

7 июня 2023 📍 Москва, МЦК ЗИЛ

БЕКОН²³

Первая в России конференция
по БЕзопасности КОНтейнеров и контейнерных сред

Distroless своими руками

Мокин Антон Юрьевич

SRE, Tinkoff



МОКИН АНТОН | SRE в AppSec

@ a.y.mokin@tinkoff.ru

**Зачем
Как**



Текущая ситуация

Варианты решения

Рецепты

Нюансы



Зачем

Потенциальные риски



DDOS

Использование уязвимостей для повышенного потребления ресурсов и/или отказа в обслуживании



Точка входа

Использование уязвимого контейнера как плацдарм для дальнейшего распространения по инфраструктуре



Botnet

Заражение контейнера для использования в качестве ноды сети botnet



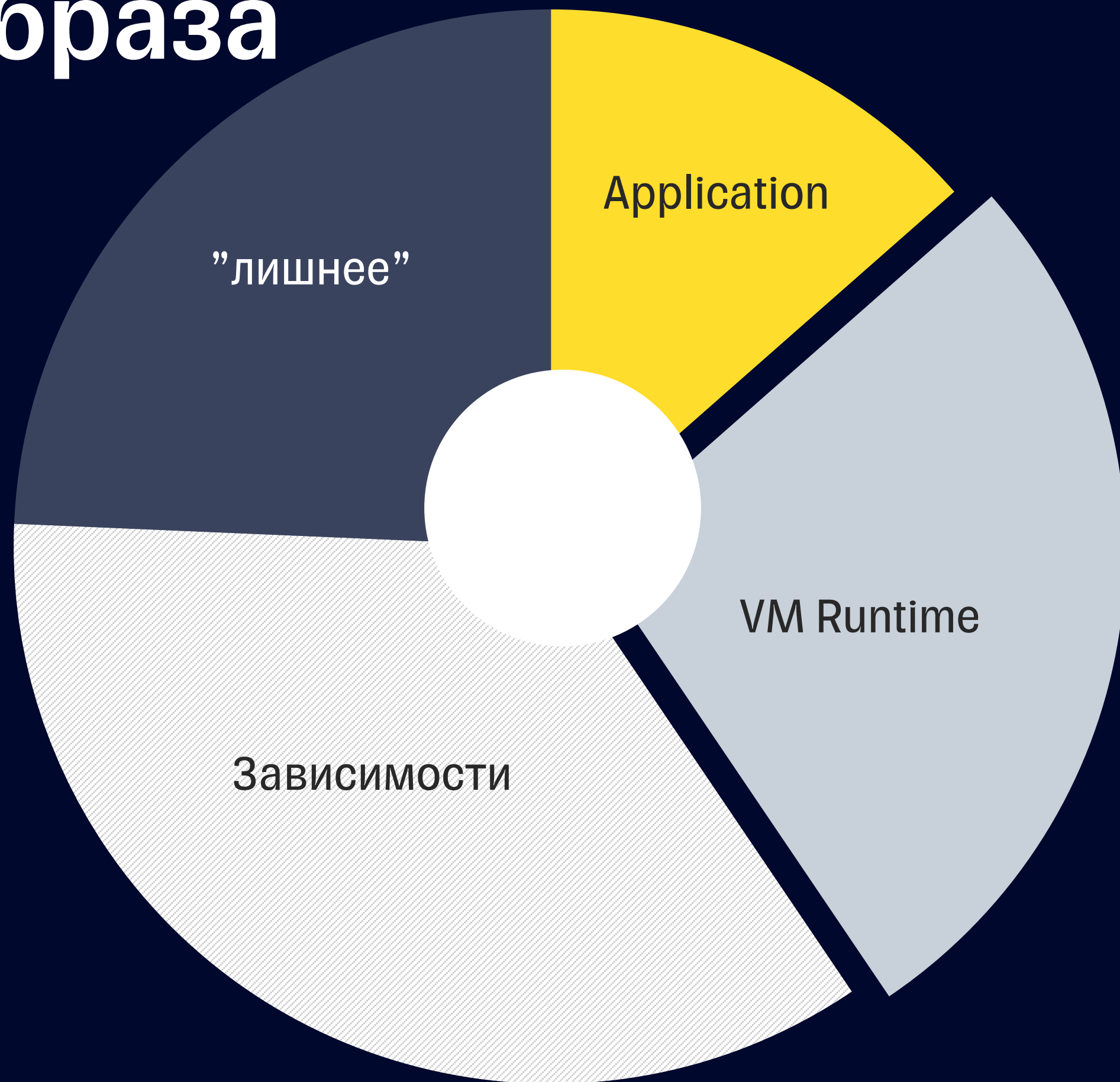
Перезапуск?

Образ с уязвимостями - ВСЕГДА с уязвимостями.

