SFWE 402/502: Software DevSecOps
Course Syllabus

Course Description

Units: 4

This course will allow software engineering students to explore key principles of a DevSecOps approach to software development. Development (Dev) and operations (Ops) is the union of people, process, and technology to continually automate and develop higher quality/more reliable software products faster. Security (Sec) is integrated into a typical DevOps pipeline to address potential security issues in code as soon as possible in the software development lifecycle.

As part of this course, students will develop software using continuous integration / continuous deployment (CI/CD) principles in a pipelined environment. Students will also learn how to use DevSecOps practices and a variety of tools that enable CI/CD, provide version control of all software artifacts, automate testing, and provide continuous project monitoring. They will also learn the key attributes of establishing and working in a DevSecOps culture which embraces collaboration, alignment, accountability, and continuous learning/improvement.

This course is accompanied by a required lab that immerses students in a representative software development environment that they will likely encounter in industry. They will be able to use a variety of open-source and commercially available tools to complete assigned labs and develop a team-based semester project that exercises the principles studied throughout the course.

Instructor and Contact Information

Instructor Name: Sharon ONeal
Email: sharononeal@arizona.edu
Cell Phone: (520)822-4040
Office: Engineering Room 255
Office Hours:

- **Online via Zoom**: By Request (AZ time zone)
- **In-Office**: Tues & Thurs 2:00 – 3:30 *(or by appointment)*

You are encouraged to reach out to your instructor frequently throughout the semester via email, phone, text, office hours, or a scheduled synchronous meeting (in-person or Zoom). Every attempt will be made to respond to questions and concerns that you may have within 24 hours.

Course Pre-/Co-requisites

- Advanced Standing is *required*.
- Completion of ECE 275 is *required*.
- Completion of SFWE 401 is *recommended.*

Course Format and Teaching Methods

This course is structured around weekly progress. It will include a combination of lectures, and team activities focused on experiential learning, in-class discussions, and web-based assessments. The expected weekly progress

is outlined in the course schedule. At a minimum it is recommended that students keep up with coursework by following the outlined course schedule on D2L. Note the DUE DATES on course deliverables are all posted on D2L.

This course also has an accompanying laboratory element where students will be required to use a variety of tools and complete lab assignments that give them practical exposure/experience in employing DevSecOps principles in software development.

Course Objectives

During this course, you will:

1. Learn what a DevSecOps culture is and how it differs from more traditional software product development and deployment methodologies.
2. Learn how/and why integrating security into the software development lifecycle stages early enables the development of more secure code.
3. Use DevSecOps processes and techniques to develop software products.
4. Use open-source and commercially available tools to create and maintain CI/CD pipelines.
5. Work in collaborative teams to develop a software product that solves a real-world challenge or problem utilizing DevSecOps principles and toolchains.
6. Use formal configuration management processes to support the DevSecOps software product development activities throughout the software development lifecycle.

Expected Learning Outcomes

Upon completion of this course, you should be able to:

1. Develop/implement a software product that meets specified requirements in a team setting using DevSecOps processes and tools.
   [ABET Student Outcome 1, 2 and 5]
2. Create reusable CI/CD pipelines in the development and automated testing of a software product using commercially available tools.
   [ABET Student Outcome 7]
3. Develop and analyze results of continuous integration automated tests that are part of a CI/CD pipeline.
   [ABET Student Outcome 6]
4. Use configuration management tools to implement software configuration management and control processes integral to a DevSecOps environment.
   [ABET Student Outcome 1]
5. Follow secure coding standards when developing and deploying a software product integral to an engineering solution.
   [ABET Student Outcome 4 & 7]
6. Evaluate the results of using DevSecOps practices for a software product and present the results to peers and other project stakeholders.
   [ABET Student Outcome 3 & 6]

7. **[Graduate Students]** Analyze the benefits of creating a DevSecOps culture and using DevSecOps processes to develop and deploy software products.

Textbooks & Software

Required Textbooks

All required textbooks are available electronically through the UArizona library for *FREE*.

Continuous Delivery with Docker and Jenkins (3rd ed.)
Rafal Leszko
ISBN-10: 1803237481
ISBN-13: 978-1803237480

Recommended Textbooks

All recommended textbooks are available electronically through the UArizona library for *FREE*.

The DevOps Handbook: How to Create World-Class Agility, Reliability, & Security in Technology Organizations
Gene Kim, Jez Humble, Patrick Debols, and John Willis
ISBN-10: 1942788002
ISBN-13: 978-1642788003

Required Software

All software required for this course is available for *FREE* through the Digital Engineering Factory. Applications used in this course include:

- GitLab
- Jenkins
- Klocwork
- Jira
- An IDE of the student's choosing

Assignments and Examinations

Individual Homework and Lab Assignments (x7)

There will be regular homework and lab assignments on the topics covered in class, with approximately a total of 7 homework/lab assignments. These assignments are to be completed on an individual basis (not a team basis).

Knowledge Checks (x8)

There will be online, essay-based knowledge check questions with the completion of each module. There will be approximately 8 knowledge checks that will be factored into your grade. Knowledge checks are an individual assessment of your understanding of the concepts and knowledge covered in a given module.

