

RELEASE NOTES ОТ 12 МАРТА 2021 Г.

РЕКОМЕНДУЕМЫЕ ОБНОВЛЕНИЯ ДЛЯ UBUNTU 14

- rusiem-kb-5.7.1-72-trusty.deb
- rusiem-kernel-5.7.1-204-trusty.deb
- rusiem-web-5.7.1-229-trusty.deb
- rvsiem-kernel-5.7.1-135-trusty.deb

РЕКОМЕНДУЕМЫЕ ОБНОВЛЕНИЯ ДЛЯ UBUNTU 18:

- rusiem-kb-6.0.1-53-bionic.deb
- rusiem-kernel-6.0.1-132-bionic.deb
- rusiem-web-6.0.1-102-bionic.deb
- rvsiem-kernel-6.0.1-90-bionic.deb

НОВОЕ В РЕЛИЗЕ

События и инциденты

1. Получение истории ip, ipv6 или домена из интерфейса системы

Источники

1. Подключение парсеров через источники

RuSIEM агент

1. Поддержка новых версий Oracle

Корреляция

1. Статистика по скорости работы правил корреляции

ДОРАБОТКИ

Установка и обновление

1. Доработан скрипт обновления

События и инциденты

1. Улучшение RuSIEM Audit - UID источника события
2. Оптимизация загрузки данных по инциденту

Источники

1. Оптимизация формы добавления источников

Дашборды

1. Отображение типов источников при редактировании виджета

Корреляция

1. Оптимизация ядра и функций корреляция
2. Доработка демона отправки электронной почты



RUSIEM

Всё под контролем

Лицензия

1. Доработка интерфейса

Общие улучшения

1. Оптимизация работы с Elasticsearch

Доработки по парсерам

1. Sendmail
2. Linux
3. PgSQL
4. RuSIEM
5. RuAgent