RELEASE NOTES ОТ 16 ЯНВАРЯ 2023 Г.
RuSIEM 3.8.0

Рекомендуемые обновления для Ubuntu 18
- rusiem-database_18.21.0-74_amd64.deb
- rusiem-kb_18.21.4-198_amd64.deb
- rusiem-kernel_18.21.4-323_amd64.deb
- rusiem-tools_22.11-286_amd64.deb
- rusiem-web_18.23.01-3.8.0-945_amd64.deb
- rvsiem-kernel_18.21.4-235_amd64.deb

События
- Режим Multitenancy. Возможность фильтрации по тенантам (https://docs.rusiem.tech/sections/390)

Новый функционал
- Обогащение событий активами (https://docs.rusiem.tech/sections/387)
- Агрегация событий (https://docs.rusiem.tech/sections/381)

Агент сбора событий
- Модуль RestAPI (https://docs.rusiem.tech/sections/391)

Корреляция
- Новый оператор inlist_contains (https://docs.rusiem.tech/sections/282)

Доработаны парсеры
- Cisco
- Kaspersky Security Center
- Ideco
- Nginx
- Windows
- MS DHCP
- Infotecs
- Linux
- Suricata
- NetGate

Новые парсеры
- Cowrie
- Система видеонаблюдения Trassir
- hMailServer
- Merak mail server
- 1C Bitrix