RELEASE NOTES ОТ 26 АВГУСТА 2019 Г.

РЕКОМЕНДУЕМЫЕ ОБНОВЛЕНИЯ

- rusiem-web-5.7.1-113 для коммерческой версии и для свободно распространяемой версии
- rusiem-kb-5.7.1-18-trusty.deb для коммерческой версии и для свободно распространяемой версии
- rusiem-kernel-5.7.1-76-trusty.deb для коммерческой версии
- rvsiem-kernel-5.7.1-48-trusty.deb для свободно распространяемой версии

НОВОЕ В РЕЛИЗЕ

Syslog_mapper

1. Блоки для AttackKiller, kerio (события от них отправляются на отдельный парсер)
2. Добавлен еще один вариант событий от cisco ASA
3. Блок для cisco Nexus (дальнейшая обработка в парсере cisco)

Парсер positive.conf для нормализации событий Positive Technologies Application Firewall

Filter_linux

1. Добавлена нормализация для dpkg, arpwatch, bash, ZyXEL (логи dhcp)

Filter_cisco

1. Добавлена нормализация http.url и http.referrer
2. Добавлены дополнительные ключи из событий
3. Блок нормализации для cisco Nexus

Парсер для FortiNet с большим количеством изменений

1. Изменено условие входа в блок для FortiGate
2. Добавлено большое число полей из событий
3. Расширен блок grok, убрано несколько условий

ДОРАБОТКИ

1. Скорректированы определения FortiGate (добавлены версии 30E/60E/VM)\
2. Скорректированы ошибки в названии поля [iface][inbound]
3. Скорректированы ошибки с отсутствием типа источника
4. Скорректирована нормализация iis для filelog.conf
5. Скорректирована ошибка установки (отсутствие файла pg_hba.conf)
6. Скорректированы ошибки в FRS.
7. Скорректированы ошибки в update-hourly.sh