Содержимое образа



Содержимое образа



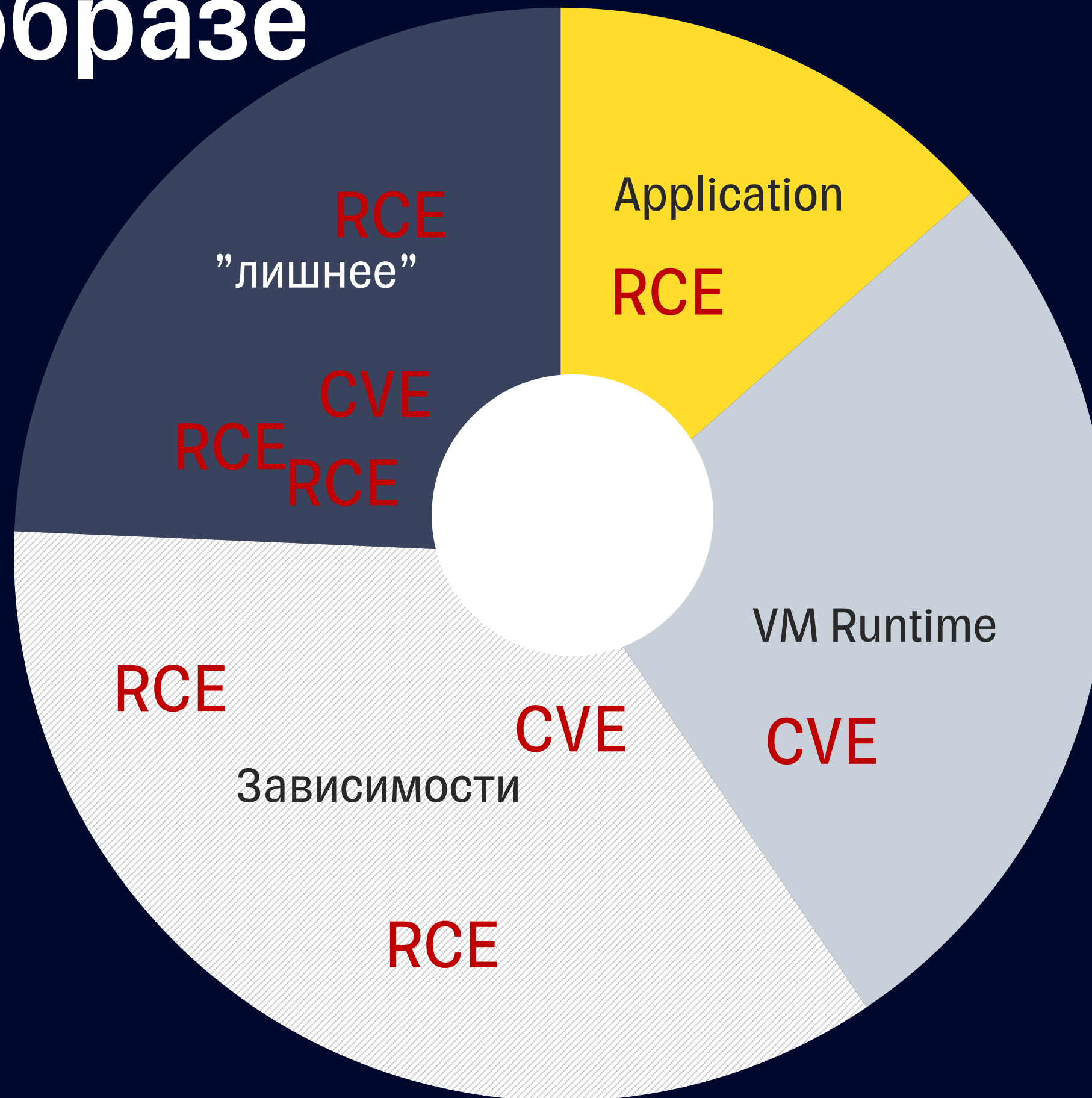
Содержимое образа



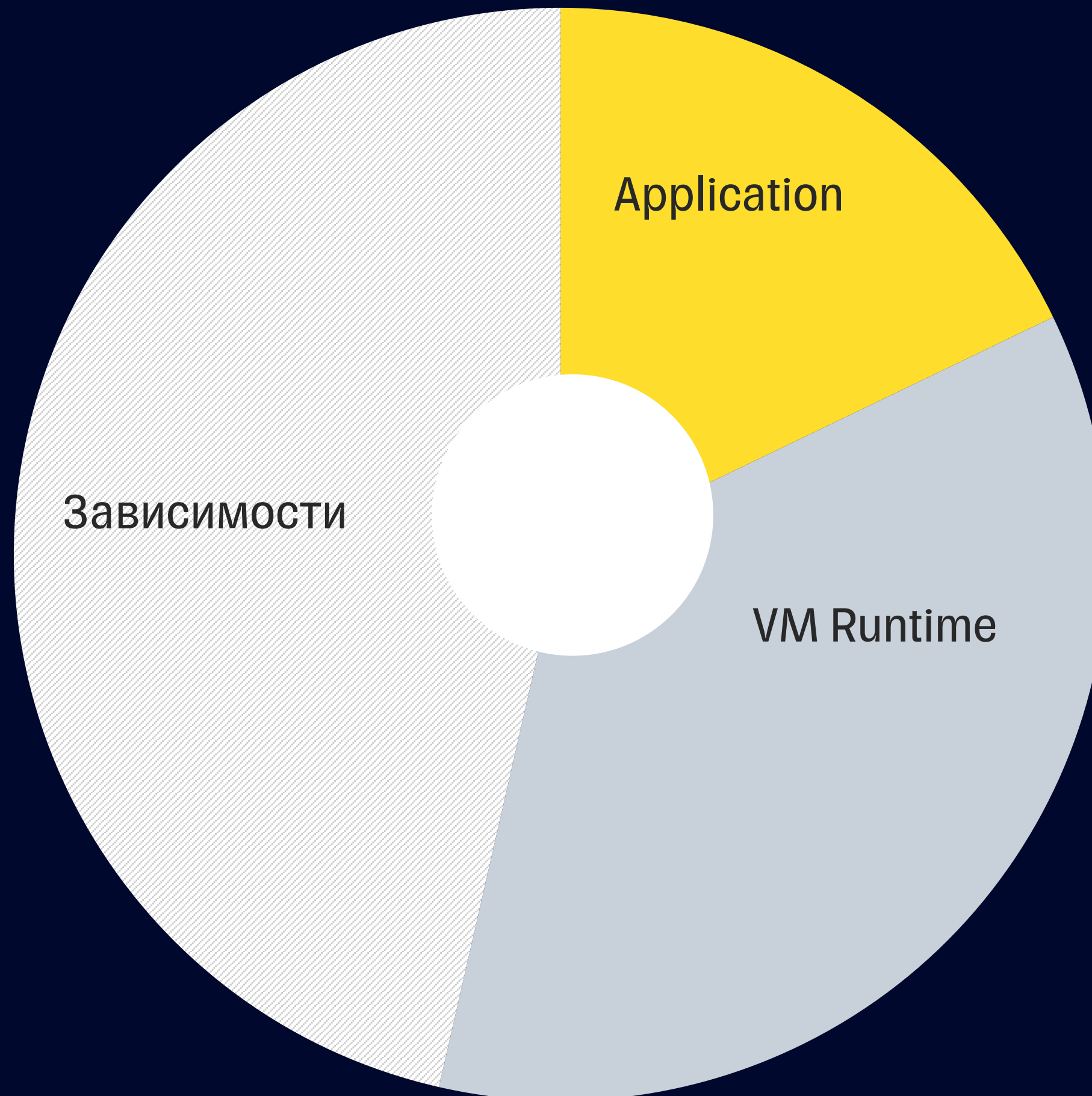
Содержимое образа



Уязвимости в образе



Distroless





**Что
делать**

Матрёшка



Static linked

CA-Certificates
locales
time-zones

glibc

Для приложений
требующих базовых
библиотек OS

Runtime

Для таких языков как
Java, Python, JS и т.д.

Application

Целевое приложение
разработанное
командой
организации и\или
дополнительное ПО

Матрёшка



Static linked

CA-Certificates
locales
time-zones

glibc

Для приложений
требующих базовых
библиотек OS

Runtime

Для таких языков как
Java, Python, JS и т.д.

Application

Целевое приложение
разработанное
командой
организации и\или
дополнительное ПО

Матрёшка



Static linked

CA-Certificates
locales
time-zones

glibc

Для приложений
