Автоматизированный программный комплекс выявления уязвимостей, разрабатываемого ПО с элементами машинного обучения, статического, динамического и компонентного анализа (Дерсканер)

Инструкция по установке и обновлению системы

Аннотация

Настоящий документ представляет собой руководство по установке и обновлению Автоматизированного программного комплекса выявления уязвимостей, разрабатываемого ПО с элементами машинного обучения, статического, динамического и компонентного анализа (Дерсканер). Документ предназначен для интеграторов и системных администраторов Дерсканер и содержит описание процедур установки и обновления комплекса.

Общая информация по установке

Дистрибутив Дерсканер поставляется в виде связанных компонентов. Для корректной работы требуется последовательно установить необходимый набор компонентов, соответствующих лицензии.

- **APP** компонент - веб-приложение, отвечает за логику работы всей системы (обязательный);
- **SAST** компонент - статический анализатор (опциональный);
- **DAST** компонент - динамический анализатор Web приложений (опциональный);
- **SCA** компонент - анализатор состава программного обеспечения (опциональный);
- **Агенты C/C++/Objective-C** - статические анализаторы для анализа языков C/C++/Objective-C со сборкой в окружениях Windows, macOS (опциональны);
- **Builder** компонент - сервис по сборке Java/Scala/Kotlin проектов из исходного кода в специализированном клиентском окружении для дальнейшей передачи собранного артефакта SAST компоненту (опциональный).

Каждый компонент из списка, включая **APP/SAST/DAST/SCA**, поставляется с собственным окружением, представленным в виде системы контейнеризации и инструмента для автоматизированного сбора лог-файлов системы - **log-bringer**.
Агенты C/C++/Objective-C поставляются с окружением jdk-11 для Windows или macOS.
Builder поставляется с окружением jdk-11 для Linux.

Требования к серверу для базовых компонентов
В большинстве дистрибутивов данные требования соблюдаются по умолчанию.

- Для обеспечения оптимальной производительности и стабильности рекомендуется выполнять установку на чистую операционную систему;
- Отсутствие установленных систем контейнеризации;
- Отсутствие ограничений для работы систем контейнеризации;
- Версия ядра Linux 3.10 или выше, поддерживаются только generic ядра; рекомендуется использовать последнюю версию ядра;
- Версия *iptables* 1.4 или выше;

- Версия *git* 1.7 или выше;
- Версия *XZ Utils* 4.9 или выше;
- Исполняемый файл *ps*, предоставляемый *procps* или аналогичным пакетом.

Поддерживаются следующие дистрибутивы

- Ubuntu 20.04
- Ubuntu 22.04
- Ubuntu 24.04
- Debian 12
- CentOS 7
- AlmaLinux 8
- Red Hat Enterprise Linux 8
- Red Hat Enterprice Linux 9

Замечания

- Дистрибутив Дерсканер может быть сконфигурирован на одном или нескольких узлах. Конфигурация дистрибутива Дерсканер на нескольких узлах требует выполнения следующих условий:
  APP компонент устанавливается один раз и не реплицируется на другие узлы.
- Опциональные компоненты - **SAST**, **DAST**, **SCA**, **Агенты C/C++/Objective-C**, **Builder** могут быть реплицированны на любое количество узлов.
  При установке нескольких компонентов на одном узле минимальные требования суммируются.

Минимальные характеристики оборудования

Требования к конфигурации объема дискового пространства

Корректная работа дистрибутива требует соблюдения одного из следующих условий при разбиении диска:

- Объем всего диска выделяется на корневую директорию **(/)**;
- При специфическом дисковом разбиении на директорию **/opt** необходимо выделить не менее 90% от требуемого дискового пространства для каждого компонента.

В ходе эксплуатации продукта в зависимости от использования, через некоторое время может потребоваться расширение дискового пространства.

