

AI Скоринг активов

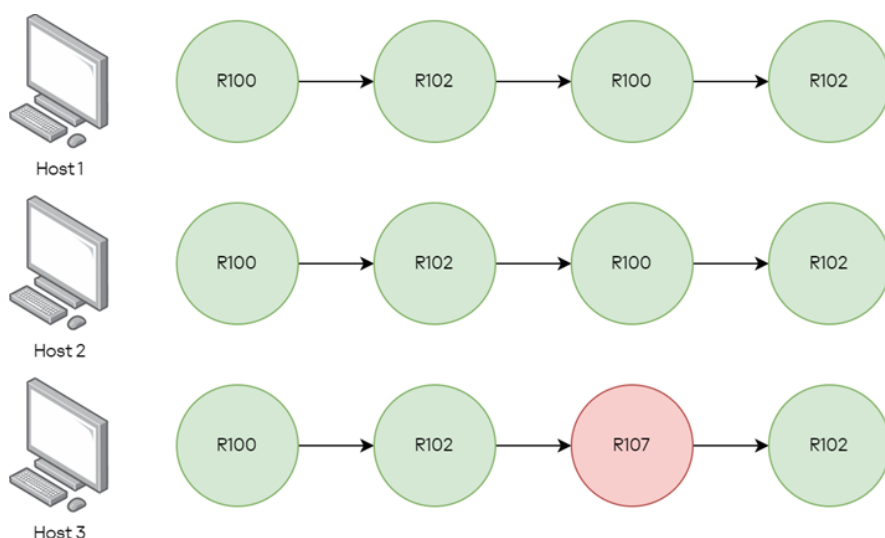
Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Официальная документация по данному разделу приведена в Онлайн-справке на продукт: <https://support.kaspersky.com/help/KUMA/3.4/ru-RU/292782.htm>

Описание

AI-сервис позволяет уточнить критичность корреляционных событий, сгенерированных в результате срабатывания правил корреляции.

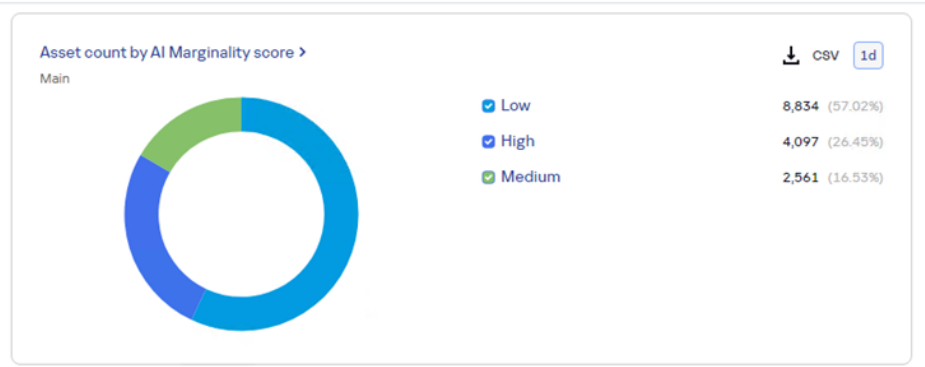
AI-сервис получает из доступных кластеров хранения корреляционные события, содержащие непустое поле Affected assets, выстраивает ожидаемую последовательность событий и обучает модель AI. На основании цепочки срабатываний корреляционных правил AI-сервис высчитывает, является ли такая последовательность срабатываний характерной в этой инфраструктуре. Нехарактерные паттерны повышают рейтинг актива.



По результатам расчетов AI-сервиса в карточке активов становится доступным для просмотра Рейтинг AI и Статус. Рейтинг – это число, которое отражает степень нетипичной активности на активе, на которую стоит обратить внимание. Доступные значения поля Статус: Low, Medium, High, Critical.

