# H8DOS: DevOpsSec

Module Code:		H8DOS				
Long Title		DevOpsSec APPROVED				
Title		evOpsSec				
Module Level:		EVEL 8				
EQF Level:						
EHEA Level:		irst Cycle				
Credits:						
Module Coordinator:						
Module Author:		Alex Courtney				
Departments:		School of Computing				
Specifications of the qualifications and experience required of staff		Master's degree in computing or cognate discipline.				
Learning Ou	tcomes					
On successfu	l completion of this modu	ıle the learner will be able to:				
#	Learning Outcome	me Description				
LO1	Describe in detail the	the theory, concepts and methods pertaining to DevOpsSec.				
LO2	Develop a Continuo	uous Integration (CI)/Continuous Delivery (CD) Pipeline.				
LO3	Apply Security to the	e DevOps Pipeline.				
LO4	Collaboratively utilise	tools and techniques in creating a DevOpsSec Pipeline.				
Dependencie	es					
Module Recommendations						
No recommendations listed						
Co-requisite Modules						
No Co-requisite modules listed						
Entry requirements		Learners should have attained the knowledge, skills and competence gained from stage 3 of the BSc (Hons) in Computing.				

# H8DOS: DevOpsSec

#### **Module Content & Assessment**

#### **Indicative Content**

### DevOps

DevOps. Reference Architecture for DevOps. Change Management. Continuous Integration (CI). Continuous Delivery (CD). Continuous Testing. Infrastructure as a Service. Continuous Security

#### **Continuous Integration**

CI pipeline. Code Repository. CI Platform.

#### Continuous Delivery

CD Pipeline. Container Repository. Production Infrastructure. Deployment Automation and Release Management

#### **DevOpsSec - Continuous Security**

Test Driven Security. Application Security. Infrastructure Security. Pipeline Security. Testing Continuously. Monitoring and Responding to Attacks. Assessing Risks and Maturing

## Protecting Web Applications

Securing and testing web apps. Website attacks and content security. Methods for authenticating users. Managing dependencies

#### Automating security testing of the Infrastructure in the CD pipeline

Securing and testing cloud infrastructure: the deployer app. Restricting network access. Building a secure entry point. SSH Security Considerations. Opening access between security groups. Controlling access to the database. . Multifactor Authentication. Database permission models to control access. Database admin credentials

Securing communication
Secure communication. SSL/TLS. HTTPS

#### Securing the delivery pipeline

Access control to code-management infrastructure. Access control for container storage. Access control for infrastructure management.

#### Collecting and analysing logs

Collecting logs from systems and applications. Streaming logging events through message brokers. Processing events in log consumers. Storing and archiving logs. Accessing logs. Architecture of a log analysis layer. Detecting attack using string signatures. Statistical models for fraud detection. Using geographic data to find abuses. Detecting anomalies in known patterns. Raising alerts to operators and end users

Assessment Breakdown	%	
Coursework	100.00%	

#### Assessments

#### **Full Time**

Coursework							
Assessment Type:	Formative Assessment	% of total:	Non-Marked				
Assessment Date:	n/a	Outcome addressed:	1,2,3,4				
Non-Marked:	Yes						
Assessment Description: Formative assessment will be provided on the in-class individual or group activities.							
Assessment Type:	Labs	% of total:	60				
Assessment Date:	n/a	Outcome addressed:	1,2,3				
Non-Marked:	No						
Assessment Description: A series of labs that demonstrate the securing of the DevOps pipeline.							
Assessment Type:	Project	% of total:	40				
Assessment Date:	n/a	Outcome addressed:	sed: 4				
Non-Marked:	No						
Assessment Description: Learners work in teams to create a DevOpsSec pipeline							

No End of Module Assessment

No Workplace Assessment

#### Reassessment Requirement

#### Repeat examination

Reassessment of this module will consist of a repeat examination. It is possible that there will also be a requirement to be reassessed in a coursework element.

# **Reassessment Description**

Learners who fail this module will be required to sit a repeat module assessment where all learning outcomes will be examined. Learning EnvironmentLearning will take place in a classroom/lab environment with access IT resources. Learners will have access to library resources, both physical and electronic and to faculty outside of the classroom where required. Module materials will be placed on Moodle, the College's virtual learning environment

# H8DOS: DevOpsSec

Module Workload									
Module Target Workload Hours 0 Hours									
Workload: Full Time									
Workload Type	Workload Description	Hours	Frequency	Average Weekly Learner Workload					
Lecture	Classroom & Demonstrations (hours)	24	Every Week	24.00					
Tutorial	Other hours (Practical/Tutorial)	12	Every Week	12.00					
Independent Learning	Independent learning (hours)	89	Every Week	89.00					
Total Weekly Contact Hours									

## Module Resources

#### Recommended Book Resources

Jim Bird. DevOpsSec, [ISBN: 9781491971413].

Julien Vehent. (2018), Securing DevOps, Manning Publications, p.400, [ISBN: 1617294136].

#### Supplementary Book Resources

Gene Kim, Patrick Debois, John Willis, Jez Humble. (2015), The DevOps Handbook, It Revolution Press, p.480, [ISBN: 1942788002].

Modula Assassment

The module is practical in nature and promotes graduate attributes such as team work and therefore the assessment is based on continuous assessments and a Collaborative Project..

Assessment Type.

Assessment Description.

Assessment Learning Outcomes.

Assessment Percentage of Total Mark.

Assessment Timing.

Formative Assessment.

Formative assessment will be provided on the in-class individual or group activities..

1,2,3, 4.

Labs.

A series of labs that demonstrate the securing of the DevOps pipeline..

1,2,3.

ongoing.

Project.

Learners work in teams to create a DevOpsSec pipeline.

Week 12

Specifications for module staffing requirements.

Master's degree in computing or cognate discipline. May have industry experience also..

Module Re-assessment.

Learners who fail this module will be required to sit a repeat module assessment where all learning outcomes will be examined..

This module does not have any article/paper resources

This module does not have any other resources

Discussion Note: