NURTURE
Education Solutions
TOMORROW'S HERE

Chapter 2.2

Complete Certificate of Cloud Security

Aim

To provide the students with the knowledge of complete certificate of cloud security

Instructional Objectives

Objectives of this chapter are:

- Explain Cloud Controls Matrix
- Explain the concepts required for Certificate of Cloud Security Knowledge (CCSK)

Cloud Controls Matrix

Cloud Controls Matrix

- The Cloud Security Alliance Cloud Controls Matrix (CCM) is specifically designed to provide basic security principles to guide cloud providers and to assist prospective cloud consumers in assessing the overall security risk of a cloud provider.
- The Cloud Controls Matrix provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains.
- The basics of the Cloud Security Alliance Controls Matrix relies on its customized relationship to other industry-accepted security standards, regulations, and controls frameworks.
- CCM also provides standardized security and operational risk management.

Domains of Cloud Control Matrix

The first domain of CCM deals with compliance concerns for regular audits, inspections and reviews of data, objects, application, infrastructure and hardware at regular intervals

Data Governance domain of CCM will handle all the possible scenarios of data theft, misuse, leakage, disposal, retention and related risks.

The third domain of CCM Facility Security is all about the protection of the physical location of data in the cloud

Fourth domain of CCM deals with an employee's background screening, employment agreements and terminations to enforce technology based restriction on Cloud

Information Security domain of CCM gives the cloud customer a chance to discuss managerial issues with the cloud vendor.

In order to ensure continuity and availability of operations, a separate domain of operations management is included in CCM, which deals with establishments of policies and procedures for equipment maintenance

CCM has included a risk management domain to ensure that formal risk assessments are planned and scheduled at right intervals to determine the likelihood and impact of identified risks, using qualitative and quantitative methods.

Video Lecture

Click the image to view the video lecture

Video Lecture Explanation

Quiz / Assessment

1) Which of the following is a non-profit organization with a mission to promote the use of best practices for providing security assurance within cloud computing?

a) CSA
b) CCSK
c) CCM
d) ENISA

2) What are the domains of cloud control matrix?

Complete Certificate of Cloud Security Knowledge (CCSK)

Complete Certificate of Cloud Security Knowledge (CCSK)

The Cloud Security Alliance (CSA) established the Complete Certificate of Cloud security Knowledge (CCSK) certification as a basis of cloud security knowledge.

The CCSK provides a strong basis of cloud security essential knowledge and best practices for cloud computing.

CCSK has 13 domains which are included in three main areas. These three areas are cloud architecture (include domain 1), cloud governance (domain 2-6) and cloud operations (domain 7-13).

.

Cloud Architecture

This area include domain 1

Domain 1: Cloud Computing Architectural Framework

Cloud Governance

This area include domain 2 to domain 6

Domain 2: Governance and Enterprise Risk management

Domain 3: Legal and Electronic Discovery

Domain 4: Compliance and Audit

Domain 5: Information Lifecycle Management

Domain 6: Portability and Interoperability

Cloud Operations

This area include domain 7 to domain 13

- Domain 7: Traditional Security, Business Continuity, Disaster Recovery
- Domain 8:Data Center Operations
- Domain 9: Incident Response
- Domain 10: Application Security
- Domain 11: Encryption and Key Management
- Domain 12: Identity and Access Management
- Domain 13: Virtualization

Video Lecture

Click the image to view the video lecture.

