

RELEASE NOTES ОТ 04 СЕНТЯБРЯ 2020 Г.

РЕКОМЕНДУЕМЫЕ ОБНОВЛЕНИЯ ДЛЯ UBUNTU 14

- rusiem-kb-5.7.1-30-trusty.deb
- rusiem-web-5.7.1-167-trusty.deb
- rusiem-kernel-5.7.1-121-trusty.deb
- rvsiem-kernel-5.7.1-90-trusty.deb

РЕКОМЕНДУЕМЫЕ ОБНОВЛЕНИЯ ДЛЯ UBUNTU 18

- rusiem-web-6.0.1-41-bionic.deb
- rusiem-kb-6.0.1-12-bionic.deb
- rusiem-kernel-6.0.1-53-bionic.deb
- rvsiem-kernel-6.0.1-43-bionic.deb

НОВОЕ В РЕЛИЗЕ

1. Установка на Ubuntu 14 через Proxu.
2. В общих настройках RuSIEM добавлена настройка таймаута сессии
3. Добавлены отчеты по инцидентам и по задачам инцидентов.

ДОРАБОТКИ

1. Исправлена ошибка. При назначении задачи внутри инцидента не корректно формировалась ссылка
2. Исправлена ошибка при закрытии задачи внутри инцидента
3. Исправлена ошибка при создании инцидентов.
4. Оптимизация скрипта обновления. (custom_config=1 для сохранения скрипта обновления)
5. Доработана интеграция с R-Vision. Отображение полей событий и объектов группировки
6. Доработки в разделе списков (Пользовательский тип по умолчанию)
7. Доработки по парсерам:
 - Linux
 - Cisco ASA
 - PostgreSQL
 - veeam
 - Brocade
 - VipNet Coordinator
 - события и демоны RuSIEM
8. Оптимизации по парсерам:
 - nginx
 - Касперский



RUSIEM

Всё под контролем

- Panda
- Oracle audit
- netgate
- iptables
- paloalto
- cef