RELEASE NOTES ОТ 26 МАРТА 2025 Г.
RuSIEM 4.4.0

Обновления для операционных систем

UBUNTU 22
- rusiem-kb | 25.3-1444
- rusiem-tools | 25.3-565
- rusiem-web | 25.03-4.4.0-2626
- rusiem-ls | 25.3-39
- rvsiem-ls | 25.3-35

Astra 1.7
- rusiem-kb | 25.3-893-astra.0
- rusiem-web | 25.3-4.4.0-82-astra.0
- rusiem-ls | 25.3-48-astra.0
- rvsiem-ls | 25.3-23-astra.0

Debian 12 – UBUNTU 22 – Astra 1.8
- rusiem-kb | 25.3-342-all
- rusiem-web | 25.3-4.4.0-15-all
- rusiem-ls | 25.3-7-all
- rvsiem-ls | 25.3-3-all

Основное
- **Linux агент**
- Корреляция. Оптимизация счетчиков и триггеров
- Аналитика. Оптимизация и исправление модуля

Источники
- Оптимизация изучения источников

Инциденты
- Динамические названия и описания инцидентов

Агент
- Linux агент с модулями
  - FTP Log
  - File Log
  - MSSQL Server Log
  - MySQL Log, ODBC
  - Oracle Server
  - PostgreSQL Log
  - АПКШ Континент 3.x
  - SSH
  - Telnet

Экспорт/импорт

• YAML: парсеры, симптомы, правила обогащения, правила корреляции.

Rest API

• информация о лицензии

Аналитика

• Оптимизация и исправление модуля

Новые правила корреляции

- 36 правил корреляции и 52 правила симптоматики Dr.Web
- 14 правил корреляции и 90 правил симптоматики SwordFish AppSecHub (14 правил и 90 симптомов)
- 11 правил корреляции HPE
- 2 правила корреляции Kaspersky KESL
- 2 правила корреляции MITRE

Новые парсеры

• Cyberprotect
• Commvault
• Forcepoint
• Jetbrains
• Stakhanovets
• Telekom
• Avsoft
• Ruijie
• Authelia
• Bi.zone

Доработано парсеров: 54 шт.