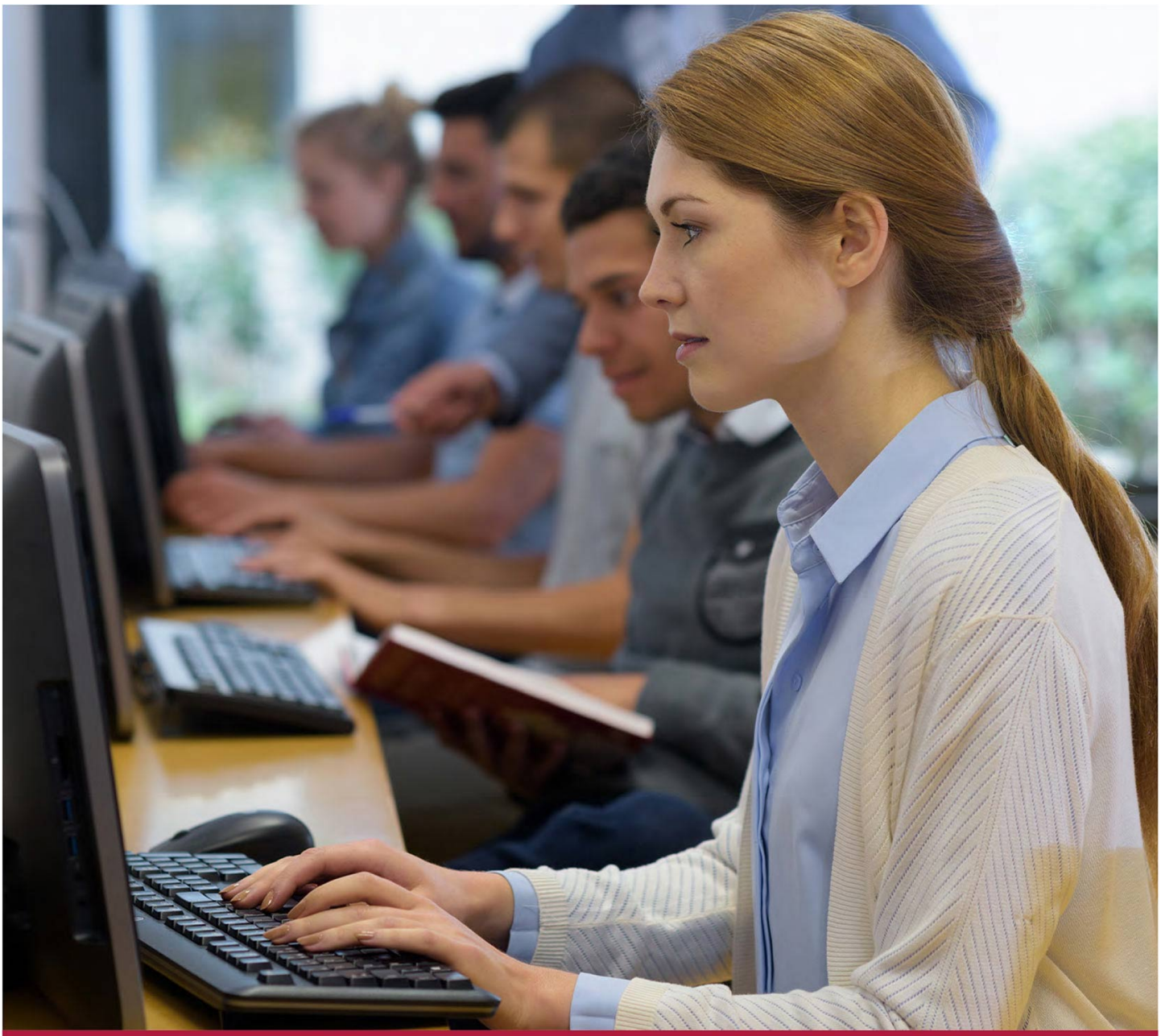
Академия АйТи
a Softline Company



Специалист DevSecOps

Код курса: pp_devsecops

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

© Академия АйТи, 2024

Специалист DevSecOps

Код курса: pp_devsecops

Длительность	272 ак. часа
Формат	Очно; Дистанционно
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Актуальность программы вызвана необходимостью подготовки новых профессиональных кадров для Цифровой экономики Российской Федерации, так называемых DevSecOps инженеров, способных к внедрению безопасного инженерного процесса разработки современных цифровых платформ и экосистем на основе лучших международных практик разработки безопасного программного обеспечения (ПО). Кратко основные достоинства такой подготовки и переподготовки можно выразить в трех основных тезисах: скорость, безопасность и эффективность программного кода.

Подробная информация

Программа профессиональной переподготовки разработана на основании:

- Федерального закона от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;
- Приказа Министерства образования и науки Российской Федерации от 01.07.2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;
- Приказа Министерства образования и науки РФ от 23.08.2017 г. № 816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;
- Профессионального стандарта № 424н «Программист», утвержденный 20.07.2022 г.

Успешное окончание обучения по программе данного курса позволит специалистам:

- Взаимодействовать с командами разработки ПО и операционными подразделениями для анализа функциональных и не функциональных требований, пользовательских сценариев на предмет безопасности;
- Заниматься подготовкой требований по безопасности, а также контролировать соблюдение требований в процессе разработки ПО;
- Проводить ревью безопасности разработанной архитектуры приложений (монолитной, SOA, микросервисной), ревью исходного кода ПО, тестирование безопасности релизов и систем в продакшене;
- Управлять требованиями по безопасности, в частности моделировать и анализировать угрозы

© Академия АйТи, 2024

безопасности;
