

## RELEASE NOTES ОТ 07 ФЕВРАЛЯ 2020 Г.

### РЕКОМЕНДУЕМЫЕ ОБНОВЛЕНИЯ

- `rusiem-web-5.7.1-123-trusty.deb` для коммерческой версии и для свободно распространяемой версии
- `rusiem-database-5.7.1-12-trusty.deb` для коммерческой версии и для свободно распространяемой версии
- `rusiem-kernel-5.7.1-84-trusty.deb` для коммерческой версии
- `rvsiem-kernel-5.7.1-58-trusty.deb` для свободно распространяемой версии

### НОВОЕ В РЕЛИЗЕ

1. RuSIEM агент. Модуль сбора данных из PostgreSQL
2. Добавлен скрипт расширенной технической поддержки в дистрибутив (`/opt/rusiem/support/rusiem_support.sh`)
3. Оптимизирована работа функции `uniq.count` в правилах корреляции

### ДОРАБОТКИ

1. `rusiem-database`. Исправлена установка Java и изменена версия устанавливаемой ES с 5.6.14 до 5.6.16
2. Исправлена ошибка выгрузки событий с выборкой по фильтру
3. Исправлен поиск инцидента по ID
4. Исправлена ошибка для Oracle модуля агента. Сбрасывались позиции обработанных событий при изменении статусов модуля, а также при их создании и удалении
5. Исправлена ошибка, когда инцидент создавался с датой фактического возникновения 01-01-1970
6. Исправлен конфигурационный файл `lfilter` для RvSIEM bionic
7. Исправлена ошибка для агрегации метаданных инцидента

Готов релиз на 18 версии Ubuntu. Желающим пройти тестовые установки просьба обращаться на [info@rusiem.com](mailto:info@rusiem.com)

Обновляем на ближайшие полгода дорожную карту. Пожелания по доработке принимаются на почту [info@rusiem.com](mailto:info@rusiem.com) – у всех есть шансы быть услышанными и большая вероятность, что именно ваши потребности включим в ближайшую дорожную карту.