управление устройствами	15
Вход в веб-консоль программы	16
Обращение в службу технической поддержки	17
Примеры настройки KUMA	18
Создание правил корреляции	18
Корреляция событий с использованием бакета	18
Корреляция событий с использованием активных списков	25
Связь правил корреляции с Коррелятором	32
Проверка правильности работы правила корреляции	35
Добавление источника события с использованием стандартного нормализатора	
Подготовка ресурсов к инициализации Коллектора КUMA для КАТА	
Инициализация Коллектора для КАТА	41
Создание Коллектора для КАТА	44
Установка Коллектора для КАТА на сервере	44
Проверка состояния Коллектора для КАТА	45
Добавление источника события с использованием настраиваемого нормализатора regexp	46
Подготовка ресурсов к инициализации Коллектора KUMA для Cisco WSA	46
Инициализация Коллектора для Cisco WSA	50
Создание Коллектора для Cisco WSA	51
Установка Коллектора для Cisco WSA на сервере	52
Проверка состояния Коллектора Cisco WSA	52
Команды для запуска и установки компонентов вручную	54
Информация о стороннем коде	55
Уведомления о товарных знаках	56

О программе Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Unified Monitoring and Analysis Platform (далее КUMA или «программа») – 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 продукты «Лаборатории Касперского», так и сторонних производителей. Kaspersky Unified Monitoring and Analysis Platform сочетает в себе следующие функциональные возможности:

- получение, обработка и хранение событий информационной безопасности;
- анализ и корреляция;
- поиск полученных событий;
- создание уведомлений о выявленных инцидентах.

Программа построена на микросервисной архитектуре. Это означает, что вы можете создавать и настраивать только необходимые микросервисы, что позволяет использовать KUMA и как систему управления журналами, и как полноценную SIEM-систему. Кроме того, благодаря гибкой маршрутизации потоков данных вы можете использовать сторонние сервисы для дополнительной обработки событий.

В этом разделе

Комплект поставки	. 4
Аппаратные и программные требования	. 5

Комплект поставки

В комплект поставки входят следующие файлы:

- kuma-0.3.26-<номер сборки>.el8.x86_64 для установки на серверах Коллектора, Коррелятора и Хранилища KUMA;
- kuma-storage-0.3.0-<номер сборки>.el8.x86_64 для установки на серверах Хранилища КUMA;
- пакет kuma-core-0.3.0-<номер сборки>.el8.x86_64;
- пакет kuma-console-0.3.28-<номер сборки>.el8.x86_64;
- kuma.exe для установки Агента KUMA для Windows®;
- kuma-installer для установки компонентов KUMA;
- файлы с текстом Лицензионного соглашения на английском и русском языках;
- файлы с информацией о версии (примечания к выпуску) на английском языке.

В комплект поставки также входит бинарный файл для установки MongoDB, Elasticsearch OSS 7.5.1, Prometheus 2.12.0 и Grafana 6.3.5 вместе с лицензиями.

Аппаратные и программные требования

КUMA может работать на физическом оборудолвании и в виртуальных средах.

Рекомендуемые требования к оборудованию

На перечисленном ниже оборудовании могут обрабатываться до 40 000 событий в секунду. Этот показатель зависит от типа анализируемых событий и от эффективности настроек.

- Серверы для установки Коллекторов:
 - ЦП: 8 vCPU
 - ОЗУ: 4 ГБ
 - Диск: 100 ГБ доступного места на диске, смонтированного в разделе /opt
- Серверы для установки Корреляторов:
 - ЦП: 8 vCPU
 - ОЗУ: 16 ГБ
 - Диск: 100 ГБ доступного места на диске, смонтированного в разделе /opt
- Серверы для установки Ядра:
 - ЦП: 4 vCPU
 - ОЗУ: 8 ГБ
 - Диск: 100 ГБ доступного места на диске, смонтированного в разделе /opt
- Серверы для установки Хранилища:
 - ЦП: 24 vCPU
 - ОЗУ: 48 ГБ
 - Диск: 500 ГБ доступного места на диске, смонтированного в разделе /opt

Использование твердотельных накопителей позволяет улучшить индексирование кластерных узлов и повысить эффективность поиска.

Смонтированные локально жесткие диски или твердотельные накопители эффективнее внешних дисковых массивов (JBOD). Рекомендуется использовать RAID 0 для скорости, а RAID 10 – для избыточности.

Для повышения надежности не развертывайте все кластерные узлы на одном JBOD-массиве или одном физическом сервере (если используются виртуальные серверы).

Для повышения эффективности рекомендуется развернуть все серверы в одном центре обработки данных.

Требования к программному обеспечению

На каждом сервере, который используется для установки микросервисов KUMA, необходимо установить операционную систему CentOS 8.х.

Требования к сети

Пропускная способность сетевого интерфейса должна быть не менее 100 Мбит/с

Дополнительные требования

На компьютерах, используемых для веб-консоли KUMA, необходимо установить бразуер Google Chrome™ 78 или более поздней версии либо Mozilla™ Firefox™ 70 или более поздней версии.

Архитектура программы

Стандартная установка программы включает следующие компоненты:

- один или несколько Коллекторов, которые получают сообщения из источников событий и осуществляют их парсинг, нормализацию и, если требуется, фильтрацию и/или агрегацию;
- Коррелятор, который анализирует полученные из коллекторов нормализованные события, выполняет необходимые действия с активными листами и создает инциденты в соответствии с правилами корреляции;
- Ядро, поставляемое с графическим интерфейсом для мониторинга и управления настройками компонентов системы;
- Хранилище, в котором содержатся нормализованные события и зарегистрированные инциденты.

События передаются между компонентами по надежным транспортным протоколам (при желании с шифрованием). Вы можете настроить балансировку нагрузки для ее распределения между экземплярами микросервисов, а также включить автоматическое переключение на резервный компонент в случае недоступности основного. Если недоступны все компоненты, события сохраняются в буфере жесткого диска и передаются позже. Размер буфера для временного хранения событий на диске можно настраивать.



В этом разделе

Ядро	
Коллектор	
Коррелятор	
Хранилище	

Ядро

Ядро – это центральный компонент КUMA, через который производится управление всеми микросервисами. Предоставляемый ядром графический пользовательский интерфейс веб-консоли предназначен как для повседневного использования операторами и аналитиками, так и для настройки системы в целом.

Ядро позволяет решать следующие задачи:

- создание и настройка микросервисов (или компонентов) программы;
- централизованное управление микросервисами и учетными записями пользователей программы;
- визуальное представление статистических данных о работе программы;
- расследование угроз безопасности на основе полученных событий.

Коллектор

Коллектор – это компонент программы, который получает сообщения из источников событий, обрабатывает их и передает в Хранилище, Коррелятор и/или сторонние сервисы.

Для каждого Коллектора нужно настроить как минимум один коннектор и один нормализатор. Вы также можете настроить любое количество дополнительных нормализаторов, фильтров, правил обогащения и правил агрегации. Для того чтобы Коллектор мог отправлять нормализованные события в другие микросервисы, необходимо добавить точки назначения. В стандартном развертывании обычно используются две точки назначения: Хранилище и Коррелятор.

Алгоритм работы Коллектора включает следующие этапы:

а. Получение сообщений из источников событий

Для получения сообщений требуется настроить активный или пассивный коннектор. Пассивный коннектор может только получать сообщения из источника события, а активный – инициировать подключение к источнику события, например, к системе управления базами данных.

Коннекторы различаются по типу. Выбор типа коннектора зависит от транспортного протокола для передачи сообщений. Например, для источника события, передающего сообщения по протоколу TCP, необходимо установить коннектор типа TCP.

В программе доступны следующие типы коннекторов:

- internal
- tcp
- udp
- netflow
- nats
- kafka
- http
- file
- sql

b. Парсинг и нормализация событий

События, полученные коннектором, обрабатываются с помощью парсера и правил нормализации, заданных пользователем. Выбор нормализатора зависит от формата сообщений, получаемых из источника события. Например, для источника, отправляющего события в формате CEF, необходимо выбрать корневой нормализатор типа CEF.

В программе доступны следующие нормализаторы:

- JSON
- CEF
- CSV/TSV
- Key-value
- Regexp
- Syslog (в соответствии с RFC3164 и RFC5424)
- XML
- NetFlow v9
- SQL

с. Фильтрация нормализованных событий

Вы можете настроить фильтры, которые позволяют отбирать для дальнейшей обработки только события, удовлетворяющие заданным условиям Событие, не удовлетворяющее условиям фильтрации, дальше не обрабатывается.

d. Обогащение и преобразование нормализованных событий

Правила обогащения позволяют дополнить содержимое события информацией из внутренних и внешних источников. В программе представлены следующие источники обогащения:

- constant
- cybertrace
- dictionary
- dns
- event
- Idap
- template

Правила преобразования позволяют преобразовать содержимое события в соответствии с заданными условиями. В программе представлены следующие методы преобразования:

- lower перевод всех символов в нижний регистр
- upper перевод всех символов в верхний регистр
- regexp извлечение подстроки с использованием регулярных выражений RE2
- substring выбор текстовых строк по заданным номерам позиции
- replace замена текста введенной строкой
- trim удаление заданных символов
- append добавление символов в конец значения поля
- prepend добавление символов в начало значения поля

е. Агрегация нормализованных событий

Вы можете настроить правила агрегации, чтобы уменьшить количество схожих сообщений, передаваемых в Хранилище и/или Коррелятор. Например, вы можете агрегировать в одно событие все сообщения о сетевых подключениях, выполненных по одному и тому же протоколу (транспортного и прикладного уровней) между двумя IP-адресами и полученных в течение заданного интервала времени. Если настроены правила агрегации, несколько сообщений могут обрабатываться и сохраняться как одно событие. Это помогает снизить нагрузку на микросервисы, отвечающие за дальнейшую обработку событий, и сэкономить место для хранения.

f. Передача нормализованных событий

По завершении всех этапов обработки событие отправляется в настроенные точки назначения.

Коррелятор

Коррелятор – это компонент программы, который в режиме близком к реальному времени анализирует нормализованные события. В процессе корреляции может использоваться информация из активных листов и/или словарей.

Полученные в ходе анализа данные применяются для решения следующих задач:

- выявление инцидентов;
- уведомление о выявленных инцидентах;
- управление содержимым активных списков;
- отправка корреляционных событий в настроенные точки назначения.

Принцип работы Коррелятора основан на сигнатурном анализе событий. Это значит, что каждое событие обрабатывается в соответствии с правилами корреляции, заданными пользователем. При обнаружении последовательности событий, удовлетворяющих условиям правила корреляции, программа создает корреляционное событие и отправляет его в Хранилище. Корреляционное событие может стать базовым для других правил корреляции. Результаты одного корреляционного правила могут использоваться другими корреляционными правилами.

Вы можете вручную распределять корреляционные правила и используемые ими активные листы между Корреляторами, регулируя распределение нагрузки между микросервисами. В этом случае Коллекторы будут отправлять одни и те же нормализованные события во все доступные Корреляторы.

Алгоритм работы Коррелятора включает следующие этапы:

а. Получение события

Коррелятор получает нормализованное событие из Коллектора или другого микросервиса.

b. Применение правил корреляции

Вы можете настроить правила корреляции на срабатывание на основе одного события или последовательности событий. Если по правилам корреляции не был выявлен инцидент, обработка события завершается.

с. Реагирование на инцидент

Вы можете задать действия, которые программа должна выполнить при выявлении инцидента.

В программе доступны следующие действия:

- обогащение события;
- операции с активными листами;
- отправка уведомлений;
- сохранение корреляционного события.

d. Отправка корреляционного события

При обнаружении последовательности событий, удовлетворяющих условиям правила корреляции, программа создает корреляционное событие и отправляет его в Хранилище. На этом обработка события Коррелятором завершается.

