RELEASE NOTES ОТ 28 НОЯБРЯ 2024 Г.
RuSIEM 4.3.0

Обновления для операционных систем

• Ubuntu 18

- rusiem-analytics_21.0-294_amd64.deb
- rusiem-analytics-sa_21.0-294_amd64.deb
- rusiem-kb_24.11-1198-ubuntu18.04_all.deb
- rusiem-kernel_24.11-401-ubuntu18.04_amd64.deb
- rusiem-tools_24.11-543-ubuntu18.04_all.deb
- rusiem-web_24.11-4.3.0-2434.ubuntu18.04_all.deb
- rvsiem-kernel_24.11-282-ubuntu18.04_amd64.deb

• Ubuntu 22

- rusiem-analytics_21.0-295_amd64
- rusiem-analytics-sa_21.0-295_amd64
- rusiem-frs_24.11-27-ubuntu22.04_amd64
- rusiem-kb_24.11-1195-ubuntu22.04_all
- rusiem-kernel_24.11-25-ubuntu22.04_amd64
- rusiem-ls_24.11-36-ubuntu22.04_amd64
- rusiem-tools_24.11-544-ubuntu22.04_all
- rusiem-web_24.11-4.3.0-2435.ubuntu22.04_all
- rvsiem-frs_24.11-20-ubuntu22.04_amd64
- rvsiem-kernel_24.11-23-ubuntu22.04_amd64
- rvsiem-ls_24.11-34-ubuntu22.04_amd64

• Astra Linux

- rusiem-analytics_24.11-14-astra.0_amd64.deb
- rusiem-frs_24.11-25-astra.0_amd64.deb
- rusiem-kb_24.11-648-astra.0_all.deb
- rusiem-ls_24.11-47-astra.0_amd64.deb
- rusiem-tools_24.11-192-astra.0_all.deb
- rusiem-web_24.11-4.3.0-74-astra.0_amd64.deb
- rvsiem-frs_24.11-17-astra.0_amd64.deb
- rvsiem-ls_24.11-21-astra.0_amd64.deb

Основное

• Обогащение из статических таблиц
• Новый модуль Baseline

Инциденты

• Экспорт в файл формата json

События

• Многопоточная архивация

Отчеты

• Новый тип отчета «Статистика»

Списки и таблицы
- Обогащение из статических таблиц
- Обновление Rest API для управления таблицами

Агенты
- Модуль Redcheck

Аналитика
- Новый модуль Baseline

Новые правила корреляции (6 шт.)
- Iptables
- Windows
- Indeed
- UserGate
- Paloalto
- Auditd

Новые парсеры (10 шт.)
- Watchguard
- Spectrum
- Pcp
- Poligon
- Distkontrol
- Bastion-tech
- 3Com
- Extreme Networks
- Falcongaze
- Qtech

Доработанные парсеры (38 шт.)
- Kaspersky
- Windows
- Auditd
- Filelog
- Elastic
- Linux
- UserGate
- Kerio
- Qnap
- Nginx
- MikroTik
- Ideco
- Staffcop
- HPE
- Cryptopro
- PaloAlto

- Ossec
- Drweb
- Indeed
- SNR
- Cisco
- 1c-bitrix
- Fortinet
- Grafana
- Influxdata
- Etcd
- Python
- Multifactor
- Infotecs
- CommuniGate
- 1C
- Sonatype
- Perco
- Gitlab
- Hashicorp
- Isimplelab
- RedCheck
- CheckPoint