Dashboard

Updated 2024-11-30 18:06



После каждого перезапуска AI-сервиса, AI-сервис заново обучает модель и выполняет переоценку рейтинга активов, указанных в событиях за сегодня. Активы со скорингом выглядят следующим образом:

И

+ Добавить условие

+ Добавить группу

Свернуть

Рейтинг AI > 0.25

<input type="checkbox"/>	Название	Полное доменное имя	IP-адрес	MAC-адрес	Статус	Рейтинг AI ↑
<input type="checkbox"/>	KESW	kesw.sales.lab	10.0.0.1	00:50:56:89:99:45	Средний	0.3333333333333333
<input type="checkbox"/>	kscdk	kscdk	10.0.0.2	00:50:56:89:99:46	Средний	0.3636363636363636
<input type="checkbox"/>	fd3c5a1db02c	fd3c5a1db02c	10.0.0.3	00:50:56:89:99:47	Средний	0.4
<input type="checkbox"/>	dc-01.sales.lab	dc-01.sales.lab	10.0.0.4	00:50:56:89:99:48	Средний	0.4285714285714286
<input type="checkbox"/>	xdr-ksc.demo.lab	xdr-ksc.demo.lab	10.0.0.5	00:50:56:89:99:49	Средний	0.4285714285714286
<input type="checkbox"/>	wec.truecompany.local	wec.truecompany.local	10.0.0.6	00:50:56:89:99:50	Высокий	0.5714285714285714
<input type="checkbox"/>	wec	wec	10.0.0.7	00:50:56:89:99:51	Высокий	0.5714285714285714

В директории, указанной в конфигурационном файле, хранятся события, которые AI-сервис получил из кластеров хранения KUMA за указанное количество дней. Например, если в конфигурационном файле указано 12 дней (period_for_train_days), AI-сервис будет получать события за последние 12 дней. Самые давние события удаляются из директории. В этой же директории будет храниться обученная модель.

Переобучение модели происходит в полночь по UTC. Переоценка рейтинга активов происходит раз в час для всех активов, которые были в событиях за сегодня по UTC.

Если лицензию удалить, поля Рейтинг AI и Статус будут скрыты из карточки актива. Если лицензию снова добавить, значения полей Рейтинг AI и Статус снова будут отображаться.

Журналы сервиса хранятся в /var/log/syslog.

Установка

1. Скачайте архив: [ссылка](#). Архив содержит скрипты для установки и удаления сервиса, а также конфигурационный файл `config.yaml`.
2. В конфигурационном файле `config.yaml` укажите порт, по которому хост Ядра будет ожидать подключения от AI-сервиса. Например, в установке в отказоустойчивой конфигурации должен быть указан порт 7226. Для остальных параметров можно оставить значения по умолчанию.
3. Перейдите в директорию с файлами сервиса и из этой папки выполните команду:
`bash ./install <путь к ИНВЕНТОРИ.yaml>`
4. По умолчанию сервис устанавливается на хост с Ядром. Если вы хотите установить сервис на другой хост, укажите в конфигурационном файле `<hostname>:<port>` ядра KUMA в `kuma_address` и убедитесь в наличии сетевого доступа.
5. Установщик генерирует необходимые сертификат и ключ в процессе установки и помещает их в директорию, указанные в конфигурационном файле, по умолчанию: `/opt/kaspersky/mlservice/`. Сертификат необходимо загрузить в KUMA. В веб-интерфейсе KUMA в разделе (появляется при наличии лицензии AI) **Параметры - AI-сервис** во вкладке **AI рейтинг и статус активов** заполните следующие поля:
 - В поле **URL** укажите **адрес и номер порта**, по которому Ядро будет ожидать подключения от AI-сервиса. Например, **:7226** (означает поднять порт на ядре 0.0.0.0:7226). Номер порта должен соответствовать указанному в конфигурационном файле.
 - В поле **Сертификат** в раскрывающемся списке выберите Создать и в открывшемся окне Создание сертификата укажите тип сертификата Certificate и загрузите сертификат из директории, указанной в конфигурационном файле, по умолчанию `/opt/kaspersky/mlservice/service.crt`.

AI-сервис

AI рейтинг и статус активов Kaspersky Investigation & Response Assistant

Выключено

☐

URL*

:7226

Сертификат*

ml_service

Сохранить

Сразу после установки сервис будет пытаться в течение 15 минут подключиться к KUMA с интервалом в 1 минуту. Если сертификат не добавлен в веб-интерфейсе KUMA, подключение не будет выполнено и сервис остановится. В таком случае можно добавить сертификат и перезапустить (`systemctl restart mlservice.service`) AI-сервис, сервис опять попытается

подключиться. AI-сервис установлен.

Revision #5

Created 26 February 2025 09:28:25 by Boris RZR

Updated 21 April 2025 08:08:55 by Boris RZR