RELEASE NOTES ОТ 15 АВГУСТА 2024 Г.
RuSIEM 4.2.0

Обновления для операционных систем
- Ubuntu 18
- Ubuntu 22
- Astra Linux

Рекомендуемые обновления для Ubuntu 18
- rusiem-kb_24.8-986
- rusiem-kernel_24.8-398
- rusiem-web_24.08-4.2.0-2193
- rvsiem-kernel_24.8-278

Рекомендуемые обновления для Ubuntu 22
- rusiem-frs-24.8-24
- rusiem-kb-24.8-979
- rusiem-ls-24.8-30
- rusiem-tools-24.8-530
- rusiem-web-24.08-4.2.0-2194
- rvsiem-frs-24.8-19
- rvsiem-ls-24.8-33

Рекомендуемые обновления для Astra Linux
- rusiem-frs - 24.8-18-astra.0
- rusiem-kb - 24.8-430-astra.0
- rusiem-ls - 24.8-33-astra.0
- rusiem-web - 24.8-4.2.0-60-astra.0
- rvsiem-frs - 24.8-16-astra.0
- rvsiem-ls - 24.8-20-astra.0

Основное
- Сбор событий по протоколу SNMP
- Мониторинг syslog источников

Дашборды
- Массовый импорт и экспорт
- Поиск по названию
- Доработан конструктор линейного виджета

Коррелятор
- Оптимизация правил с несколькими блоками условий

Инциденты
- Отображение идентификатора инцидента

Отчеты

- Доработка области видимости пользовательских отчетов

Списки и таблицы

- Экспорт содержимого статических и динамических таблиц
- Вывод правил со статическими списками

Агенты

- Управление локальной базой агента

Настройки

- Логирование парольной политики
- Доработка прав доступа просмотра сущностей системы

Multitenancy

- Закрытие инцидента из головной ноды

Доработано парсеров: 36 шт.