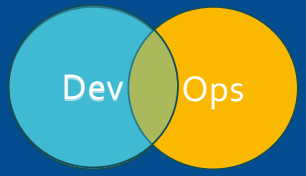
Teaching DevSecOps using a Project-Based Learning Approach

Yuting Zhang
Boston University

DevOps: What and Why?

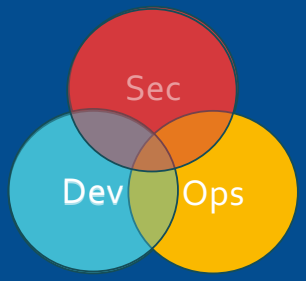


- Goals: Improve business agility and software quality
- Issue: gaps between development and operation
- Solution: integrate Dev (development) and Ops (Operations)
  - Culture changes: open communication, collaboration and shared ownership
  - Short iterations and continuous improvement: continuous integration (CI), continuous delivery (CD) and continuous monitoring and feedback
  - Automation from initial software development all the way to the final deployment/execution in production using a set of tools.

DevOps Pipeline

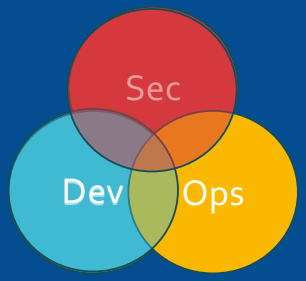
- May also referred to as a CI/CD pipeline.
- Version control to handle code changes
- CI: automated merge to the (main) branch, triggering automated builds and tests
- Automated testing: various types of tests (unit, integration, functional, security, etc) are automatically executed after each build to detect bugs (or defects).
- CD: if tests pass, the code is automatically deployed to staging environment for further testing and validation
  - Apps are often packaged in containers and deployed to cloud
- Release: once approved, the code is deployed to the final production environment, delivering to users
- Monitoring and feedback: continuously monitor the application performance and issues to provide feedback for improvements.

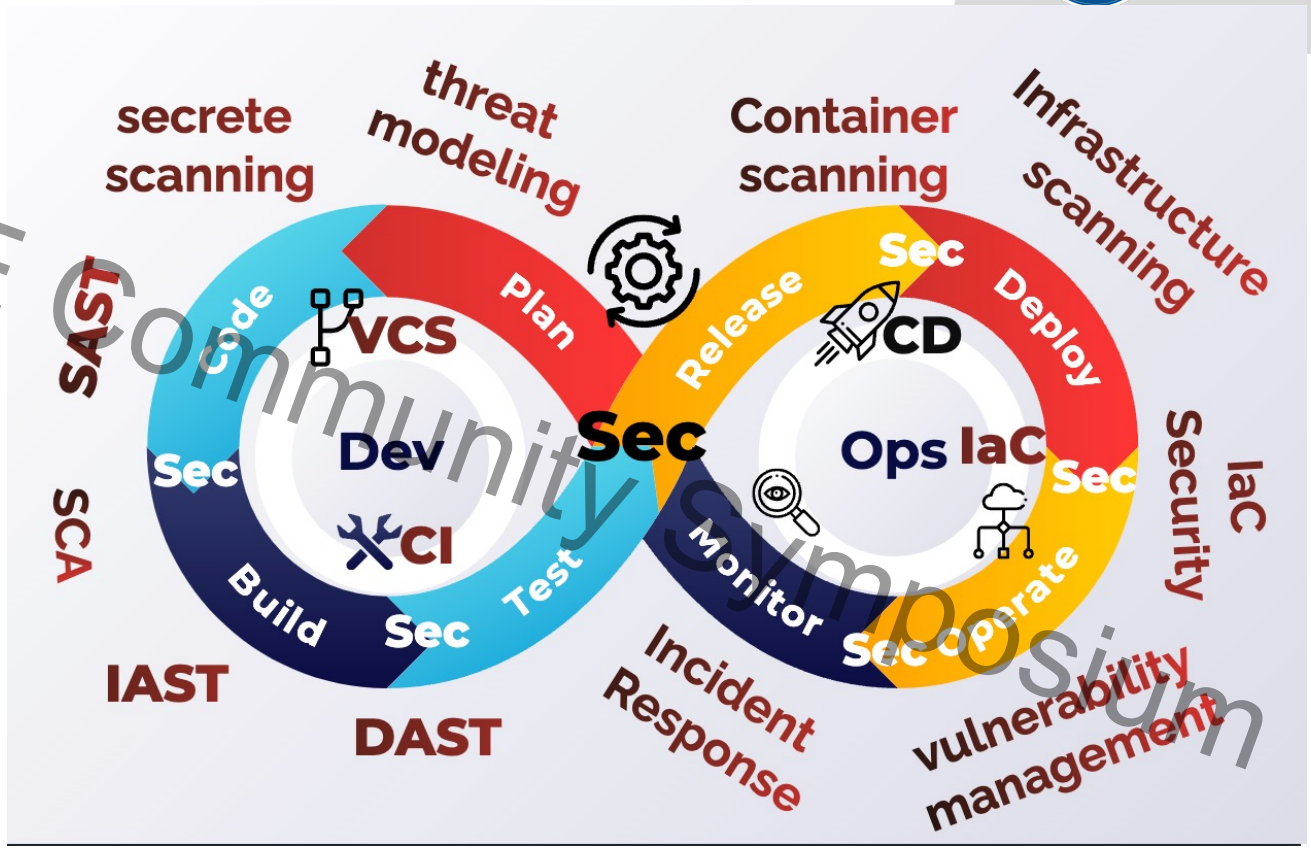
DevSecOps: What and Why?