Для установки на одном узле

Для функционирования Дерсканер с компонентом статического анализа (**APP+SAST**) на одном узле требуется оборудование со следующими минимальными характеристиками:

- 8 cores CPU 2.2GHz;
- 32 GB RAM;
- 512 GB SSD/SAS HDD.

Для функционирования Дерсканер с компонентами статического и динамического анализа (**APP+SAST+DAST**) на одном узле требуется оборудование со следующими минимальными характеристиками:

- 10 cores CPU 2.2GHz;
- 40 GB RAM;
- 512 GB SSD/SAS HDD.

Для функционирования Дерсканер со всеми подключенными компонентами (**APP+SAST+SCA+DAST**) на одном узле требуется оборудование со следующими минимальными характеристиками:

- 12 cores CPU 2.2GHz;
- 64 GB RAM;
- 512 GB SSD/SAS HDD.

Для установки на разных узлах

APP

- 4 cores CPU 2.2GHz;
- 8 GB RAM;
- 512 GB SSD/SAS HDD.

SAST

- 4 cores CPU 2.2GHz;
- 32 GB RAM;
- 128 GB SSD/SAS HDD.

DAST

- 4 cores CPU 2.2GHz;
- 8 GB RAM;

- 128 GB SSD/SAS HDD.

SCA

- 4 cores CPU 2.2GHz;
- 16 GB RAM;
- 128 GB SSD/SAS HDD.

Компонент APP

Важно
Компонент используется в единственном экзмемпляре без возможности реплицирования.

Описание
Компонент обеспечивает логику работы системы и представление через веб-интерфейс.

Требования

- Привилегии root-пользователя;
- 4 cores CPU 2.2GHz;
- 8 GB RAM;
- 512 GB SSD/SAS HDD;
- Свободные TCP порты: 80, 443, 61616;
- Аппаратные ресурсы сервера, на котором развернут Компонент **APP** не должны изменяться, так как это приведет к изменению идентификатора лицензии;
- vMotion и любой другой функционал, который позволяет выполнять миграцию или изменение аппаратной части ВМ, должен быть отключён для узла компонента **APP**.

Установка/обновление

Важно
Перед обновлением компонента завершить все начатые сканирования в системе.
Время инициализации системы при обновлении зависит от размера базы данных и может занимать продолжительное время (в некоторых случаях до нескольких часов). При длительном процессе обновления для определения состояния системы рекомендуется воспользоваться файлом:
/opt/derscanner/app/services/backend/logs/derscanner_debug.log
Если последние актуальные данные в файле связаны с процессом запуска *changelogs*, это означает, что процесс инициализации выполняется корректно. В противном случае отправьте данный файл в службу технической поддержки.

1. Скачать и распаковать архив;
2. Открыть в терминале директорию распакованного архива;

3. Выполнить команду:

   ```
   sudo bash actions.sh
   ```

   и следовать инструкциям;

4. Перейти в браузере по адресу http://localhost или при доступности машины по сети извне по адресу http://installation_address
   с другого компьютера сети;

5. Во всплывающем окне для загрузки лицензии скопировать идентификатор установки и отправить его по почте для
   создания лицензии под конкретную инсталляцию;

6. Загрузить полученную лицензию через интерфейс;

7. Зайти в систему с учётными данными (требуется только при установке):
   логин - **admin**
   пароль - **r@78bJM=45**

8. Сменить пароль в разделе **Личный кабинет**;

9. Перейти в раздел **Настройки > Система > Правила** и загрузить описания правил **Rules.zip**, которые
   находятся в директории **/opt/derscanner/app**.

Лог установки/обновления располагается в файле
/var/log/derscanner/derscanner_app.log.

Компонент SAST

Описание
Компонент обеспечивает работу алгоритмов статического анализа. Может быть реплицирован на нескольких узлах.

Требования

- Привилегии root-пользователя;
- 4 cores CPU 2.2GHz;
- 32 GB RAM;
- 128 GB SSD/SAS HDD;
- При распределенной установке, сетевая доступность хоста с компонентом **APP**.