Хранилище

Нормализованные события помещаются в кластер Elasticsearch (или Хранилище). Технология Elasticsearch позволяет выполнять поиск и агрегацию событий в Хранилище.

При выборе кластера конфигурации Elasticsearch учитывайте следующее:

- политики хранения события для вашей организации;
- лучшие практики по проектированию кластера Elasticsearch.

Установка KUMA

Вы можете развернуть компоненты KUMA на одном сервере с помощью приложения kuma-installer.

Имя сервера, на котором запускается установщик, должно отличаться от localhost или localhost.<домен>. Установщик через kuma-installer можно запустить из любой папки, но RPM-пакеты должны находится в одной папке с файлом kuma-installer.

После первоначальной установки вы можете использовать установщик повторно. При этом установщик повторит свои действия, не удаляя пользовательские данные. Это можно использовать при восстановлении системных файлов KUMA или примеров ресурсов и микросервисов, которые были изменены или удалены по ошибке.

Для установки продукта требуются root-привилегии.

Для запуска kuma-installer выполните следующую команду:

kuma-installer [--with-example-services]

Действия, выполняемые установщиком

Установщик выполняет следующие действия:

- 1. Запрос на подтверждение установки программы.
- 2. Отключение SELinux.
- 3. Установка RPM-пакетов kuma, kuma-core и kuma-console.
- 4. Установка и запуск микросервиса kuma-core systemd.

На этом шаге необходимо указать, принимаете ли вы условия Лицензионного соглашения. Если вы не принимаете условия Лицензионного соглашения, установка программы не выполняется.

- 5. Импорт примеров ресурсов.
- 6. Открытие портов для отправки сообщений между микросервисами КUMA.
- 7. Предоставление пользователю веб-адреса веб-консоли KUMA.
- 8. Предоставление имени и пароля пользователя для доступа к веб-консоли.

Действия, выполняемые установщиком при использовании флага --with-example-services

Помимо описанного ранее установщик также выполняет следующие действия:

- 1. Установка RPM-пакета kuma-storage.
- 2. Изменение конфигурации Elasticsearch и перезапуск микросервиса elasticsearch systemd.
- 3. Установка примеров Коллекторов, Коррелятора и Хранилища, а также запуск их микросервисов в systemd.
- 4. Открытие портов, через которые Коллекторы должны получать события из источников событий.

Подготовка к установке программы

Адресация компонентов KUMA осуществляется по полному доменному имени (FQDN) хоста. Перед установкой программы убедитесь, что команда hostnamectl status возвращает правильное имя FQDN хоста в поле Static hostname.

Перед развертыванием программы убедитесь, что серверы, предназначенные для установки ее компонентов, соответствуют аппаратным и программным требованиям.

- Для подготовки программы к установке сделайте следующее:
 - 1. При установке операционной системы выберите минимальный набор пакетов.
 - 2. Задайте следующую разметку дискового пространства сервера:
 - корневой раздел /: Standard Partition, XFS, 16 Гб, разрешено шифрование;
 - раздел /opt: LVM, XFS, все доступное дисковое пространство, разрешено шифрование.
 - 3. После установки операционной системы и перезагрузки сервера отключите SELinux.
 - a. Если параметр SELINUX имеет значение enforcing, отключите запуск SELinux при загрузке системы. Для этого в файле /etc/selinux/config укажите SELINUX=disabled вместо SELINUX=enforcing.
 - b. Если для параметра SELinux status значение включено, отключите SELinux, выполнив следующую команду:

setenforce 0

О лицензионном соглашении

Пицензионное соглашение – это юридически обязывающий договор между вами и "Лабораторией Касперского", где определены условия, на которых вы можете использовать программу.

Перед началом использования программы внимательно прочитайте лицензионное соглашение.

Ознакомиться с условиями лицензионного соглашения можно следующими способами:

- в ходе установки KUMA;
- прочитав файл EULA_<идентификатор языка>, входящий в пакет поставки программы;
- выполнив следующую команду:

kuma license

При установке программы вы принимаете условия лицензионного соглашения, подтверждая свое согласие с ними. Если вы не согласны с условиями лицензионного соглашения, отмените установку и не используйте программу.

Работа с инцидентами

В разделе **Alerts** веб-интерфейса KUMA можно просматривать и обрабатывать инциденты, зарегистрированные программой.

В верхней части раздела Alerts показана панель инструментов для фильтрации и поиска инцидентов.

В основной части раздела **Alerts** представлена таблица, в столбцах которой содержится информация о зарегистрированных инцидентах:

- Priority (≡) степень значимости потенциальной угрозы безопасности: критическая ^Щ, высокая ≡, умеренная ≡, низкая ≡.
- Status текущее состояние инцидента:
 - new новый, еще не обработанный инцидент;
 - **assigned** инцидент обработан и передан сотруднику службы безопасности для расследования или реагирования;
 - closed инцидент закрыт. Инцидент был ложный или угроза безопасности устранена.
- Assigned to имя сотрудника службы безопасности, которому инцидент передан для расследования или реагирования.
- **First seen** дата и время создания первого корреляционного события в последовательности событий, приведшего к созданию инцидента.
- Last seen дата и время создания последнего корреляционного события в последовательности событий, приведшего к созданию инцидента.

События и инциденты можно сортировать и фильтровать по значениям в столбцах.

При создании инцидента открывается окно со сведениями о нем.

Работа с событиями

В разделе **Events** веб-консоли Ядра КUMA вы можете просматривать события, хранящиеся в кластере Elasticsearch, чтобы расследовать угрозы безопасности или создавать правила корреляции.

События можно фильтровать. Для отображения самых последних записей по выбранным событиям обновите веб-страницу или установите флажок автоматического обновления **Auto refresh**.

События загружаются в браузер пакетами. Чтобы загрузить очередной пакет событий, прокрутите таблицу событий до конца и нажмите кнопку Load next 250 events.

Управление устройствами

В разделе **Assets** веб-консоли KUMA можно просматривать и изменять информацию об известных устройствах и их категории.

В левой части раздела **Assets** отображается дерево категорий устройств. Вы можете просматривать дерево, а также развертывать и свертывать его узлы. Если выбрать узел, в правой части окна отображаются устройства, относящиеся к соответствующей категории.

Если щелкнуть по устройству, в правой части окна открывается область **Asset details** со следующими параметрами устройства:

- Name имя устройства.
- ІD идентификатор устройства.
- Created дата и время добавления устройства в КUMA.
- Updated дата и время изменения информации об устройстве.
- IP address IP-адрес устройства (если предоставлен).
- DNS name доменное имя устройства (если предоставлено).
- IP address IP-адрес устройства (если предоставлен).
- Related alerts инциденты, с которыми связано устройство (если есть).

Для просмотра списка инцидентов, с которыми связано устройство, можно щелкнуть по ссылке **Find in Alerts**. Откроется вкладка **Alerts** с поисковым выражением, позволяющим отфильтровать все устройства с соответствующим идентификатором.

• Categories – категории, к которым относится устройство (если есть).

Вход в веб-консоль программы

- Для входа в веб-консоль программы сделайте следующее:
 - 1. В браузере введите следующий адрес:

https://<IP-адрес или FQDN сервера Ядра КUMA>:7220

Откроется страница авторизации веб-консоли с запросом на ввод имени и пароля для входа.

- 2. В поле User name введите имя учетной записи.
- 3. В поле Password введите пароль указанной учетной записи.
- 4. Нажмите на кнопку Login.

Откроется главное окно веб-консоли программы.

Для выхода из веб-консоли программы сделайте следующее:

Откройте веб-консоль KUMA, в левом нижнем углу окна щелкните по имени учетной записи пользователя и в открывшемся меню учетной записи нажмите на кнопку **Logout**.

Обращение в службу технической поддержки

Если вам не удается найти решение своей проблемы в документации к программе, обратитесь к специалисту по технической поддержке в "Лабораторию Касперского".

Примеры настройки KUMA

В этом разделе приводятся примеры настройки KUMA.

Это только пример. При настройке КUMA в своей сети используйте собственную конфигурацию.

В этом разделе

Создание правил корреляции	18
Добавление источника события с использованием стандартного нормализатора	37
Добавление источника события с использованием настраиваемого нормализатора regexp	45

Создание правил корреляции

В этом разделе приведены примеры создания правил корреляции:

- Правило корреляции на основе бакетов
- Правило корреляции на основе активного списка

Также описано, как добавить правила корреляции и активный список в существующий Коррелятор и как проверить их работу.

В этом разделе

Корреляция событий с использованием бакета

Корреляция событий с использованием активных списков

Связь правил корреляции с Коррелятором

Проверка правильности работы правила корреляции

Корреляция событий с использованием бакета

В этом примере показано создание правила корреляции, использующего бакеты для обнаружения корреляций.

Задача – выявить события создания учетной записи, которая затем была удалена в течение часа. Необходимо обнаружить событие создания (Windows EventID 4720) и событие удаления (Windows EventID 4726), промежуток времени между которыми менее одного часа.

Корреляция выполняется одним правилом корреляции, в котором используется два фильтра для поиска соответствующих событий. При получении события, удовлетворяющего условиям фильтра, правило корреляции ожидает другого события в течение 3600 секунд. Если оба события произошли в течение часа, создается событие корреляции.

Настройка корреляции выполняется поэтапно:

- Создание фильтров, используемых для поиска соответствующих событий. В данном примере это фильтры событий создания учетной записи и удаления учетной записи.
- Создание ресурса Правило корреляции.
- Связь Правила корреляции с существующим микросервисом Коррелятор.
- Проверка правильности работы правила корреляции.

В этом примере используются ресурсы, добавленные в КUMA как часть демонстрационного развертывания. Инструкции, приведенные в этом разделе, можно использовать для создания аналогичных ресурсов для ваших целей.

В этом разделе

Создание фильтра для поиска событий создания учетной записи	.19
Создание фильтра для поиска событий удаления учетной записи	.20
Создание правила корреляции для выявления создания и удаления учетных записей	.22

Создание фильтра для поиска событий создания учетной записи

- Чтобы создать ресурс Фильтр для поиска событий создания учетной записи, выполните следующие действия:
 - 1. Откройте веб-консоль KUMA и выберите закладку Filters в разделе Resources.
 - 2. Нажмите на кнопку Add.

Откроется окно для настройки параметров ресурса Фильтр.

- 3. В поле Name введите название фильтра, которое позволит идентифицировать созданный ресурс: [Пример] [AD] Созданная учетная запись.
- Перейдите по ссылке Add condition, чтобы добавить первое условие фильтра.
 Откроется окно Condition.
- 5. Задайте параметры для первого условия фильтра, как описано ниже:
 - В раскрывающемся списке Operation выберите =.
 - В группе параметров Left operand задайте параметры, как описано ниже:
 - В раскрывающемся списке Kind выберите event.
 - В раскрывающемся списке Field выберите DeviceEventClassID.
 - В группе параметров **Right operand** задайте параметры, как описано ниже:
 - В раскрывающемся списке Kind выберите constant.
 - В поле Value введите 4720.

6. Нажмите на кнопку Сохранить.

Окно Condition закроется, и отобразится созданное условие.

- Перейдите по ссылке Add condition, чтобы добавить второе условие фильтра. Откроется окно Condition.
- 8. Задайте параметры для второго условия фильтра, как описано ниже:
 - В раскрывающемся списке Operation выберите =.
 - В группе параметров Left operand задайте параметры, как описано ниже:
 - В раскрывающемся списке Kind выберите event.
 - В раскрывающемся списке Field выберите DeviceVendor.
 - В группе параметров **Right operand** задайте параметры, как описано ниже:
 - В раскрывающемся списке Kind выберите constant.
 - **В поле Value введите** Microsoft.
- 9. Нажмите на кнопку Сохранить.

Окно Condition закроется, и отобразится созданное условие.

10. Нажмите на кнопку Сохранить.