- Управлять уязвимостью программных систем. Вести их учет, оценивать критичность и контролировать исправления в разработке ПО;
- Разрабатывать шаблоны безопасной архитектуры приложений, внедрять стандартны безопасного программирования, доводить требования безопасности до команд разработки ПО;
- Внедрять лучшие практики разработки безопасного ПО, DevSecOps (SAST, DAST, dependency check и др);
- Своевременно информировать команды разработчиков ПО об обнаружении новых и ранее неизвестных уязвимостях программного кода и предлагать обоснованные решения для их нейтрализации.

Успешное окончание обучения по программе данного курса позволит специалистам:

Знать:

- Основные методы и практики DevSecOps
- Методы и приемы алгоритмизации поставленных задач безопасной разработки ПО
- Основные структуры данных Python
- Алгоритмы решения типовых задач, области и способы их применения
- Синтаксис выбранного языка Python,
- Особенности программирования на Python,
- Стандартные библиотеки языка Python
- Технологии безопасного программирования
- Особенности выбранной среды программирования
- Методы и приемы отладки программного кода
- Типы и форматы сообщений об ошибках и уязвимостях ПО

Уметь:

- Применять Python для написания безопасного программного кода
- Использовать выбранную среду программирования
- Отлаживать программный код
- Использовать вспомогательные инструментальные программные средства для обработки исходного текста программного кода
- Выявлять ошибки в программном коде
- Контролировать компоненты с открытым исходным кодом при попадании в периметр разработки (Open Source Analysis, OSA);
- Проводить статический анализ кода (Static Application Security Testing, SAST);
- Контролировать состав компонент ПО (Software Composition Analysis, SCA);
- Проводить динамический анализ кода (Dynamic Application Security Testing, DAST/Interactive Application Security Testing, IAST/Behavioral Application Security Testing, BAST);
- Проводить анализ бинарного кода и контроль состава контейнеров (Bytecode and Container Analysis, BCA);
- Применять известные технические меры безопасности для разработки безопасного ПО.