Установка/обновление

Важно

- Перед обновлением компонентом завершить все начатые SAST сканирования в системе;
- Компонент **APP** необходимо обновить до последней релизной версии.

1. Скачать и распаковать архив;
2. Открыть в терминале директорию распакованного архива;
3. Выполнить команду:

   ```
   sudo bash actions.sh
   ```

   и следовать инструкциям;
4. При установке компонента на узел, отличный от узла компонента **APP**, в файле **/opt/derscanner/core/sast/configs/daemon.env** требуется изменить значение поля *queueURI* на адрес узла с установленным компонентом **APP**, например:
   queueURI=tcp://192.168.1.10:61616
   После чего перезапустить службу компонента командой:

   ```
   sudo systemctl restart derscanner-sast.service
   ```

Лог установки/обновления располагается в файле ***/var/log/derscanner/derscanner_sast.log***.

Компонент DAST

Описание
Компонент обеспечивает работу алгоритмов динамического анализа. Может быть реплицирован на нескольких узлах.

Требования

- Привилегии root-пользователя;
- 4 cores CPU 2.2GHz;
- 8 GB RAM;
- 200 GB SSD/SAS HDD;
- При распределенной установке, сетевая доступность хоста с компонентом **APP**.

Установка/обновление

Важно

- Перед обновлением компонента завершить все начатые DAST сканирования в системе;
- Компонент **APP** необходимо обновить до последней релизной версии.

1. Скачать и распаковать архив;
2. Открыть в терминале директорию распакованного архива;
3. Выполнить команду:

   ```
   sudo bash actions.sh
   ```

   и следовать инструкциям;
4. При установке компонента на узел, отличный от узла компонента **APP**, в файле **/opt/derscanner/core/dast/configs/dast-daemon.env** требуется изменить значение поля *queueURI* на адрес узла с установленным компонентом **APP**, например:
   queueURI=tcp://192.168.1.10:61616
   После чего перезапустить службу компонента командой:

   ```
   sudo systemctl restart derscanner-dast.service
   ```

Лог установки/обновления располагается в файле ***/var/log/derscanner/derscanner_dast.log***.

Компонент SCA

Описание
Компонент обеспечивает анализ состава программного обеспечения. Может быть реплицирован на нескольких узлах.

Требования

- Привилегии root-пользователя;
- 4 cores CPU 2.2GHz;
- 16 GB RAM;
- 128 GB SSD/SAS HDD;
- При распределенной установке, сетевая доступность хоста с компонента **APP**.

Установка/обновление

Важно

- Перед обновлением компонента завершить все начатые SCA сканирования в системе;
- Компонент **APP** необходимо обновить до последней релизной версии.

1. Скачать и распаковать архив;
2. Открыть в терминале директорию распакованного архива;
3. Выполнить команду:

```
sudo bash actions.sh
```

и следовать инструкциям;

4. При установке компонента на узел, отличный от узла компонента **APP**, необходимо внести следующие изменения в конфигурационные файлы:

   - На узле с **SCA** компонентом в файле **/opt/derscanner/core/sca/configs/sca-daemon.env** требуется изменить значение поля *jms.url* на адрес узла с установленным компонентом **APP**, например:
     jms.url=tcp://192.168.1.10:61616
     После чего перезапустить службу компонентом командой:

```
sudo systemctl restart derscanner-sca.service
```

   - Перейти в раздел "*Настройки*" -> "*Система*" -> "*Общие*";

   - В поле "*Внешний адрес системы*" указать IP адрес/домен хоста компонента **APP**
     Например: http://192.168.1.10

Лог установки/обновления располагается в файле ***/var/log/derscanner/derscanner_sca.log***.

Компонент DerAI

Описание

Компонент **DerAI** предоставляет функции, основанные на искусственном интеллекте, такие как **DerCodeFix** и **DerTriage**.

