Версия документа: 003-2024

Инструкция по установке системы «ASPM Platform»

Москва, 2024

Содержание

1. Аннотация 3

2. Общие сведения 4

2.1 Назначение и краткая характеристика системы 4

3. Аппаратные и программные требования 6

3.1 Аппаратные требования 6

3.2 Программные требования 6

4. Развертывание платформы 7

4.1 Проверка доступа к хранилищу образов (Docker Images) 7

4.2 Подготовка к установке 7

4.3 Развертывание платформы 7

5. Остановка, перезапуск и обновление платформы 9

5.1 Остановка платформы 9

5.2 Перезапуск платформы 9

5.3 Обновление платформы 10

1. Аннотация

Данный документ представляет собой подробную инструкцию по развёртыванию платформы ASPM Platform. Эта инструкция предназначена для специалистов, выполняющих установку данной платформы.

Для успешного развёртывания платформы ASPM Platform необходимо выполнить ряд шагов, которые подробно описаны в данном документе. Эти шаги включают в себя подготовку к установке, установку программного обеспечения, настройку параметров безопасности и тестирование работы платформы.

После выполнения всех шагов, описанных в инструкции, платформа ASPM Platform будет готова к использованию. Она обеспечит высокий уровень защиты информации и позволит предотвратить несанкционированный доступ к данным.

Важно отметить, что установка и настройка платформы ASPM Platform требует определённых знаний и навыков. Поэтому перед началом работы с этим документом рекомендуется ознакомиться с основами работы с информационными системами и безопасностью данных.

2. Общие сведения

2.1 Назначение и краткая характеристика системы

ASPM Platform (далее – платформа, система) позволяет проводить комплексный анализ приложений для обеспечения безопасности и централизованного управления процессами обнаружения и устранения уязвимостей. Платформа обеспечивает взаимодействие между командами разработки и специалистами по безопасности, способствуя совместному выявлению и устранению уязвимостей на всех этапах жизненного цикла продукта.

Платформа поддерживает работу со следующими классами решений:

- SAST;
- IAC;
- OSA;
- SCA;
- DAST;
- API fuzzing;
- BCA.

Сканирование продукта включает в себя 4 ключевых этапа:

a) Настройка и запуск анализа. На этом этапе производится конфигурация инструментов и автоматический запуск анализа приложения.

b) Агрегация и корреляция данных. По результатам проведенного анализа данные централизованно собираются в едином репозитории для последующей обработки. Далее платформа осуществляет корреляцию уязвимостей, выявленных на разных уровнях анализа, что помогает определить взаимосвязи между ними и их совокупное влияние на безопасность приложения.

c) Оценка рисков и генерация рекомендаций. Платформа предоставляет интерфейс для обработки найденных уязвимостей, осуществляет замену исходных данных значениями, соответствующими заданным правилам из внутренней базы, обеспечивая единый механизм оценки и управления уязвимостями.

d) Создание отчетов и интеграция с другими системами. Платформа автоматически формирует отчеты о результатах проведенного анализа, выявленных уязвимостях и предложенных мерах по их устранению.

В результате система позволяет не допустить включения в состав разрабатываемых приложений уязвимых компонентов, исключить использование уязвимого функционала, определить ошибочную и вредоносную программную логику.

3. Аппаратные и программные требования

3.1 Аппаратные требования

Рекомендуемые системные требования платформы (до 1000 веток), представлены в таблице №1.

Таблица №1 - Системные требования платформы (до 1000 веток)

Параметр	Минимальное значение
Количество ядер процессора	8
Частота процессора	2.4
ОЗУ, Гигабайт	16
Емкость локальных дисков, Гигабайт	2000

Рекомендуемые системные требования платформы (более 1000 веток), представлены в таблице №2.

Таблица №2 - Системные требования платформы (более 1000 веток)

Параметр	Минимальное значение
Количество ядер процессора	10
Частота процессора	2.4
ОЗУ, Гигабайт	20
Емкость локальных дисков, Гигабайт	6000

3.2 Программные требования

Рекомендуемые минимальные требования к операционным системам (ОС) представлены в таблице №3.

Таблица №3 – Требования к ОС

Параметр	Минимальное значение
Операционная система	Astra Linux версии 2.12 или Ubuntu 22.04 и выше или Debian 11 и выше

Внимание: в данной системе используются контейнеры Docker, и она привязана к файловой системе хоста. Категорически не рекомендуется удалять тома Docker (docker volumes), поскольку это может привести к потере всех данных системы.

