Miami Dade College

Course Description

CIS3644C |Cloud Security | 4.00 credits

This course equips students with essential principles, tools, and techniques to effectively secure, configure, and operate cloud-based information systems. Students will learn cloud services essentials, such as computing, storage, databases, and networking. Additionally, they'll delve into security tools, key management services, digital signatures, certificates, authentication protocols, SSO services, firewalls, and access control lists. Prerequisites: CTS1120 and CTS2375C.

Course Competencies

Competency 1: The student will demonstrate an understanding of Identity and Access Management (IAM) on the Cloud by:

1. Discussing the Cloud shared responsibility model
2. Explaining how to share and control individual and group access to Cloud resources
3. Discussing how Identity and Access Management (IAM) integrates with Cloud services
4. Discussing the benefits of granular permissions and the principle of least privilege
5. Discussing the benefits and implementation of multi-factor authentication (MFA)
6. Identifying and interpreting Identity and Access Management (IAM) Policies, including:
    a. Service control policies
    b. Identity-based policies
    c. Resource-based policies

Competency 2: The student will demonstrate an understanding of Access Control of the Cloud by:

1. Describing different methods for access control, role-based access control (RBAC), and attribute-based access control (ABAC)
2. Identifying permission boundaries
3. Identifying an Identity and Access Management (IAM) policy structure
4. Performing an Identity and Access Management (IAM) policy evaluation
5. Launching a policy generator and policy simulator

Competency 3: The student will demonstrate how to implement Logging and Monitoring on the Cloud by:

1. Identifying applications that help collect and visualize real-time logs, metrics, and event data
2. Utilizing dashboards to aid with infrastructure and application maintenance
3. Identifying how to record and monitor activity from accounts across the Cloud infrastructure
4. Determining remediation actions based on logs and audit reports
5. Describing the components needed to create a custom metric to analyze accounts' logging and use
6. Identifying features that will enable the capture of IP traffic coming in and out of network interfaces on a virtual private cloud (VPC)
7. Describing the process of creating alarms based on metrics and enabling automatic notifications

Competency 4: The student will demonstrate how to implement and deploy Incident Response on the Cloud by:

1. Identifying the proper procedures to recognize an incident. b) Discussing the different phases of incident response, including:
    a. Discovery
    b. Recognition
    c. Resolution, and iv. Recovery
2. Inspecting a Cloud environment and making recommendations for applications to improve discovered security gaps
3. Identifying the proper applications to use for vulnerability management, threat intelligence, and distributed denial of service (DDoS) attack prevention

4. Identifying the current and past resource configurations to help analyze and troubleshoot outages
5. Discussing the use of templates to create and deploy a Cloud environment, and use the templates to re-create a new environment for recovery
6. Discussing the process of identifying key personnel and external resources needed. h) Discussing the creation and development of an incident response plan, constant evaluation of the incident response plan, and rehearsal, run, or simulation of the incident response plan

Competency 5: The student will demonstrate an understanding of infrastructure security and edge security on the Cloud by:

1. Describing techniques to deploy a secure virtual private cloud (VPC) design
2. Describing a custom virtual private cloud (VPC) with subnets
3. Identifying the process to secure customer and server management keys using a key management service (KMS)
4. Discussing protection of data at rest and data in transit
5. Discussing the difference between stateful and stateless firewalls and their implementations
6. Identifying security groups and network access control lists (NACLs), usage, and implementations
7. Discussing Virtual Private Cloud (VPC) peering
8. Describing different ways to connect to a Cloud environment using a site-to-site virtual private network (VPN) and direct connect
9. Understanding domain name service (DNS) resolution and routing, including canonical name (CNAME) and alias records
10. Describing secure content delivery using content delivery networks to help distribute fast, high-performance, scalable, and secure user experiences for applications and content
11. Discussing the advantages of a web application firewall (WAF)

Competency 6: The student will demonstrate an understanding of federation and single sign-on (SSO) techniques on the Cloud by:

1. Describing the integrated mechanism of administration experience to define, customize, and assign fine-grained access
2. Discussing identity federation as a system of trust between multiple identity management systems to authenticate users and convey information needed to authorize their access to resources
3. Describing single sign-on (SSO) as an authentication mechanism enables users to authenticate multiple applications and websites using just one set of credentials
4. Identifying the use and implementation of directory services to provide a storage area for users' and resources' identities and enable access to the infrastructure