RELEASE NOTES ОТ 8 ФЕВРАЛЯ 2024 Г.
RuSIEM 4.0.0

Рекомендуемые обновления для Ubuntu 22
- rusiem-kb 24.2-622
- rusiem-web 24.02-4.0.0-1762
- rusiem-tools 24.2-488
- rusiem-frs 24.2-18
- rusiem-kernel 24.2-17
- rusiem-ls 24.2-19
- rvsiem-frs 24.2-16
- rvsiem-ls 24.2-26
- rvsiem-kernel 24.2-18

Рекомендуемые обновления для Ubuntu 18
- rusiem-kernel 24.2-390
- rusiem-kb 24.2-638
- rusiem-tools 24.2-486
- rusiem-web 24.02-4.0.0-1760
- rvsiem-kernel 24.2-270

Рекомендуемые обновления для Astra Linux
- rusiem-frs 24.2-16
- rusiem-kernel 24.2-17
- rusiem-tools 24.2-128
- rusiem-kb 24.2-84
- rusiem-ls 24.2-28
- rusiem-web 24.2-4.0.0-44
- rvsiem-frs 24.2-14
- rvsiem-ls 24.2-17
- rvsiem-kernel 24.2-15

Обновления для операционных систем
- Ubuntu 22
- Ubuntu 18
- Astra Linux

Основное
- Новый дизайн (с возможностью переключения на старый)
- Переработанный раздел «Источники»
- Статические таблицы

Панель мониторинга
- Новый виджет «Гистограмма с накоплением»

Инциденты

• Массовое удаление инцидентов, сгруппированных по тенанту, по наименованию или по категории

Корреляция

• Оптимизация операторов для работы со статическими списками (inlist, notinlist и т.п.)
• Оптимизация уведомлений в telegram

Отчеты

• Доработка валидации, права доступа

Новые парсеры

• SNR
• ODBC
• Maipu
• Mate
• Modsecurity
• Laurel
• Ssecline

Доработанные парсеры

• Kerio
• Cisco
• OpenVPN
• Linux
• Windows
• UserGate
• Amazon
• Fortinet
• InfluxData
• Strongswan
• Synology
• Apache
• Freeradius
• Panda
• Ubiquiti
• Infowatch
• AuditD
• Squid
• Kaspersky
• Zyxel
• Arbor Networks
• Allied Telesis
• IBM
• SendMail
• Nagios
• Rusiem

- Cowrie
- D-link
- kubernetes
- Avaya
- Oracle
- Infotecs
- HPE
- Ideco
- Python
- Rt-solar
- VMware
- SecurityCode
- ElasticSearch
- NewSecurity
- Dovecot
- NextCloud
- RedHat
- Symantec
- T8
- Eltex
- SIGUR
- DrWeb
- Amavis
- Ossec
- Zimba
- BlueCoat
- PSQL
- Asus
- Sysco
- Etcd
- Cbr
- Docker
- Drupal
- Sophos
- Yandex
- Exim
- Abrt
- Caddy
- Cryptopro
- Haproxy
- PHP
- Rspamd
- Isimplelab