# RELEASE NOTES ОТ 21 ИЮЛЯ 2021 Г.

## РЕКОМЕНДУЕМЫЕ ОБНОВЛЕНИЯ ДЛЯ UBUNTU 18

- rusiem-kernel_18.21.4-72_amd64.deb
- rusiem-database-18.21.0-18_amd64.deb
- rusiem-kb_18.21.4-29_amd64.deb
- rusiem-tools_21.5-18_amd64.deb
- rusiem-web_18.21.4-137_amd64.deb
- rusiem-analytics_21.0-79_amd64.deb
- rvsiem-kernel_18.21.4-64_amd64.deb

## НОВОЕ В РЕЛИЗЕ

Настройки

1. Добавлена новая опция "Время хранения инцидентов"

Отчеты

1. Генерация отчетов в csv формате

Парсеры

1. Yum
2. Avaya
3. PTAFwifi Ubiquiti
4. named
5. SSHD
6. SSH (ruagent)
7. sysmon (ruagent)
8. system info (ruagent)

Правила корреляции

1. Windows: Подозрение на PrintNightmare (CVE-2021-1675)
2. Инструментальное сканирование Nikto
3. Sysmon: Credential Dumping

API

1. Добавлена новая функция для получения событий инцидента

События

2. Архивация событий (https://docs.rusiem.tech/sections/296)

Агент

1. Оптимизация модуля агента ssh
2. Новый модуль Sysmon (https://docs.rusiem.tech/sections/298)
3. Новый модуль System Info (https://docs.rusiem.tech/sections/299)
4. Архивация событий при передаче

**ДОРАБОТКИ**

Агент

1. Оптимизация модуля агента ssh
2. Улучшенное шифрование при передаче
3. Доработка формата лога модуля 1С

Корреляция

1. Оптимизация динамических списков
2. Доработка импорта и экспорта правил корреляций
3. Оптимизированы правила корреляции

Система

1. Оптимизация скрипта для сбора логов системы
2. Доработка по сбору логов Netflow.
3. Поддержка Netflow 5
4. Обновление переводов языковых файлов

Настройки

1. Обновление списка полей настроек системы

События

1. Доработано отображение событий
2. Оптимизация фильтров в настройках представления

API

1. Доработана фильтрация для получения списка инцидентов

Инциденты

1. Исправлена сортировка по датам
2. ГосСОПКА. Комментариев для всех статусов, кроме архивных
3. Доработан подсчет количества событий инцидентов

Аналитика

1. Дополнительные поля активов
2. Доработка для правил аналитики

ВАЖНО: Если у Вас отключено автоматическое обновление агента для его функционирования агент необходимо обновить