## ЧТО НОВОГО

**Новый релиз RuSIEM 3.5.0**

**Рекомендуемые обновления для Ubuntu 18**

* rusiem-kb 18.21.4-78
* rusiem-kernel 18.21.4-222
* rusiem-tools 21.5-155
* rvsiem-kernel 18.21.4-185
* rusiem-web 18.22.04-3.5.0-518

**Инциденты**

* Звуковое оповещение о новом инциденте (<https://docs.rusiem.tech/sections/172>)
* Привязка событий к инцидентам, созданным вручную (<https://docs.rusiem.tech/sections/367>)
* Динамические таблицы (<https://docs.rusiem.tech/sections/360>)
* Автообновление таблицы инцидентов

**Дашборды**

* Настройка линейных виджетов в дашборде
* Переработан выбор периода и количество точек на графике, что дает возможность строить график, показывающий количество событий в секунду и проводить любые математические вычисления с параметром EPS

**Настройки микросервисов**

* Добавлен дополнительный статус «modified» для конфигураций микросервисов

**Multitenancy**

* Добавлено отображение наименование тенанта в отчетах

**Доработаны парсеры**

* Ideco UTM
* SecretNET 8
* DrWeb
* OSSEC
* Windows EventLog
* VmWare
* RedHat
* OpenVPN
* Apache

**Новые парсеры**

* Nextcloud
* Kubernetes
* Zelax

## Привязка событий к инцидентам, созданным вручную

Нажать на кнопку редактирования  инцидента, который был создан вручную. В открывшемся окне в поле «События инцидента» нажать на кнопку «Привязать события».



Откроется окно, показанное ниже.



Для привязки определенных событий к инциденту необходимо выбрать события, установив галочки напротив них. При нажатии на кнопку «Закрыть» окно закроется без сохранения изменений. Далее следует нажать на кнопку «Привязать», появится окно подтверждения действия, показанное ниже.



Нажать на кнопку «Да», в окне редактирования инцидента отобразятся выбранные привязанные события. При выборе события появляется кнопка «Отвязать событие». При нажатии на данную кнопку всплывает окно подтверждения действия.



Нажатие на кнопку «Да» на странице редактирования инцидента удалит выбранные ранее события.

## Звуковое оповещение о новом инциденте

В настройках пользователя появилась новая опция «Звуковое оповещение», включаемая при активной опции «Всплывающее уведомление о новых инцидентах».



## Автоматическое обновление таблицы инцидентов



Работает аналогично автообновлению в разделе «События».