RELEASE NOTES ОТ 24 ОКТЯБРЯ 2021 Г.

RuSIEM 3.3.0

Рекомендуемые обновления для Ubuntu 18

rusiem-analytics_21.0-165
rusiem-analytics-sa_21.0-165
rusiem-database_18.21.0-29
rusiem-kb_18.21.4-47
rusiem-kernel_18.21.4-118
rusiem-tools_21.5-61
rusiem-web_18.21.10-3.3.0-254
rvsiem-kernel_18.21.4-91

Доработки

- симптоматика - https://docs.rusiem.tech/sections/307
- полностью переработанный интерфейс
- новый конструктор симптомов
- оптимизация и повышение производительности
- добавление возможности обогащения событий

Агент

- Новый модуль сбора информации об активе - "System Info". https://docs.rusiem.tech/sections/299
- Оптимизация работы ioc агента
- Оптимизация модуля FileLog
- Обработка событий EventLog с некорректной датой
- Поддержка Win7 модулем NetStat

Аналитика - Активы

- Скрипты для автозагрузки активов https://docs.rusiem.tech/sections/321
- Скрипты для автозагрузки уязвимостей
- Оптимизация раздела просмотра активов
- Обогащение активов из событий модуля агента "System Info" https://docs.rusiem.tech/sections/266
- Автосоздание активов при установленном агенте https://docs.rusiem.tech/sections/266

Система

- Оптимизация обработки событий NetFlow
- Обновлена база Geo данных
- Выгрузка правил корреляции на другие ноды
- Доработка выгрузки парсеров на другие ноды

Дашборды

- Оптимизация страницы отображения виджетов
- Новый виджет с последними инцидентами

Инциденты

- Возможность создания инцидентов вручную
- Доработка раздела ГосСопка

Корреляция
- Функционал расписаний запуска правил корреляций
https://docs.rusiem.tech/sections/305
- Новый блок действий, выполняющийся после условий
https://docs.rusiem.tech/sections/304
- Доработка выполнения скриптов с передачей параметров
https://docs.rusiem.tech/sections/280

Архивация
- Повышение производительности JSON-архивации

Источники
- Модуль для подключения 1С 8.3 https://docs.rusiem.tech/sections/302

Доработаны парсеры
- Bastion
- Juniper
- MSSQL Kaspersky
- Kaspersky syslog
- Windows
- Dallas Lock 8.0
- Suricata
- Yum
- FortiNet
- Linux (systemd-timesyncd,snmpd,sudo,pam)
- Monit
- Ruagent
- Windows Defender
- Apache
- IIS - форматы NCSA, IIS
- postfix

Новые парсеры
- Trend Micro
- 1C syslog (CEF format)
- CentOS
- Red Hat IDM (freeIPA)
- Sophos XG Firewall SFVH
- Sophos Antivirus

Подробное описание
https://rusiem.com/ru/company/pressroom/news/rusiem_release_330?utm_source=news-25-10&utm_medium=Email