Vendor: EC-Council

Exam Code: 312-40

Exam Name: EC-Council Certified Cloud Security Engineer (CCSE)

Version: DEMO

QUESTION 1
Cindy Williams works as a cloud security engineer in an IT company located in Seattle, Washington. Owing to the cost-effective security, governance, and storage features provided by AWS, her organization adopted AWS cloud-based services. Cindy would like to detect any unusual activity in her organization's AWS account. She would like to obtain the event history of her organization's AWS account activity for security analysis and resource change tracking. Which of the following AWS service enables operational auditing, compliance, governance, and risk auditing for her organization's AWS account?

A. AWS Security Hub
B. AWS CloudTrail
C. AWS Config
D. AWS CloudFormation

Answer: B
Explanation:
AWS CloudTrail is a service that enables operational auditing, compliance, governance, and risk auditing by providing a history of AWS account activity, including API calls and resource changes. It helps Cindy detect unusual activities in her organization's AWS account and is essential for security analysis and resource change tracking.

QUESTION 2
Katie Holmes has been working as a cloud security engineer over the past 7 years in an MNC. Since the outbreak of the COVID-19 pandemic, the cloud service provider could not provide cloud services efficiently to her organization. Therefore, Katie suggested to the management that they should design and build their own data center. Katie's requisition was approved, and after 8 months, Katie's team successfully designed and built an on-premises data center. The data center meets all organizational requirements; however, the capacity components are not redundant. If a component is removed, the data center comes to a halt. Which tier data center was designed and constructed by Katie's team?

A. Tier III
B. Tier I
C. Tier II
D. Tier IV

Answer: B
Explanation:
A Tier I data center has basic capacity components and is not redundant, meaning that if a component fails or is removed, the entire data center could come to a halt. It provides a single path for power and cooling, which is characteristic of Tier I data centers. In contrast, higher tiers (Tier II, III, IV) include redundancy and fault tolerance.

QUESTION 3
Daffod is an American cloud service provider that provides cloud-based services to customers worldwide. Several customers are adopting the cloud services provided by Daffod because they are secure and cost- effective. Daffod complies with the cloud computing law enacted in the US to realize the importance of information security in the economic and national security interests of the US. Based on the given information, which law order does Daffod adhere to?

A. FERPA
B. FISMA

C. ECPA
D. CLOUD

Answer: D
Explanation:
The CLOUD Act (Clarifying Lawful Overseas Use of Data Act) addresses the legal framework for accessing data stored in the cloud by U.S. law enforcement. It recognizes the importance of information security in both economic and national security interests, aligning with Daffod's compliance with cloud computing law and its focus on security in its services.

QUESTION 4
Falcon Computers is an IT company that runs its IT infrastructure on the cloud. The organization must implement cloud governance in its corporate cloud environment to align its business vision with the cloud vision. Which of the following cloud governance components can help the organization to align the cloud vision and business vision?

A. Cloud business office
B. Processes for the cloud service lifecycle
C. Cloud center of excellence
D. Norms, models, reference architectures, best practices, guidelines, and policies

Answer: A
Explanation:
The Cloud Business Office serves as a governance component that helps align the cloud vision with the business vision. It focuses on the strategic management of cloud initiatives, ensuring that cloud adoption and usage support the overall business goals and objectives.

QUESTION 5
The GCP environment of a company named Magnitude IT Solutions encountered a security incident. To respond to the incident, the Google Data Incident Response Team was divided based on the different aspects of the incident. Which member of the team has an authoritative knowledge of incidents and can be involved in different domains such as security, legal, product, and digital forensics?

A. Communications Lead
B. Operations Lead
C. Subject Matter Experts
D. Incident Commander

Answer: C
Explanation:
Subject Matter Experts (SMEs) possess authoritative knowledge of incidents and can provide insights across various domains such as security, legal, product, and digital forensics. They play a critical role in addressing specific aspects of an incident and informing the response team about the intricacies involved.

QUESTION 6
Jimmi Simpson has been working as a cloud security engineer in an IT company situated in Livonia, Michigan. His organization uses Microsoft Azure's cloud-based services. Jimmi wants a cloud-based, scalable SIEM and SOAR solution that uses threat intelligence and provides intelligent security analytics across his organization. Which of the following Microsoft Azure

services provides a single solution for threat visibility, alert detection, threat response, and proactive hunting that reduces the number of attacks, provides a birds-eye view across the organization, generates high volumes of alerts, and ensures long resolution time frames?

A. Anomaly Detector
B. Application Insights
C. Azure Sentinel
D. Cloud App Security

Answer: C
Explanation:
Azure Sentinel is a cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution provided by Microsoft Azure. It offers a comprehensive solution for threat visibility, alert detection, threat response, and proactive hunting. Azure Sentinel uses threat intelligence and provides intelligent security analytics, helping organizations reduce the number of attacks and gain a birds-eye view of their security posture.

QUESTION 7
A security incident has occurred within an organization's AWS environment. A cloud forensic investigation procedure is initiated for the acquisition of forensic evidence from the compromised EC2 instances. However, it is essential to abide by the data privacy laws while provisioning any forensic instance and sending it for analysis. What can the organization do initially to avoid the legal implications of moving data between two AWS regions for analysis?

