RELEASE NOTES ОТ 29 МАРТА 2023 Г.
RuSIEM 3.9.0

Рекомендуемые обновления для Ubuntu 18
- rusiem-analytics 21.0-228
- rusiem-analytics-sa 21.0-228
- rusiem-web 18.23.03-3.9.0-1082
- rusiem-kb 18.21.4-256
- rusiem-tools 23.02-314
- rvsiem-kernel 18.21.4-245
- rusiem-kernel 18.21.4-340

Основной функционал
- Возможность фильтрации приходящих событий (https://docs.rusiem.tech/sections/394)
- Telegram-уведомления об инцидентах (https://docs.rusiem.tech/sections/400)

Дополнительные доработки

События
- Получение значения EPS через API

Нормализация
- Преобразования значения int в ipv4
- Преобразование timestamp в дату указанного формата

Отчеты
- Возможность выбора полей инцидентов
- Генерация отчетов в формате docx

Микросервисы
- Отображение имени хоста

Multitenancy
- Функционал копирования списков на подчиненные ноды

Агент
- Оптимизация модуля EventLog
- Оптимизация модуля FTP
- Оптимизация модуля FileLog

Доработаны парсеры
- Cisco
- Mikrotik
- CheckPoint
- Vmware
- Windows
- IIS

- Kaspersky
- Garda Monitor
- Netflow
- Dr.Web
- Auditd
- Suricata
- Infotecs

Новые парсеры

- Маршрутизатор huawei
- DWDM Volga
- КриптоПро NGate
- Elastic auditbeat (Filelog)