требующих базовых
библиотек OS

Runtime

Для таких языков как
Java, Python, JS и т.д.

Application

Целевое приложение
разработанное
командой
организации и\или
дополнительное ПО

Матрёшка



Static linked

CA-Certificates
locales
time-zones

glibc

Для приложений
требующих базовых
библиотек OS

Runtime

Для таких языков как
Java, Python, JS и т.д.

Application

Целевое приложение
разработанное
командой
организации и\или
дополнительное ПО

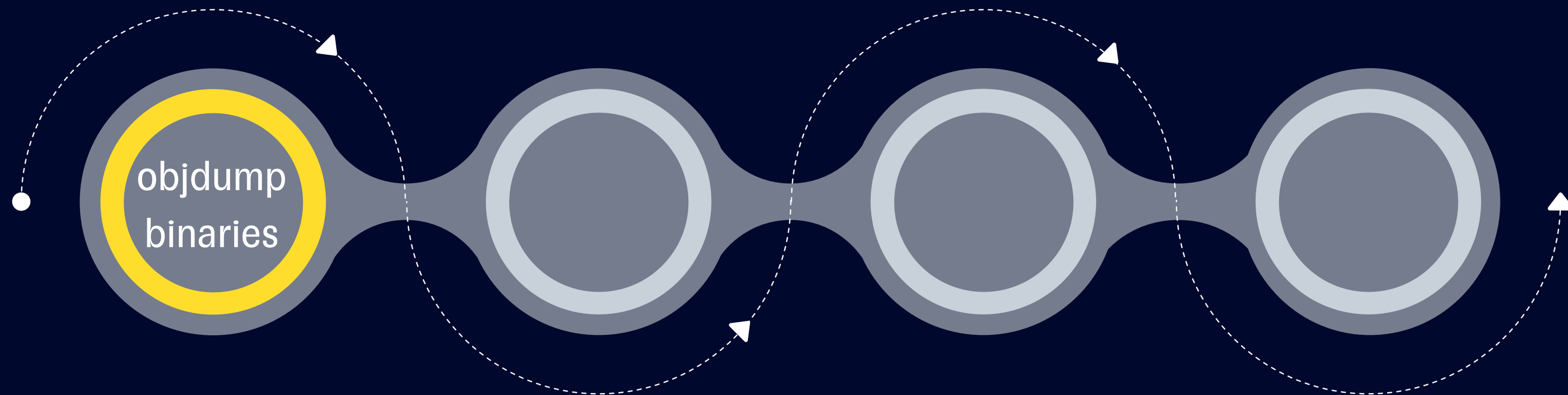
Сравнение различных distroless

Google (debian-11)	Chainguard (alpine)	Tinkoff (debian, ubuntu)
	▪ dotNet 7	▪ dotNet 6, 7 ▪ dotNet-deps 6, 7
▪ Java 11, 17	▪ Java 11, 17	▪ Java 11, 17, 18, 19
▪ Python 3.9	▪ Python 3.10	▪ Python 3.9, 3.10
▪ NodeJS 16, 18, 20	▪ NodeJS 14, 16, 18, 20	▪ NodeJS 19, 20
	▪ Nginx 1.25	▪ Nginx 1.18
	▪ PHP 8	▪ PHP 8
		▪ Haskell



