RELEASE NOTES ОТ 18 ИЮНЯ 2024 Г.
RuSIEM 4.1.0

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

Рекомендуемые обновления для Ubuntu 22
- rusiem-kb - 24.6-866
- rusiem-frs - 24.6-21
- rusiem-ls - 24.6-24
- rusiem-kernel - 24.6-21
- rusiem-tools - 24.6-511
- rusiem-web - 24.06-4.1.0-2045
- rusiem-analytics - 21.0-265
- rvsiem-frs - 24.6-17
- rvsiem-ls - 24.6-29
- rvsiem-kernel - 24.6-21

Рекомендуемые обновления для Ubuntu 18
- rusiem-analytics - 21.0-262
- rusiem-analytics-sa - 21.0-262
- rusiem-kb - 24.6-878
- rusiem-tools - 24.6-512
- rusiem-web - 24.06-4.1.0-2046
- rusiem-kernel - 24.6-396
- rvsiem-kernel - 24.6-276

Рекомендуемые обновления для Astra Linux
- rusiem-kb - 24.6-324-astra.0
- rusiem-frs - 24.6-17-astra.0
- rusiem-ls - 24.6-30-astra.0
- rusiem-tools - 24.6-141-astra.0
- rusiem-web - 24.6-4.1.0-59-astra.0
- rusiem-analytics - 24.6-11-astra.0
- rvsiem-frs - 24.6-15-astra.0
- rvsiem-ls - 24.6-18-astra.0

Основное
- Оптимизация нормализатора
- Оптимизация коррелятора
- Оптимизация модуля отчетности

Инциденты
- Уведомления в telegram для переоткрытых инцидентов

Взаимосвязи
- Запоминание последнего фильтра
- Улучшение отображения узлов

Нормализация
- Оптимизация потребления памяти

Корреляция
- Оптимизация функции подсчета уникальных значений

Таблицы и списки
- Постраничный поиск значений статического списка
- Сортировка значений таблиц
- Массовое удаление значений таблиц

Агенты
- Экспорт списка агентов и модулей
- Групповое управление агентами
- Шаблоны настроек модулей агентов

Отчеты
- Оптимизация генерации отчетов

Новый набор правил корреляции
- PowerShell
- Sysmon
- Rusiem IoC

Новые парсеры
- Indeed
- BDCom
- Ssec
- Aoavt
- Shtormtech
- Multifactor
- Kron
- SwordFish
- SearchInform
- CrushFTP
- OpenVAS
- Safib
- Xello
- Aide
- Zalando

- Cybertec-Postgresql
- Unlimited
- Grafana

Доработанные парсеры

- PostgreSQL
- Infotecs
- SolidSoft
- UserGate
- PulseSecure
- Ntop
- Linux
- Python
- Rusiem
- TrafficMonitor
- Ssecline
- Mikrotik
- Huawei
- Windows
- VmWare
- DrWeb
- S-Terra
- Cisco
- Fortinet
- Group-IB
- 1C
- RT-solar
- DHCP
- SecurityCode
- CheckPoint
- NetGate
- MSSQL
- Nmap
- Forcepoint
- Veem
- Kaspersky
- Etcd
- PHP
- Amavis
- Communigate
- Ideco
- Zecurion
- Proxmox
- Brocade
- PaloAlto
- Apache
- AuditD

- Ubiquiti
- Suricata
- Filelog
- Sophos
- OpenVPN
- Exim
- Haproxy