DevSecOps: безопасная разработка и эксплуатация

01 Кому подойдёт курс

DevOps-инженерам, системные администраторам и специалистам по инфраструктуре
Освоите принципы и практики DevSecOps, чтобы эффективно интегрировать их в существующие DevOps-процессы и обеспечить защиту приложений на всех этапах жизненного цикла

Архитекторам, техлидам, СТО и специалистам по ИБ
Изучите концепции и практики DevSecOps, чтобы осознанно интегрировать их в архитектуру системы и обеспечить защиту приложений с самого начала разработки

Разработчикам ПО
Освоите лучшие практики безопасного программирования, чтобы предотвращать уязвимости на этапе написания кода

02 Чему научитесь на курсе

- Объяснять принципы DevSecOps и описывать, как безопасность интегрируется в DevOps-процессы на всех этапах SDLC
- Настраивать и внедрять в CI/CD-пайплайны инструменты безопасности: SAST, SCA, DAST, WAF, Trivy, Vault и другие
- Оценивать уязвимости в коде, зависимостях, контейнерах и инфраструктуре при помощи современных средств автоматизации
- Разрабатывать и внедрять безопасные пайплайны с учётом угроз, рисков и лучших практик DevSecOps
- Анализировать и минимизировать риски, используя фреймворки угроз и зрелости безопасности
- Повышать уровень безопасности контейнеров и кластеров Kubernetes при помощи защитных мер по рекомендациям CIS Benchmarks
- Настраивать безопасное хранение секретов и контролировать доступ к инфраструктуре при помощи Vault, Keycloak и LDAP
- Использовать Linux-механизмы безопасности (AppArmor, SELinux, Seccomp) для защиты среды исполнения
- Проводить тестирование на проникновение и анализ инцидентов при помощи Nmap, Metasploit, SIEM и других инструментов

DevSecOps: безопасная разработка и эксплуатация

03 Как проходит обучение

- Сопровождение кураторами
- Обратная связь от опытных наставников
- Воркшопы с экспертами
- Теория на платформе Практикума
- Практические задания с ревью на готовой инфраструктуре в облаке

Что вас ждёт на обучении

Актуальные методы для безопасности инфраструктуры, приложений и данных

Фреймворки для оценки уровня зрелости безопасности в компании

Удостоверение о повышении квалификации

DevSecOps: безопасная разработка и эксплуатация

3 месяца

продолжительность курса

1 ЧАС

00

Бесплатная часть. Основы изоляции и поиск уязвимостей в контейнерах

- Знакомство с курсом
- Зачем нужна изоляция в контейнерах и как она нарушается
- Приватные реестры и анализ уязвимостей образов

1 НЕДЕЛЯ

01

Введение в DevSecOps

- Принципы DevSecOps
- Пайплайны DevSecOps
- Основные типы уязвимостей и атак

2 НЕДЕЛИ

02

Инструменты и технологии DevSecOps

- Виды анализа безопасности приложений
- Интеграция SAST-, SCA — и DAST-инструментов
- Использование Secure SDLC и Shift Left Testing

1 НЕДЕЛЯ

03

Безопасность Linux

- Основные механизмы безопасности Linux
- Настройка контроля доступа
- Средства защиты ядра и процессов

2 НЕДЕЛИ

04

Безопасность Docker

- Изоляция в Docker, угрозы и атаки на контейнеры
- Сборка и запуск контейнеров
- Docker Registry с Harbor
- Анализ безопасности контейнеров

2 НЕДЕЛИ

05

Безопасность Kubernetes

- Угрозы безопасности в K8s
- Политики безопасности в K8s
- Защита K8s-кластеров

1 НЕДЕЛЯ

06

Безопасность инфраструктуры

- Управление пользователями и доступами
- Хранение секретов
- Инфраструктура как код (IaC)
- Интеграция в CI/CD

1 НЕДЕЛЯ

07

Тестирование безопасности

- Принципы тестирования безопасности
- Инструменты для тестирования безопасности
- Безопасное окружение

