EET-4200: CLOUD SECURITY FOR MANUFACTURING

Cuyahoga Community College

Viewing: EET-4200 : Cloud Security for Manufacturing

Board of Trustees:

September 2023

Academic Term:

Fall 2024

Subject Code

EET - Electrical/Electronic Engineer

Course Number:

4200

Title:

Cloud Security for Manufacturing

Catalog Description:

Cloud Security for Manufacturing provides an overview of cloud security while allowing students to gain insights into issues such as detecting suspicious traffic flows, policy violations, compromised sensors and IIoT devices, implementing data security controls, identity and access management, and key management.

Credit Hour(s):

3

Lecture Hour(s):

1

Lab Hour(s):

4

Requisites

Prerequisite and Corequisite

EET-3210 CyberOps for Manufacturing.

Outcomes

Course Outcome(s):

Build, design, and manage applications on the cloud platform for organizations. Estimate data compromise through exfiltration or ransomware lock down.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Examine cloud computing challenges.
2. Identify and evaluate cloud security scope, responsibilities, and models.
3. Recommend and evaluate improvement in areas of critical focus in cloud security.

Course Outcome(s):

Examine potential cloud security hazards for manufacturing businesses to reduce or eliminate their financial impact.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Evaluate cloud governance and accessibility tools.
2. Analyze risk management for enterprise in the cloud.
3. Identify service/deployment models and their effects.
4. Estimate and analyze cloud risk trade-offs.

Course Outcome(s):

Analyze legal issues and considerations in cloud management.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Evaluate legal frameworks governing data protection.
2. Analyze and examine contracts and provider selection.
3. Analyze and evaluate electronic discovery.

Course Outcome(s):

Evaluate and manage short comings associated with audits and compliance.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Evaluate and identify compliance in the Cloud.
2. Evaluate and identify audit management in the Cloud.

Course Outcome(s):

Make recommendations for the management of information in a safe and effective manner to support industry goals and comply with laws and regulations.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Analyze governance domains.
2. Evaluate and identify the six phases of the data security lifecycle and their key elements.
3. Evaluate and analyze data security functions, actors and controls.

Course Outcome(s):

Assess and determine the importance of management plan and business continuity.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Analyze business continuity and disaster recovery in the cloud.
2. Analyze and determine architect for failure.
3. Determine, examine, and recommend management plan security.

Course Outcome(s):

Analyze and evaluate infrastructure security.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Analyze cloud network virtualization.
2. Analyze security changes with cloud networking.
3. Analyze challenges of virtual appliances.
4. Analyze Software Defined Networking (SDN) security benefits.
5. Analyze micro-segmentation and the software defined perimeter.
6. Analyze hybrid cloud considerations.
7. Analyze cloud compute and workload security.

Course Outcome(s):

Assess by comparison/contrast the function of virtualization and containers.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Examine major virtualizations categories.
2. Analyze and evaluate networks.
3. Analyze and evaluate storage.
4. Analyze and evaluate containers.

Course Outcome(s):

Estimate and determine the influence of Incident Response.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Analyze incident response lifecycle.
2. Analyze how the cloud impacts incident response.

Course Outcome(s):

Analyze criteria of application security.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Examine opportunities and challenges of application security.
2. Examine secure software development lifecycle.
3. Analyze how cloud impacts application design and architectures.

Course Outcome(s):

Distinguish the function of Data Security and Encryption.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Analyze data security controls.
2. Analyze cloud data storage types.
3. Analyze managing data migrations to the Cloud.
4. Analyze securing data in the Cloud.

Course Outcome(s):

Evaluate the influence of identity, entitlement, and access management (IAM).

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Evaluate IAM standards for Cloud Computing.
2. Analyze the management of users and identities.
3. Analyze authentication and credentialing.
4. Evaluate entitlement and access management.

Methods of Evaluation:

1. Programs writing
2. Hands-on exercises
3. Quizzes
4. Midterm examination
5. Final examination

Course Content Outline:

1. Principle and concepts
    a. Least privileged
    b. Defense in depth
    c. Threat Actors, Diagrams, and Trust Boundaries
    d. Cloud delivery models
    e. Risk Management
2. Data Asset Management and Protection
    a. Data identification and Classification
    b. Data asset Management in the Cloud
    c. Protecting Data in the Cloud
3. Cloud Asset Management and Protection
    a. Difference from Traditional IT
    b. Types of Cloud Assets
    c. Asset Management Pipeline
    d. Tagging Cloud Management
4. Identity and Access Management
    a. Differences from traditional IT
    b. Life Cycle for Identity and Access
    c. Request/Approve
    d. Create, Delete, Grant, or Revoke

  e. Authentication
  f. Authorization

5. Vulnerability Management
   a. Differences from Traditional IT
   b. Vulnerable areas
   c. Finding and Fixing Vulnerabilities
   d. Risk Management Processes
   e. Vulnerability Management Matrix
   f. Change Management
6. Network Security
   a. Concept and Definitions
   b. Differences from Traditional IT
7. Detecting, Responding to, and Recovery
   a. Differences from Traditional IT
   b. What to Watch
   c. How to Watch
   d. Preparing for a Incident
   e. Responding to a Incident
   f. Recovery
   g. Example Metrics
   h. Example tools for Detection, Response

Resources

Avinash Shukla, Japla Patel. *Cisco Cloud Infrastucture*. 1st. Cisco Press, 2023. February 10th.

Chris Jackson. *CCNA Cloud CLDADM 210-455 LiveLessons*. 1st. Cisco Press, 2016. October 28th.

Chris Dotson. *Practical Cloud Security: A Guide for Secure Design and Deployment.*. 1st. 2019. March 30th.

Top of page
Key: 5137