RELEASE NOTES ОТ 16 ИЮНЯ 2021 Г.

РЕКОМЕНДУЕМЫЕ ОБНОВЛЕНИЯ ДЛЯ UBUNTU 18

- rusiem-kernel_18.21.4-43_amd64.deb
- rusiem-web_18.21.4-100_amd64.deb
- rusiem-kb_18.21.4-20_amd64.deb
- rusiem-analytics_21.0-68_amd64.deb
- rusiem-analytics-sa_21.0-68_amd64.deb
- rvsiem-kernel_18.21.4-40_amd64.deb

НОВОЕ В РЕЛИЗЕ

Парсеры

1. Network Manager
2. update-notifier.desktop
3. ntpd
4. dnsmasq
5. Keepalived
6. Cisco WLC
7. Klnagent
8. Allied telesis(switch)
9. failoverd
10. Arbor Networks
11. session watcher
12. Ubiquiti UniFi AP LR

Настройки

1. Возможность перемещения в дереве нод
2. Парсеры. Функция разбора xml (https://docs.rusiem.tech/sections/290)
3. Сохранение почтовых настроек

Актив

1. Новый раздел "Активы" (https://docs.rusiem.tech/sections/264):

Новая база уязвимостей

Агент

1. Опция "События классифицированы" (https://docs.rusiem.tech/sections/146)

Корреляция

1. Включение/отключение статистики
2. Динамические списки (https://docs.rusiem.tech/sections/274)
3. Поддержка MITRE Att&ck

ДОРАБОТКИ

Инциденты

1. Оптимизация событий инцидентов
2. Оптимизация агрегированных полей событий

Настройки

1. LDAP. Оптимизация поиска
2. Доработка отображения настроек

Агент

1. Доработка модуля FileLog

Корреляция

1. Оптимизация демона

Установка и обновление

1. Поддержка ElasticSearch 7

Система

1. Оптимизация вывода нагрузок

События

1. Оптимизирован функционал
2. Переработано отображение раздела

Парсеры

1. Доработка парсера CEF
2. Auditd
3. Monit
4. Cisco ASA
5. Windows EventLog
6. Apache
7. Linux
8. CheckPoint