

Факултет: ФАКУЛТЕТ ПО ТЕЛЕКОМУНИКАЦИИ И МЕНИДЖМЪНТ

Катедра: ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

Професионално направление: 5.3. КОМУНИКАЦИОННА И КОМПЮТЪРНА ТЕХНИКА

Специалност: ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

Образователно-квалификационна степен: МАГИСТЪР

ОПИСАНИЕ НА ЛЕКЦИОНЕН КУРС

1.Наименование на курса: *Практики за киберсигурност в DevOps*

2.Код на курса: *M.01.027.2*

3. Вид на курса: *избираем*

4. Ниво: *магистър*

5. Година на изучаване: *втора*

6. Семестър: *трети*

7. Брой кредити: *4.5*

8. Име на лекторите: *гл.ас.д-р Страхил Соколов, ас. Орхан Идириз*

9. Резултати от обучението за дисциплината:

Целта на курса е да покаже подходите за възприемане на DevOps техники за непрекъснато подобряване на сигурността на една организация на всяко ниво, вместо усилията на архитектите да бъдат фокусирани единствено върху защитата на инфраструктура....

Студентите, приключили обучението си по дисциплината, трябва да придобият:

Основни знания по защита на облачни услуги и използване на техники и способности за интегриране на сигурността директно в разработвания продукт; внедряване на елемент за сигурност на всеки слой, като например за слоевете на уеб приложението, облачната инфраструктура, комуникацията и процеса по доставка на софтуер. С помощта на практически примери биват разучени основните аспекти на сигурността, като блокиране на атаки, откриване на измами, облачна криминалистика и реакция при инциденти. В курса са застъпени и теми по разширяване на сигурността на DevOps, като оценка на риска, моделиране на заплахи и непрекъсната сигурност.

Практически умения за работа на база съвременни практики в индустрията за разработка на сигурен код, като например CERT, CWE, защита на Android приложения и OWASP код; Инструменти за преглед на кода и анализ посредством подхода Whitebox за идентифициране на специфични проблеми със сигурността, като XXE, десериализация и SQL инжекция; Работа със съвременни инструменти за тестване на сигурността. Основните елементи на системи за тестване, които включват тестване на сигурността, уеб и мобилни връзки, конфигурация, комуникация, проверка на компоненти, предоставени от трети страни и чувствителна информация.

Компетенции: След успешно приключване на курса студентите трябва да могат:

- Подходи за проверка и постигане на съответствие със сигурността, регулации и изисквания на пазара;
- Умения за внедряване на практики за сигурност в различни области, базирани на платформата OWASP SAMM.
- Знания за извършване на дейности в различни роли като управление на сигурността,
- Екипи за разработка на защитени приложения, QA и оперативни екипи. Знания за ролята, отговорността и взаимоотношенията на екипа по сигурността в организационната структура също оказват влияние..

10. Начин на преподаване:

Начинът на преподаване: Обучението по дисциплината „Практики за киберсигурност в DevOps” се извършва през трети семестър, съгласно действащия учебен план чрез лекции, групирани на блок или по един учебен час седмично в продължение на 15 седмици и практически упражнения, групирани по два учебни часа седмично в продължение на 15

седмици или на блок. Практически упражнения се провеждат по класическия начин като студентите се запознават последователно с предвидения материал. Твърденията се илюстрират с примери, които максимално улесняват работата на студентите в упражненията. Практическите упражнения се провеждат в лаборатория или на собствен компютър на студента, снабдени с необходимото оборудване – хардуер и платформи за разработване на практики по киберсигурност в DevOps. Преди всяко практическо занятие студентите са информирани за необходимостта от предварителна подготовка по съответната тема.

11. Предварителни изисквания:

Студентите следва да имат Облачни технологии, Управление на облачни инфраструктури, Системи за наблюдение на облачни инфраструктури, Програмиране на Python, Програмиране на Java, Автоматизирано управление на конфигурация под Linux.

Курсове, ползващи дисциплината са: Автоматизирано осигуряване на качеството на софтуера, разработване на магистърска теза.

12. Съдържание на курса:

Въведение в курса. Практиките DevSecOps мотивация и съвременни предизвикателства. Security compliance. Съответствие със закони и политики за сигурност в организацията. Определяне на цели и показатели за сигурност. Организационна цел. Цел/показател за развитие. Оценка на заплахи. Определяне на QA цел/показатели. Оперативни цели/показатели. Подобряване на сигурността на инфраструктурната среда. Оперативно активиране на поставени цели.

Програма и организация за осигуряване на сигурност. Програма за осигуряване на сигурността. SDL (Жизнен цикъл на разработки за защита на приложения). Преглед на платформата OWASP SAMM. Съвременни практики, насоки и моделиране на процеси за сигурност. Подход за определяне на изисквания за сигурност и съответствие. Представяне на обобщена система за оценка на уязвимости (CVSS). Изисквания за сигурност за уеб приложения. Стандарт за проверка на сигурността на приложенията OWASP (ASVS). Изграждане на портал със знания за сигурност. Изисквания за сигурност за големи данни. Технически рамки за сигурност на големи данни. Изисквания за поверителност за GDPR.

