RELEASE NOTES ОТ 08 ОКТЯБРЯ 2020 Г.

РЕКОМЕНДУЕМЫЕ ОБНОВЛЕНИЯ ДЛЯ UBUNTU 14

- rusiem-database-5.7.1-15-trusty.deb
- rusiem-kb-5.7.1-41-trusty.deb
- rusiem-web-5.7.1-173-trusty.deb
- rusiem-kernel-5.7.1-126-trusty.deb
- rvsiem-kernel-5.7.1-94-trusty.deb

РЕКОМЕНДУЕМЫЕ ОБНОВЛЕНИЯ ДЛЯ UBUNTU 18:

- rusiem-database-6.0.1-9-bionic.deb
- rusiem-kb-6.0.1-22-bionic.deb
- rusiem-web-6.0.1-47-bionic.deb
- rusiem-kernel-6.0.1-58-bionic.deb
- rvsiem-kernel-6.0.1-46-bionic.deb

НОВОЕ В РЕЛИЗЕ

Парсеры

1. Bastion
2. Kaspersky Secure Mail Gateway
3. Juniper
4. Anacron

ДОРАБОТКИ

Функционал

1. Доработка в разделе "Корреляция": возможность отслеживания статуса активации правила корреляции
2. Доработки в разделе "Интеграции": передача ссылки на инцидент в R-Vision, передача информации об активах в рамках инцидента в R-Vision
3. Доработка в разделе "Инциденты": пользователь с определенными правами имеет возможность удалить инцидент по кнопке из раздела "Инциденты"
4. Доработка в разделе "События": Добавлена возможность переключения между событиями клавишами ↑ и ↓
5. Оптимизация записи данных в Elasticsearch

Парсеры

1. Squid
2. Checkpoint
3. Palo Alto
4. Касперский

5. Cisco
6. Bind (named)
7. sshd
8. события и демоны RuSIEM
9. su
10. sshd
11. Linux kernel