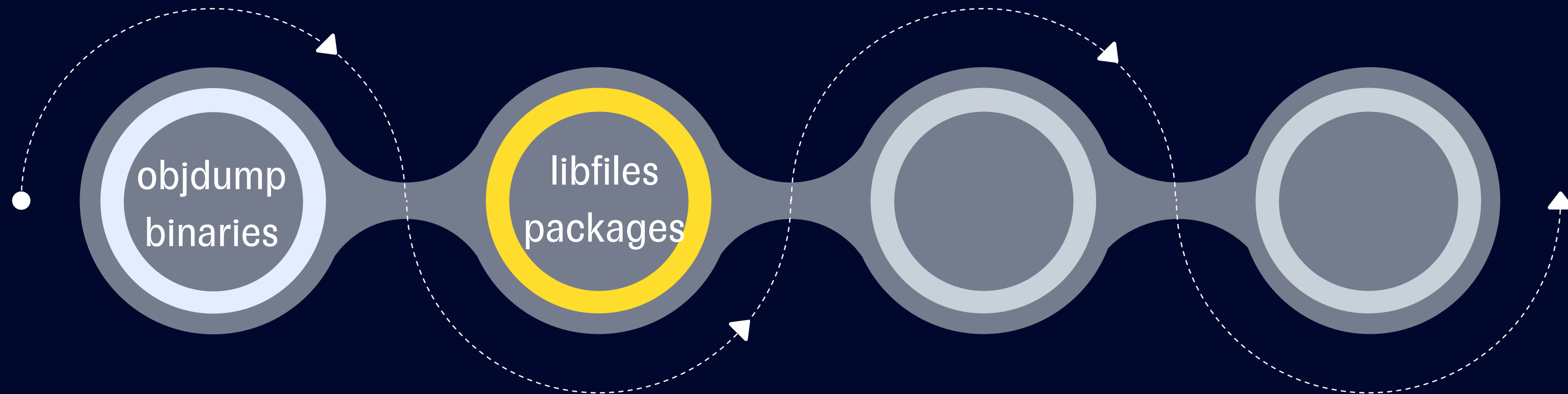
**Как
делать**

Подготовка зависимостей приложений



**Список
зависимостей**
Составление
зависимостей shared
libraries

Подготовка зависимостей приложений



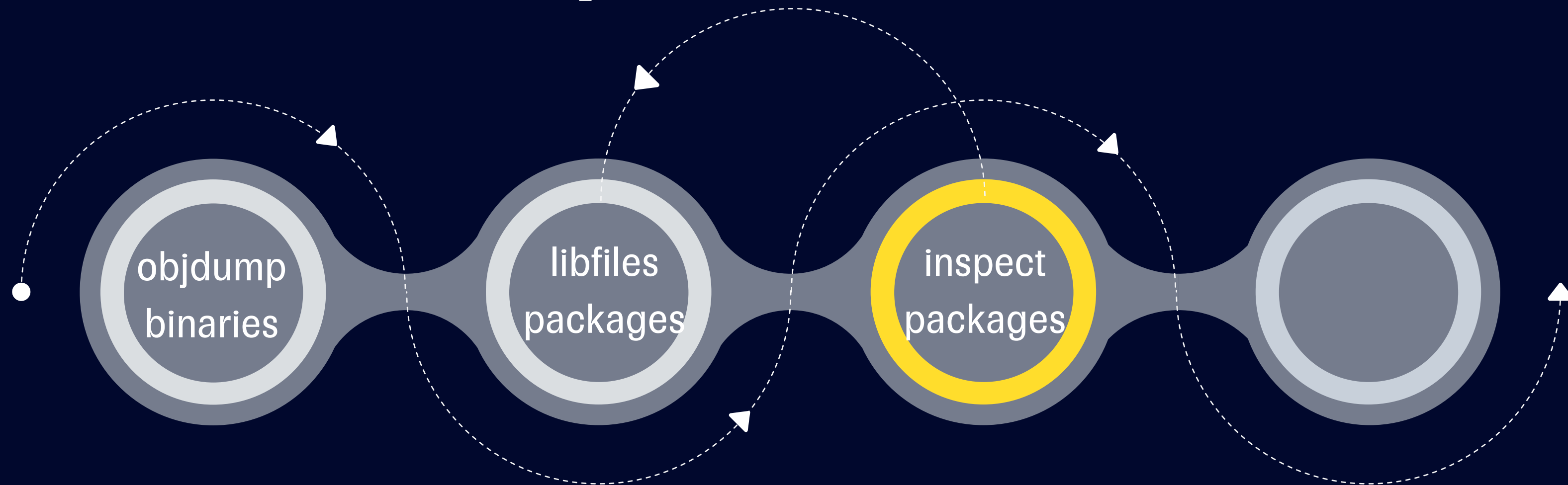
**Список
зависимостей**

Составление
зависимостей shared
libraries

**Определение
пакетов**

Составление списка
пакетов дистрибутива

Подготовка зависимостей приложений



Список зависимостей

Составление
зависимостей shared
libraries

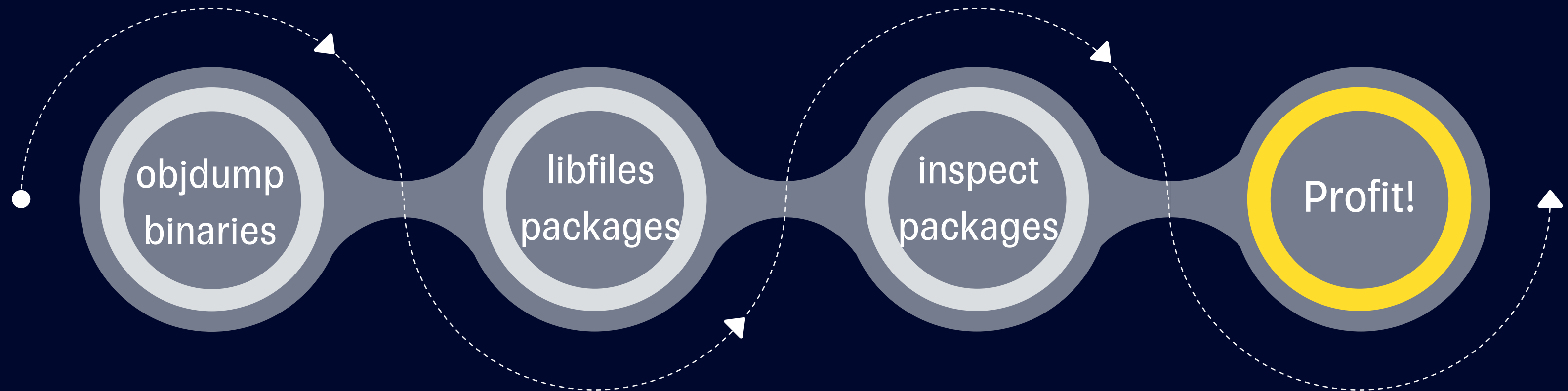
Определение пакетов

Составление списка
пакетов дистрибутива

Исследование пакетов

По содержанию
пакетов определяем их
зависимости

Подготовка списка пакетов



Список зависимостей

Составление
зависимостей shared
libraries

Определение пакетов

Составление списка
пакетов дистрибутива

Исследование пакетов

По содержанию
пакетов определяем их
зависимости

Конфиг файл

Описание пакетов их
версий и контрольной
суммы

Жесткое определение версий

```
...  
applicationName: "java",  
packages:  
  runtime: [...],  
  cica: [...]  
versions:  
  - version: "19",  
    packages:  
      runtime:  
        - name: "openjdk-19-jre-headless"  
          version: "19.0.2+7-0ubuntu3~22.04"  
          sha256_amd64: "f021cbd4f14a7c70dc707e7ffe..."  
      cica:  
        - name: "openjdk-19-jdk-headless"  
