

RELEASE NOTES ОТ 17 ИЮЛЯ 2025 Г.
RuSIEM 5.0.0

Обновления для операционных систем

- rusiem-tools_25.7-15-all_amd64.deb
- rusiem-analytics_21.0-335_amd64.deb
- rusiem-analytics-sa_21.0-335_amd64.deb
- rusiem-frs_25.7-4-all_amd64.deb
- rusiem-kernel_25.7-4-all_amd64.deb
- rusiem-ls_25.7-5-all_amd64.deb
- rusiem-kb_25.7-18-all_all.deb
- rusiem5-web_25.07-5.0.0-3_amd64.deb
- rvsiem-frs_25.7-4-all_amd64.deb
- rvsiem-kernel_25.7-4-all_amd64.deb
- rvsiem-ls_25.7-5-all_amd64.deb

В RuSIEM 5.0.0 вошел ряд существенных изменений. Остается поддержка Ubuntu 22.04, Astra Linux 1.8.x, Debian 12.

Основное

- Оптимизация и ускорение веб-интерфейса. Переход на PHP 8.4
- Агентский модуль F6ManagedXDR

Обогащение

- Обогащение событий из динамических таблиц

Корреляция

- Групповое управление настройками переоткрытия инцидентов

Инциденты

- Сохранение фильтра при переходе из событий инцидента в раздел «События»

Списки

- Импорт в динамические и статические таблицы из файлов

Агенты

- Агентский модуль F6ManagedXDR
- Обработка многострочных событий в модуле FileLog
- Linux Агент. Модуль сбора событий RedCheck

Коррелятор

- Оптимизация обработки цепочки событий



RUSIEM

Всё под контролем

Новые парсеры:

- 389ds
- 3proxy
- GIS
- f6mxdr
- OpenBSD
- Mongodb
- Tacacs
- Privacyidea
- Victorimetrics
- Virtuozzo
- Celery
- Graphite
- Red Soft
- VK Workmail

Доработано парсеров: 35 шт.