Semester Project

Team Component - The semester project is a team-based project. Teams will be formed consisting of 5-6 students. Each team will be given a high-level software product description and a list of system and software level requirements. Using DevSecOps methodologies and tools, the team will be required to develop the software product, in a language of their choosing, that meets the given requirements. We will be using Jira to keep track of team tasking and issue resolution throughout the semester, and each team will be required to have 6 Agile sprints throughout the semester. The project will culminate in a

comprehensive Project Status Review and Demonstration with the course instructor and all students in the course.

Individual Components - In addition to the team portions of the project, you will be required to write a 2-page individual reflection of your experience working on the team, developing the requirements and test plan for the product the team was given, and also any lessons learned that you personally had working on the project.

Team Participation (part of the Individual Components) - Over the course of working on the semester team project, you will be required to individually submit 2 team evaluations for all deliverables for the semester project. Every team member is expected to contribute equally to the project. If there are team dynamics that are preventing a collaborative working environment, it is best to inform the instructor ahead of time so that adjustments can be made to facilitate effective teaming and communication amongst the team.

Your individual final team project grade will be factored by the average score of all team members' inputs from these evaluations. Failure to submit a team evaluation will result in the loss of 10 points from your personal team semester project score.

[Graduate Students] Graduate Students will complete an additional term paper; this term paper will be factored into the grade for the semester project. This term paper will describe the essential elements of setting up a DevSecOps environment and how to create a DevSecOps culture for a specific industry. The paper will also include how this may impact the overall quality and reliability of software products developed in the described environment.

Grade Distribution, Scale & Policies

The grading distribution for course assignments is as follows:

Homework (4) / Lab Assignments (4) (x8)	20%
Agile Backlogs (x6)	10%
Knowledge Checks (x8)	20%
Semester Project	50%
See total grade distribution below	
Team Charter (1%)	
Semester Project Tool Stack (1%)	
MVP1 (15%) (including source code)	
MVP2 (25%) (including source code + preliminary GitLab workflow)	
Team Evaluation #1 (3%)	
MVP3 (50%) (including source code, GitLab workflow, Static Analysis Report, and Final Demo)	
Team Evaluation #2 (5%)	
Total	**100%**

Late Work Policy

All assignments are due at the time that is specified in the course schedule and/or D2L content pages. Late assignments *will not* be accepted without prior approval by the instructor and will receive zero points.

Make-up exams may only be given under extraordinary circumstances. The student requesting a make-up exam should contact the instructor well in advance and provide *written* documentation for the reason that they will not

be able to attend the regularly scheduled exam. It is up to the discretion of the instructor to accept the justification provided by the student.

Instructor Grading & Student Appeals Policy

All assignments will be graded by the instructor within one week of the submission deadline. Feedback will be posted to D2L in the form of (1) detailed rubrics and (2) individualized written remarks. This feedback is designed to help you improve your craft; questions regarding your assignment feedback is welcomed during Office Hours or via email.

To appeal a grade on any assignment, submit an email identifying the assignment, question, and justification for the appeal within two weeks of the grade being posted to D2L.

Grading Scale

The following scale will be used to award final grades:

A	90-100%
B	80-89%
C	70-79%
D	60-69%
E	less than 60%

Incomplete (I) or Withdrawal (W):

Requests for incomplete (I) or withdrawal (W) must be made in accordance with University policies, which are available at http://catalog.arizona.edu/policy/grades-and-grading-system#incomplete and http://catalog.arizona.edu/policy/grades-and-grading-system#Withdrawal respectively.

Course Behavior Policy

To foster a positive learning environment, students and instructors have a shared responsibility. We want a safe, welcoming, and inclusive environment where all of us feel comfortable with each other and where we can challenge ourselves to succeed. To that end, our focus is on the tasks at hand and not on extraneous activities (e.g., texting, chatting, reading a newspaper, making phone calls, web surfing, etc.).

Generative AI Policy

In this course, generative artificial intelligence/large-language-models tools, such as ChatGPT, Dall-e, Bard, Bing, may be used for written homework assignments and portions (not all) of the semester project with appropriate acknowledgment and citation, ***but not for Knowledge Checks, quizzes or exams***. If you are in doubt as to whether you are using generative AI tools appropriately in this course, I encourage you to discuss your situation with me. Be aware that many AI companies collect information; do not enter confidential information as part of a prompt. LLMs may make up or hallucinate information. These tools may reflect misconceptions and biases of the data on which they were trained and the human-written prompts used to steer them. You are responsible for checking facts, finding reliable sources for, and making a careful, critical examination of any work that you submit.

Safety on Campus and in the Classroom

For a list of emergency procedures for all types of incidents, please visit the website of the Critical Incident Response Team (CIRT): https://cirt.arizona.edu/case-emergency/overview.

Also watch the video available at https://arizona.sabacloud.com/Saba/Web_spf/NA7P1PRD161/common/learningeventdetail/crtfy0000000000003560.

University Policies

Links to the following UA policies are available at, https://academicaffairs.arizona.edu/syllabus-policies:

- Absence and Class Participation Policies
- Threatening Behavior Policy
- Accessibility and Accommodations Policy
- Code of Academic Integrity
- Nondiscrimination and Anti-Harassment Policy
- Subject to Change Statement