RELEASE NOTES ОТ 26 ЯНВАРЯ 2022 Г.
RuSIEM 3.4.0

Рекомендуемые обновления для Ubuntu 18
- rusiem-web 18.22.01-3.4.0-414
- rusiem-analytics 21.0-172
- rusiem-analytics-sa 21.0-172
- rusiem-database 18.21.0-41
- rusiem-kb 18.21.4-60
- rusiem-kernel 18.21.4-194
- rusiem-tools 21.5-128
- rvsiem-kernel 18.21.4-157

Важно: в рамках данного релиза происходит перенос настроек всех сервисов в БД для управления из интерфейса системы

Инциденты
- Приоритет в оповещения об инциденте
- Добавлены категории инцидентов (https://docs.rusiem.tech/sections/340)
- Оптимизация удаления инцидентов

Система
- Оптимизация раздела «Система»
- Управление подчиненных нод
- LsInput - Доработка настройки буффера UDP
- Оптимизация ротации логов
- Сбор EPM системных демонов
- Обновление геобазы

Настройки
- Новый раздел "Настройка микросервисов" (https://docs.rusiem.tech/sections/349)
- Управление сертификатами (https://docs.rusiem.tech/sections/354)

Multitenancy
- Переключение режима ноды (https://docs.rusiem.tech/sections/350)
- Мультипоиск событий (https://docs.rusiem.tech/sections/351)
- Синхронизация правил корреляции (https://docs.rusiem.tech/sections/341)
- Синхронизация парсеров (https://docs.rusiem.tech/sections/178)
- Синхронизация симптомов (https://docs.rusiem.tech/sections/342)
- Состояние сервисов нод (https://docs.rusiem.tech/sections/188)

Доработаны парсеры
- FileLog (dns 2012)
- Windows EventLog
- Auditd
- Ideco UTM

- Ideco UTM mail gateway и ids
- OpenVPN
- VipNet
- Модули Ruagent
- Коммутаторы Dell Networking
- VmWare
- Infowatch Traffic Monitor
- Confident (Dallaslock)
- Kaspersky

Новые Парсеры
- Garda Monitor
- Garda DB
- Nagios
- Secret Net Studio 8.x

Корреляция и симптомы
- Переработка структуры всех правил корреляции
- Обнаружение Log4shell
- Kaspersky