          version: "19.0.2+7-0ubuntu3~22.04"  
          sha256_amd64: "478f3718ba9b5528331e3a60f..."
```

Два типа образов

CICD

Базовая OS

- Стандартный набор утилит
- CICD утилиты

VM Runtime

- Open JRE
- Open JDK

Дополнительное ПО

- imagemagick + deps
- ffmpeg + deps

Runtime

- ShellWrapper

- Open JRE

- imagemagick + deps
- ffmpeg + deps

Подготовка базовых образов

Create java-17-cicd

```
FROM repo/sec/baseimage as cicd  
RUN install_packages.sh RuntimeList.yml CICDList.yml
```

Create java-17-runtime

```
FROM repo/sec/java-17-cicd as cicd  
RUN extract_packages.sh RuntimeList.yml  
  
FROM scratch  
COPY --from cicd /target /
```



Нюансы

Проблемы



FFI

Foreign Function

Interface

Интерфейс внешних

функций – головная

боль с неизвестным

решением

Проблемы



FFI

Foreign Function
Interface

Интерфейс внешних
функций – головная
боль с неизвестным
решением



Additional soft

Дополнительное ПО
которое необходимо
командам
разработки
(imagemagic, ffmpeg,
nginx-brotli и т.д.)

Проблемы



FFI

Foreign Function
Interface

Интерфейс внешних
функций – головная
боль с неизвестным
решением



Additional soft

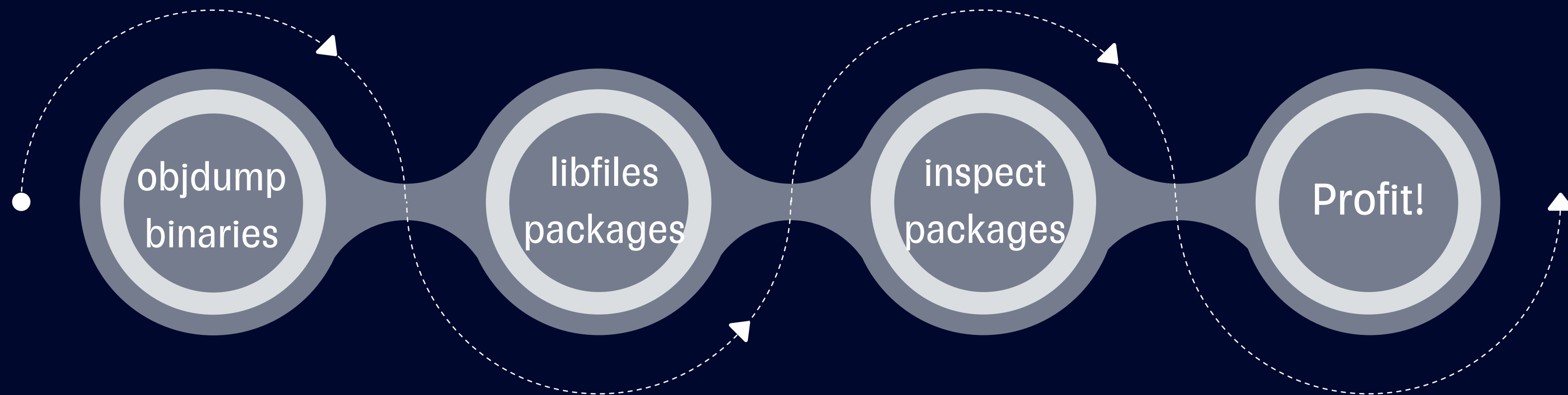
Дополнительное ПО
которое необходимо
командам
разработки
(imagemagic, ffmpeg,
nginx-brotli и т.д.)