Video Lecture Explanation

Quiz / Assessment

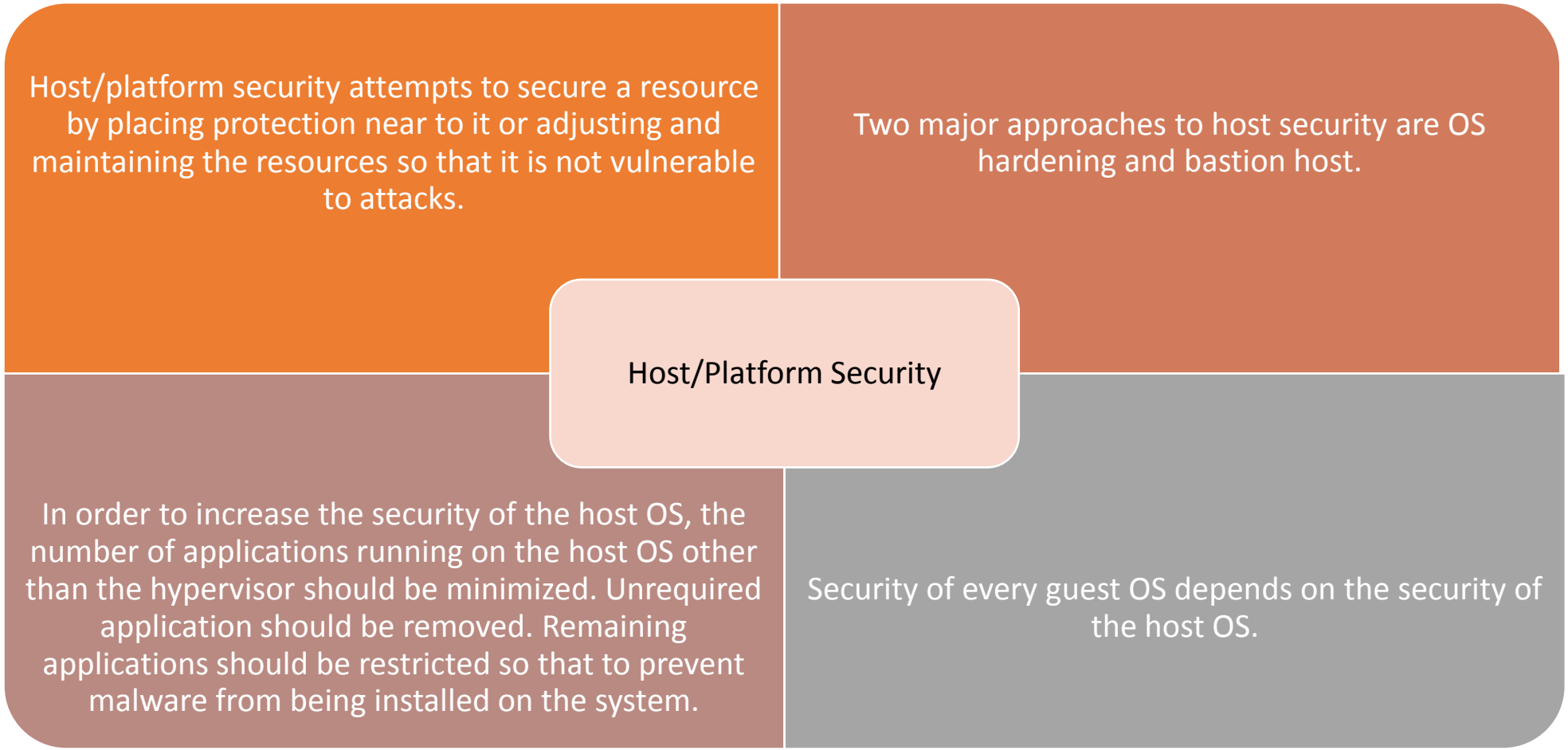
1) Cloud Security Alliance (CSA) established the _____ certification as a basis of cloud security knowledge.

a) ENISA
b) CCSK
c) ERM
d) CCM

2) List various domains of CCSK.

Host/Platform Security

Host/Platform Security



Securing Communications

Securing Communications

- Securing communications among hosts is important in order to prevent data leakage, eavesdropping and other attacks.
- Most of the host platform supports security protocols such as IPSec (IP Security) or SSL (secure socket layer) for any communications that are required.
- Virtualization provides a model of hardware such as network interfaces and storage which is important to the security of a virtualized guest OS as the physical hardware.
- Access controls are implemented to the networking virtual hardware in many virtualization systems which denotes access to the virtual hardware is strictly limited to the guest operating systems that use it.

Security recommendations to secure communications

Guest OS should not have management network access.