Фильтр будет создан и отобразится на закладке Filters.



Создание фильтра для поиска событий удаления учетной записи

- Чтобы создать ресурс Фильтр для поиска событий создания учетной записи, выполните следующие действия:
 - 1. Откройте веб-консоль КUMA и выберите закладку Filters в разделе Resources.
 - 2. Нажмите на кнопку Add.

Откроется окно для настройки параметров ресурса Фильтр.

- 3. В поле Name введите название фильтра, которое позволит идентифицировать созданный ресурс: [Пример] [AD] Удаленная учетная запись.
- Перейдите по ссылке Add condition, чтобы добавить первое условие фильтра.
 Откроется окно Condition.

- 5. Задайте параметры для первого условия фильтра, как описано ниже:
 - В раскрывающемся списке Operation выберите =.
 - В группе параметров Left operand задайте параметры, как описано ниже:
 - В раскрывающемся списке Kind выберите event.
 - В раскрывающемся списке Field выберите DeviceEventClassID.
 - В группе параметров **Right operand** задайте параметры, как описано ниже:
 - В раскрывающемся списке Kind выберите constant.
 - В поле Value введите 4726.
- 6. Нажмите на кнопку Сохранить.

Окно **Condition** закроется, и отобразится созданное условие.

- 7. Перейдите по ссылке **Add condition**, чтобы добавить второе условие фильтра. Откроется окно **Condition**.
- 8. Задайте параметры для второго условия фильтра, как описано ниже:
 - В раскрывающемся списке Operation выберите =.
 - В группе параметров Left operand задайте параметры, как описано ниже:
 - В раскрывающемся списке Kind выберите event.
 - В раскрывающемся списке Field выберите DeviceVendor.
 - В группе параметров **Right operand** задайте параметры, как описано ниже:
 - В раскрывающемся списке Kind выберите constant.
 - **В поле Value введите** Microsoft.
- 9. Нажмите на кнопку Сохранить.

Окно Condition закроется, и отобразится созданное условие.

10. Нажмите на кнопку Сохранить.

Фильтр будет создан и отобразится на закладке Filters.

\leftrightarrow \rightarrow C $($ kuma.example.com:722	0/resources/filters/(form:a471223e-a1a	aa-41c8-b945-3ed680b18331)	🔄 🖈 🕝 🔮 a
≡	Resources		
· · · · ·	Connectors Normalizers F Response rules Connections	Filters Enrichment rules Aggregation rules Destinations Dictionary Proxies	Correlation rules Active lists
Kaspersky Unified Monitoring and	+ Add	Name *	
Analysis Platform	[Example][AD] A member was added to a security-enabled global group (4728)	Example][AD] Account Deleted	
♪ Alerts	[Example][AD] A member was added to a security-enabled universal group	AND Add condition / Add group / Toggle OR / Toggle NOT event::DeviceEventClassID = 4726	
Pt Events	(4/56) [Example][AD] A member was	event::DeviceVendor = Microsoft	
Assets	removed from a security-enabled global group (4729)	Save	

Создание правила корреляции для выявления создания и удаления учетных записей

- Чтобы создать ресурс корреляции, выполните следующие действия:
 - 1. Откройте веб-консоль KUMA и выберите закладку Correlation rules в разделе Resources.
 - 2. Нажмите на кнопку Add.

Откроется окно для настройки параметров ресурса Правило корреляции.

- 3. В поле Name введите название фильтра, которое позволит идентифицировать созданный ресурс: [Пример] [AD] Учетная запись создана и удалена за короткий период времени.
- 4. В раскрывающемся списке **Kind** выберите **standard**. Корреляция на основе бакетов доступна только для правил корреляции стандартного типа.
- 5. В раскрывающемся списке Identical fields выберите DestinationUserName и DestinationNtDomain.
- 6. В поле Window, sec укажите, сколько времени должен существовать бакет. Введите значение 3600.
- 7. В раскрывающемся списке **Priority** выберите приоритет созданного правила корреляции. Выберите **Medium**.
- 8. В группе параметров **Selectors** добавьте фильтры, которые будут отбирать события для передачи в это правило корреляции:
 - Добавьте первый фильтр:
 - В поле Alias введите название фильтра: Создана учетная запись.
 - В поле **Threshold, count** введите количество событий, которое должно получить правило корреляции для срабатывания. Введите значение 1.
 - В раскрывающемся списке Filter выберите созданный ранее фильтр [Пример] [AD] Создана учетная запись.
 - Добавьте второй фильтр:
 - В поле Alias введите название фильтра: Удалена учетная запись.
 - В поле **Threshold, count** введите количество событий, которое должно получить правило корреляции для срабатывания. Введите значение 1.

• В раскрывающемся списке Filter выберите созданный ранее фильтр [Пример] [AD] Удалена учетная запись.

← → C 🔒 kuma.example.com:7220)/resources/correlation-rules/(form:a5812acf-7039-4b8	:-b592-f851	le8c335a8)	🖻 🕸 😮 📵
≡	[Example][AD] Account created and deleted within a short period of time	00	[Example][AD] Account created and deleted within a short period of time	
	[Example][AD] Granted TGS without TGT (Golden Ticket)	00	Kind*	
[-`@`-]	[Example][AD] Membership of sensitive group was modified	00	standard	× ×
	[Example][AD] Successful authentication with the same	DD	Identical fields *	
Kaspersky Unified Monitoring and	Example IADI Technical 14768 TGT Requested	പെക	DestinationUserName * DestinationNtDomain *	
Analysis Platform				
			Unique fields	
↓ Alerts				
Br. Curren			Window, sec *	
Fix Events			3600	
Assets			Priority*	
III Sonicos			E Medium	~
III Services			Selectors	
Resources			Event 'Account Created'	
Settings			Aline*	
			Account Created	
🚍 Metrics			Threshold count*	
			1	
			These t	
				× 0
			Tevanise (h.e). Leconic elected	
			Event Account Deleted	
			Autos	
			Account Deleted	
			Threshold, count *	
			Filter *	
Administrator >			[Example][AD] Account Deleted	XQ

Оба фильтра добавлены к ресурсу Правило корреляции, но помимо этого необходимо убедиться, что правило срабатывает, только если событие создания учетной записи предшествует событию удаления учетной записи. Это условие можно задать в разделе **Join filter**.

9. В разделе Join filter перейдите по ссылке Setup inline.

Откроется окно **Filter**, в котором можно настроить условия фильтрации. Добавьте условие фильтрации, как описано ниже:

а. Перейдите по ссылке Add condition.

Откроется окно Condition.

- b. В раскрывающемся списке Operation выберите <.
- с. В группе параметров Left operand задайте параметры, как описано ниже:
 - В раскрывающемся списке Kind выберите event.
 - В поле Name введите название одного из фильтров из раздела Selector. Введите Создана учетная запись.
 - В раскрывающемся списке Field выберите EndTime.
- d. В группе параметров Right operand задайте параметры, как описано ниже:
 - В раскрывающемся списке Kind выберите event.
 - В поле Name введите название одного из фильтров из раздела Selector. Введите Удалена учетная запись.
 - В раскрывающемся списке Field выберите EndTime.
- е. Нажмите на кнопку Сохранить.

Будет создано условие для объединенного фильтра, что обеспечит срабатывание правила корреляции, только если события от разных фильтров получены в определенном порядке.

Condition	
Operation	
<	× ×
Not	
Ignore case	
Left operand	
Kind	
event	× ~
Name	
Field	
EndTime	× *
Right operand	
Kind	
event	× ~
Name	
Account Deleted	
Field	
EndTime	× •
Link filter	
Filter	
	Q

10. Нажмите на кнопку **Оk**, чтобы завершить настройку объединенного фильтра.

Когда все фильтры будут настроены, необходимо выбрать действия, которые будут выполняться при срабатывании правила.

11. В группе параметров Actions в разделе on EveryThreshold установите флажок Output.

Это означает, что при каждом срабатывании правила корреляции будет создаваться событие корреляции и отправляться дальше микросервису Коррелятор.

12. Нажмите на кнопку Сохранить.

Правило корреляции будет создано и отобразится на закладке Correlation rules.

Корреляция событий с использованием активных списков

В этом примере показано создание правила корреляции, использующего активные списки для обнаружения корреляций.

Задача состоит в том, чтобы идентифицировать события запроса службы предоставления билетов (Ticket Granting Service – TGS) без предшествующего события билета на получение билетов (Ticket Granting Ticket – TGT). При получении TGT контроллер домена формирует событие с идентификатором 4768. При получении запроса TGS контроллер домена формирует событие с идентификатором 4769. Следовательно, потенциальный инцидент можно определить как получение события запроса TGS без предварительного получения события TGT.

Поскольку контроллеры домена получают большое количество событий с идентификаторами 4768 и 4769, а TGT действителен в течение 10 часов, использование правил корреляции на основе бакетов неэффективно. В этом случае следует использовать корреляцию на основе активного списка.

Корреляция будет осуществляться по двум правилам корреляции:

- 1. Первое правило срабатывает, когда пользователь получает TGT. Это событие записывается в активный список, где информация о нем хранится в течение 10 часов.
- 2. Второе правило срабатывает при получении события запроса TGS. Правило корреляции проверяет, содержит ли активный список информацию о событии TGT и созданном событии корреляции, если ничего не найдено.

Настройка правила корреляции выполняется поэтапно:

- Создание активного списка для хранения информации о событиях TGT.
- Создание правила корреляции для фильтрации событий TGT и их записи в активный список.
- Создание правила корреляции для фильтрации событий TGS и поиска соответствующих событий TGT в активном списке.
- Связь Правила корреляции с существующим микросервисом Коррелятор.
- Проверка правильности работы правила корреляции.

В этом примере используются ресурсы, добавленные в КUMA как часть демонстрационного развертывания. Инструкции, приведенные в этом разделе, можно использовать для создания аналогичных ресурсов для ваших целей.

В этом разделе

Создание активного списка для хранения ТСТ	25
Создание правида корредяции для записи в активный список	26
ободание правила корролиции для записи в активный описок	
Создание правила корреляции для проверки, предшествует ли событие TGT запросу TGS	29

Создание активного списка для хранения TGT

- Чтобы создать активный список для хранения информации о событиях TGT, выполните следующие действия:
 - 1. Откройте веб-консоль КUMA и выберите закладку Active lists в разделе Resources.
 - 2. Нажмите на кнопку Add и задайте параметры, как описано ниже.

- В поле Name введите название активного списка, которое позволит идентифицировать созданный ресурс: [Пример] [AD] Список запрашиваемых TGT. EventID 4768.
- В поле **TTL** укажите, сколько секунд запись будет храниться в активном списке. Необходимо, чтобы запись в активном списке была доступна в течение периода времени, пока действует TGT, то есть в течение 10 часов. Введите значение 36000.
- 3. Нажмите на кнопку Save.

Активный список будет создан и отобразится на закладке Active lists.

← → C	20/resources/active-lists/(form:f4ccfd1c-e45c-	4f0c-9b27-3ce50e02b6b7)	🖻 🛧 G 🥑 a
≡	Resources		
	Connectors Normalizers Filters Response rules Connections Press	Enrichment rules Aggregation rules Destinations Dictionary oxies	Correlation rules Active lists
Naspersky Unified Monitoring and Analysis Platform	+ Add [Example][AD] End-users tech D D	Name * [Example][AD] List of requested TGT. EventID 4768	
♪ Alerts	[Example][AD] List of requested TGT. D to EventID 4768 [Example][AD] List of sensitive groups D to	TTL 36000	\$
		Save	

Создание правила корреляции для записи в активный список

- Чтобы создать правило корреляции для записи информации о TGT в активный список, выполните следующие действия:
 - 1. Откройте веб-консоль KUMA и выберите закладку Correlation rules в разделе Resources.
 - 2. Нажмите на кнопку Add.

