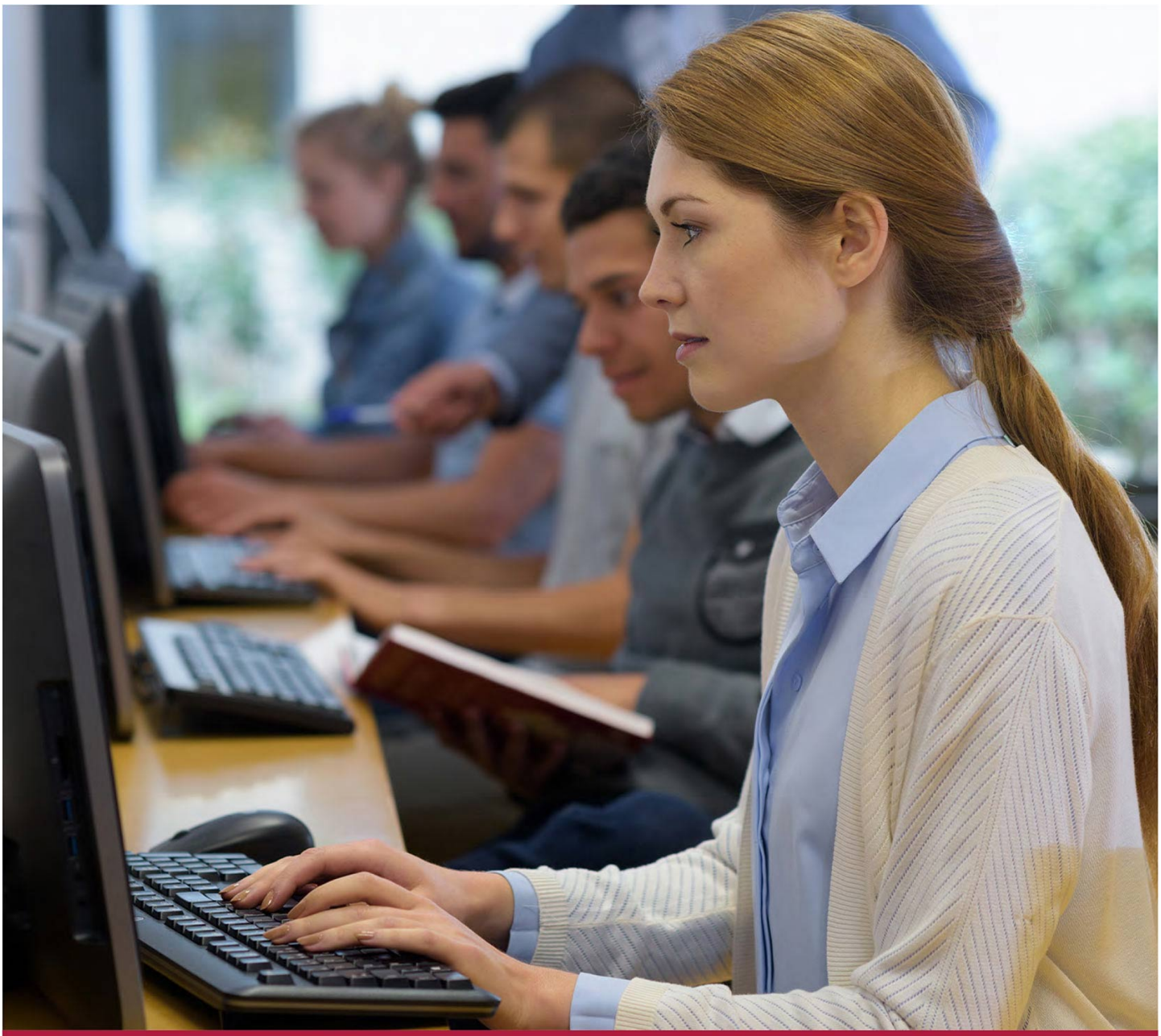
Академия АйТи
a Softline Company



Безопасное окружение: DevOps с углубленным изучением информационной безопасности

Код курса: DSO_1

+7 (495) 150 96 00 | academy@academyit.ru | academyit.ru

Безопасное окружение: DevOps с углубленным изучением информационной безопасности

Код курса: DSO_1

Длительность	40 ак. часов
Формат	
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Курс предназначен для DevOps инженеров и разработчиков, стремящихся углубить свои знания в информационной безопасности. В рамках обучения рассматриваются современные технологии контейнеризации и оркестрации, такие как Docker и Kubernetes, а также методы обеспечения кибербезопасности. Особое внимание уделяется практическим навыкам: участники научатся защищать операционные системы и контейнеры, настраивать и улучшать конфигурации безопасности, работать с реестрами контейнеров и применять базовые методы защиты окружения в реальных проектах.

Подробная информация

Профиль аудитории:

- DevOps-инженеры: обладающие базовыми навыками автоматизации развертывания приложений и управления инфраструктурой
- разработчики ПО: имеющие базовые знания IAC и стремящиеся понимать специфику безопасного окружения в разработке
- начинающие DevSecOps-специалисты: которые хотят освоить практики обеспечения безопасности окружения приложений

Предварительные требования:

- опыт работы с Linux, установка, настройка, system service
- понимание bash
- базовые знания о контейнеризации (Docker) и оркестрации (Kubernetes)

По окончании курса слушатели смогут:

- находить и устранять проблемы, связанные с окружением приложений
- обеспечивать базовую гигиену безопасности конфигураций ОС и контейнеров
- обеспечивать базовую гигиену безопасности для раннеров, используемых в CI/CD
- разрабатывать политики безопасности для Kubernetes

- обеспечивать базовую гигиену безопасности для container registry

Программа курса

Модуль 1. Основы Linux/Docker/K8S

- Введение в окружение продукта и разработку, анализ проблем
- Файловая система и права доступа
- Управление процессами
- Работа с логами
- Сетевые утилиты
- Основы SELinux и AppArmor
- Изоляция контейнеров
- Ограничение ресурсов
- Использование секретов
- K8s RBAC
- Network Policies Persistent Volumes

Модуль 2. OS Hardening

- Виды харденинга для ОС/VM/Docker/K8s
- Практики аудита ОС/VM/Docker/K8s на безопасность
- Подготовка конфигурации Linux OS для production

Модуль 3. Docker (runner) hardening

- Безопасные настройки Docker (Capabilities, Namespaces и т. д.)
- Shared Runners,
- Self-Hosted Runners,
- Docker-in-Docker (DinD)
- Docker-outside-of-Docker (DooD)
- Побеги из контейнеров

Модуль 4. K8S security contexts

- Безопасность на уровне узлов, подов и контейнеров
- Разница между runAsUser и runAsGroup
- Работа с файловой системой
- Ограничение ресурсов и процессов
- Политики безопасности
- Сбор логов

Модуль 5. Управление контейнерными реестрами и предотвращение злоупотреблений

- Обзор контейнерных реестров, Public Registry, Private Registry, типов атак
- Цифровые подписи Docker-образов с помощью cosign
- Immutable Tags
- Атака dependency confusion

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

+7 (495) 150 96 00 | academy@academyit.ru