RELEASE NOTES ОТ 12 ФЕВРАЛЯ 2021 Г.

РЕКОМЕНДУЕМЫЕ ОБНОВЛЕНИЯ ДЛЯ UBUNTU 14

- rusiem-kb-5.7.1-70-trusty.deb
- rusiem-web-5.7.1-222-trusty.deb
- rusiem-kernel-5.7.1-188-trusty.deb
- rvsiem-kernel-5.7.1-126-trusty.deb

РЕКОМЕНДУЕМЫЕ ОБНОВЛЕНИЯ ДЛЯ UBUNTU 18:

- rusiem-kb-6.0.1-51-bionic.deb
- rusiem-web-6.0.1-95-bionic.deb
- rusiem-kernel-6.0.1-117-bionic.deb
- rvsiem-kernel-6.0.1-81-bionic.deb
- rusiem-analytics-5.0.0-67-bionic.deb
- rusiem-analytics-sa-5.0.0-54-bionic.deb

НОВОЕ В РЕЛИЗЕ

Интеграция с ФинЦЕРТ - агент сбора IOC (инструкция по установке и настройке: https://files.rusiem.tech/nextcloud/s/imearjaKiiiiiE2)

ДОРАБОТКИ

Доработан скрипт расширенной технической поддержки

События

1. Оптимизация поиска по событиям

Источники

1. Исправление удаления сторонних источников

Инциденты

1. удаление старых инцидентов
2. поиска событий по событиям инцидентов

Аналитика

1. Оптимизация Baseline, повышена стабильность

Корреляции

1. Оптимизация и доработка системных правил

Парсеры

1. Kaspersky
2. Usergate

3. IDS HS
4. SSHD
5. Postgresql
6. Iptables
7. Linux
8. Lsfilter
9. D-LINK