Откроется окно для настройки параметров ресурса Правило корреляции.

- 3. В поле Name введите название фильтра, которое позволит идентифицировать созданный ресурс: [Пример] [AD] [Технический] 4768. Запрашиваемый ТGT.
- 4. В раскрывающемся списке Kind выберите operational.
- 5. В разделе **Selectors** перейдите по ссылке **Setup inline**, чтобы добавить фильтр, который будет отбирать события для передачи в это правило корреляции.

Откроется окно **Filter**, в котором можно настроить условия фильтрации. Добавьте условия фильтра с помощью кнопки **Add condition**, как описано ниже:

- Первое условие:
 - В раскрывающемся списке Operation выберите =.
 - В группе параметров Left operand задайте параметры, как описано ниже:
 - В раскрывающемся списке Kind выберите event.
 - В раскрывающемся списке Field выберите DeviceEventClassID.
 - В группе параметров **Right operand** задайте параметры, как описано ниже:
 - В раскрывающемся списке Kind выберите constant.
 - В поле Value введите 4768.

- Второе условие:
 - В раскрывающемся списке **Operation** выберите **endsWith**.
 - Установите флажок Not, чтобы создать фильтр, НЕ содержащий записей, соответствующих условию.
 - В группе параметров Left operand задайте параметры, как описано ниже:
 - В раскрывающемся списке Kind выберите event.
 - В раскрывающемся списке Field выберите DestinationUserName.
 - В группе параметров **Right operand** задайте параметры, как описано ниже:
 - В раскрывающемся списке Kind выберите constant.
 - B поле Value введите S.
- Третье условие:
 - В раскрывающемся списке **Operation** выберите **startsWith**.
 - Установите флажок **Not**, чтобы создать фильтр, НЕ содержащий записей, соответствующих условию.
 - В группе параметров Left operand задайте параметры, как описано ниже:
 - В раскрывающемся списке Kind выберите event.
 - В раскрывающемся списке Field выберите DestinationUserName.
 - В группе параметров **Right operand** задайте параметры, как описано ниже:
 - В раскрывающемся списке Kind выберите constant.
 - В поле Value введите S.
- Четвертое условие:
 - В раскрывающемся списке Operation выберите =.
 - В группе параметров Left operand задайте параметры, как описано ниже:
 - В раскрывающемся списке Kind выберите event.
 - В раскрывающемся списке Field выберите DeviceVendor.
 - В группе параметров **Right operand** задайте параметры, как описано ниже:
 - В раскрывающемся списке Kind выберите constant.
 - В поле Value введите Microsoft.

Условия фильтра будут созданы.

←	→ C (🕯 kuma.example.com:7220/resources/correlation-rules/(form:5a6ddc65-ff68-4c53-8cca-123bb3616c77) 🔯 🟠 🤇	3 9 0
≡		Resources Connectors Normalizers Filters Enrichment rules Aggregation rules Destinations Dictionary Correlation rules Response rules Connections Proxies	Active lists
U	nified Mo Analysi	opitoring and sl Filter	
¢	Alerts	▼ AND Add condition / Add group / Toggle OR / Toggle NOT	× ~
ŀα	Events	event::DeviceEventClassID = 4768 event::DestinationUserName not endsWith S	
Ē	Assets	event::DestinationUserName not startsWith S	
	Services	event::DeviceVendor = Microsoft	
ŪŦ	Resources	Ok Cancel	
ø	Settings		

6. Нажмите на кнопку **Оk**, чтобы сохранить фильтр в правиле корреляции.

Когда фильтр будет настроен, необходимо выбрать действия, которые будут выполняться при срабатывании правила.

- 7. В разделе onEveryEvent в группе параметров Actions перейдите по ссылке Add action with active list и задайте значения параметров, как описано ниже:
 - В поле Name введите название создаваемого триггера: [Пример] [AD] Список запрашиваемых TGT. EventID 4768.
 - В раскрывающемся списке **Operation** выберите тип операции, которую требуется выполнить с активным списком. Выберите **set**.
 - В раскрывающемся списке **Key fields** выберите имена полей события, которые будут использоваться в идентификаторе записи активного списка. Выберите **DestinationUserName** и **DestinationNtDomain**.
 - В разделе Mapping задайте правила записи значений полей события в поля активного списка:
 - В поле Active list field введите Account и в раскрывающемся списке справа от этого поля выберите значение DestinationUserName.
 - В поле Active list field введите Domain и в раскрывающемся списке справа от этого поля выберите значение DestinationNtDomain.

• В поле Active list field введите DateTime и в раскрывающемся списке справа от этого поля выберите значение DeviceReceiptTime.

← → C	20/resources/correlation-rules/(form:5a6ddc65-ff68-4c53	-8cca-123b	b3616c77)					बेंब ☆	<u>e</u>	
	[Example][AD] Account created and deleted within a short period of time	00	[Example][AD][Technical] 4768. TGT Requested							
	[Example][AD] Granted TGS without TGT (Golden Ticket)	00	Kind *							
	[Example][AD] Membership of sensitive group was modified	00	operational							× ~
Kaspersky	[Example][AD] Successful authentication with the same account on multiple hosts	00	Selectors							
Unified Monitoring and	[Example][AD][Technical] 4768. TGT Requested	ЪФ	Event #1							
Analysis Platform			Filter *							
			Setup inline							
Alerts			Remove inline							
Par Events			Actions *							
E Assets			▼ onEveryEvent							
III Services			Active lists							
			Active list '[Example][AD] List of requested TGT.	EventID 4768'						
Resources			Name							
Settings			[Example][AD] List of requested TGT. EventID 4768							ХQ
—			Operation							
I Metrics			set							× ×
			Key fields							
			DestinationUserName 🕷 DestinationNtDomain 🕷							
			Mapping							
			Account	DestinationUserName	×	~ /	Constant			
			Domain	DestinationNtDomain	×	~ /	Constant			
			DateTime	DeviceReceiptTime	×	~ /	Constant			
			Active list field			~ /	Constant			
			Remove active list #1							
			Add action with active list							
Administrator			Save							

8. Нажмите на кнопку Save.

Событие корреляции будет создано и отобразится на закладке Correlation rules.

Создание правила корреляции для проверки, предшествует ли событие TGT запросу TGS

- Чтобы создать правило корреляции для чтения информации о TGT из активного списка при получении событий запроса TGS, выполните следующие действия:
 - 1. Откройте веб-консоль КUMA и выберите закладку Correlation rules в разделе Resources.
 - 2. Нажмите на кнопку Add.

Откроется окно для настройки параметров ресурса Правило корреляции.

- 3. В поле Name введите название фильтра, которое позволит идентифицировать созданный ресурс: [Пример] [AD] Предоставленный TGS без TGT (Golden Ticket).
- 4. В раскрывающемся списке Kind выберите simple.
- 5. В раскрывающемся списке Identical fields выберите **DestinationUserName**, **SourceUserName** и **SourceAddress**.
- 6. В раскрывающемся списке **Priority** выберите приоритет созданного правила корреляции. Выберите **Medium**.
- 7. В разделе **Selectors** перейдите по ссылке **Setup inline**, чтобы добавить фильтр, который будет отбирать события для передачи в это правило корреляции.

Откроется окно **Filter**, в котором можно настроить условия фильтрации. Добавьте условия фильтра с помощью кнопки **Add condition**, как описано ниже:

• Первое условие:

- В раскрывающемся списке Operation выберите =.
- В группе параметров Left operand задайте параметры, как описано ниже:
 - В раскрывающемся списке Kind выберите event.
 - В раскрывающемся списке Field выберите DeviceEventClassID.
- В группе параметров **Right operand** задайте параметры, как описано ниже:
 - В раскрывающемся списке Kind выберите constant.
 - В поле **Value** введите 4769.
- Второе условие:
 - В раскрывающемся списке **Operation** выберите **endsWith**.
 - Установите флажок **Not**, чтобы создать фильтр, НЕ содержащий записей, соответствующих условию.
 - В группе параметров Left operand задайте параметры, как описано ниже:
 - В раскрывающемся списке Kind выберите event.
 - В раскрывающемся списке Field выберите DestinationUserName.
 - В группе параметров **Right operand** задайте параметры, как описано ниже:
 - В раскрывающемся списке Kind выберите constant.
 - В поле Value введите S.
- Третье условие:
 - В раскрывающемся списке Operation выберите startsWith.
 - Установите флажок **Not**, чтобы создать фильтр, НЕ содержащий записей, соответствующих условию.
 - В группе параметров Left operand задайте параметры, как описано ниже:
 - В раскрывающемся списке Kind выберите event.
 - В раскрывающемся списке Field выберите DestinationUserName.
 - В группе параметров **Right operand** задайте параметры, как описано ниже:
 - В раскрывающемся списке Kind выберите constant.
 - B поле Value введите S.
- Четвертое условие:
 - В раскрывающемся списке Operation выберите inActiveList.
 - Установите флажок **Not**, чтобы создать фильтр, НЕ содержащий записей, соответствующих условию.
 - В раскрывающемся списке Name выберите имя активного списка, из которого должна считываться информация о TGT: [Пример] [AD] Список запрашиваемых TGT. EventID 4768.
 - В раскрывающемся списке **Key fields** выберите поля, которые будут использоваться в качестве ключа записи активного списка. Они должны совпадать с ключевыми полями,

используемыми при создании записи активного списка. Выберите DestinationUserName и DestinationNtDomain.

Условия фильтра будут созданы.

По этим условиям фильтра выполняется поиск всех событий с eventID 4769, у которых поля DestinationUserName и DestinationNtDomain HE находятся в активном списке, в котором хранится информация обо всех действительных TGT.

\leftrightarrow \rightarrow C \square	kuma.example.com:7220/resources/correlation-rules/(form:65077d3b-dfca-4a26-b3fa-a03357064be3)	G 👂
≡	Resources	
-	Connectors Normalizers Filters Enrichment rules Aggregation rules Destinations Dictionary Correlation rules	Active lists
<u> </u>	Response rules Connections Proxies	
Unified Mor	pitoring and there	
Analysis	Filter	
		-
🗘 Alerts	▼ AND Add condition / Add group / Toggle OR / Toggle NOT	× ~
P ≖ Events	event::DeviceEventClassID = 4769	
	event::DestinationUserName not endsWith \$	
Assets	event::DestinationUserName not startsWith \$	
	not inActiveList [Example][AD] List of requested TGT. EventID 4768[DestinationUserName,DestinationNtDomain]	
		~
Resources	Ok Cancel	
A Cottings		

8. Нажмите на кнопку **Оk**, чтобы сохранить фильтр в правиле корреляции.

Когда фильтр будет настроен, необходимо выбрать действия, которые будут выполняться при срабатывании правила.

9. В разделе onEveryEvent в группе параметров Actions установите флажок Output.

Это означает, что при каждом срабатывании правила корреляции будет создаваться событие корреляции и отправляться дальше микросервису Коррелятор.

10. Нажмите на кнопку Сохранить.

Правило корреляции будет создано и отобразится на закладке Correlation rules.



Связь правил корреляции с Коррелятором

При создании правила корреляции и активного списка, их необходимо связать с микросервисом Коррелятор, чтобы затем использовать при обработке событий.

- Чтобы связать правило корреляции и активный список с существующим микросервисом Коррелятор, выполните следующие действия:
 - 1. Откройте веб-консоль КUMA и выберите закладку Correlator в разделе Services.

← → C	kuma.example.com:7220/services/correlators/(form:f4afc42e-670b-4376-9028-e6078d5fcfcb)									
=	Services		_							
(-joje)	Overview Collectors	Correlators	Agents Storage							
Kaspersky	+ Add		🔀 Edit							
Unified Monitoring and Analysis Platform	[Example] Correlator	ъФ	General							
⚠ Alerts			Name [Example] Correlator Debug							
P ≖ Events			no							
E Assets			Resources							
Services			Connector							
If Resources			[Example] Correlator							
😳 Settings			Correlation rules							
耍 Metrics			[Example][AD] Successful authentication with the same account on multiple hosts [Example][AD] Account created and deleted within a short period of time [Example][AD] Membership of sensitive group was modified [Example][AD] Granted TGS without TGT (Golden Ticket)							

2. Выберите требуемый Коррелятор и нажмите на кнопку Edit.

