RELEASE NOTES ОТ 22 АПРЕЛЯ 2021 Г.

РЕКОМЕНДУЕМЫЕ ОБНОВЛЕНИЯ ДЛЯ UBUNTU 14

- rusiem-database_14.21.0-5_amd64.deb
- rusiem-kb_14.21.4-5_amd64.deb
- rusiem-kernel_14.21.4-12_amd64.deb
- rusiem-web_14.21.4-20_amd64.deb
- rvsiem-kernel_14.21.4-12_amd64.deb

РЕКОМЕНДУЕМЫЕ ОБНОВЛЕНИЯ ДЛЯ UBUNTU 18

- rusiem-database_18.21.0-5_amd64.deb
- rusiem-kb_18.21.4-5_amd64.deb
- rusiem-kernel_18.21.4-12_amd64.deb
- rusiem-web_18.21.4-20_amd64.deb
- rvsiem-kernel_18.21.4-12_amd64.deb

НОВОЕ В РЕЛИЗЕ

Списки

1. Добавлена поддержка TTL (время жизни записей)

Новые парсеры

1. gnome-shell
2. php-fpm7.1
3. Asterisk
4. Radware Defence pro
5. ESET Endpoint Security
6. Kiwi solarwinds
7. FreeRADIUS
8. WAF Fortiweb
9. ДБО (Бифит)
10. Amavis
11. VMware ESXi

Новые правила корреляции

1. Rusiem IoC: обращение к вредоносному домену
2. Rusiem IoC: обращение к вредоносному IP

ДОРАБОТКИ

Агент

1. модуль Telnet
2. модуль SSH
3. Оптимизация работы агента

4. Установка агента через GPO
5. Оптимизация модуля EventLog
6. Доработано сохранение настроек агента
7. Функционал настройки модулей по умолчанию

Установка и обновление

1. Оптимизация и доработка инсталятора Rusiem
2. Оптимизация настроек демонов Rusiem

Настройки

1. Валидация формы добавления пользователя

Система

1. Доработка раздела "Система"
2. Функционал диагностики парсеров

Интеграции

1. Интеграция с Rusiem IoC
2. Интеграция с ГосСОПКА

Симптомы

1. Доработка создания симптомов и их категорий

Инциденты

1. Кастомные поля событий в инцидентах и уведомлениях
2. Страница инцидентов. Убран "Суммарный вес симптомов"

Корреляции

1. Оптимизация правил корреляции

Доработка по парсерам

1. Оптимизация парсеров формата CEF
2. Mikrotik: DNS, SMB, web-proxy
3. McAfee ESM
4. systemd
5. Windows Eventlog
6. Bastion
7. systemd-resolved
8. RuAgent
9. Cisco ASA-5 и ASA-6
10. dbus-daemon
11. sshd
12. PostgreSQL
13. Oracle Audit
14. PTAF
15. Paloalto
16. Linux postmaster
17. Juniper
18. DLP DeviceLock 8.3
19. Symantec Endpoint Protection
20. Clearswift Secure Email Gateway

21. D-LINK
22. Linix kernel
23. Cisco NGIPS
24. Fortinet FortiMail