Guest OS should be protected by a firewall running on the host OS or running locally

Security of activities occurring between guest operating systems must be monitored

If two guest operating systems are not communicating each other, then each should run on a separate virtual local area network

Quiz / Assessment

1) Which of the following are the security protocols supported by the host platform?
   a) TCP
   b) IPSec
   c) SSL
   d) UDP
2) List various security recommendations to secure communications.
3) Describe the two major approaches to host security.

ENISA Document

ENISA Document

- The European Network and Information Security Agency (ENISA) is an EU (European Union) agency created to improve the functioning of the internal market.
- ENISA is a centre of excellence for the European Member States and European institutions in network and information security.
- ENISA document says that the clouds economies of scale and flexibility are both a friend and an enemy at the same time from a security point of view.
- The huge amount of resources and data present a more attractive target to attackers but cloud based defences can be more robust, cost effective and scalable.
- This document provides an assessment of security benefits and risks of using cloud computing. This gives security guidance for potential and existing users of cloud computing.

ENISA Document – Top Security Benefits

- Security and the benefits of scale
- Security as a market differentiator
- Standardised interfaces for managed security services
- Rapid, smart scaling of resources
- Audit and evidence gathering
- More timely, effective and efficient updates and defaults
- Benefits of resource concentration

ENISA Document – Top Security Risks

- Loss of governance
- Lock-in
- Isolation failure
- Compliance risks
- Management interface compromise
- Data Protection
- Insecure or incomplete data deletion
- Malicious insider

Quiz / Assessment

1) The_____ document says that the clouds economies of scale and flexibility are both a friend and an enemy at the same time from a security point of view.

a) CSA
b) ERM
c) CCSK
d) ENISA

2) 'The risk occurs if cloud provider (CP) does not permit audit by cloud customer'. State true or false.

a) True
b) False

Activity

Activity can be either offline or online

Offline Activity
(30 min)

- Using the content developed for CCSK. Prepare objective questions on day 1 and try to answer those questions on the next day without going through the theory provided.

Note: Refer Table of Content for the activities

Summary

- ✓ The Cloud Security Alliance (CSA) founded in 2008 is a non-profit organization with a mission to promote the use of best practices for providing security assurance within cloud computing, and to provide education on the uses of cloud computing to help secure all other forms of computing.
- ✓ The Cloud Security Alliance Cloud Controls Matrix (CCM) is specifically designed to provide basic security principles to guide cloud providers and to assist prospective cloud consumers in assessing the overall security risk of a cloud provider.
- ✓ The certificate of cloud security knowledge (CCSK) was first released by CSA in 2010.
- ✓ The CCSK provides a strong basis of cloud security essential knowledge and best practices for cloud computing.
- ✓ The U.S. National Institute of Standards and Technology (NIST) defines cloud computing by describing five characteristics, three cloud service models and four cloud deployment models.

e-References

1) https://cloudsecurityalliance.org/education/ccsk/#_info-video1

2) Cloud security alliance. (2016, Jan 21). Cloud Control Matrix. Retrieved May 15, 2016, from https://cloudsecurityalliance.org/group/cloud-controls-matrix/

3) https://cloudsecurityalliance.org/wp-content/uploads/2013/02/CCSK-Prep-Guide-V3.pdf

External Resources

1) Kris James (2013), Cloud Computing. Library of Congress
2) Barrie Sosinsky (2011), Cloud Computing Bible A –Wiley publication
3) RajkumarBuyya, James Broberg, AndrzejGoscinski (2011) -Cloud Computing: Principles And Paradigms–Wiley publication
4) Tim Mather, SubraKumaraswamy, ShahedLatif (2009) - Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance –O'Reilly publication
5) Cengage Learning (2011), Virtualization Security- EC-Council press
6) Matthew Metheny (2012). Federal Cloud Computing: The Definitive Guide for Cloud Service Providers- Syngress
7) Ian Lim, E. Coleen Coolidge, Paul Hourani (2013).Securing Cloud and Mobility: A Practitioner's Guide-CRC Press