A. Create evidence volume from the snapshot
B. Provision and launch a forensic workstation
C. Attach the evidence volume to the forensic workstation
D. Mount the evidence volume on the forensic workstation

Answer: A
Explanation:
By creating an evidence volume from a snapshot of the compromised EC2 instance, the organization can ensure that the original data remains intact and is not directly moved or altered during the forensic investigation. This approach helps mitigate legal implications related to data privacy laws when transferring data between AWS regions for analysis.

QUESTION 8
Martin Sheen is a senior cloud security engineer in SecGlob Cloud Pvt. Ltd. Since 2012, his organization has been using AWS cloud-based services. Using an intrusion detection system and antivirus software, Martin noticed that an attacker is trying to breach the security of his organization. Therefore, Martin would like to identify and protect the sensitive data of his organization. He requires a fully managed data security service that supports S3 storage and provides an inventory of publicly shared buckets, unencrypted buckets, and the buckets shared with AWS accounts outside his organization. Which of the following Amazon services fulfills Martin's requirement?

A. Amazon GuardDuty
B. Amazon Macie
C. Amazon Security Hub
D. Amazon Inspector

Answer: B
Explanation:
Amazon Macie is a fully managed data security service that helps identify and protect sensitive data in AWS. It supports Amazon S3 storage and provides features such as an inventory of publicly shared buckets, unencrypted buckets, and buckets shared with AWS accounts outside the organization. This makes it suitable for Martin's requirement to monitor and secure sensitive data.

QUESTION 9
Melissa George is a cloud security engineer in an IT company. Her organization has adopted cloud-based services. The integration of cloud services has become significantly complicated to be managed by her organization. Therefore, her organization requires a third-party to consult, mediate, and facilitate the selection of a solution. Which of the following NIST cloud deployment reference architecture actors manage cloud service usage, performance, and delivery, and maintains the relationship between the CSPs and cloud consumers?

A. Cloud Auditor
B. Cloud Carrier
C. Cloud Provider
D. Cloud Broker

Answer: D
Explanation:
A Cloud Broker manages the cloud service usage, performance, and delivery, and facilitates the relationship between cloud service providers (CSPs) and cloud consumers. They help organizations navigate the complexities of integrating multiple cloud services, making them the ideal choice for consulting and mediation in the selection of solutions.

QUESTION 10
SeaCloud Soft Pvt. Ltd. is an IT company that develops software and applications related to the healthcare industry. To safeguard the data and applications against attackers, the organization adopted cloud computing. The organization did not trust the cloud service provider; therefore, it implemented an encryption technique that secures data during communication and storage. SeaCloud Soft Pvt. Ltd. performed computation on the encrypted data and then sent the data to the cloud service provider. Based on the given information, which of the following encryption techniques was implemented by SeaCloud Soft Pvt. Ltd.?

A. Ciphertext attribute-based encryption
B. Fully homomorphic encryption
C. Key policy attribute-based encryption
D. Identity-based encryption

Answer: B
Explanation:
Fully homomorphic encryption allows computations to be performed on encrypted data without needing to decrypt it first. This technique ensures that the data remains secure during communication and storage while still enabling the organization to perform necessary computations before sending it to the cloud service provider.

QUESTION 11
Georgia Lyman works as a cloud security engineer in a multinational company. Her organization uses cloud-based services. Its virtualized networks and associated virtualized resources

encountered certain capacity limitations that affected the data transfer performance and virtual server communication. How can Georgia eliminate the data transfer capacity thresholds imposed on a virtual server by its virtualized environment?

A. By restricting the virtual server to bypass the hypervisor and access the I/O card of the physical server directly
B. By allowing the virtual appliance to bypass the hypervisor and access the I/O card of the physical server directly
C. By allowing the virtual server to bypass the hypervisor and access the I/O card of the physical server directly
D. By restricting the virtual appliance to bypass the hypervisor and access the I/O card of the physical server directly

Answer: C
Explanation:
Allowing the virtual server to bypass the hypervisor enables it to access the physical server's I/O card directly, which can help eliminate the capacity limitations imposed by the virtualized environment. This approach can improve data transfer performance and enhance communication between virtual servers.

QUESTION 12
SecAppSol Pvt. Ltd. is a cloud software and application development company located in Louisville, Kentucky. The security features provided by its previous cloud service provider was not satisfactory, and in 2012, the organization became a victim of eavesdropping. Therefore, SecAppSol Pvt. Ltd. changed its cloud service provider and adopted AWS cloud-based services owing to its robust and cost-effective security features. How does SecAppSol Pvt. Ltd.'s security team encrypt the traffic between the load balancer and client that initiate SSL or TLS sessions?

A. By enabling RADIUS Authentication
B. By enabling Cloud Identity Aware Proxy
C. By enabling HTTPS listener
D. By enabling Amazon GuardDuty

Answer: C
Explanation:
Enabling an HTTPS listener on the load balancer allows for the encryption of traffic between the load balancer and clients. This process initiates SSL or TLS sessions, ensuring that data transmitted over the network is encrypted and secure from eavesdropping.