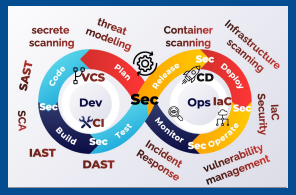
- Goal: Proactively identify and address security issues from the very beginning to reduce security risks and vulnerability and thus enhance security.
- Solution: extend DevOps philosophy by integrating security throughout all DevOps phases .
  - Promote better communication, collaboration and shared responsibility for security across development, operations and security teams.
  - Shift-left security, and focus on security awareness and continuous improvement in security practices

DevSecOps Pipeline



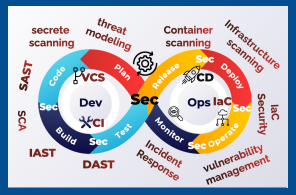


DevSecOps in Industry



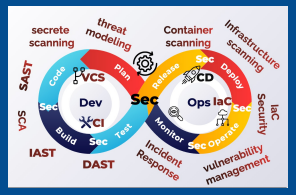
- DevOps/DevSecOps have gained increasing popularity in the software development industry
- 86% of organizations see the value of DevOps as important to have (Harvard Business Review Analytic services Study)
- 74% of organizations have adopted DevOps in some form. (RedGate).
- 36% of organizations had adopted DevSecOps in some form. (Gartner survey in 2022)
- Found many professional training courses/videos on specific platforms or tools through Internet search.
- DevSecOps industry certificates:
  - Certified DevSecOps Engineer (E-CDE) by EC-Council
  - DevSecOps Practitioner Certificate by DevOps institute
  - Certified DevSecOps Professional (CDE) and Certified DevSecOps Expert (CDE) by Practical DevSecOps

DevSecOps in Academic



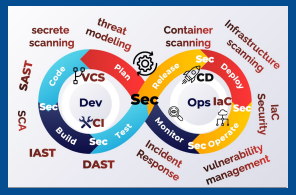
- Seldom used in student projects or research projects.
- Not included in
  - CAE KU
  - CC2023 – ACM/IEEE – CS/AAAI Computer Science Curricula recommendation
  - Software Engineering Body of Knowledge (SWEBOK) (IEEE Computer Society)
- Limited offers from Coursera and Udacity, most are focused primarily on specific topics or platforms.
- Very few universities offer related courses or programs.
  - Found about 10 universities in the USA offering specific DevSecOps courses, most are at introduction level and used for specific training purposes.
- There exists a gap between industry and academia in terms of DevSecOps adoption.