4. Развертывание платформы

4.1 Проверка доступа к хранилищу образов (Docker Images)

Для получения Docker образов, являющихся составляющими платформы, необходим доступ к их хранилищу (https://update.arx-security.ru). Проверить его можно при помощи команды «curl update.arx-security.ru». При возникновении проблем с доступом к репозиторию образов обратиться в Техническую поддержку по почте support@arx-security.ru.

4.2 Подготовка к установке

Для развертывания платформы ASPM Platform необходимо выполнить следующие подготовительные этапы (некоторые из них могут быть пропущены, если необходимые пакеты уже установлены):

1. Убедиться, что на хосте установлен Docker и Docker Compose необходимых версий (указаны выше)
2. Учетная запись пользователя ОС имеет root права
3. Имеется более 100 гигабайт свободного дискового пространства

Чтобы развернуть платформу, необходимо чётко следовать инструкции. Команды должны быть выполнены без ошибок. Если у вас возникли проблемы, обратитесь в Техническую поддержку по почте support@arx-security.ru .

4.3 Развертывание платформы

Для установки платформы ASPM Platform следуйте следующим шагам:

1. Скопируйте необходимые файлы (скрипты и файл окружения) на сервер. Это можно сделать, используя следующие инструменты SCP (Secure Copy Protocol) или FTP (File Transfer Protocol). Пример с использованием SCP:

```
scp -r path/to/folder/w/scripts
```

`user@host:/folder_with_scripts`, где `path/to/folder/w/scripts` - путь к директории со скриптами на локальной машине, `user` - пользователь, под которым выполняется администрирование удаленной машины, `host` - адрес удаленной машины, `folder_with_scripts` - конечная директория копирования.

2. При помощи SSH произведите подключение к удаленному серверу. Пример `ssh user@host`, где `user` - пользователь, под которым выполняется администрирование удаленной машины, `host` - адрес удаленной машины.

3. Перейдите директорию, в которую произвели копирование в первом шаге. Пример `cd folder_with_scripts/`.

4. Проверьте что у всех скриптов есть право на выполнение. Пример `ls -la`, права файлов должны быть вида `-rwxr-xr-x`.

5. Для запуска платформы выполните соответствующий скрипт от имени администратора. Пример `sudo ./run.sh`.

5. Остановка, перезапуск и обновление платформы

5.1 Остановка платформы

Для остановки платформы ASPM Platform следуйте следующим шагам:

1. При помощи SSH произведите подключение к удаленному серверу. Пример `ssh user@host`, где `user` - пользователь, под которым выполняется администрирование удаленной машины, `host` - адрес удаленной машины.
2. Перейдите директорию, в которую произвели копирование скриптов при установке. Пример `cd folder_with_scripts/`.
3. Для остановки платформы выполните соответствующий скрипт от имени администратора. Пример `sudo ./stop.sh`.

5.2 Перезапуск платформы

Для перезапуска платформы ASPM Platform следуйте следующим шагам:

1. При помощи SSH произведите подключение к удаленному серверу. Пример `ssh user@host`, где `user` - пользователь, под которым выполняется администрирование удаленной машины, `host` - адрес удаленной машины.
2. Перейдите директорию, в которую произвели копирование скриптов при установке. Пример `cd folder_with_scripts/`.
3. Для перезапуска платформы выполните соответствующий скрипт от имени администратора. Пример `sudo ./restart.sh`.

5.3 Обновление платформы

Для обновления платформы ASPM Platform следуйте следующим шагам:

1. При помощи SSH произведите подключение к удаленному серверу. Пример `ssh user@host`, где `user` – пользователь, под которым выполняется администрирование удаленной машины, `host` - адрес удаленной машины.
2. Перейдите директорию, в которую произвели копирование скриптов при установке. Пример `cd folder_with_scripts/`.
3. Для перезапуска платформы выполните соответствующий скрипт от имени администратора. Пример `sudo ./update.sh`.
4. Что бы запустить платформу выполните соответствующий скрипт от имени администратора. Пример `sudo ./run.sh`.

Важно заметить, что при выполнении скрипта `./update.sh` обновятся все образы (Docker images) платформы.