Откроется окно настройки микросервиса Коррелятор. Закладки настройки Коррелятора отображаются в верхней части окна: вы можете выбрать нужную закладку, щелкнув по ней, или переключаться между закладками с помощью кнопок **Next** и **Previous**.

- 3. Откройте закладку Correlation Rules и добавьте правила корреляции:
 - a. Нажмите на кнопку Link и в раскрывающемся списке Choose resources выберите правило корреляции, которое требуется добавить в Коррелятор.
 - b. Нажмите на кнопку **Apply**.

Правило корреляции будет добавлено в Коррелятор и отобразится на закладке **Correlation Rules**.

Повторите этот шаг для каждого правила корреляции, которое требуется добавить в Коррелятор.



4. Если вы хотите добавить активные списки в Коррелятор, откройте закладку Active Lists:

Если правила корреляции, которые вы добавили в Коррелятор, используют активные списки, убедитесь, что они также добавлены в Коррелятор.

- a. Нажмите на кнопку Link и в раскрывающемся списке Choose resources выберите активный список, который требуется добавить в Коррелятор.
- b. Нажмите на кнопку Apply.

Активный список будет добавлен в Коррелятор и отобразится на закладке Active Lists.

Повторите этот шаг для каждого активного списка, который требуется добавить в Коррелятор.

\leftrightarrow \rightarrow C $$ kuma.example.com:722	20/services/correlators/f4afc42e	-670b-4376-9028	-e6078d5fcfcb/wizard	l/active-lists			🖻 ☆ 🄇	B 🔮 🛛 a 🗄
≡	Services							
	Overview Collectors	Correlators	Agents Stora	ge				
Kaspersky	Connector * Corre	elation Rules	Dictionaries	Active Lists	Enrichment	Destinations	Responses	Summary *
Unified Monitoring and Analysis Platform	C Link							
	[Example][AD] List of sensitive groups Go to or	rigin 凸面						
▲ Alerts	[Example][AD] List of requested TGT. EventID Go to of 4768	rigin						
₽ ¤ Events	[Example][AD] End-	റർ						
E Assets	accounts Go to or	rigin						
Services								
In Resources								
🧔 Settings								
굘 Metrics								
Administrator Admi	Previous Next	Save						

- 5. Откройте закладку Summary.
- 6. Нажмите на кнопку Сохранить.

Если после нажатия на кнопку **Save** появится сообщение о том, что требуется указать название, убедитесь, что поле **Name** не пусто на обеих закладках: **Connector** и **Summary**.

В конфигурацию Коррелятора будут добавлены новые ресурсы.

Необходимо перезагрузить микросервис Коррелятор, чтобы он начал использовать новую конфигурацию.

- Чтобы перезагрузить микросервис Коррелятор, выполните следующие действия:
 - 1. Откройте веб-консоль КUMA и выберите вкладку **Overview** в разделе **Services**.
 - 2. Щелкните мышью по значку **П**рядом с микросервисом Коррелятор, который требуется перезагрузить, и выберите **Reload**.

Микросервис Коррелятор перезагрузится и будет обрабатывать события с использованием обновленной конфигурации.

🎁 Чат Microsoft Teams 🛛 🗙 🋞) Services – KUMA	× +							- 0 ×
← → C	220/services/overview							See 2	G 🖉 🗐 :
	Services Overview Collector	Correlators	Agents Sto	rage					
	+ Create								C Refresh
Kaspersky Unified Monitoring and	Kind Name	Version	FQDN	Address	Port RPC	Metrics Status	Uptime	Updated	Created
Analysis Platform	collector [Example]	EF 0.3.26	kuma.example.com	10.70.74.242	7324	7224 green	31h9m7s	28 мая 2020 г., 23:57:48	27 мая 2020 г., 16:48:16
	collector [Example]	yslog 0.3.26	kuma.example.com	10.70.74.242	7325	7225 green	31h8m6s	28 мая 2020 г., 23:57:48	27 мая 2020 г., 16:49:41
♪ Alerts	correlator [Example]	Correlator 0.3.26	kuma.example.com	10.70.74.242	7323	7223 green	31h9m7s	28 мая 2020 г., 23:57:48	27 мая 2020 г., 16:42:27
P ⊈ Events		luster				red		28 Mag 2020 r., 23:57:48	27 Mag 2020 F., 16:38:46
	G Beload								
E Assets									
Services	Delete								
If Resources									
🔯 Settings									
In Metrics									
Administrator >									

Проверка правильности работы правила корреляции

Например, можно проверить, правильно ли выполняется анализ событий правилами корреляции, выполнив поиск связанных правил корреляции в Хранилище КUMA с помощью раздела **Events** веб-консоли KUMA. Для поиска событий корреляции определенного Коррелятора требуется его параметр **ServiceID**.

Чтобы выполнить поиск событий корреляции из Коррелятора, выполните следующие действия:

- 1. Откройте веб-консоль КUMA и выберите раздел Events.
- 2. Щелкните мышью в поле **Search**, перейдите на закладку **Builder** и настройте фильтр поиска событий:
 - В раскрывающемся списке слева выберите значение ServiceID.
 - В раскрывающемся списке посередине выберите оператор =.
 - В раскрывающемся списке справа введите значение ServiceID для Коррелятора, правила корреляции которого требуется найти.

← → C	20/events				🖻 🕁 🤇	6 🔮
≡	Events	Auto refresh 📿 15 second	Is v 🕒 Last 5 minute	s 🗸 🔀 Cluster: [Exampl	le] Cluster 👻 🗛	ctions ~
	Builder Source mod	le				
Kaspersky Unified Monitoring and	AND Add condition	Add group				
Analysis Platform	ServiceID	× =	v b8db33eb-550f-4de2-8	3988-c25af3d2bc8b	×	
♪ Alerts	Search Can	cel Save search				New search
Par Events						

- 3. Нажмите на кнопку Search.
- На закладке событий будут отображаться отфильтрованные события.

Если в Коррелятор поступают события, удовлетворяющие условиям фильтра правил корреляции, на закладке событий будут отображаться события с параметрами DeviceVendor=Kaspersky и DeviceProduct=KUMA. Название сработавшего правила корреляции будет отображаться как название этих событий корреляции.

Если события корреляции не найдены

Можно создать более простую версию правила корреляции, чтобы найти возможные ошибки. Используйте правило корреляции типа simple и одно действие **Output**.

← → C (i kuma.example.com.2220/resources/correlation-tules/(form.)									
≡	Resources								
(-joj	Connectors Normalizers Filters Enrichment rules Aggregation rules Destinations Dictionary Correlation rules Active lists Response rules Connections Proxies								
Kaspersky	+ Add Name*								
Unified Monitoring and	[Example]/ADJ Account created and deleted within a short 口合合								
Analysis Flatform	[Exemple][AD] Granted TGS without TGT (Golden Ticket) 👔 📷 Kind *								
O Alorro	Example(JAD) Membership of sensitive group was modified 🖞 📅 simple		;	× ~					
Alers	IEsamoli/ADI Successful authemicision with the same D 🛱 Identical fields *								
P¤ Events	Example[A0]Technical 4758.TGT Requested D 🗄 ServiceID 🗵								
t Assets	Priority*								
PII Services	Low			~					
IIII Services	Salastor								
Resources	Sectors								
Settings	Event va								
I Maria	Setup inline								
Hetrics	Nemove inline								
	Actions *								
	✓ onEveryEvent								
	Output								

Рекомендуется создать фильтр для поиска событий, которые КUMA получает регулярно. Если КUMA находится в начале процесса развертывания и количество полученных событий очень мало (несколько событий в секунду), вы можете использовать параметры фильтра, приведенные ниже, чтобы правило корреляции обрабатывало каждое событие, передаваемое в Коррелятор.

← → C 🔒 k	xuma.example.com:7220/resources/correlation-rules/(form:)	№ ☆
≡		
	Operation	
·È	=	× ~
<u>,</u>	✓ Not	
Unified Mon	Ignore case	
Analysis I	Left operand	
	Kind	
🗘 Alerts	event	× ~
P¤ Events	Field	
-	ServiceID	× ~
E Assets	Right operand	
Services	Kind	
	constant	× •
H Resources	Value	
Settings	1	
🕮 Metrics	Link filter	,
	Filter	
Administrator		Q

При обновлении, добавлении или удалении правила корреляции, микросервис Коррелятор должен быть перезагружен.

Когда вы закончите тестирование правил корреляции, необходимо удалить все тестовые и временные правила корреляции из КUMA и перезагрузить Коррелятор.

Добавление источника события с использованием стандартного нормализатора

В этом примере показано, как настроить KUMA для получения событий от Kaspersky Anti Targeted Attack (далее KATA). Сервер KATA (источник событий) настроен на отправку событий в формате CEF через порт TCP:5146. В KUMA события должны направляться в Хранилище KUMA и Коррелятор KUMA. В этом разделе описаны действия для выполнения этой задачи.

В примере предполагается, что микросервисы Хранилище и Коррелятор уже установлены и для них настроены точки назначения.

В этом разделе

Подготовка ресурсов к инициализации Коллектора КUMA для КАТА	
Инициализация Коллектора для КАТА	41
Создание Коллектора для КАТА	43
Установка Коллектора для КАТА на сервере	44
Проверка состояния Коллектора для КАТА	45

Подготовка ресурсов к инициализации Коллектора КUMA для КАТА

В этом разделе описано создание ресурсов, необходимых Коллектору КUMA для КАТА.

Для микросервиса Коллектор требуются только ресурсы Соединение и Нормализатор.

В этом разделе

Создание Соединения для КАТА	38
Создание Коннектора для КАТА	39
Создание Нормализатора для КАТА	40

Создание Соединения для КАТА

В веб-консоли КUMA нам нужно создать ресурс Соединение, который позволит ресурсу Коннектор использовать порт TCP:5146:

- Для создания ресурса Соединение сделайте следующее:
 - 1. Откройте веб-консоль КUMA и выберите вкладку Connections в разделе Resources.
 - 2. Нажмите на кнопку Add и задайте параметры, как описано ниже.
 - В поле Name введите имя ресурса Соединение для его идентификации. Введите КАТА (5146/tcp).
 - В раскрывающемся списке Kind выберите tcp, чтобы получать события по протоколу TCP.

- В поле URLs введите адрес, по которому Коннектор должен получать события. Значение может иметь формат <FQDN>:<порт>, <IP-адрес>:<порт> или :<порт>. Введите :5146.
- 3. Нажмите на кнопку Save.

На вкладке Connections появится новое соединение КАТА (5146/tcp).

← → C ▲ Not secure kuma.ex	ample.com:7220/resources/connections/(form:)			☆ 🛛 :
≡	Resources			
-:@:-)	Connectors Normalizers Filters	Enrichment rule	as Aggregation rules Destinations Dictionary Correlation rules Active lists Response rules Connections Proxies	
Kaspersky	+ Add		Name *	
Unified Monitoring and	correlator (9999/tcp)	00	KATA (5146/tcp)	
Analysis Platform	storage (9200/tcp)	00	Kind *	
Alerts				
Ptr Events				
E Assets			2 URL of destination	
Services			TLS mode	
Resources			TLS mode	~
🔅 Settings			Save	
e Metrics				

Создание Коннектора для КАТА

В веб-консоли КUMA нам нужно создать ресурс Коннектор.

