?????????? ?????????? CIS Benchmark

Зона ответственности: Printum + Заказчик / Интегратор

Коротко: Printum реализует ряд рекомендаций CIS Benchmark для контейнерных сред, включая использование непривилегированных пользователей, удаление SUID/SGID-файлов, применение профилей безопасности SELinux и отказ от хранения секретов внутри контейнерных образов.

??????????

Контейнерная платформа должна соответствовать рекомендациям по безопасной настройке и эксплуатации контейнерных сред.

Рекомендации CIS Benchmark направлены на снижение рисков компрометации контейнеров, ограничения привилегий процессов и обеспечение безопасного развёртывания приложений.

??? ??? ????????? ? Printum

В составе контейнерной платформы Printum реализованы следующие меры безопасности:

- использование непривилегированных пользователей внутри контейнеров;
- отказ от запуска контейнеров в privileged-режиме;
- отсутствие дополнительных Linux capabilities через cap_add;
- удаление SUID/SGID-файлов и утилит повышения привилегий;
- применение профилей безопасности SELinux;
- отсутствие встроенных секретов, паролей и токенов в контейнерных образах;
- использование фиксированных версий контейнерных образов.

Подробная информация приведена в соответствующих статьях раздела «Контейнеры».

??? ????????? ?? ??????????

Часть рекомендаций CIS Benchmark относится к настройке контейнерной платформы и инфраструктуры заказчика.

К таким настройкам относятся:

- параметры контейнерного рантайма;
- ограничения CPU и памяти;
- использование read-only файловых систем контейнеров;
- аудит операционной системы;
- сканирование контейнерных образов;
- настройки оркестратора контейнеров.

Настройка указанных механизмов выполняется администраторами инфраструктуры заказчика.

Revision #1
Created 2026-06-08 19:39:07 UTC by DD
Updated 2026-06-08 19:39:07 UTC by DD