DerAI — Компонент для работы с ИИ-инструментами, такими как DerCodeFix и DerTriage.

- **DerTriage** — это интеллектуальный инструмент Дерсканер для автоматической верификации результатов SAST анализа. После применения триажа уязвимости будут получат статус "Подтверждено ИИ" или "Отклонено ИИ".
- **DerCodeFix** — генератор исправлений, который использует код уязвимости, найденной SAST анализом, и его контекст для для формирования рекомендаций по её устранению. К Дерсканер может быть подключен облачный Компонент **DerAI** или Компонент, который развернут локально.

Дерсканер может подключаться к облачному или локально развернутому компоненту **DerAI**.

Требования

- Выделенный хост;
- Привилегии root-пользователя;
- Производитель видеопроцессора: NVIDIA

- Одна видеокарта, конфигурации с несколькими графическими процессорами не поддерживаются;
- Дискретный графический процессор NVIDIA, основанный на архитектуре Ada Lovelace или Hopper, с объемом памяти GDDR6 не менее 24 ГБ и поддержкой конфигурации с одним графическим процессором (минимально приемлемой видеокартой является NVIDIA RTX 4090 объемом 24 ГБ);
- Не менее 32 Gb GDDR6/GDDR7 GPU Memory (VRAM)
- Сетевая доступность хоста с компонентом **APP**;
- 4 cores CPU 2.2GHz;
- 8 GB RAM;
- 128 GB SSD/SAS HDD;
- Доступ в Интернет требуется только во время первоначальной установки драйверов NVIDIA. После первоначальной настройки сервис будет работать и получать обновления без необходимости активного подключения к Интернету;
- Свободный TCP порт: 10005;
- Сетевая доступность к сервису через порт 10005 с хоста компонентом **APP**;
- Доступ к базовым репозиториям дистрибутива.

Поддерживаемые дистрибутивы:

- Ubuntu 24.04
- Ubuntu 22.04
- Debian 12
- RHEL 9
- RHEL 8
- Rocky 9
- Rocky 8

Установка/обновление

1. Скачать и распаковать архив;
2. Открыть в терминале директорию распакованного архива;
3. Выполнить команду:

   ```
   sudo bash actions.sh
   ```

   и следовать инструкциям;

4. Подключить Компонент **DerAI** через пользовательский интерфейс:

- Перейти в раздел "*Настройки*" -> "*Система*" -> "*Общие*";
- В поле "*DerAI*" указать внешний IP адрес/домен хоста компонента **DerAI**
  Пример: http://192.168.1.50:10005

Важно
Компонент прослушивает все интерфейсы порта 10005.

Лог установки/обновления располагается в файле
/var/log/derscanner/derscanner_derai.log.

Компонент Builder

Описание
Компонент обеспечивает сборку *Java/Scala/Kotlin* проектов из исходного кода в специализированном клиентском окружении для дальнейшей передачи собранного артефакта **SAST** компонента..
Может быть реплицирован на нескольких узлах.

Требования

- Привилегии root-пользователя;
- Свободный TCP порт: 8080 (для установки по умолчанию);
- Сетевая доступность хоста с компонентом **APP**;
- Окружение, в котором успешно собирается *Java/Scala/Kotlin* проект.

Установка/обновление

Важно

- Перед обновлением Компонент **APP** необходимо обновить до последней релизной версии;
- После установки компонента *Builder* сервис будет работать по протоколу *HTTP*. Информация по настройке *Builder* агентов и изменение протокола на *HTTPS* описана в документе "Руководство администратора системы".

1. Скачать и распаковать архив;
2. Открыть в терминале директорию распакованного архива;
3. Выполнить команду:

   ```
   sudo bash actions.sh
   ```

   и следовать инструкциям;

4. Настоятельно рекомендуется изменить учетную запись для подключения к агенту по умолчанию. Инструкция описана в документе "Руководство администратора системы".

