ITIS 180D: SECURITY IN AMAZON WEB SERVICES

Citrus College Course Outline of Record

Heading	Value
Effective Term:	Fall 2022
Credits:	3
Total Contact Hours:	54
Lecture Hours :	54
Lab Hours:	0
Hours Arranged:	0
Outside of Class Hours:	108
Prerequisite:	ITIS 180A.
Strongly Recommended:	ITIS 109, ENGL 101.
Transferable to CSU:	No
Transferable to UC:	No
Grading Method:	Standard Letter

Catalog Course Description

This course focuses on protecting the confidentiality, integrity and availability of computing systems and data. Students learn how Amazon Web Service (AWS) uses redundant and layered controls, continuous validation and testing, and a substantial amount of automation to ensure the underlying infrastructure is continuously monitored and protected. Students examine the AWS Shared Responsibility Model and access the AWS Management Console to learn more about security tools and features provided by the AWS platform. 54 lecture hours.

Course Objectives

- Describe the AWS Shared Responsibility Model
- Describe security best practices employed with AWS applications
- Manage security groups, access control lists, users, roles and permissions
- Create secure websites using SSL/TLS certificates
- Support multi-factor authentication in their AWS applications
- Monitor and log security events using AWS tools

Major Course Content

1. Introduction to AWS, the Management Console and the Security Services Category
2. Security Best Practices and Case Studies
3. The Shared Responsibility Model
4. Security Groups and Network Access Control Lists
5. Managing User Credentials, Roles And Permissions
6. Managing SSL/TLS Certificates For Secure Websites
7. Monitoring and Logging
8. Multi-Factor Authentication

Examples of Outside Assignments

Using the Amazon Web Services console, track user session handling in order to completevarious auditing tasks.

Instruction Type(s)

Lecture, Online Education Lecture