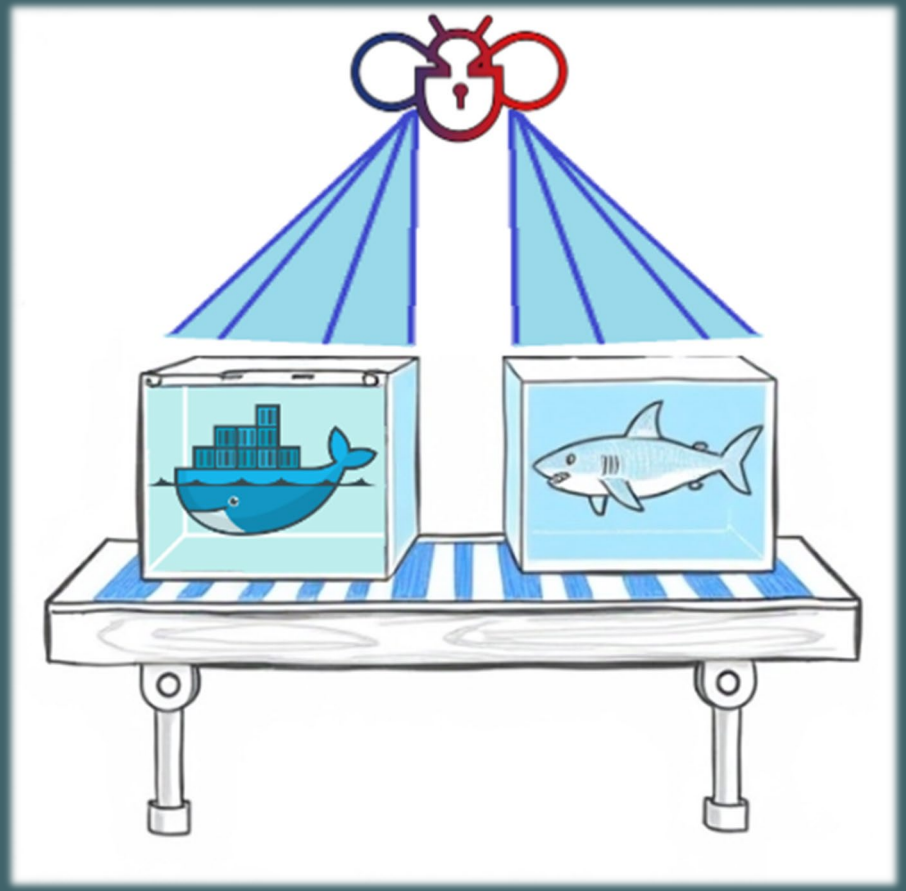
Разработка инструмента оценки безопасности приложений и информационных систем



Презентация разработанного командой «5HM3L» инструмента оценки защищенности средств контейнеризации

Проблематика

Для реализации задачи обеспечения автоматизированной проверки средств контейнеризации разработан текущий инструмент, который решает следующие задачи поиска уязвимостей:

1. OS Vulnerabilities – в базовом образе и системных пакетах, включенных в этот образ;
2. Dependencies – уязвимости в сторонних зависимостях;
3. Software Vulnerabilities – уязвимости непосредственно в коде приложений, которые запускаются в контейнерах.

Описание инструмента

Разработанный инструмент получает на вход путь контейнеру или архиву с кодом, производит его анализ и возвращает отчет о найденных уязвимостях в контейнере или программном коде.

Технические требования и ограничения

1. Для работы инструмента используется только открытый по лицензиям стек технологий;
2. Работа инструмента подтверждена в среде отечественной операционной системы (Astra Linux 1.7);
3. Для работы конечного пользователя реализован минималистичный, дружелюбный интерфейс в виде утилиты командной строки для ввода данных и получения отчетов.

Благодаря проработанной архитектуре, чистому коду, использованию подходов GitOps и преднастроеным автотестам реализована возможность гибкого горизонтального масштабирования, а также интеграции с существующими системами или добавление дополнительных функциональных блоков.

Краткое описание работы инструмента

1. Принимает на вход путь к локальному файлу с контейнером в архиве .tar или название образа (поддерживается табуляция при указании образа с Docker Hub).
2. Сохраняет получаемые данные в локальном S3-хранилище, а задание на проверку помещается в брокер сообщений.
3. После проверки выводится отчет о найденных уязвимостях в образе, а также формируется список файлов с указанием версий.

Все необходимые для работы инструмента компоненты автоматически разворачиваются и настраиваются. Внедрение инструмента сводится к его развертыванию, выполняемому "одной командой".

Руководство для работы пользователя и администратора оформлено в виде отдельного документ

«Подготовительные процедуры и руководство по эксплуатации».

Спасибо за ознакомление!