- Для создания ресурса Коннектор сделайте следующее:
 - 1. Откройте веб-консоль КUMA и выберите вкладку Connectors в разделе Resources.
 - 2. Нажмите на кнопку Add и задайте параметры, как описано ниже.
 - В поле Name введите имя ресурса Коннектор для его идентификации. Введите КАТА.
 - В раскрывающемся списке **Kind** выберите **tcp**, поскольку нам нужно получать события по протоколу TCP.
 - В раскрывающемся списке **Connection** выберите ресурс Соединение, созданный на предыдущем этапе. Выберите KATA (5146/tcp).
 - 3. Нажмите на кнопку Save.

На вкладке Connectors появится новый коннектор КАТА.

← → C ▲ Not secure kuma.ex	← → C ▲ Not secure kuma.example.com/220/resources/connectors/(form)												☆ \varTheta
≡	Resourc	es											
÷¢÷	Connectors	Normalizers	Filters	Enrichment rules	Aggregation rules	Destinations	Dictionary	Correlation rules	Active lists	Response rules	Connections	Proxies	
Kaspersky	+ Add				Name *								
Unified Monitoring and					KATA								
Analysis Platform					Kind *								
▲ Alarts					tcp								× ~
					Connection *								
Pt Events					KATA (5146/tcp)								ХQ
E Assets					Delimiter								
Services					Delimiter of connec	tor							
····					Buffer size								
Resources					Buffer size of conne	ctor							
Settings					Character encoding								
Metrics					default: UTF-8								~
					Compression								
													~
					Debug								
					Save								

Создание Нормализатора для КАТА

При отправке событий КАТА используется формат CEF. Чтобы система KUMA могла найти корреляции в этих событиях, события КАТА необходимо преобразовать в модель данных событий KUMA (или нормализовать) с помощью стандартного нормализатора CEF.

- Для создания ресурса Нормализатор сделайте следующее:
 - 1. Откройте веб-консоль КUMA и выберите вкладку Normalizer в разделе Resources.
 - 2. Нажмите на кнопку Add и задайте параметры, как описано ниже.
 - В поле Name введите имя ресурса Нормализатор для его идентификации. Введите КАТА (CEF).
 - В списке Kind выберите тип нормализатора. Выберите CEF.
 - Настройте сопоставление полей полученного события с полями события КUMA. В этом примере мы получаем события в формате CEF со стандартными полями. Щелкните по ссылке **Apply** default mapping.

Правила сопоставления автоматически добавятся в таблицу сопоставлений.

Остальные параметры ресурса Нормализатор необязательны.

3. Нажмите на кнопку Save.

На вкладке Normalizer появится новый нормализатор КАТА (CEF).

← → C ▲ Not secure kuma.ex	🗧 🔶 😋 🔺 Not secure kumaexample.com/7220/resources/normalizers/(form)											\$	θ	
≡	Resource	es												
÷	Connectors	Normalizers	Filters	Enrichment rules	Aggregation rules	Destinations	Dictionary	Correlation rules	Active lists	Response rules	Connections	Proxies		
Kaspersky	+ Add				Name *									
Analysis Platform					KATA (CEF)									
					Kind *									
🗘 Alerts					cef								× •	~
Pa Events					Mapping									
t= Assets					Apply default mapping	l i								
E Services					Clear mapping			Destination			Labor			
III centers					Source			Destination			Label			
II Resources					act		₹.	DeviceAction		× ~			1	Ô
A Sattings					арр		£	ApplicationProtoco	Ы	× ×			1	Û
age occurrigo					c6a1		×	DeviceCustomIPv6	iAddress1	× ×			1	Û
P Metrics					c6a1Label		R	DeviceCustomIPv6	iAddress1Label	× ×			1	Û

Инициализация Коллектора для КАТА

На этом этапе все необходимые ресурсы уже готовы, и их можно использовать для создания (или инициализации) Коллектора.

- Для инициализации Коллектора сделайте следующее:
 - 1. Откройте веб-консоль КUMA и выберите вкладку Collector в разделе Services.
 - 2. Нажмите на кнопку Add.

Откроется окно для настройки микросервиса Коллектор. В верхней части окна отображаются вкладки для настройки Коллектора. Чтобы выбрать нужную вкладку, щелкните по ней или используйте для перехода между вкладками кнопки **Next** и **Previous**.

Обязательными являются только вкладки Connector, Normalizer и Summary.

- 3. Откройте вкладку Connector.
- 4. Нажмите на кнопку Link и в раскрывающемся списке Choose resource выберите ресурс Коннектор, созданный на предыдущем этапе. Выберите KATA.

\leftarrow \rightarrow C (\blacktriangle Not secure kuma.e	example.com:7220/services/co	llectors/new/wizard/connector						☆ \varTheta :				
≡	Services	Services										
	Overview Collector	s Correlators Agents	Storage									
	Connector*	Normalizer *	Filters	Dictionaries	Enrichment	Aggregation	Destinations	Summary*				
Kaspersky Unified Monitoring and	6 Link											
Analysis Platform	Nar Choose resource											
▲ Alerts		Q										
Ptr Events	Kinc Apply C	ancel						~				
E Assets	Connection *											
Services								م				
	Character encoding											
If Resources	default: UTF-8							~				
Settings	Compression											
=								~				
별 Metrics	Debug											
	Next Save											

5. Нажмите на кнопку **Apply**.

На вкладке появится конфигурация выбранного ресурса.

← → C ▲ Not secure kuma.ex	xample.com:7220/services/collectors/new/wizard/connector	☆ \varTheta :
≡	Services	
- ```	Overview Collectors Correlators Agents Storage	
	Connector* Normalizer* Filters Dictionaries Enrichment Aggregation Destinations St	ummary *
Unified Monitoring and	🔗 Go to origin 🛛 🤃 Unlink	
Analysis Platform	Name*	
△ Alerts	KATA	
Dr. Guerre	Kind *	
Fu Events		
E Assets	Connection *	
Services	Delimiter	
Resources	Delimiter of connector	
Settings	Buffer size	
🗐 Metrics	Buffer size of connector	
	Character encoding	
	Corolle U Mo	
	Compression	
	Debug	
	Next Save	

- 6. Откройте вкладку Normalizer.
- 7. Нажмите на кнопку Link и в раскрывающемся списке Choose resource выберите ресурс Нормализатор, созданный на предыдущем этапе. Выберите KATA CEF.
- 8. Нажмите на кнопку Apply.

На вкладке появится конфигурация выбранного ресурса.

← → C ▲ Not secure kuma.ex	kerample.com?220/services/collectors/new/wizard/normalizer 🏠 🛠										
≡	Services	ervices									
	Overview Collectors	Correlators Agents	Storage								
	Connector*	Normalizer*	Filters	Dictionaries	Enrichment	Aggregation	Destinations	Summary *			
Kaspersky Unified Monitoring and	🔗 Go to origin 🛛 👸 U	Inlink									
Analysis Platform											
	Name										
	NATA (CEP)										
Par Events	Kind *										
t Assets											
51 1	Mapping										
Services	Apply default mapping										
Resources	Clear mapping										
Settings	source			Destination		Label	Label				
ER Marrier	act		1	DeviceAction							
Hernes	app		F	ApplicationProtocol				11			

- 9. Откройте вкладку **Destinations**.
- 10. Нажмите на кнопку Link и в раскрывающемся списке Choose resource выберите ресурс Точка назначения, созданный ранее.
- 11. Нажмите на кнопку **Apply**.

На вкладке появится имя выбранного ресурса.

12. Повторите действия 10–11 для каждой точки назначения, которую нужно привязать к Коллектору.

← → C ▲ Not secure kuma.ex	ample.com:7220/services/collect	ors/new/wizard/destinations						☆ \varTheta :
≡	Services							
	Overview Collectors	Correlators Agents Ste	orage					
	Connector*	Normalizer *	Filters	Dictionaries	Enrichment	Aggregation	Destinations	Summary *
Kaspersky Unified Monitoring and Analysis Platform	+ Add 🔗 Link							
Ĩ	[PoC] correlator	Go to origin 🗗 🗇						
▲ Alerts	[PoC] storage	Go to origin 🗗 🗇						
Par Events								
t Assets								
Services								
Resources								
🚯 Settings								
Hetrics								

- 13. Откройте вкладку **Summary**.
- 14. В поле Name введите имя Коллектора. Введите КАТА.

← → C ▲ Not secure kuma.es	xample.com:7220/services/collecte	ors/new/wizard/summary						☆ \varTheta :
≡	Services							
	Overview Collectors	Correlators Agents	Storage					
	Connector*	Normalizer *	Filters	Dictionaries	Enrichment	Aggregation	Destinations	Summary*
Kaspersky Unified Monitoring and	General							
Analysis Platform	Name							
△ Alerts	КАТА							
TT Evente	Workers							
PA LVents	default: vCPU count							
E Assets	Debug							
Services	Resources							
Resources	Connector							
🐼 Settings	КАТА							
Metrics	Normalizer							
<u></u>	KATA (CEF)							
	Filters							
	Dictionaries							
	Enrichment rules							
	Aggregation rules							
	Destinations							
	[PoC] correlator							
	[PoC] storage							
Administrator >	Previous Save							

15. Нажмите на кнопку Save.

Если после нажатия на кнопку **Save** появляется сообщение о том, что требуется имя, убедитесь в том, что поле **Name** не пустое на всех обязательных вкладках: **Connector**, **Normalizer** и **Summary**.