Владеть навыками/выполнять следующие трудовые действия:

- Составление формализованных описаний решений поставленных задач по разработке безопасного ПО в соответствии с требованиями технического задания или других принятых в организации нормативных документов

 © Академия АйТи, 2024

- Создание безопасного программного кода в соответствии с техническим заданием (готовыми спецификациями)
- Оптимизация программного кода с использованием специализированных программных средств DevSecOps
- Приведение наименований переменных, функций, классов, структур данных и файлов в соответствие с установленными в организации требованиями по безопасности
- Структурирование исходного программного кода в соответствии с установленными в организации требованиями по безопасности
- Форматирование исходного программного кода в соответствии с установленными в организации требованиями по безопасности
- Слияние, разделение и сравнение исходных текстов безопасного программного кода
- Анализ и проверка исходного программного кода на требования по безопасности.

Получение компетенций для профессиональной деятельности в области программирования и создания ИТ- продуктов:

- формализация и алгоритмизация поставленных задач разработки безопасного ПО;
- написание безопасного программного кода с использованием языков программирования, определение данных и манипулирование ими;
- оформление программного кода в соответствии с установленными требованиями безопасности;
- проверка и отладка программного кода современных цифровых платформ и экосистем;
- проверка программного обеспечения на соответствие требованиям устойчивости и безопасности;
- разработка тестовых наборов данных;
- рефакторинг и оптимизация безопасного программного кода.

Целевая аудитория:

- DevOps-инженеры.
- Архитеторы ПО
- Программисты
- Специалисты по ИБ.

Необходимая подготовка: Знание основ программирования на языке Python.

Программа курса

Модуль 1. Основы программирования и составления алгоритмов

- Алгоритм – свойства и способы представления. Типы данных – назначение и роль в программе. Операнды и операторы – вычисление выражений
- Модели разработки программ. Структурное программирование. Базовые принципы: блочная структура кода – блоки и подпрограммы. типовые структуры управления – последовательность, ветвление, цикл
- Практические примеры составления блок-схем и псевдокода. Простейшие алгоритмические задачи. Перевод алгоритма в код. Подпрограммы (функции) как основные блоки кода. Типовые задачи на обработку текста

 © Академия АйТи, 2024

- Установка интерпретатора Python. Основные операции и типы данных. Операторы ветвления и циклы. Установка и запуск среды разработки. Типы данных: числа, строки, списки, логический тип, None. Функции преобразования типов. Простой ввод и простой вывод
- Ветвления. Оператор if. Базовая форма цикла while. Операторы break и continue. Перебор (for).
- Понятие массива. Типовые задачи с массивами: доступ к элементу, обход элементов, инициализация элементов
- Строки. Методы и функции. Использование срезов. Кортеж. Основные операции с кортежем. Распаковка кортежа. Список. Основные операции со списком. Словарь. Основные операции со словарем. Множества. Основные операции с множеством
- Основные алгоритмы поиска и сортировки. Вычисление сложности алгоритмов. Анализ эффективности работы программы.
- Простейшие конструкции данных: список, стек, очередь, дерево. Поиск элемента и сортировка элементов. Реализация динамического стека

Модуль 2. Профильный модуль. Разработка безопасного ПО.