QUESTION 13
Rachel McAdams works as a senior cloud security engineer in a cloud service provider company. Owing to the robust services and security features provided by her organization, the number of cloud consumers continues to increase. To meet the increasing cloud consumer requirements, her organization decided to build more data centers. Therefore, Rachel's organization formed a new team to design and construct data centers. Rachel is also part of the team and was given the responsibility of designing the data center. How can Racheal maintain a stable temperature in the HVAC unit?

A. Rachel can design HVAC such that the heat generated by the data center equipment is taken outside and cool air to supply the equipment is taken inside.
B. Rachel can design HVAC such that the cool air and heat generated by data center equipment should remain inside to stabilize the temperature.

C. Rachel can design HVAC such that the heat generated by the data center equipment is taken inside and cool air to supply the equipment is taken outside.
D. Rachel can design HVAC such that the cool air and heat generated by data center equipment should remain outside to stabilize the temperature.

Answer: A
Explanation:
To maintain a stable temperature in the HVAC unit, it is essential to remove the heat generated by the data center equipment and replace it with cool air from outside. This design helps ensure that the internal temperature remains controlled and stable, preventing overheating and ensuring optimal performance of the equipment.

QUESTION 14
Jack Jensen works as a cloud security engineer in an IT company located in Madison, Wisconsin. Owing to the various security services provided by Google, in 2012, his organization adopted Google cloud-based services. Jack would like to identify security abnormalities to secure his organizational data and workload. Which of the following is a built-in feature in the Security Command Center that utilizes behavioral signals to detect security abnormalities such as unusual activity and leaked credentials in virtual machines or GCP projects?

A. Cloud Anomaly Detection
B. Cloud Armor
C. Security Health Analytics
D. Anomaly Detector

Answer: A
Explanation:
Cloud Anomaly Detection is a built-in feature in Google Cloud's Security Command Center that uses behavioral signals to identify security abnormalities, such as unusual activity and potential leaked credentials, in virtual machines or GCP projects. This feature helps organizations enhance their security posture by detecting and responding to anomalies in their cloud environment.

QUESTION 15
Jordon Bridges works as a cloud security engineer in a multinational company. His organization uses Google cloud-based services (GC) because Google cloud provides robust security services, better pricing than competitors, improved performance, and redundant backup. Using IAM security configuration, Jordon implemented the principle of least privilege. A GC IAM member could be a Google account, service account, Google group, G Suite, or cloud identity domain with an identity to access Google cloud resources. Which of the following identities is used by GC IAM members to access Google cloud resources?

A. For Google Account, Google group, and service account, the identity used is an email address, whereas in G Suite and cloud identity domain, the identity used is the domain name.
B. For Google Account, Google group, and G suite, the identity used is an email address, whereas in service account and cloud identity domain, the identity used is the domain name.
C. For Google Account, Google group, and G suite, the identity used is the domain name, whereas in service account and cloud identity domain, the identity used is an email address.
D. For Google Account, Google group, and service account, the identity used is the domain name, whereas in G Suite and cloud identity domain, the identity used is an email address.

Answer: A
Explanation:

In Google Cloud IAM, Google Accounts, Google groups, and service accounts are identified by email addresses. In contrast, G Suite and cloud identity domains are associated with a domain name, which can represent multiple users or accounts under that domain. This distinction is essential for configuring permissions and access to Google Cloud resources.

QUESTION 16
Steven Smith has been working as a cloud security engineer in an MNC for the past 4 years. His organization uses AWS cloud-based services. Steven handles a complex application on AWS that has several resources and it is difficult for him to manage these resources. Which of the following AWS services allows Steven to make a set of related AWS resources easily and use or provision them in an orderly manner so that he can spend less time managing resources and more time on the applications that run in the AWS environment?

A. AWS Control Tower
B. Amazon CloudFront
C. AWS CloudFormation
D. AWS Config

Answer: C
Explanation:
AWS CloudFormation allows users to define and provision a set of related AWS resources as a single unit, known as a stack. This service enables Steven to manage complex applications more easily by automating the provisioning and management of resources, allowing him to focus more on the applications rather than the underlying infrastructure.

QUESTION 17
The organization TechWorld Ltd. used cloud for its business. It operates from an EU country (Poland and Greece). Currently, the organization gathers and processes the data of only EU users. Once, the organization experienced a severe security breach, resulting in loss of critical user data. In such a case, along with its cloud service provider, the organization should be held responsible for non-compliance or breaches. Under which cloud compliance framework will the company and cloud provider be penalized?

A. NIST
B. ITAR
C. GDPR
D. HIPAA

Answer: C
Explanation:
The General Data Protection Regulation (GDPR) is a regulation in EU law that governs data protection and privacy. Since TechWorld Ltd. operates in the EU and processes data of EU users, both the organization and its cloud service provider can be held responsible for non-compliance or breaches under GDPR, especially following incidents like security breaches that result in the loss of user data.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**