RELEASE NOTES ОТ 23 НОЯБРЯ 2020 Г.

РЕКОМЕНДУЕМЫЕ ОБНОВЛЕНИЯ ДЛЯ UBUNTU 14

- rusiem-kb-5.7.1-53-trusty.deb
- rusiem-kernel-5.7.1-131-trusty.deb
- rusiem-web-5.7.1-181-trusty.deb
- rvsiem-kernel-5.7.1-100-trusty.deb

РЕКОМЕНДУЕМЫЕ ОБНОВЛЕНИЯ ДЛЯ UBUNTU 18

- rusiem-kb-6.0.1-34-bionic.deb
- rusiem-kernel-6.0.1-63-bionic.deb
- rusiem-web-6.0.1-55-bionic.deb
- rvsiem-kernel-6.0.1-52-bionic.deb

ДОРАБОТКИ

Модуль "Система"

1. Исправлено отображения состояния микросервисов
2. Добавлена справочная информация по функционалу.
3. Добавлена информация о текущей загрузки ноды.
4. Добавлен раздел "Хранилище" - состояние нод хранения.
5. Добавлен раздел "Ноды" - Статус подчиненных серверов.

Исправление для интеграции с Oracle - "Oracle DBA Audit logs"

Парсеры

1. Парсер DrWeb
2. Парсер Netgate
3. Парсер микросервисов Rusiem
4. Парсер Cisco
5. Парсер Bastion
6. Парсер Mikrotik
7. FRS - исправление обновления статусов парсеров

Правила корреляции

1. Оптимизация и доработка системных правили
2. Пакет правил обнаружения Mimikatz
3. Правила обнаружения Zerologon (CVE-2020-1472)
4. Правила обнаружения BlueKeep (CVE-2019-0708)
5. Правила обнаружения Kali Linux
6. Правила обнаружения инструментов удаленного администрирования (TeamViewer, RMS, Ammyy Admin и др)
7. Правила обнаружения инструментов взлома PWDump
8. Правила проверки активации Windows (отсутствие активации, сбой активации)