DevSecOps: Related fields and Job Roles



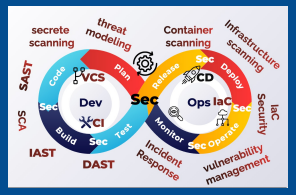
- Related fields
  - Software engineering, including software architecture, software testing, software operations, etc.
  - Cloud computing, including containerization technology, serverless computing, cloud infrastructure management, cloud security, etc.
  - Cybersecurity including software security, container security, cloud security, etc.
- Related Job Roles:
  - Software Engineer
  - DevOps/DevSecOps Engineer
  - Cloud Engineer
  - Security Engineer

DevSecOps Curriculum: Topics



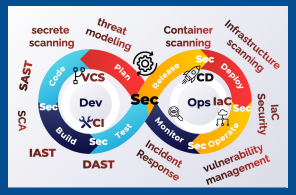
- DevOps and DevSecOps Key principles
- DevOps and DevSecOps Practices
  - Version control Core Concepts and Branching Strategies
  - Automated testing, Continuous Integration and continuous deployment
  - Security testing, including SAST, DAST, IAST, penetration testing, risk-based testing
  - Containerization and container security
  - Infrastructure management, including Infrastructure as Code and configuration management, and infrastructure security
  - Software Component analysis, compliance security, and secrete management
  - Vulnerability management
  - Monitoring and alerting
- DevOps and DevSecOps Pipeline and Tools
- Measurement and metrics
- Other important related topics:
  - Agile methodology
  - Web-based microservices and REST
  - Virtualization and Containerization
  - Software Testing and Building
  - Security analysis and security coding

DevSecOps: Learning Outcomes



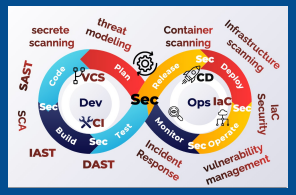
- Explain the key principles and working culture of DevSecOps
- Describe the phases of DevSecOps
- Perform basic security analysis
- Create docker files to package the application in docker containers
- Apply Infrastructure as Code to define required infrastructure
- Create automated tests and build a simple CI/CD pipeline to automate test, build, and deployment.
- Integrate SAST and DAST tools into CI/CD pipeline
- Integrate various security scanning tools such as SCA, secrete scanning, compliance scanning, license scanning, infrastructure scanning, etc, into CI/CD pipeline
- Manage detected vulnerabilities and analyze the vulnerability reports
- Monitor continuously the operational stability and security of the application in the deployed environment.

Dedicated Courses on DevSecOps



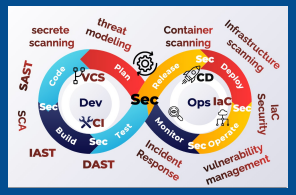
- Develop one or two dedicated DevSecOps courses
- Examples:
  - Introduction to DevSecOps by John Hopkins University via Coursera
  - DevSecOps Process and Implementation (CMU SEI) (2.5 day training course)
- Pros:
  - Easy management of curriculum
  - Structured learning
  - Better industry recognition
  - In-depth learning
- Cons:
  - Can only be an elective
  - Hard to fit into the schedule
  - Students may lack of background knowledge
  - More costly

Dedicated Modules in Related Courses



- Embed dedicated modules into existing courses such as
  - Software Engineering (most popular choice)
  - Software Security
  - Cloud Computing
- Pros:
  - Well integrated with other related topics in those courses
  - Provide better context and background knowledge
  - Suitable for different needs
- Cons:
  - Harder to manage and update curriculum across multiple courses
  - Need to coordinate the curriculum design to ensure consistency and avoid too much overlap

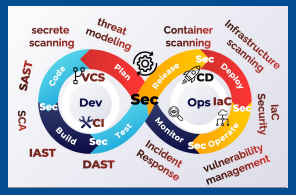
Broaden the adoption in Academic Programs



In all courses, we can

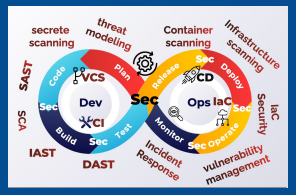
- Advocate shift-left Security
- Advocate automation using tools
- Advocate collaboration
- Advocate hands-on skills
- Advocate real-world projects
- Require to design a set of standards and criteria, as well as provide ready-to-use toolset