Лог установки/обновления располагается в файле
/var/log/derscanner/derscanner_builder.log.

Дополнительные агенты для компонента SAST

Описание
Агенты статического анализа. Установка агентов необходима, если требуется анализ кода, написанного на C/C++ со сборкой в окружении Windows x64 или анализ кода C/C++/Objective-C со сборкой в окружении macOS x64.

Компонент iccheck Windows

Требования

- OS Windows 10 x64/Windows 11 x64/Windows Server 2019 x64/Windows Server 2022 x64;
- 4 cores CPU 2.2GHz;
- 16 GB RAM;
- 128 GB SSD/SAS HDD;
- Привилегированный пользователь;
- Сетевое соединение с узлом компонента **APP**;
- Установленная Visual Studio или Microsoft Build Tools той же версии, на которой происходит сборка проекта;
- Отсутствие установленных Java-машин и переменных среды **%JAVA_HOME%**;
- Окружение, в котором успешно собирается проект для анализа.

Обращаем внимание на последнее требование: данный Компонент необходимо устанавливать на машину, на которой возможна полная автоматическая сборка анализируемого проекта.

Установка/обновление

Важно

- Перед обновлением компонента завершить все начатые SAST сканирования в системе;
- Компонент **APP** необходимо обновить до последней релизной версии.

1. Проверить сетевую доступность порта 61616 узла с компонентом **APP**;
2. Запустить установочный файл от имени администратора и внимательно следовать инструкциям.

Замечания:

- Анализатор управляется службой **derscanner-daemon**;
- Ключ **daemonThread** в **\%DERSCANNER_HOME\%\daemon\daemon.properties** регулирует количество одновременных задач для анализа; изменять его необходимо через добавление новой системной переменной среды **daemonThreads** со значением желаемого количества потоков, после чего перезапустить сервис анализатора **derscanner-daemon**;
- При запуске анализа C/C++ проектов из веб-интерфейса системы в настройках языков выберите опцию ”Windows”;
- Поддерживается анализ со сборкой для проектов Visual Studio и GNU CMake.

\newpage
Переменная **\%derscanner_HOME\%** — путь до директории системы Дерсканер, например: **C:\%derscanner**; **D:\sast\%DerScanner**; ...

Компонент iccheck macOS

Требования

- macOS bigsur x64 и выше + инструмент bear версии от 3.1.2 (возможно установить с помощью утилиты homebrew) при использовании функциональности «Межмодульный анализ»;
- 4 cores CPU 2.2GHz;
- 16 GB RAM;
- 128 GB SSD/SAS HDD;
- Права root;
- Сетевое соединение с узлом компонента **APP**;
- Наличие установленных Xcode, clang, cmake, cocoapods;
- Отсутствие установленных Java-машин и переменных среды **$JAVA_HOME**;
- Подготовленное окружение, в котором успешно собирается анализируемый проект;
- Выход в интернет, а также наличие установленных git и/или svn, при необходимости загрузки библиотек из внешних источников.

Обращаем внимание на последнее требование: данный Компонент необходимо устанавливать на машину, на которой возможна полная автоматическая сборка анализируемого проекта.

Установка

1. Скачать архив;
2. Извлечь содержимое в любую директорию и перейти в нее;
3. Открыть конфигурационный файл для редактирования *daemon/daemon.properties* и заменить переменную **${APP_MODULE_ADDRESS}** на домен/ip адрес компонента APP, а так же заменить *все вхождения* переменной **${ICCHECK_AGENT_HOME}** на абсолютный путь распакованной директории архива, например:

- **queueURI=tcp://${APP_MODULE_ADDRESS}:61616** заменить на **queueURI=tcp://10.10.10.10:61616**
- **workDir=${ICCHECK_AGENT_HOME}/files/d/** заменить на **workDir=/Users/user/derscanner_iccheck/files/d/**

1. В распакованной директории архива запустить из терминала: `_OpenJDK11/bin/java -jar daemon/daemon.jar_` - с данного момента управление консоли переходит к запущенному процессу демона.