Compiled Deps

Модули-
зависимости,
собираемые
менеджером из
исходного кода
shared linked
(python-psycopg2)

Подготовка дополнительных зависимостей приложений



Сканирование

Сканирование директории – подготовленного дерева для переноса

Определение пакетов

Составление списка пакетов дистрибутива

Исследование пакетов

По содержанию пакетов определяем их зависимости

Копирование

Копирование библиотек в директорию

Дополнительное ПО

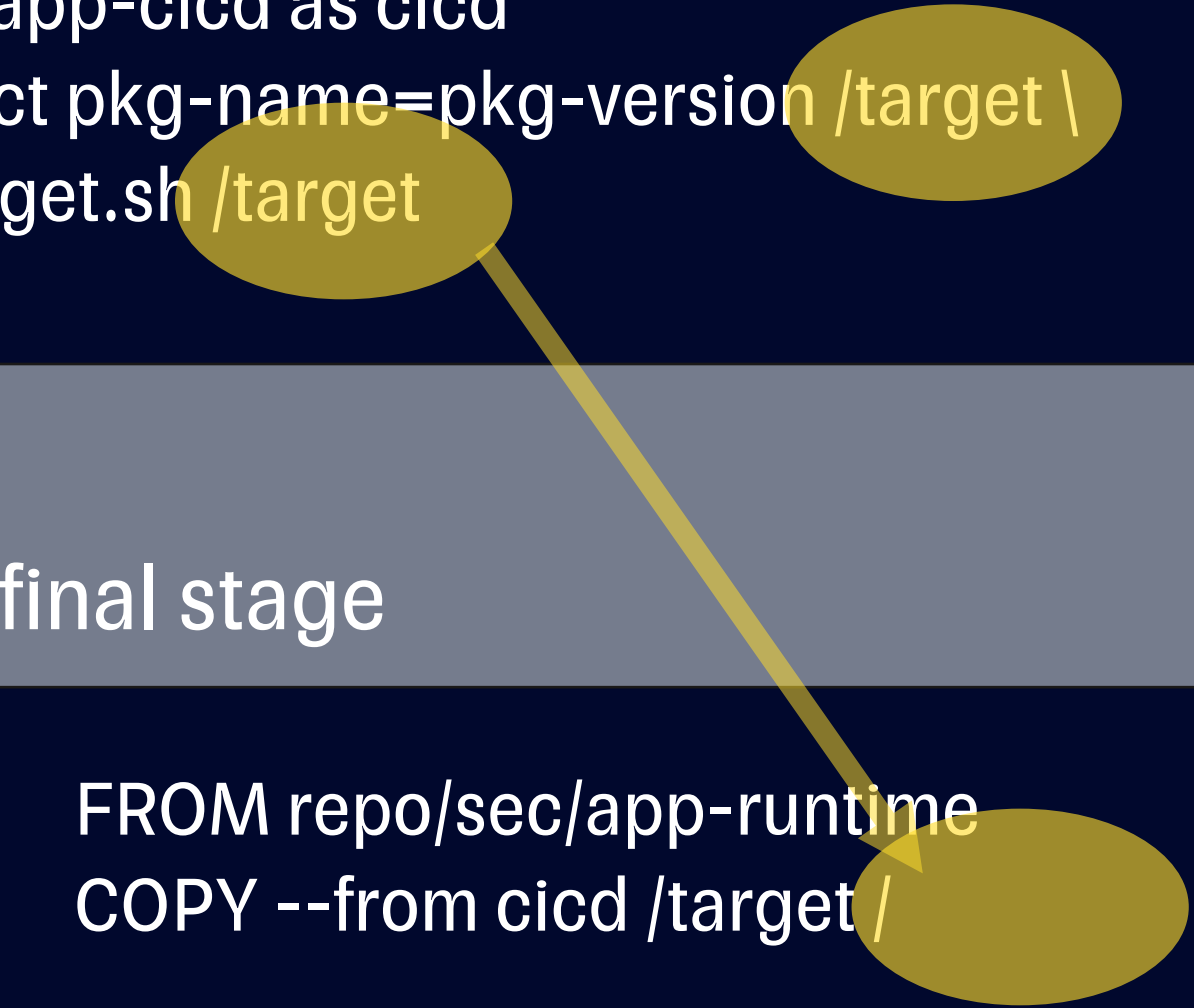
Копирование, подготовленного в cicd-stage сборки, дерева distroless

Build stage

```
FROM repo/sec/app-cicd as cicd
RUN dpkg-extract pkg-name=pkg-version /target \
    && bindeps2taget.sh /target
```

final stage

```
FROM repo/sec/app-runtime
COPY --from cicd /target /
```





ShellWrapper



Приложение должно само
читать ENV



Конфигурировать нужно
JAVA_TOOL_OPTIONS



Не только JAVA

```
# /bin/sh – не shell
```

```
# JVM запустится с pid = 1. Для передачи параметров jvm следует использовать $JAVA_TOOL_OPTIONS.  
ENTRYPOINT ["java", "основной_класс"]
```

```
# JVM будет запущен НЕ с 1 пидом, но все сигналы процессу будут проброшены.  
CMD java $JVM_OPTS $основной_класс
```