Project-Based Learning



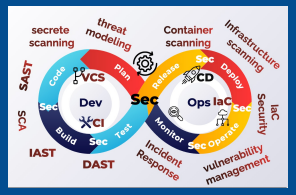
- DevSecOps: involve highly practical skills, practices, and tools
- Labs: short-term, specific instructions, same for all students, useful to learn individual tools
- Project-based learning:
  - student centered
  - help identify and understand real world issues
  - apply knowledge and skills learned to solve real problems
  - Customizable to individual
  - Critical for high-education
- Involve a real-world software project.
  - Develop a new software project
  - Extend an existing software project
- Explore tools and build pipeline
  - Depending on the implementation stack and type of software project.
  - Automate build & deployment
  - Automate security scanning and testing
- Preferably, long-term and group-based.

DevSecOps Tools



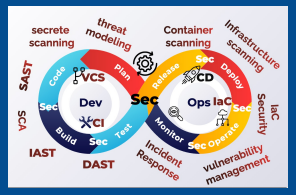
- Requirements and Project Management Tools: JIRA, Pivotaltracker, Trello
- Communication Tools: slack, discord, zoom, Microsoft team
- Build Tools: Maven, Gradle, Npm
- Automated Testing Frameworks: Junit, Pyunit, Selenium, Cypress
- SAST: SonarQube, Fortify
- DAST: ZAP, Burp suite
- SCA: GitHub dependabot, Synk
- Integration Tools: GitHub workflow/actions, Jenkins, Circle CI
- Containerization: Docker, Kubernetes, Docker Hub
- Container Scanning: Clair, Trivy
- IaC Tools: Terraform, CloudFormation, Checkov
- Configuration Management Tools: Ansible, Chef
- Cloud Platform: AWS, GCP, Azure
- Cloud monitor: CloudTrail, GuardDuty

Our Curriculum



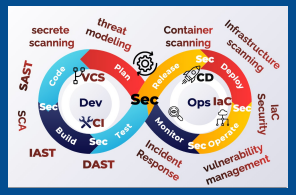
- Our courses are mostly graduate courses
- DevSecOps topics are mainly embedded into the following two courses, both courses feature a semester-long project.
- **Software Engineering (CS673)**
  - Related topics covered : agile, microservice, automated testing, devSecOps principles, CI/CD pipeline, containerization, IaC, security practices overview
  - Large group with 5-7 students to develop a new application with some basic DevSecOps practices in 4 iterations. One student is assigned to be the security lead in the group. Utilize GitHub, emphasize automated testing and CI/CD, encourage basic security practices.
- **Secure Software Development (CS763)**
  - Related topics covered: secure software development frameworks, DevSecOps principles and pipeline, Security requirements, Security analysis and threat modeling, Security coding, security testing (SAST, DAST, IAST, RASP), penetration testing, vulnerability taxonomy and management, security monitoring.
  - Small group project with 2 students to integrate and extend security analysis, features and practices into existing software projects.

Our Curriculum



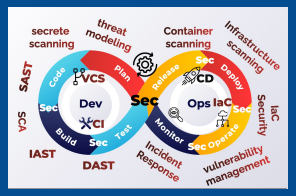
- DevSecOps related topics are also included in:
- Network and Cloud Security (CS690)
  - Containerization and virtualization
  - Identity management
  - IaC security and Infrastructure management
  - Attack and defend cloud-based web services and serverless applications
  - Security Monitoring
- Enterprise architecture (CS782):
  - Microservice, containerization and orchestra, cloud service and infrastructure management, security awareness, DevSecOps principles, case studies