Подход за разработка на програма за осигуряване на защита на приложения. Microsoft SDL и SAMM. Обучение и осведоменост за киберсигурност. Култура на киберсигурност. Платформи за осигуряване на киберсигурност на уеб приложения. Подход за осигуряване на непрекъснат процес по интегриране на практики за киберсигурност посредством DevOps. Архитектура на сигурността и принципи на проектиране на защитени приложения. Подход за анализ на архитектурата за сигурност на облачните услуги. Подход за оценка и избор на Java платформа за осигуряване на сигурността на уеб приложения. Преглед на съществуващи платформи за уеб сигурност. Защита на поверителността на данните при уеб приложения. Управление на данните: Apache Ranger и Atlas. Управление на защитата на компоненти с отворен код, предоставени от трети страни.

Практики за моделиране на заплахи и дизайн на защитени приложения. Моделиране на заплахи със STRIDE. Съвременни практики за разработка на защитен код. Създаване на сигурна база за изходен код. Инструменти за преглед на код. Инструменти за сканиране на защитата на код. Компилиране със защита. Обработка на проблеми и изключения при защитен код. Сигурност и поверителност при проектиране на приложения. Преглед на защитена архитектура. Удостоверяване. Оторизация. Управление на сесията. Защита на входно-изходните на данни. Платформи за осигуряване на защита и поверителност: Управление на компоненти от трети страни. План и практики за тестване на сигурността. Изграждане на база от знания за тестване на сигурността. Шаблони за планове за тестване на сигурността. Изграждане на среда за тестване на сигурността и стратегия за тестване. Преглед на подходи за хакване на приложения: Експлойти и CVE. Хакерски техники. Информация за злонамерен софтуер. Изграждане на среда за обучение по киберсигурност.

Практики за тестване по подхода Whitebox. Подготовка за преглед на Whitebox. Преглед на целия проект и определяне на високорисков модул. Контролен списък за преглед на Whitebox. Модели на защита и ключови думи за разработка на защитен код. Използване на набор от инструменти за тестване на сигурността. Общи инструменти за тестване на

сигурността. Критерии за тестване на автоматизацията. Тестване на сигурността на Android. Защита на инфраструктурна конфигурация. Сканиране за сигурност на Docker. Интегрирани инструменти за сигурност. Автоматизация на сигурността в процес по непрекъсната интеграция на доставката на софтуер. Практики за киберсигурност при разработката и разгръщането на софтуер. IDE плъгини за автоматизиране на прегледа на кода. Автоматизация на сигурността в Jenkins. Съвременни практики за реакция при инциденти в киберсигурността. Подготовка, детекция и анализ. Ограничаване и възстановяване на работно състояние. Платформи за моделиране на процес по реакция на инциденти със сигурност (SIRP). Структура на екип SOC. Техники за киберразследване на инциденти. Мониторинг на сигурността. Рамка за наблюдение на сигурността. Набор от инструменти за разпознаване на заплахи. Набор от инструменти за сканиране на сигурността. Платформа за анализ на поведението на злонамерен софтуер: YARA. Анализ на защитата с помощта на BigData платформи. TheHive: платформа за анализ на заплахи с отворен код. Платформа Apache Metron.

13. Библиография

Основна литература:

1. Hsu, Tony Hsiang-Chih. Hands-On Security in DevOps: Ensure continuous security, deployment, and delivery with DevSecOps. Packt Publishing Ltd, 2018.
2. Zeeshan, Afzaal Ahmad, "DevSecOps for .NET Core", Apress, 2020.
3. Wei Lien Dang and Ajmal Kohgadari, "DevSecOps in Kubernetes", O'Reilly Media, Inc., ISBN: 978-1-098-10177-0, 2021..

Допълнителна литература:

1. Hsu, Tony Hsiang-Chih. "Practical security automation and testing: tools and techniques for automated security scanning and testing in DevSecOps". Packt Publishing Ltd, 2019.
2. Pendyala, Vishnu. "Evolution of Integration, Build, Test, and Release Engineering Into DevOps and to DevSecOps." In Tools and Techniques for Software Development in Large Organizations: Emerging Research and Opportunities. edited by Pendyala, Vishnu, 1-20. Hershey, PA: IGI Global, 2020. <http://doi:10.4018/978-1-7998-1863-2.ch001>
3. Turner, Richard. "Systems Engineering and DevSecOps: Reviewing the Principles." INSIGHT 24, no. 2 (2021): 38-43..

14. Методи и критерии на оценяване:

Дисциплината завършва с изпит.

Окончателната оценка по дисциплината се оформя чрез финален тест. Писменият тест обхваща отворени и затворени въпроси върху материала, посочен в конспекта и представен на лекциите по дисциплината. Критериите са: изчерпателност, точност и задълбоченост при отговаряне на поставените въпроси в теста.

15. Език на преподаване: български/английски