RELEASE NOTES ОТ 03 ИЮЛЯ 2020 Г.

РЕКОМЕНДУЕМЫЕ ОБНОВЛЕНИЯ

- rusiem-kb-5.7.1-24-trusty.deb для коммерческой версии и для свободно распространяемой версии
- rusiem-kernel-5.7.1-108-trusty.deb для коммерческой версии
- rusiem-web-5.7.1-153-trusty.deb для коммерческой версии и для свободно распространяемой версии
- rvsiem-kernel-5.7.1-81-trusty.deb для свободно распространяемой версии

НОВОЕ В РЕЛИЗЕ

Парсеры

1. Добавлен парсер Panda
2. Добавлен парсер БОСС-кадровик
3. Добавлен парсер Synology
4. Добавлен парсер Staffcop
5. Добавлен парсер Infotecs TIAS

Функционал

1. frs_server. Добавлена возможность (codec) пересылки сырого события
2. frs_server. Добавлена возможность пересылки событий по UDP
3. Добавлена интеграция с R-Vision

ДОРАБОТКИ

Функционал

1. sfilter. Исправления для работы со списками (CIDR)
2. lsfilter. Улучшено выполнение правил корреляции
3. Доработки API для функции получения событий по ID инцидента

Rusiem агент

1. Модуль Eventlog: Улучшена работы с журналами Forwarding Events
2. Модуль Eventlog: Оптимизирована работа агента для больших потоков событий

Парсеры

1. Доработан парсер PTAF
2. Доработан парсер Fortigate
3. Доработан парсер Cisco ASA и PIX
4. Доработан парсер Windows
5. Доработан парсер Nginx

Прочее

1. Оптимизированы системные правила корреляции