Коллектор инициализируется и появится на вкладке Collector.

Создание Коллектора для КАТА

После инициализации коллектора можно создать микросервис Коллектор.

• Для создания микросервиса Коллектор сделайте следующее:

- 1. Откройте веб-консоль КUMA и выберите вкладку **Overview** в разделе **Services**.
- 2. Нажмите на кнопку **Create** и в раскрывающемся списке выберите ранее созданный Коллектор. Выберите collector/KATA.
- 3. Нажмите на кнопку Create.

В списке микросервисов появится новый Коллектор с именем КАТА.

Установка Коллектора для КАТА на сервере

Чтобы Коллектор мог получать и обрабатывать события, необходимо установить соответствующий микросервис на сервере Коллектора КUMA. Установку Коллектора на сервере выполняют администраторы сети.

В ходе установки этого микросервиса требуются следующие параметры: **RPC** и **Metrics**. Эти параметры находятся на вкладке **Overview** в разделе **Services** веб-консоли KUMA.

- Для установки Коллектора на сервере КИМА сделайте следующее:
 - 1. Откройте SSH-консоль сервера Коллектора КUMA с правами администратора сети.
 - 2. Выполните следующие команды:

rpm -Uhv kuma-0.3.26-<номер сборки>.el8.x86 64.rpm

/opt/kuma/kuma collector --core <адрес сервера, с которого микросервис Коллектора получает параметры конфигурации> --id <идентификатор микросервиса, скопированный из веб-консоли KUMA> --metrics <порт, используемый для метрик установленных микросервисов> --rpc <порт, используемый для RPC установленных микросервисов> --install

При развертывании нескольких микросервисов КUMA на одном хосте в процессе установки необходимо указать уникальные порты для каждого компонента с помощью параметров -- metrics <порт> --rpc <порт>. По умолчанию используются значения --metrics 7221 -rpc 7331.

3. Укажите, принимаете ли вы условия Лицензионного соглашения.

Если вы не принимаете условия Лицензионного соглашения, установка программы не выполняется.

Микросервис Коллектора устанавливается. Он готов получать и передавать на обработку сообщения из источника события.

Проверка состояния Коллектора для КАТА

После установки Коллектора на соответствующем сервере КUMA убедитесь в том, что этот микросервис работает.

- Проверить готовность Коллектора к получению событий можно следующим образом:
 - 1. Откройте веб-консоль KUMA и выберите вкладку **Overview** в разделе **Services**.
 - 2. Убедитесь, что для Коллектора, установленного на сервере kuma.example.com, отображается значение green в столбце Status.

← → C ▲ Not secure kuma.ex	cample.com:7220/servi	ces/overview										☆ 😶
≡	Services											
	Overview Col	lectors Correlators	Agents	Storage								
	+ Create											C Refresh
Kaspersky Unified Monitoring and	Kind	Name	Version	FQDN	Address	Port	RPC	Metrics	Status	Uptime	Updated	Created
Analysis Platform	≡ collector	KATA	0.3.22	kuma.example.com	10.70.74.242		7325	7225	green	15s	May 21, 2020, 3:38:23 PM	May 21, 2020, 3:32:16 PM
	correlator	[PoC] Correlator	0.3.22	kuma.example.com	10.70.74.242		7323	7223	green	3h9m47s	May 21, 2020, 3:38:23 PM	May 21, 2020, 12:28:27 PM
	≡ storage	kuma	0.3.22	kuma.example.com	10.70.74.242	9200	7322	7222	green	3h9m43s	May 21, 2020, 3:38:23 PM	May 21, 2020, 12:28:27 PM
Pa Events												
ta Assets												
Services												
Resources												
Settings												
🚍 Metrics												

Если все микросервисы установлены на одном сервере, как в данном примере, порты для параметров RPC и Metrics должны быть разными.

Добавление источника события с использованием настраиваемого нормализатора regexp

В этом примере показано, как настроить KUMA для получения файла журнала access.log с сервера Cisco ™ WSA и его обработки. На сервере Коллектора файл журнала access.log монтируется в папку /mnt/cisco_wsa. События в КUMA отправляются в Хранилище KUMA и Коррелятор KUMA. В этом разделе описаны действия для выполнения этой задачи.

В примере предполагается, что микросервисы Хранилище и Коррелятор уже установлены и для них настроены точки назначения.

В этом разделе

Подготовка ресурсов к инициализации Коллектора KUMA для Cisco WSA	46
Инициализация Коллектора для Cisco WSA	50
Создание Коллектора для Cisco WSA	51
Установка Коллектора для Cisco WSA на сервере	52
Проверка состояния Коллектора Cisco WSA	52

Подготовка ресурсов к инициализации Коллектора KUMA для Cisco WSA

В этом разделе описано создание ресурсов, которые будут использоваться при инициализации Коллектора KUMA для Cisco WSA.

Для микросервиса Коллектор требуются только ресурсы Соединение и Нормализатор.

В этом разделе

Создание Соединения для Cisco WSA	.46
Создание Коннектора для Cisco WSA	.47
Создание Нормализатора для Cisco WSA	.48

Создание Соединения для Cisco WSA

В веб-консоли KUMA нам нужно создать ресурс Соединение для чтения файла журнала в каталоге /mnt/cisco_wsa/access.log.

- Для создания ресурса Соединение сделайте следующее:
 - 1. Откройте веб-консоль KUMA и выберите вкладку Connections в разделе Resources.
 - 2. Нажмите на кнопку Add и задайте параметры, как описано ниже.
 - В поле Name введите имя ресурса Соединение для его идентификации. Введите Cisco WSA (file).
 - В раскрывающемся списке Kind выберите file, поскольку нам нужно получать события из файла.

- В поле URLs введите путь к файлу. Введите /mnt/cisco wsa/access.log.
- 3. Нажмите на кнопку Save.

На вкладке Connections появится новое соединение Cisco WSA (file).

← → C ▲ Not secure kuma.ex	ample.com:7220/resources/connections/(form:7912	15fc-563f-470b-	95f3-2589b4f5b988)	☆ \varTheta :
≡	Resources			
÷¢÷	Connectors Normalizers Filters	Enrichment rule	as Aggregation rules Destinations Dictionary Correlation rules Active lists Response rules Connections Proxies	
Kaspersky	+ Add		Name *	
Unified Monitoring and	Cisco WSA (file)	00	Cisco WSA (file)	
Analysis Platform	KATA (5146/tcp)	00	Kind*	
	correlator (9999/tcp)	D @	file	× •
▲ Alerts	storage (9200/tcp)	6		
Par Events			URLs*	
•			/mnt/cisco_wsa/access.log	
E Assets			Save	
III Services				
T Resources				
🔯 Settings				
Atrics				

Создание Коннектора для Cisco WSA

В веб-консоли КUMA нам нужно создать ресурс Коннектор.

- Для создания ресурса Коннектор сделайте следующее:
 - 1. Откройте веб-консоль КUMA и выберите вкладку Connectors в разделе Resources.
 - 2. Нажмите на кнопку Add и задайте параметры, как описано ниже.
 - В поле Name введите имя ресурса Коннектор для его идентификации. Введите Cisco WSA.
 - В раскрывающемся списке Kind выберите file.
 - В раскрывающемся списке **Connection** выберите ресурс Соединение, созданный на предыдущем этапе. Выберите Cisco WSA (file).
 - 3. Нажмите на кнопку Save.

На закладке Connectors появится новый Коннектор Cisco WSA.

← → C ▲ Not secure kuma.exa	C A Not secure kuma.example.com:7220/resources/connectors/(form:7b111827-59d8-43a6-b04d-8545b183c0e7)											* 6	•	
≡	Resource	es												
(·iki)	Connectors	Normalizers	Filters	Enrichment rules	Aggregation rules	Destinations	Dictionary	Correlation rules	Active lists	Response rules	Connections	Proxies		
Kaspersky	+ Add				Name *									
Unified Monitoring and	Cisco WSA			ටෙම	Cisco WSA									
Analysis Platform	KATA			마마	Kind *									
Alerts					file								× ~]
_					Connection *									
Par Events					Cisco WSA (file)								× C	2
E Assets					Character encoding									_
Services					default: UTF-8								~	,
I Resources					Debug									
Settings					Save									
🖶 Metrics														

Создание Нормализатора для Cisco WSA

Для того чтобы решение KUMA смогло найти корреляции в событиях Cisco WSA, их необходимо нормализовать, используя синтаксический анализатор на основе регулярных выражений.

В КUMA используются регулярные выражения типа RE2.

Для создания ресурса Нормализатор сделайте следующее:

- 1. Откройте веб-консоль КUMA и выберите вкладку Normalizer в разделе Resources.
- 2. Нажмите на кнопку Add и задайте параметры, как описано ниже.
 - В поле Name введите имя ресурса Нормализатор для его идентификации. Введите Cisco WSA access log.
 - В списке Kind выберите тип нормализатора. Выберите regexp.
 - В полях **Expressions** введите одно или несколько регулярных выражений. Все переменные в выражении должны быть именами, чтобы их можно было использовать для установления соответствия.

Пример содержимого файла WSA – access.log:

