



RUSIEM

Всё под контролем

RELEASE NOTES ОТ 22 ЯНВАРЯ 2021 Г.

РЕКОМЕНДУЕМЫЕ ОБНОВЛЕНИЯ ДЛЯ UBUNTU 14

- rusiem-kb-5.7.1-68-trusty.deb
- rusiem-web-5.7.1-211-trusty.deb
- rusiem-kernel-5.7.1-170-trusty.deb
- rvsiem-kernel-5.7.1-124-trusty.deb

РЕКОМЕНДУЕМЫЕ ОБНОВЛЕНИЯ ДЛЯ UBUNTU 18

- rusiem-kb-6.0.1-49-bionic.deb
- rusiem-web-6.0.1-84-bionic.deb
- rusiem-kernel-6.0.1-101-bionic.deb
- rvsiem-kernel-6.0.1-79-bionic.deb
- rusiem-analytics-5.0.0-66-bionic.deb

ДОРАБОТКИ

События

1. Оптимизация и исправления по фильтрам

Инциденты

1. Исправления при просмотре инцидентов

Агент

1. Доработка настроек агента
2. Дублирование событий на syslog коллектор

Аналитика

1. Оптимизация Baseline

Отчеты

1. Валидация для отчетов по инцидентам

Система

1. Доработки по автоматическому обновлению

Парсеры

1. Bastion
2. Microtik
3. Clearswift Secure Email Gateway
4. McAfee ESM
5. Apache

Корреляции

1. Оптимизация и доработка системных правил
2. Пакет правил Bastion