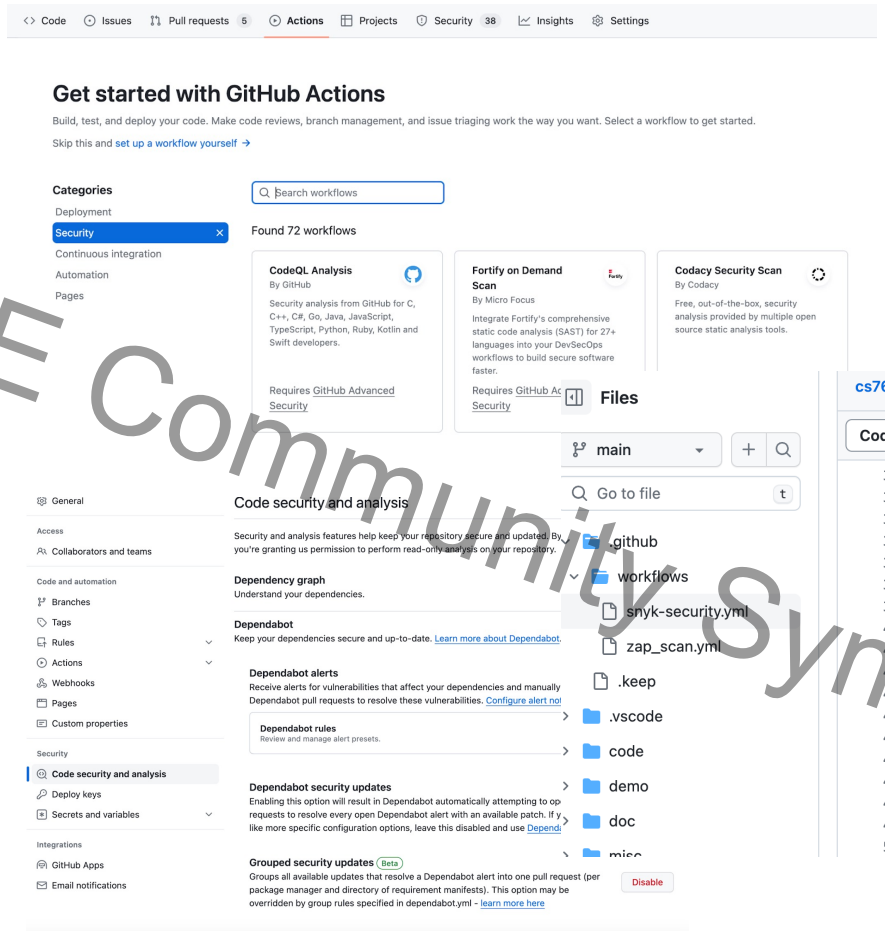
GitHub Support for DevSecOps

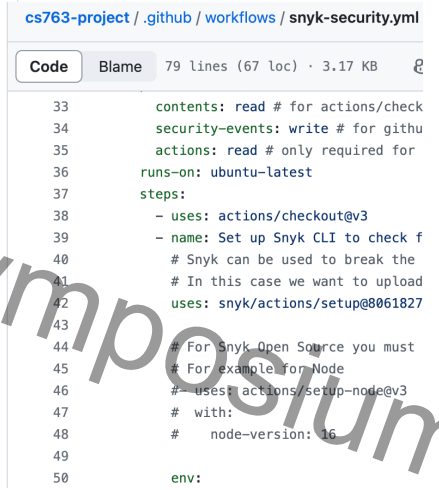


- Most students' software projects are hosted on GitHub
- GitHub workflows provide a powerful and flexible way to automate the various stages within a DevSecOps pipeline..
- Workflows can integrate with various DevSecOps tools and services. Github provides over 100 workflow templates for various tools integration.
- GitHub actions are reusable building blocks that perform specific tasks within a workflow. A vast library of GitHub actions are available to use, including building, testing, deploying, security scanning.
- GitHub also supports dependency scanning and secrete scanning directly.