```
1579866468.772 104 8.8.8.8 TCP_MISS/200 3642 CONNECT
tunnel://ipmcloud.example.com:443/ "DOMAIN\username"
DIRECT/ipmcloud.example.com application/octet-stream ALLOW_WBRS_12-
DefaultGroup-DefaultGroup-NONE-NONE-DefaultGroup-NONE
<"IW_csec",9.2,1,"-",-,-,1,"-",-,-,"-",1,-,"-","-",-,-
,"IW_csec",-,"-","Computer Security","-","Unknown","Unknown","-","-
",280.15,0,-,"-","-",1,"-",-,-,"-","-",-,1,"-",-> -
```

Для синтаксического анализа строк, аналогичных приведенной выше, можно использовать следующее регулярное выражение:

```
^(?P<timestamp>\S+) \s+(?P<xElapsedTime>\d+) \s+(?P<cIp>\d{1,3}\.\d{1,3}
}\.\d{1,3}\.\d{1,3}) \s+(?P<srcResultCode>[^\/].*?) \/(?P<scResultCodeD
enial>\d+) \s+(?P<scBytes>\d+) \s+(?P<xReqFirstLine>[A-
Z]+\s\S+) \s+(?P<csUsername>\S+) \s+(?P<sHierarchy>[^\/].*?) \/(?P<sHost
name>\S+) \s+(?P<csMimeType>\S+) \s+(?P<xAcltag>\S+) \s+(?P<xResultCode>
.*?\>) \s+(?P<xSuspectUserAgent>\S+)
```

Переменные названы в соответствии с форматом файла журнала W3C. Разобранные посредством анализа строки можно использовать для установления соответствия.

Альтернативное именование переменных

Допускается альтернативный подход к именованию переменных. Например, можно использовать имена CEF. Это позволит автоматически применять соответствие CEF с помощью команды **Use CEF mapping** и избежать добавления правил соответствия вручную.

Kind *	
rege	xp X Y
Expres	isions*
1.	$(PStarting (P\S+) handshake with (P\S+)) (P\S+): (P\d+\.\d+\.\d+\.\d+\.\d+)) (P\d+) for (P\S+) sessive (P\S+) (P$
2.	(?P <name>Starting SSL handshake with (?P<cs4>\S+)) (?P<deviceinboundinterface>\S+):(?P<src>\d+.\d+.\d+.\d+)\/(?P<sport>\d+) to (?P<dst>\d+.\d+.\d+.\d+.\d+)/(?P<dpt>\d+)</dpt></dst></sport></src></deviceinboundinterface></cs4></name>
3.	

Mapping

Use CEF mapping Clear mapping

Source		Destination	Label	
act	.€	DeviceAction X ~		Û
арр	€	ApplicationProtocol X 🗸		Û
c6a1	€	DeviceCustomIPv6Address1 X V	Label	0
c6a1Label	æ	DeviceCustomIPv6Address1Label X 🗸	Label) d
c6a2	æ	DeviceCustomIPv6Address2 × v	Label) 🖻
c6a2Label	×	DeviceCustomIPv6Address2Label × ~	Label) 🖻
сба3	×	DeviceCustomIPv6Address3 × ~	Label) d
сбаЗLabel	×	DeviceCustomIPv6Address3Label X 🗸	Label) d
сба4	€	DeviceCustomIPv6Address4 × ~	Label) đ
сба4Label	×	DeviceCustomIPv6Address4Label X V	Label) d

• В группе параметров **Mapping** добавьте правила установления соответствия, как показано на рисунке ниже:

← → C A Not secure kuma.example.com:7220/resources/normalizers/flom:3e28698-008f-4005-85f2-ca141fc66448) ☆														
≡	Resource	es Normalizers	Filters	Enrichment rules	Aggregation rules	Destinations	Dictionary	Correlation rules	Active lists	Response rules	Connections	Proxies		
·	connectors	Normalizers	There	chinement rates	Aggregation rates	Destinations	bictionary	conclusion rates	Active uses	Response rates	connections	rioxic3		
Kaspersky	+ Add				No									
Unified Monitoring and	Cisco WSA access.log		00											
Analysis Platform	KATA (CEF)			00	UISCO WIDH BCCESS.IOG									
					Kind *									
					regexp								×	
P⊈ Events					Expressions *									
•					1. ^(?P <timestam< td=""><td>p>\S+)\s+(?P<xela< td=""><td>psedTime>\d+)\s</td><td>s+(?P<clp>\d{1,3}\.1</clp></td><td>,3}\.\d{1,3}\.1</td><th>,3})\s+(?P<srcresultco< th=""><td>de>[^\/].*?)\/(?P<s< td=""><td>cResultCodeDenia</td><td>al>\d+)\s+(?P<scbytes></scbytes></td></s<></td></srcresultco<></th></xela<></td></timestam<>	p>\S+)\s+(?P <xela< td=""><td>psedTime>\d+)\s</td><td>s+(?P<clp>\d{1,3}\.1</clp></td><td>,3}\.\d{1,3}\.1</td><th>,3})\s+(?P<srcresultco< th=""><td>de>[^\/].*?)\/(?P<s< td=""><td>cResultCodeDenia</td><td>al>\d+)\s+(?P<scbytes></scbytes></td></s<></td></srcresultco<></th></xela<>	psedTime>\d+)\s	s+(?P <clp>\d{1,3}\.1</clp>	,3}\.\d{1,3}\.1	,3})\s+(?P <srcresultco< th=""><td>de>[^\/].*?)\/(?P<s< td=""><td>cResultCodeDenia</td><td>al>\d+)\s+(?P<scbytes></scbytes></td></s<></td></srcresultco<>	de>[^\/].*?)\/(?P <s< td=""><td>cResultCodeDenia</td><td>al>\d+)\s+(?P<scbytes></scbytes></td></s<>	cResultCodeDenia	al>\d+)\s+(?P <scbytes></scbytes>	
E Assets					2.									
Services														
					Mapping									
Resources					Use CEF mapping									
Settings					Clear mapping									
					Source			Destination			Label			
🚆 Metrics					timestamp		r	EndTime		× ~				
					xElapsedTime		F	DeviceCustomNu	mber1	× ×	ElapsedTime			
					clp		£	SourceAddress		× ~				
							, ,	Device Antice		· · ·				
					srcResultCode		~	DeviceAction		× *				
					scResultCodeDenial		8	DeviceEventClass	D	× ~				
					scBytes		F	BytesIn		× ~				
					xReqFirstLine		F	Message		× ~				
					csUsername		F	SourceUserName		× ~				
					sHierarchy			DeviceCustomStri	nol	× ~	Hierarchy			
					Si nerororiy		-				- nerorony			

- В группе параметров Enrichment можно добавить правила обогащения, например, для обновления значений полей DeviceVendor, DeviceProduct и DeviceHostName:
 - а. Перейдите по ссылке Add enrichment.

Откроется группа параметров Enrichment rule:

- b. В раскрывающемся списке Source kind выберите constant.
- с. В раскрывающемся списке Target field выберите DeviceVendor.
- d. В поле Constant введите CISCO.

Повторите эти шаги для каждого правила обогащения. См. рисунок ниже для справки.

← → C ▲ Not secure kuma.example.com:7220/resources/no	rmalizers/(form:3e288698-008f-4005-85f2-ca141fce6a48)	\$
=	Extra normalizers Add extra normalizer	
	Enrichment	
Kaspersky	Enrichment #1	
Unified Monitoring and	Source kind	
Analysis Platform	constant	×
	Target field	
Fix Events	DeviceVendor	×
•	Constant	
E Assets	CISCO	
T# Services	Remove enrichment #1	
	Enrichment #2	
II Resources	Source kind	
A Settings	constant	×
ter settings	Target field	
🚍 Metrics	DeviceProduct	×
	Constant	
	WSA	
	Remove enrichment #2	
	Enrichment #3	
	Source kind	
	constant	×
	Target field	
	DeviceHostName	×
	Constant	
	proxy example.com	
	Remove enrichment #3	

1. Нажмите на кнопку Save.

На закладке Normalizer появится новый Нормализатор Cisco WSA access log.

Инициализация Коллектора для Cisco WSA

На этом этапе все необходимые ресурсы уже готовы, и их можно использовать для создания (или инициализации) Коллектора.

- Для инициализации Коллектора сделайте следующее:
 - 1. Откройте веб-консоль KUMA и выберите вкладку Collector в разделе Services.
 - 2. Нажмите на кнопку Add.

Откроется окно для настройки микросервиса Коллектор. В верхней части окна отображаются вкладки для настройки Коллектора. Чтобы выбрать нужную вкладку, щелкните по ней или используйте для перехода между вкладками кнопки **Next** и **Previous**.

Обязательными являются только вкладки Connector, Normalizer и Summary.

3. Откройте вкладку Connector.

- 4. Нажмите на кнопку Link и в раскрывающемся списке Choose resource выберите ресурс Коннектор, созданный на предыдущем этапе. Выберите Cisco WSA (file).
- 5. Нажмите на кнопку **Apply**.

На вкладке появится конфигурация выбранного ресурса.

- 6. Откройте вкладку Normalizer.
- 7. Нажмите на кнопку Link и в раскрывающемся списке Choose resource выберите ресурс Нормализатор, созданный на предыдущем этапе. Выберите Cisco WSA log file.
- 8. Нажмите на кнопку Apply.

На вкладке появится конфигурация выбранного ресурса.

- 9. Откройте вкладку Destinations.
- 10. Нажмите на кнопку Link и в раскрывающемся списке Choose resource выберите ресурс Точка назначения, созданный ранее.
- 11. Нажмите на кнопку Apply.

На вкладке появится имя выбранного ресурса.

- 12. Повторите действия 10-11 для каждой точки назначения, которую нужно привязать к Коллектору.
- 13. Откройте вкладку **Summary**.
- 14. В поле Name введите имя Коллектора. Введите Cisco WSA.
- 15. Нажмите на кнопку Save.

Если после нажатия на кнопку **Save** появляется сообщение о том, что требуется имя, убедитесь в том, что поле **Name** не пустое на всех обязательных вкладках: **Connector**, **Normalizer** и **Summary**.

Коллектор инициализируется и появится на вкладке Collector.

Создание Коллектора для Cisco WSA

После инициализации коллектора можно создать микросервис Коллектор.

Для создания микросервиса Коллектор сделайте следующее:

- 1. Откройте веб-консоль КUMA и выберите вкладку Overview в разделе Services.
- 2. Нажмите на кнопку **Create** и в раскрывающемся списке выберите ранее созданный Коллектор. Выберите collector/Cisco WSA.
- 3. Нажмите на кнопку Create.

В списке микросервисов появится новый микросервис Коллектор - Cisco WSA.

Установка Коллектора для Cisco WSA на сервере

Чтобы Коллектор мог получать и обрабатывать события, необходимо установить соответствующий микросервис на сервере Коллектора КUMA. Установку Коллектора на сервере выполняют администраторы сети.

В ходе установки этого микросервиса требуются следующие параметры: **RPC** и **Metrics**. Эти параметры находятся на вкладке **Overview** в разделе **Services** веб-консоли KUMA.

- Чтобы установить Коллектор на сервере Коллекторов КUMA, выполните следующие действия:
 - 1. Откройте SSH-консоль сервера Коллектора КUMA с правами администратора сети.
 - 2. Выполните следующие команды:

rpm -Uhv kuma-0.3.26-<номер сборки>.el8.x86_64.rpm

/opt/kuma/kuma collector --core <адрес сервера, с которого микросервис Коллектора получает параметры конфигурации> --id <идентификатор микросервиса, скопированный из веб-консоли KUMA> --metrics <порт, используемый для метрик установленных микросервисов> --rpc <порт, используемый для RPC установленных микросервисов> --install

При развертывании нескольких микросервисов КUMA на одном хосте в процессе установки необходимо указать уникальные порты для каждого компонента с помощью параметров --metrics <порт> --rpc <порт>. По умолчанию используются значения --metrics 7221 -rpc 7331.

3. Укажите, принимаете ли вы условия Лицензионного соглашения.

Если вы не принимаете условия Лицензионного соглашения, установка программы не выполняется.

Микросервис Коллектора устанавливается. Он готов получать и передавать на обработку сообщения из источника события.

Проверка состояния Коллектора Cisco WSA

После установки Коллектора на соответствующем сервере КUMA убедитесь в том, что этот микросервис работает.

- Проверить готовность Коллектора к получению событий можно следующим образом:
 - 1. Откройте веб-консоль KUMA и выберите вкладку **Overview** в разделе **Services**.

2. Убедитесь, что для Коллектора, установленного на сервере kuma.example.com, отображается значение green в столбце Status.

← → C ▲ Not secure kuma.ex	ample.com:7220/serv	ices/overview										\$	Θ
≡	E Services												
- jaja-	Overview Co	llectors Correlators	Agents	Storage									
(·*·)	+ Create											C Re	fresh
Kaspersky	Kind	Name	Version	FQDN	Address	Port	RPC	Metrics	Status	Uptime	Updated	Created	
Unified Monitoring and	collector	KATA	0.3.22	kuma.example.com	10.70.74.242		7325	7225	green	15s	May 21, 2020, 3:38:23 PM	May 21, 2020, 3:32:16 PM	
Analysis Flatform	= correlator	[PoC] Correlator	0.3.22	kuma.example.com	10.70.74.242		7323	7223	green	3h9m47s	May 21, 2020, 3:38:23 PM	May 21, 2020, 12:28:27 PM	
A	storage	kuma	0.3.22	kuma.example.com	10.70.74.242	9200	7322	7222	green	3h9m43s	May 21, 2020, 3:38:23 PM	May 21, 2020, 12:28:27 PM	
Alerts													
Pa Events													
Assets													
Services													
Resources													
Settings													
Hetrics													

Если все микросервисы установлены на одном сервере, как в данном примере, порты для параметров RPC и Metrics должны быть разными.

При создании настраиваемого ресурса Нормализатор для микросервиса Коллектор также рекомендуется проверить, успешно ли выполняется процесс нормализации.

- Чтобы проверить наличие ошибок нормализации с помощью раздела Events веб-консоли КUMA, выполните следующие действия:
 - 1. Убедитесь, что запущен микросервис Коллектор.
 - 2. Убедитесь, что источник событий передает события в КUMA.
 - 3. Убедитесь, что в разделе **Resources** веб-консоли KUMA в раскрывающемся списке **Finalization** ресурса **Normalizer** выбрано значение **error**.
 - 4. В разделе Events в KUMA выполните поиск событий со следующими параметрами:
 - ServiceID = <идентификатор микросервиса Коллектор, использующего ресурс Нормализатор, который требуется проверить>
 - Raw != ""

Если при этом поиске будут обнаружены какие-либо события, это означает, что есть ошибки нормализации, и их необходимо исследовать.

- Чтобы проверить наличие ошибок нормализации с помощью панели мониторинга Grafana, выполните следующие действия:
 - 1. Убедитесь, что запущен микросервис Коллектор.
 - 2. Убедитесь, что источник событий передает события в КUMA.
 - 3. Откройте панель мониторинга Grafana и перейдите по ссылке KUMA Collectors.
 - 4. Проверьте, отображаются ли ошибки в разделе Errors виджета Normalization.

Если в результате обнаружены ошибки нормализации, их необходимо исследовать.

Команды для запуска и установки компонентов вручную

В этом разделе описаны параметры исполняемого файла KUMA, с помощью которого можно вручную запустить или установить компоненты KUMA. Это может пригодиться в случае, если вам нужно увидеть выходные данные в консоли операционной системы сервера.

Таблица 1. Параметры команд

Параметр	Описание
tool certificates	Запуск инструмента для создания сертификатов, используемых для аутентификации компонентов KUMA и шифрования трафика между ними.
collector	Запуск или установка Коллектора.
core	Запуск или установка Ядра.
correlator	Запуск или установка Коррелятора.
help	Получение информации о доступных параметрах.
license	Получение информации о лицензии.
storage	Запуск или установка Хранилища.
version	Получение информации о версии программы.

Флаги:

-h, --h используются для получения справочной информации о файле или команде. Например: kuma <компонент> --help.

Примеры:

- kuma version получение информации о версии установщика KUMA.
- kuma core -h получение справки по команде core установщика КUMA.
- kuma collector --core <адрес сервера, где должен получить свои параметры Коллектор> --id <параметр version установленного микросервиса> --metrics <параметр metrics установленного микросервиса> --rpc <параметр RPC установленного микросервиса> - запуск установки микросервиса Коллектор.

Информация о стороннем коде

Информация о стороннем коде содержится в файле LEGAL_NOTICES, расположенном в каталоге /opt/kuma/LEGAL_NOTICES.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Cisco – зарегистрированный в Соединенных Штатах Америки и в других странах товарный знак Cisco Systems, Inc. и / или ее аффилированных компаний.

Google Chrome – товарный знак Google, Inc.

Microsoft и Windows – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Mozilla и Firefox – товарные знаки Mozilla Foundation.

CentOS – товарный знак компании Red Hat, Inc.