COURSE SYLLABUS

Utveckling, säkerhet och drift (DevSecOps)
Development Security Operations (DevSecOps)
7.5 credits (7,5 högskolepoäng)

Course code: PA2588
Main field of study: Software Engineering, Computer Science
Disciplinary domain: Technology
Education level: Second cycle
Specialization: A1N - Second cycle, has only first cycle course/s as entry requirements

Language of instruction: English
Applies from: 2022-08-29
Approved: 2022-03-01

1. Decision
This course is established by Dean 2021-11-30. The course syllabus is approved by Head of Department of Software Engineering 2022-03-01 and applies from 2022-08-29.

2. Entry requirements
Admission to the course require at least 120 credits, of which at least 90 credits are in a technical area, and a minimum of 2 years professional experience within an area related to software-intensive product and/or service development (shown by, for example, a work certificate from an employer).

3. Objective and content

3.1 Objective
The purpose of the course is to provide students with an understanding of how IT security can be involved in continuous software engineering processes. The students will learn about methods and techniques to tailor security practices to the agile and DevOps product development context.

3.2 Content
This course explains how a secure development process is expected by industry regulators, and how to implement it in an agile and DevOps lifecycle.

This course will cover secure agile and DevOps software development with a focus on the following components:
• People: Enablement of agile teams for security through awareness, training and coaching.
• Processes: Implementation of security activities into well-known agile development processes such as SCRUM or SAFe. Security activities are analyzed based on relevant industry security standards.
• Technology: Description of security tools and technologies that can automate security activities in the agile & DevOps way of working.

4. Learning outcomes
The following learning outcomes are examined in the course:

4.1 Knowledge and understanding
On completion of the course, the student will be able to:
• Understand the phases of a secure development process, based on relevant industry security standards.
• Understand the challenges of implementing a secure development process within the context of the agile and DevOps lifecycle.
• Discuss security engineering methods and techniques covered in the course.

4.2 Competence and skills
On completion of the course, the student will be able to:
• Select secure agile and DevSecOps techniques to achieve a secure development process in a given context e.g. security automation, security champion coaching.
• Develop and justify a suitable strategy to implement secure agile and DevSecOps in a given context.

4.3 Judgement and approach
On completion of the course, the student will be able to:
• Reflect on which aspects of the proposed strategy are pertinent to specific roles, whether product owner, developer, operations engineer, scrum master, security specialist, other.

5. Learning activities
The teaching is organized around online lectures, pre-recorded videos, together with written material and research literature. Throughout the course, communication, feedback, and discussions with teachers and fellow participants will take place through email and the course´s online learning platform.

6. Assessment and grading
Modes of examinations of the course

Code	Module	Credits	Grade
2210	Written assignment 1	2 credits	GU
2220	Written assignment 2	2.5 credits	GU
2230	Written assignment 3	3 credits	GU

The course will be graded G Pass, UX Fail, supplementation required, U Fail.

The information before a course occasion states the assessment criteria and make explicit in which modes of examination that the learning outcomes are assessed.

An examiner can, after consulting the Disability Advisor at BTH, decide on a customized examination form for a student with a long-term disability to be provided with an examination equivalent to one given to a student who is not disabled.

7. Course evaluation
The course evaluation should be carried out in line with BTH:s course evaluation template and process.

8. Restrictions regarding degree
The course can form part of a degree but not together with another course the content of which completely or partly corresponds with the contents of this course.

9. Course literature and other materials of instruction
The following books are recommended:
• Bird, J.: Security as Code: Security Tools and Practices in Continuous Delivery, chap. 4, pp. 32–36. O'Reilly Media, Incorporated (2016)
• Kim, G., Behr, K., Spafford, G.: The Phoenix Project: A Novel about IT, DevOps, and Helping Your Business Win. IT Revolution Press (2018)
• Humble, J., Farley, D.: Continuous Delivery: Reliable Software Releases through Build, Test, and De- ployment Automation. Pearson Education (2010)

Additional material such as research articles and other course materials, as well as recommendations for additional reading, are provided via the courses online platform.