1 НЕДЕЛЯ

08

Мониторинг и реагирование на инциденты

- SIEM-системы
- MITRE ATT&CK
- Анализ инцидентов и Postmortem

1 НЕДЕЛЯ

09

Оценка угроз и рисков

- Threat Modeling
- Управление уязвимостями
- Зрелость процессов безопасности

2 НЕДЕЛИ

10

Итоговый проект

- Харденинг SDLC, инфраструктуры, оценка зрелости

Бесплатная часть. Основы изоляции и поиск уязвимостей в контейнерах

00

~1 час
1 практическая работа

- Узнаете, как организован курс, какие задачи вас ждут на курсе
- Поймёте базовые принципы безопасности контейнеризации и идентифицируете риски и угрозы при работе с контейнерами
- Проведёте базовую проверку контейнерных образов на наличие уязвимостей
- Настроите безопасное хранение артефактов в собственном приватном Docker Registry с Harbor
- Примените лучшие практики безопасности на уровне Docker

Инструменты и технологии

- Docker
- Harbor
- Trivy

Практическая работа

Изолируете процессы в Docker и проверите параметры безопасности, повысите привилегии в небезопасных контейнерах через уязвимый suid-файл. Развернёте приватный реестр Harbor для хранения образов. Проверите уязвимости контейнерных образов с использованием Trivy

Введение в DevSecOps

01

1 неделя
1 проект

- Изучите принципы DevSecOps и роль безопасности на всех этапах SDLC, сможете определять базовые угрозы безопасности в разработке и эксплуатации
- Постройте базовый пайплайн, используя концепции Shift Left и непрерывной безопасности
- Классифицируете уязвимости и угрозы в приложениях, изучите базовые фреймворки угроз: OWASP Top 10, MITRE ATT&CK, MITRE ATLAS

Инструменты и технологии

- Shift Left
- Secure SDLC
- Threat Modeling
- OWASP Top 10
- MITRE ATT&CK
- MITRE ATLAS

Проект

Постройте схему DevSecOps-пайплайна. Классифицируете угрозы на примерах приложений. Составите чек-лист OWASP Top 10 для тестового приложения

Инструменты и технологии DevSecOps 02

2 недели
1 проект

- Изучите основные виды анализа: статический (SAST), композиционный (SCA), динамический (DAST)
- Интегрируете инструменты анализа безопасности в CI/CD-процессы
- Научитесь выявлять и устранять уязвимости в коде и зависимостях

Инструменты и технологии

- SonarQube
- Snyk
- Trivy
- OWASP ZAP
- Burp Suit
- Secure SDLC
- Shift Left Testing

Проект

Настроите SAST-анализ проекта через SonarQube или Snyk и SCA-сканирование зависимостей через Trivy. Интегрируете DAST-тестирования с OWASP ZAP в пайплайн CI/CD. Проанализируете результаты сканирования и исправите найденные уязвимости

Безопасность Linux 03

1 неделя
1 проект

- Изучите основные механизмы безопасности операционных систем на базе Linux
- Научитесь управлять пользователями, группами и правами доступа в Linux, настроите политики безопасности через AppArmor и SELinux, примените механизмы ограничения системных вызовов через Seccomp
- Научитесь применять базовые средства защиты ядра и процессов, настроите сетевые правила безопасности в Linux

Инструменты и технологии

- AppArmor
- SELinux
- Seccomp
- iptables
- nftables

Проект

Настроите политики AppArmor для ограничения прав приложений. Ограничите системные вызовы контейнера через Seccomp. Проверите и настроите базовые политики доступов к файлам и каталогам, а также к фильтрации сетевого трафика через iptables

Безопасность Docker 04

2 недели
1 проект

- Изучите принципы изоляции в Docker, сможете идентифицировать угрозы и атаки, связанные с контейнеризацией приложений
- Научитесь применять лучшие практики безопасности на этапе сборки образов (минимизация базовых образов, отказ от лишних привилегий) и запускать контейнеры в рантайме
- Развернёте и безопасно настроите приватные репозитории для хранения Docker-образов с помощью Harbor
- Проанализируете уязвимости контейнерных образов с помощью специализированных инструментов

Инструменты и технологии

- Docker
- Harbor
- Trivy
- CIS Benchmarks

Проект

Примените лучшие практики безопасности на этапах сборки образов и запуска контейнеров. Интегрируете инструменты для анализа безопасности в CI/CD-процессы