- **Тема 2.1.** Основные концепции DevSecOps.
- Тренды разработки современного ПО (внедрение практик DevOps, снижение общих сроков разработки ПО (time to market), повышение гибкости в разработке ПО, переход от монолитных к микросервисным приложениям, динамическое выделение ИТ-ресурсов, повышение внимания к вопросам разработки безопасного ПО).
- Основные понятия и определения DevOps и DevSecOps
- Ключевые компоненты DevSecOps (анализ кода, управление изменениями, мониторинг соотвествия, иследование угроз безопасности, оценка уязвимости кода, обучение и повышение осведомленности)
- Основные этапы DevSecOps (разработка приложения и работа с репозиторием программ, непрерывная интеграция (CI) и тестирование приложения, непрерывное развертывание (CD) приложения в рабочей среде, контроль новой версии приложения в рабочей среде).
- Возможные сценарии интеграции DevSecOps в процессы и инфраструктуру компании.
- Адаптации функции кибербезопасности и интеграции DevSecOps
- Проведение оценки безопасности процесса разработки, а также идентификация ключевых рисков и риск-факторов, связанных с недостатками процесса.
- Ключевые точки процесса разработки, где необходимо включение мер безопасности
- Информирование сотрудников о критических рисках и мерах для их снижения.
- **Тема 2.2.** Основные практики DevSecOps. Моделирование угроз безопасности (Threat modeling)
- Контроль компонент с открытым исходным кодом (Open Source Analysis, OSA)
- Статический анализ кода (Static Application Security Testing, SAST).
- Контроль состава компонент ПО (Software Composition Analysis, SCA).
- Динамический анализ кода (Dynamic Application Security Testing, DAST/Interactive Application Security Testing, IAST/Behavioral Application Security Testing, BAST).
- Фаззинг-тестирование (fuzzing)
- Анализ бинарного кода и контроль состава контейнеров (Bytecode and Container Analysis, BCA).
- Решения для выявления и нейтрализации уязвимостей программного кода.
- Реализация WAF (Web Application Firewall).
- **Тема 2.3.** Трансформация DevOps в DevSecOps. Использование безопасных по умолчанию библиотек, фреймворков и компонент ПО в процессе разработки (Secure-by-Default).
- Интеграция технологических практик ИБ в начало конвейера CI/CD (Shift-Left подход).
- Автоматизация процессов в концепции Everything-as-a-Code.

 © Академия АйТи, 2024

- Формирование сообщества security-чемпионов в производственных командах для повышения инженерной security-культуры.
- Применение модели зрелости DevSecOps для оценки существующего процесса и для постоянного совершенствования.
- Обеспечение прозрачности security активностей для участников инженерного производственного процесса.
- DevSecOps-оркестрация (Application Security Testing Orchestration, ASTO) для непрерывного улучшения процесса разработки безопасного ПО.
- **Тема 2.4.** Национальные требования (ГОСТ Р 56939-2016 и ГОСТ Р ИСО/МЭК 12207) в части разработки безопасного ПО.
- Требования в части идентификации и аутентификации
- Требования по защите от несанкционированного доступа к информации.
- Требования в части регистрации событий безопасности.
- Требования контроля точности, полноты и правильности входных и выходных данных.
- Требования по обработке программных ошибок и исключительных ситуаций.
- Требования класса ASE "Оценка задания по безопасности" (ГОСТ Р ИСО/МЭК 15408-3).
- Меры по разработке безопасного программного обеспечения, реализуемые при выполнении инсталляции программы и поддержки приемки программного обеспечения.
- Меры по разработке безопасного программного обеспечения, реализуемые при решении проблем в программном обеспечении в процессе эксплуатации.
- Меры по разработке безопасного программного обеспечения, реализуемые в процессе менеджмента инфраструктурой среды разработки программного обеспечения.
- **Тема 2.5.** Роли и кадровое обеспечение DevSecOps.
- Принятие методологии разработки безопасного ПО, DevSecOps (оценка текущих мер безопасности и распределение ролей в команде разработки ПО, внедрение мер безопасности на стадии проектирования программных систем, внедрение инструментов и авто-тестов безопасности в пайплайн, тестирование безопасности разработанных решений, анализ выявленных уязвимостей и подготовка рекомендаций по их устранению, обучение лучшим практикам разработки безопасного ПО, Best Practices).
- Распределение ролей в процессе DevSecOps (продакт менеджер, архитектор, команда разработки, QA, AppSec специалист, DevOps инженер).
- Воспитание чемпионов безопасности Security Champions (масштабирование безопасности с помощью нескольких команд разработки, привлечение сотрудников, не связанных с безопасностью, но связанных с DevOps, создание и развитие культуры безопасности).
- Повышение осведомленности по вопросам разработки безопасного ПО.
- Развитие корпоративной культуры DevSecOps и безопасности в целом.

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

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

© Академия АйТи, 2024