RUSIEM
Всё под контролем

RELEASE NOTES ОТ 21 НОЯБРЯ 2023 Г.
RuSIEM 3.11.0

Рекомендуемые обновления для Ubuntu 22
- rusiem-kernel - 23.11-15-ubuntu22.04
- rusiem-ls - 23.11-17-ubuntu22.04
- rusiem-frs - 23.11-15-ubuntu22.04
- rusiem-kb - 23.11-483-ubuntu22.04
- rusiem-web - 23.11-3.11.0-1586.ubuntu22.04
- rusiem-tools - 23.11-479-ubuntu22.04
- rvsiem-kernel - 23.11-16-ubuntu22.04
- rvsiem-ls - 23.11-24-ubuntu22.04
- rvsiem-frs - 23.11-15-ubuntu22.04

Рекомендуемые обновления для Ubuntu 18
- rusiem-kernel - 23.11-380-ubuntu18.04
- rusiem-kb - 23.11-480-ubuntu18.04
- rusiem-web - 23.11-3.11.0-1585.ubuntu18.04
- rusiem-tools - 23.11-478-ubuntu18.04
- rvsiem-kernel - 23.11-267-ubuntu18.04

Рекомендуемые обновления для Astra linux
- rusiem-kernel - 23.11-15-astra.0
- rusiem-ls - 23.11-25-astra.0
- rusiem-frs - 23.11-15-astra.0
- rusiem-kb - 23.11-32-astra.0
- rusiem-web - 23.11-3.11.0-43-astra.0
- rusiem-tools - 23.11-3.11.0-43-astra.0
- rvsiem-kernel - 23.11-13-astra.0
- rvsiem-frs - 23.11-13-astra.0
- rvsiem-ls - 23.11-14-astra.0

Основное
- RuAgent оптимизирован под нагрузку
- Разработан модуль сбора событий ODBC

Агент
- Оптимизирован модуль FTP Log
- Доработан модуль АПКШ континент
- Повышена стабильность модуля postgresql

Отчеты
- Доработаны отчеты по задачам инцидентов
- Доработаны отчеты по инцидентам

Настройки

- Доработана авторизация по LDAP

Микросервисы

- Оптимизирован коррелятор
- Повышена стабильность нормализатора
- Добавлена возможность удаления конфигураций

Доработаны парсеры

- VMware
- Kaspersky
- Linux
- PSQL
- Zabix
- CheckPoint
- Windows
- S-terra
- Huawei
- Suricata
- Oracle
- HPE
- Usergate
- SecurityCode
- D-link
- Moxa
- Dell
- Avaya
- Juniper
- Mikrotik
- Ideco
- ClearSwift
- Communigate
- Zyxel
- ManageEngine
- Apache
- IIS
- Cisco
- NextCloud
- Staffcop
- Positive
- Infotecs
- AuditD
- Nginx
- Courier-MTA
- PaloAlto
- Rusiem
- Eltex

- Filelog (IIS)
- Atlassian
- A-real
- Brocade
- Gamma
- Eset

Новые парсеры

- SolidSoft
- Bolid Orion
- Exim
- Courier-mta
- CyberProtego
- Echelon (Scaner-VS)
- Tripwire (enterprise)
- DejaVU (engine)
- Isimplelab
- Qnap (nas
- F5 (ASM)
- NSD (Transit2.0)
- Proxmox (PVE)