Entrypoint на golang



Подготовить конфиги из шаблонов



Сконфигурировать контейнер под окружение

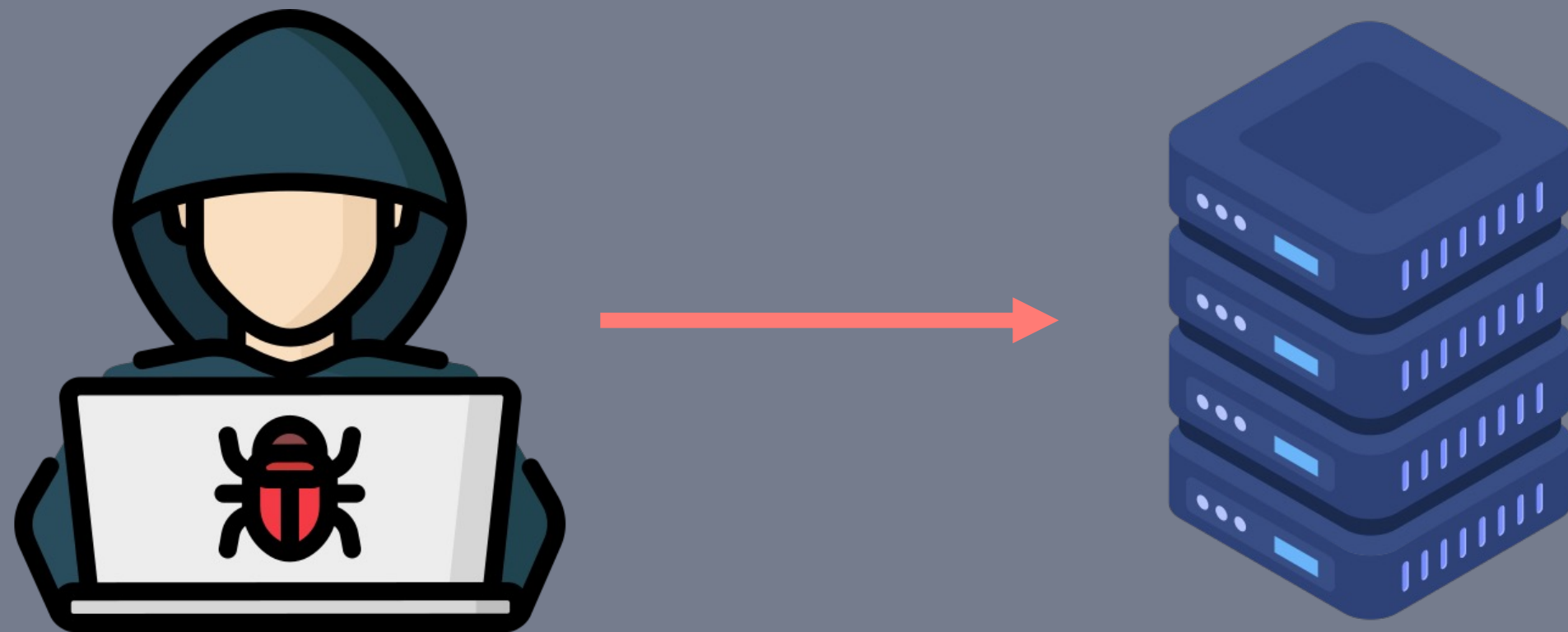
```
# /bin/nginx-starter – entrypoint for nginx
```

```
# Nginx будет запущен HE с pid=1,  
# но сигналы будут проброшены  
ENTRYPOINT ["/bin/nginx-starter"]
```

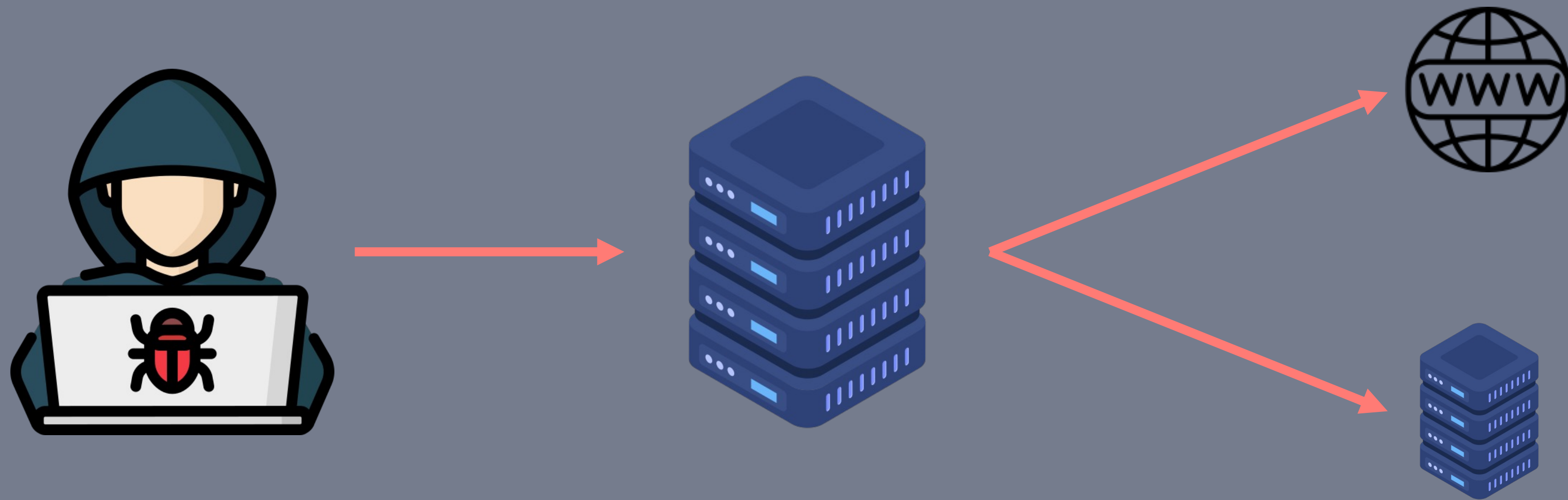
```
//// subst html in www files  
err := www.Compile(WWW_TEMPLATE_DIR, WWW_OUTPUT_DIR, "ASSETS_PREFIX", WWW_SUFFIX)  
//// subst NGINX_ENVSUBST_CONFIG_DIR in www files  
err = nginx.Compile(NGINX_CONFIG_TEMPLATES_DIR, NGINX_WRITE_DIR, CURRENT_ENVS, ".template")  
/// Run Nginx  
err = nginx.Run(NGINX_WRITE_DIR)  
if err != nil {  
    log.Println(err)  
}
```

```
func Run(configDir string) error {  
    cmd := exec.Cmd{  
        Path: "/usr/sbin/nginx",  
        Args: []string{"/usr/sbin/nginx", "-c", configDir+"/default.conf"},  
        Stdout: os.Stdout,  
        Stderr: os.Stderr,  
        Stdin: os.Stdin,  
    }  
    err := cmd.Start()  
    ...
```