Также можно установить службу с помощью гипервизора процессов **launchd**. Для этого в файле **analyzer-daemon.plist** необходимо заменить *все вхождения* переменной **${ICCHECK_AGENT_HOME}** на абсолютный путь распакованной директории архива.
При запуске анализа C/C++ проектов из веб-интерфейса системы в настройках языков выберите опцию "macOS".

Обновление

Важно

- Перед обновлением компонента завершить все начатые SAST сканирования в системе;
- Компонент **APP** необходимо обновить до последней релизной версии.

1. Убедиться в отсутствии активных задач у анализатора и завершить его процесс;
2. Сохранить копию конфигурационного файла **daemon/daemon.properties**;
3. Переименовать директорию с текущей версией анализатора для бэкапа;
4. Скачать архив;
5. Извлечь содержимое в желаемую директорию, так, чтобы имя совпадало с предыдущей версией, например:
   /Users/user/derscanner_iccheck/;
6. Перейти в директорию с распакованным архивом;
7. В случае полного совпадения ключей в старой и новой конфигурациях, перенести сохраненную копию **daemon.properties** в директорию **daemon/**;
8. В случае различия конфигураций, изменить настройки **daemon.properties** на корректные - проверить правильность значений всех ключей;

9. Запустить из терминала `_OpenJDK11/bin/java -jar daemon/daemon.jar_` - с данного момента управление консоли переходит к запущенному процессу демона;

10. При использовании службы процессов **launchd** сравнить файл **analyzer-daemon.plist** в распакованной директории с тем, что установлен в **launchd**, если есть различие в ключах, настроить новый файл для работы (заменить *все вхождения* переменной **${ICCHECK_AGENT_HOME}** на абсолютный путь распакованной директории архива) и использовать его в **launchd**.

Замечания

1. Обращаем ваше внимание, что начиная с версии **11.2**, система использует обновленный формат лицензий. В связи с этим лицензии, сформированные для старых версий, станут недействительными после обновления.
   Поэтому рекомендуем до начала обновления платформы выполнить следующие действия:

   - Выгрузите текущий файл лицензии через интерфейс системы: Администрирование > Лицензия > Выгрузить лицензию;
   - Направьте полученный файл лицензии ответным письмом;
   - После обработки запроса вам будет предоставлена лицензия в новом формате. После получения обновленного файла лицензии приступите к обновлению.

2. Подробную документацию по работе с системой можно найти на странице "*О продукте*" > "*Инструкция*".

3. Система использует технологию контейнеризации Docker и имеет привязку к файловой системе хоста в **/opt/docker/volumes/**. Ни в коем случае **не удаляйте тома docker** (docker volumes) - иначе вы потеряете все данные системы.

4. Не допускается внесение изменений в файлы ***.compose.yml**, так как при обновлениях они будут перезаписываться. Для изменения конфигурации необходимо вносить изменения в **.env** файлы, которые лежат в директории **configs** каждого компонента..

5. Анализ по ссылке из App Store доступен только через установку в облаке. Локально возможна загрузка в виде незашифрованного **.ipa**-архива, либо загрузка в виде исходных файлов Objective-C, при подключении и настройке агента на macOS.

6. Объём загружаемых файлов в Систему не должен превышать 1900 МБ.

7. Недопустимо реплицировать компоненты на одном узле.

8. Для автоматического сбора лог-файлов системы используйте установленную на узле утилиту **log-bringer**. Команда запуска: `_sudo log-bringer_`.F

Лицензия

Ее необходимо загрузить в UI инструмента после развертки.

Контакты поддержки

Для вопросов по установке и использованию ПО необходимо обратиться по телефону ниже или присылать запросы на электронную почту:

sales@dergrup.pro

+79939147652

В рабочие дни с 10 до 18.00.