Безопасность Kubernetes 05

2 недели
1 проект

- Научитесь анализировать риски и угрозы в Kubernetes-кластере
- Настроите политики безопасности и сетевые политики (PodSecurityPolicies и NetworkPolicies) в кластере Kubernetes
- Научитесь применять лучшие практики безопасности для защиты кластеров (CIS Benchmarks для Kubernetes)

Инструменты и технологии

- Kubernetes
- CIS Kubernetes Benchmark
- RBAC
- NetworkPolicies

Проект

Развернёте кластер Kubernetes и настроите базовые политики безопасности и сетевые политики для ограничения трафика. Примените рекомендации CIS Benchmark на практике. Ограничите права приложений через настройки RBAC

Безопасность инфраструктуры 06

1 неделя
1 проект

- Настроите реалмы, федерации и пользователей в Keycloak, интегрируете Keycloak с внешними системами через LDAP
- Настроите безопасное хранение секретов и политик доступа в Vault
- Научитесь использовать безопасные подходы при работе с Terraform и Ansible
- Интегрируете в CI/CD-процессы системы управления доступами и секретами для безопасной работы

Инструменты и технологии

- LDAP
- Keycloack
- Vault
- Terraform
- Ansible

Проект

Настроите Keycloak, развернёте Vault и интегрируете его в пайплайн CI/CD. Настроите в Harbor безопасное хранение Docker-образов с аутентификацией через Keycloak. Используете базовые правила безопасности при работе с Terraform и Ansible

Тестирование безопасности 07

1 неделя
1 проект

- Проведёте базовое тестирование приложения и инфраструктуры на безопасность
- Научитесь искать и анализировать уязвимости с помощью Metasploit и Nmap
- Подготовите окружение для безопасного тестирования

Инструменты и технологии

- Metasploit
- Nmap
- OWASP Testing Guide
- Penetration Testing

Проект

Развернёте тестовое приложение для проверки безопасности. Используете Nmap для сканирования портов и выявления уязвимых сервисов. Проведёте базовые тесты безопасности приложений с помощью Metasploit

Мониторинг и реагирование на инциденты

08

1 неделя
1 проект

- Настроите с помощью SIEM-систем мониторинг событий безопасности: сбор, анализ и корреляцию событий
- Научитесь применять фреймворк MITRE ATT&CK для интерпретации и классификации атак
- Проведёте первичный анализ инцидента и подготовите Postmortem по результатам инцидента

Инструменты и технологии

- SIEM-системы
- MITRE ATT&CK
- Postmortem

Проект

Настроите мониторинг событий безопасности через SIEM. Сделаете корреляцию событий в реальном времени с помощью MITRE ATT&CK. Проанализируете инцидент на основе собранных логов, напишете Postmortem по итогам анализа инцидента

Оценка угроз и рисков, фреймворки оценки уровня зрелости безопасности

09

1 неделя
2 проекта

- Постройте модель угроз для приложений и инфраструктуры, разработаете сценарии атак на основе Threat Modeling
- Научитесь использовать DefectDojo для управления уязвимостями
- Оцените процессы безопасности через фреймворки BSIMM и OWASP SAMM, примените международные стандарты безопасности (ГОСТ, ISO, NIST)

Инструменты и технологии

- OWASP Threat Modeling
- MITRE ATT&CK
- DefectDojo
- BSIMM
- OWASP SAMM
- ISO 27001
- NIST 800–53

Проект

Проведёте Threat Modeling для тестового приложения. Разработаете сценарии атак на основе построенной модели угроз, проведёте учёт и научитесь управлять уязвимостями с помощью DefectDojo. Оцените уровень зрелости безопасности проекта и разработаете стратегию его повышения на основе выявленных рисков и уязвимостей

Итоговый проект

10

2 недели
1 проект

Оцените уровень DevSecOps-практик в приложении и предложите план улучшений. В результате создадите DevSecOps-пайплайн, постройте модель угроз, проанализируете риски, проведёте оценку зрелости практик DevSecOps и сформируете набор рекомендаций.