RELEASE NOTES ОТ 03 НОЯБРЯ 2020 Г.

РЕКОМЕНДУЕМЫЕ ОБНОВЛЕНИЯ ДЛЯ UBUNTU 14

- rusiem-kb-5.7.1-50-trusty.deb
- rusiem-kernel-5.7.1-130-trusty.deb
- rvsiem-kernel-5.7.1-97-trusty.deb

РЕКОМЕНДУЕМЫЕ ОБНОВЛЕНИЯ ДЛЯ UBUNTU 18:

- rusiem-kb-6.0.1-31-bionic.deb
- rusiem-kernel-6.0.1-62-bionic.deb
- rvsiem-kernel-6.0.1-49-bionic.deb

НОВОЕ В РЕЛИЗЕ

Парсеры

1. Docker
2. S-terra
3. АРМ КБР-Н

Правила корреляции

1. Правила выявления инструментария злоумышленников
2. Правила выявления сканеров уязвимостей в локальной сети
3. Правила мониторинга состояния RuSIEM
4. Правила выявления сканирования сервисов в сети Интернет из Локальной сети
5. Правила мониторинга состояния ESXi
6. Правила выявления EternalBlue (MS17-010)
7. Правила обнаружения переполнения буфера Windows

События

1. Дополнительные группы отображения полей событий

ДОРАБОТКИ

Парсеры

1. Windows
2. Kaspersky Security for mail server
3. DrWeb

Общие улучшения

1. Оптимизация работы с Elasticsearch
2. Оптимизация и доработка системных правили