ВАШ ГАРАНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Руководство по установке

Системы сбора и анализа событий информационной безопасности «SAVA»

Установка Системы сбора и анализа событий информационной безопасности «SAVA» (далее-«Система»)

Процесс установки состоит из 4 этапов:

1. Установка всех зависимостей Системы по распределённым серверам (илина один сервер) в соответствии с расчётом нагрузки. Обязательными для установки являются Python 3.10, Elasticsearch и RabbitMQ. Остальные компоненты автоматически подтянутся при первом запуске Системы.
   - https://www.elastic.co/guide/en/elasticsearch/reference/current/install-elasticsearch.html
   - https://www.rabbitmq.com/download.html
   - https://www.python.org/downloads/release/python-3100/
2. Скачивание архива с дистрибутивом Системы по ссылке (ссылка) и распаковка. Переходим в директорию распаковки и переименовываем файл «.env.sample» в «.env»,а файл«sample.docker-compose.yml» в «docker- compose.yml»
3. Запуск пакета контейнеров через команду «docker-compose up» из директории распакованного архива
4. Настройка доступа к источникам событий информационной безопасности (клиент syslog, доступ к интерфейсам получения логов, доступ к файлам логов)