RELEASE NOTES ОТ 29 ИЮЛЯ 2020 Г.

РЕКОМЕНДУЕМЫЕ ОБНОВЛЕНИЯ

- rusiem-kb-5.7.1-25-trusty.deb для коммерческой версии и для свободно-распространяемой версии
- rusiem-kernel-5.7.1-113-trusty.deb для коммерческой версии
- rusiem-web-5.7.1-160-trusty.deb для коммерческой версии и для свободно-распространяемой версии
- rvsiem-kernel-5.7.1-85-trusty.deb для свободно-распространяемой версии

НОВОЕ В РЕЛИЗЕ

Парсеры

1. Добавлены новые парсеры
   - FortiGate FortiMail
   - Netgate
   - Infotecs VipNet Coordinator
   - Bind
   - Brocade

ДОРАБОТКИ

Интеграция с R-Vision

1. Добавлена поддержка режима multitenancy. А также добавлена возможность указать группу R-Vision по умолчанию, куда будут добавляться инциденты Rusiem

Корреляция

1. Добавлена возможность множественного выделения правил корреляции и правил аналитики для активации, деактивации и удаления
2. Исправление для функции uniq.count в правилах корреляции

RuSIEM Agent

1. Исправление фильтра по event.id в настройках EventLog для режима evt

Парсеры

1. Исправлен парсер classified
2. Доработаны парсеры
   - Cisco ASA
   - Cisco firepower SFIMS
   - Fortinet FortiGate
   - iptables
   - cron/crond
   - Nginx
   - fail2ban

- postfix
- arpwatch
- arpscan
- monit