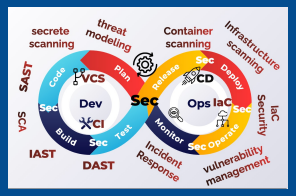
GitHub Support for DevSecOps

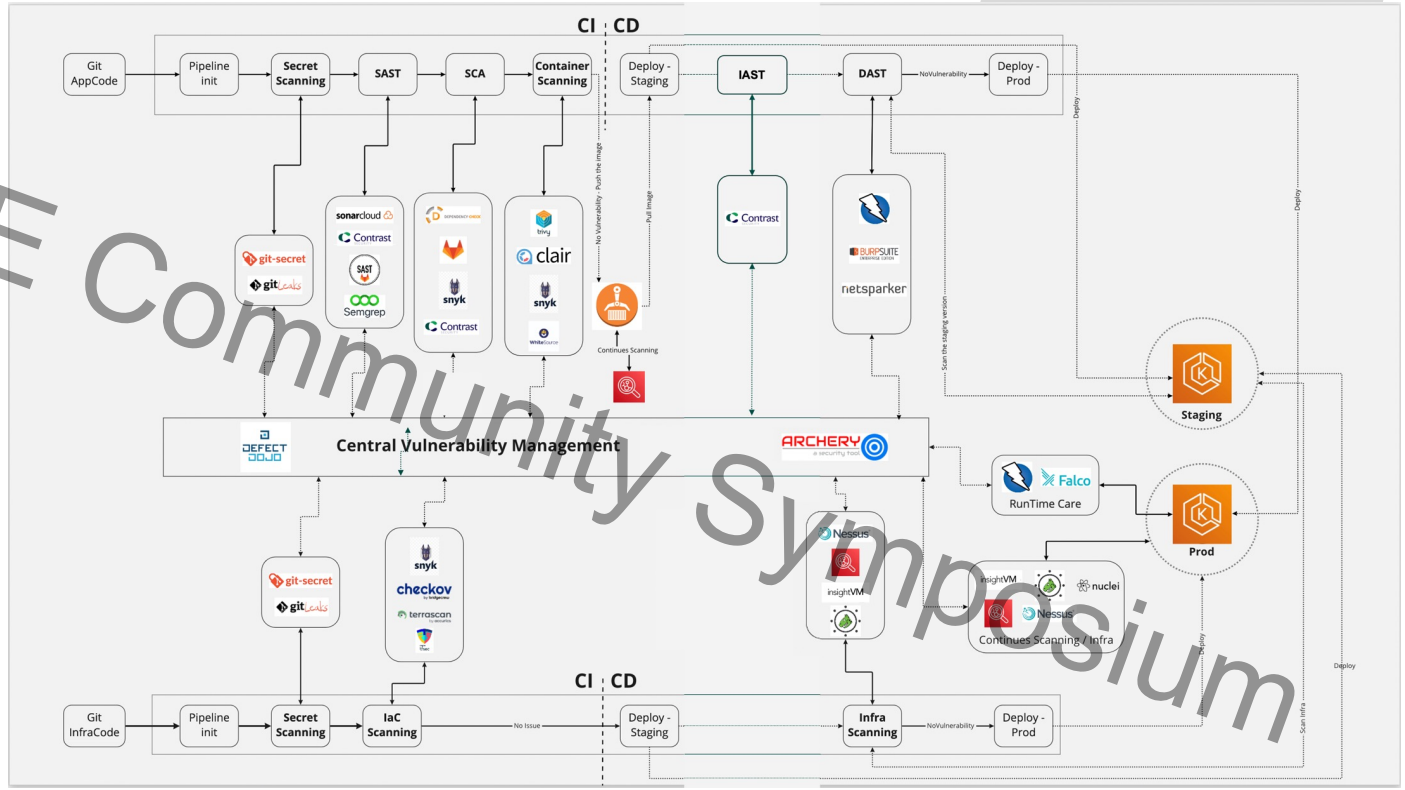






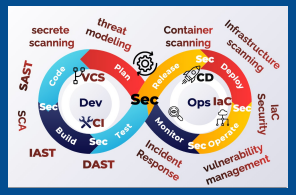
OWASP DevSecOps Guideline





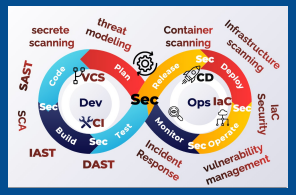
Source: OWASP DevSecOps Guideline (https://github.com/OWASP/DevSecOpsGuideline)

