RELEASE NOTES ОТ 21 СЕНТЯБРЯ 2022 Г.
RuSIEM 3.7.0

Рекомендуемые обновления для Ubuntu 18

- rvsiem-kernel - 18.21.4-208
- rusiem-kernel - 18.21.4-268
- rusiem-analytics - 21.0-205
- rusiem-analytics-sa - 21.0-205
- rusiem-database - 18.21.0-69
- rusiem-kb - 18.21.4-129
- rusiem-tools - 22.8-200
- rusiem-web - 18.22.09-3.7.0-731

Списки и таблицы

- Экспорт значений динамических списков (https://docs.rusiem.tech/sections/375)
- Экспорт значений статических списков (https://docs.rusiem.tech/sections/373)
- Динамические таблицы. Возможность ограничения длины поля text (https://docs.rusiem.tech/sections/362)

Агент

- Оптимизация инсталлятора
- Оптимизация FTP-модуля

Корреляция

- Автоматическое отключение правил корреляции (https://docs.rusiem.tech/sections/371)
- Модуль машинного обучения – выявление DGA (https://docs.rusiem.tech/sections/282)
- Возможность сравнения полей в условиях правила корреляции (https://docs.rusiem.tech/sections/282)
- Регистронезависимый поиск по статическим спискам (https://docs.rusiem.tech/sections/282)
- Поиск подстроки по значениям статических списков (https://docs.rusiem.tech/sections/282)
- Оптимизация функции uniq.count

Инциденты

- Уведомления для инцидентов, созданных вручную

Дашборды

- Возможность выполнения математических операций в виджетах

Нормализация

- Доработка логирования frs_server
- Оптимизация блока output в парсерах

Доработаны парсеры

- Dell

- Oracle
- Clearswift
- Security code (vGate)
- Kerio
- VmWare
- Linux
- Kaspersky (KLMS)
- Windows
- IIS
- Apache
- Cisco firepower
- Kubernetes

Новые парсеры

- HPE
- Mikrolink
- Gamma(krechet)
- Caddy
- NewSecurity
- Moxa