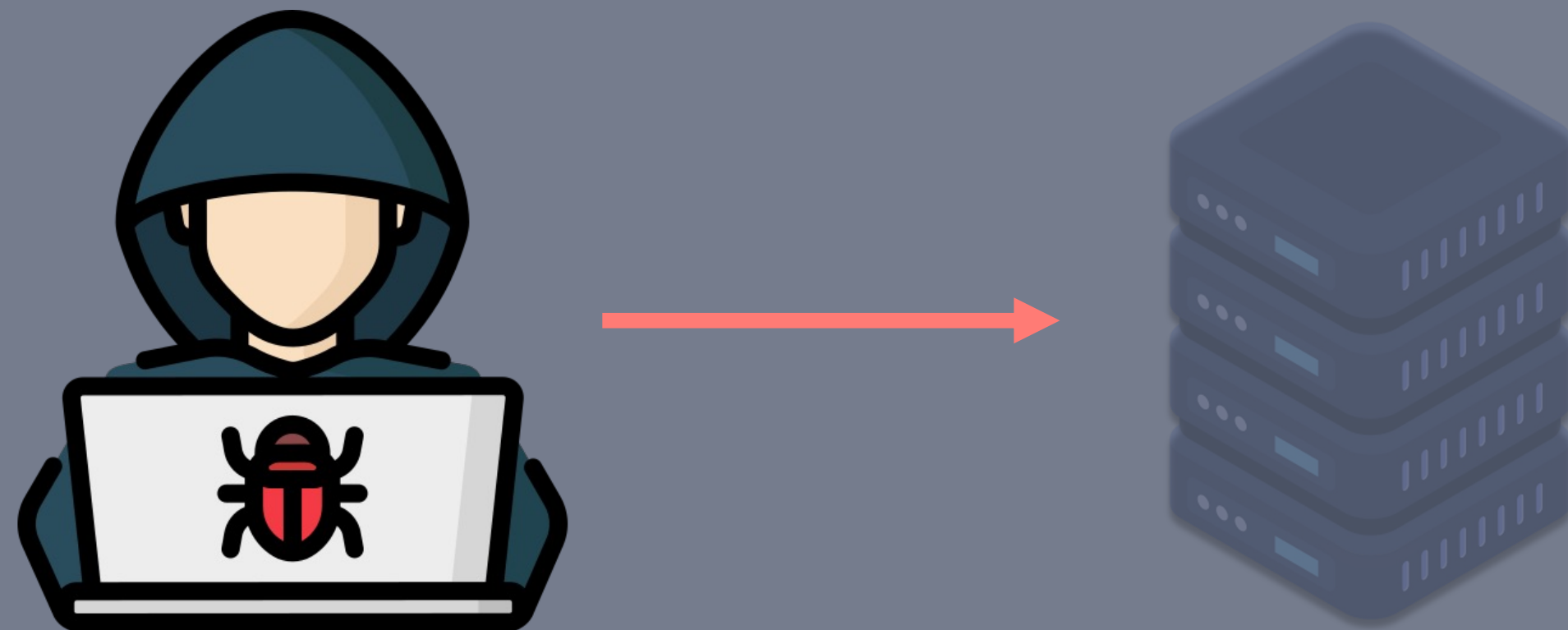
Атака на сервер



Успешная атака на сервер



Успешная атака на сервер



Атака на сервер?



?



OS-tool is Honey Pot



/bin/bash – security alert
/bin/cat – security alert
/bin/curl – security alert
/bin/ls – security alert

...

Обновление образов, исправление уязвимостей.

Новые версии?

Поиск свежих
версий пакетов по
спискам



Бранч-MP

Автоматическое
внесение
изменений и
создание MP



Ручное ревью

Отсмотреть и дать
апрув на MP (или не
дать)



Публикация

Сборка и
публикация
образов с
обновлёнными
пакетами

В результате



7 июня 2023 📍 Москва, МЦК ЗИЛ

Первая в России конференция
по БЕзопасности КОНтейнеров и контейнерных сред



Contacts:

mokanton@gmail.com