Challenges



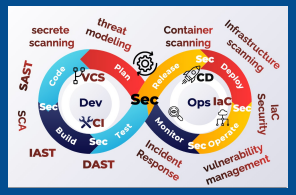
- Raid Evolution of technologies and Tools
  - require frequent curriculum updates
- Balance the depth and breadth
  - DevSecOps encompasses a broad range of topics in software development, security and infrastructure operations.
  - Delve into various specific areas in different courses.
- Project Advising
  - Individualized advising and support - small group size, additional TA
  - Promote peer learning
  - Iterative approach with quick feedback

DevSecOps Curriculum on Clark



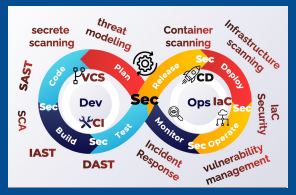
- CLARK: the largest platform of free cybersecurity curriculum https://clark.center/, developed by Towson University.
- A number of courses and modules on secure coding and software development can be found on Clark
- So far, no DevOps/DevSecOps courses or modules are available.
- I am developing 2 modules on DevSecOps and Secure Software Development that will be published on CLARK.

References: DevSecOps course Links



- https://www.edx.org/learn/devsecops
- https://www.classcentral.com/subject/devsecops
- https://www.udemy.com/course/devsecops/ , https://www.udemy.com/course/devsecops-in-aws-and-aws-security-services-asecurityguru/
- https://www.sans.org/cyber-security-courses/cloud-security-devsecops-automation/
- https://www.coursera.org/learn/introduction-to-devsecops
  https://ep.jhu.edu/courses/605609-devops-and-secure-software-development/
- https://www.sei.cmu.edu/our-work/devsecops/
- https://extendedstudies.ucsd.edu/courses-and-programs/devsecops
- https://pe.gatech.edu/courses/devsecops-and-agile-defense-acquisition , https://pe.gatech.edu/courses/devsecops-and-military-applications
- https://workforcecenter.slu.edu/public/category/courseCategoryCertificateProfile.do?method=load&certificateId=1337114 (https://workforcecenter.slu.edu/search/publicCourseSearchDetails.do?method=load&courseId=1505662)
- https://programmap.cypresscollege.edu/academics/interest-clusters/11c2c501-4273-4582-8f62-97683327dd16/programs/8f9e30b9-debb-9661-f155-2e484c3e1805?utm_source=FutureBuilt
- https://www.dau.edu/courses/swe-0027-0
- https://sie.engineering.arizona.edu/sites/sie.engineering.arizona.edu/files/SFWE-402-502-Syllabus-R1%281%29.pdf
- https://workforce.ship.edu/professional-development/self-paced-online-programs/certificate-programs-with-individual-course-options/agile-and-devsecops-courses
- https://customcareer.miami.edu/classes/devops-foundations-devsecops/
- https://professional.uchicago.edu/find-your-fit/courses/devops
- https://professional.uchicago.edu/find-your-fit/courses/devops
- https://waltoncareers.uark.edu/classes/devops-foundations-devsecops/
- https://knowltonconnect.denison.edu/classes/devops-foundations-devsecops/

References



- S. Ferino, M. Fernandes, E. Cirilo, L. Agnez, B. Batista, U. Kulesza, E. Aranha and C. Treude, "Overcoming Challenges in DevOps Education through Teaching Methods." *In Proceedings of the 45th International Conference on Software Engineering: Software Engineering Education and Training (ICSE-SEET '23)*.
- I. Alves and C. Rocha, "Qualifying software engineers undergraduates in DevOps - challenges of introducing technical and non-technical concepts in a project-oriented course.," in *Proceedings of the 43rd International Conference on Software Engineering: Joint Track on Software Engineering Education and Training*, 2021.
- R. Hobeck, I. Weber, L. Bass and H. Yasar, "Teaching DevOps: a tale of two universities," in *2021 ACM SIGPLAN International Symposium on SPLASH-E*, Chicago, 2021.
- E. Bobrov , A. Bucchiarone, N. Guelfi, M. Mazzara and S. Masyagin, "Teaching DevOps in academia and industry: reflections and vision," in *DEVOPS*, 2019.

Questions?