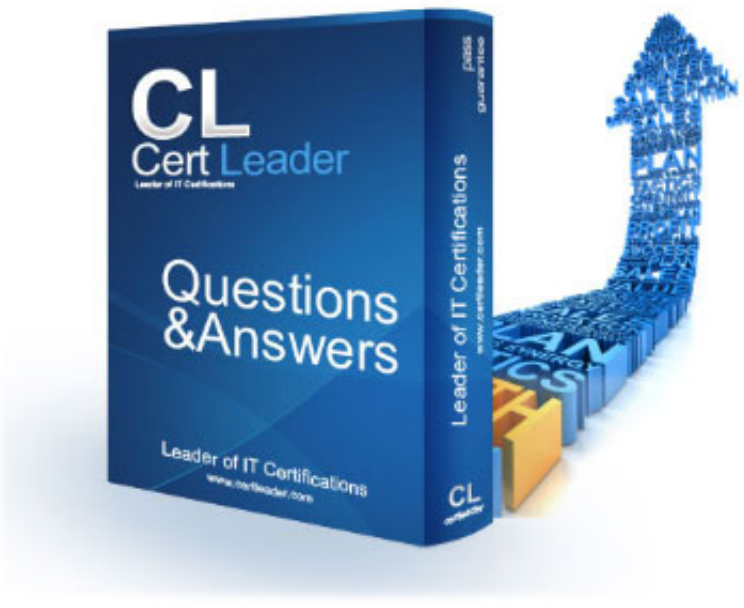
CCSP Dumps

Certified Cloud Security Professional

https://www.certleader.com/CCSP-dumps.html



NEW QUESTION 1
- (Exam Topic 1)
Under EU law, a cloud customer who gives sensitive data to a cloud provider is still legally responsible for the damages resulting from a data breach caused by the provider; the EU would say that it is the cloud customer's fault for choosing the wrong provider.
This is an example of insufficient _____ .

A. Proof
B. Evidence
C. Due diligence
D. Application of reasonableness

Answer: C

NEW QUESTION 2
- (Exam Topic 1)
You are the security manager for a small application development company. Your company is considering the use of the cloud for software testing purposes.
Which cloud service model is most likely to suit your needs?
Response:

A. IaaS
B. PaaS
C. SaaS
D. LaaS

Answer: B

NEW QUESTION 3
- (Exam Topic 1)
According to the (ISC)2 Cloud Secure Data Life Cycle, which phase comes soon after (or at the same time as) the Create phase?

A. Store
B. Use
C. Deploy
D. Archive

Answer: A

NEW QUESTION 4
- (Exam Topic 1)
Which strategy involves using a fake production system to lure attackers in order to learn about their tactics?
Response:

A. IDS
B. Honeypot
C. IPS
D. Firewall

Answer: B

NEW QUESTION 5
- (Exam Topic 1)
Which cloud storage type uses an opaque value or descriptor to categorize and organize data? Response:

A. Volume
B. Object
C. Structured
D. Unstructured

Answer: D

NEW QUESTION 6
- (Exam Topic 1)
All of the following are usually nonfunctional requirements except _____.
Response:

A. Color
B. Sound
C. Security
D. Function

Answer: D

NEW QUESTION 7
- (Exam Topic 1)
What type of device is often leveraged to assist legacy applications that may not have the programmatic capability to process assertions from modern web

services?

A. Web application firewall
B. XML accelerator
C. Relying party
D. XML firewall

Answer: B

NEW QUESTION 8
- (Exam Topic 1)
The cloud deployment model that features organizational ownership of the hardware and infrastructure, and usage only by members of that organization, is known as:
Response:

A. Private
B. Public
C. Hybrid
D. Motive

Answer: A

NEW QUESTION 9
- (Exam Topic 1)
Which concept of cloud computing pertains to the ability to reuse components and services of an application for other purposes?

A. Portability
B. Interoperability
C. Resource pooling
D. Elasticity

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
You have been tasked with creating an audit scope statement and are making your project outline. Which of the following is NOT typically included in an audit scope statement?

A. Statement of purpose
B. Deliverables
C. Classification
D. Costs

Answer: D

NEW QUESTION 10
- (Exam Topic 1)
Which of the following best describes SAML? Response:

A. A standard for developing secure application management logistics
B. A standard for exchanging authentication and authorization data between security domains
C. A standard for exchanging usernames and passwords across devices
D. A standard used for directory synchronization

Answer: B

NEW QUESTION 12
- (Exam Topic 1)
Of the following, which is probably the most significant risk in a managed cloud environment? Response:

A. DDoS
B. Management plane breach
C. Guest escape
D. Physical attack on the utility service lines

Answer: B

NEW QUESTION 14
- (Exam Topic 1)
Which document will enforce uptime and availability requirements between the cloud customer and cloud provider?
Response:

A. Contract
B. Operational level agreement
C. Service level agreement
D. Regulation

Answer: C

NEW QUESTION 16
- (Exam Topic 1)
Which of the following best describes data masking? Response:

A. A method where the last few numbers in a dataset are not obscure
B. These are often used for authentication.
C. A method for creating similar but inauthentic datasets used for software testing and user training.
D. A method used to protect prying eyes from data such as social security numbers and credit card data.
E. Data masking involves stripping out all similar digits in a string of numbers so as to obscure the original number.

Answer: B

NEW QUESTION 21
- (Exam Topic 1)
You are in charge of creating the BCDR plan and procedures for your organization. Your organization has its production environment hosted by a cloud provider, and you have appropriate protections in place.
Which of the following is a significant consideration for your BCDR backup? Response:

A. Enough personnel at the BCDR recovery site to ensure proper operations
B. Good cryptographic key management
C. Access to the servers where the BCDR backup is stored
D. Forensic analysis capabilities

Answer: B

NEW QUESTION 23
- (Exam Topic 1)
You are the security policy lead for your organization, which is considering migrating from your
on-premises, legacy environment into the cloud. You are reviewing the Cloud Security Alliance Cloud Controls Matrix (CSA CCM) as a tool for your organization.
Which of the following benefits will the CSA CCM offer your organization? Response:

A. Simplifying regulatory compliance
B. Collecting multiple data streams from your log files
C. Ensuring that the baseline configuration is applied to all systems
D. Enforcing contract terms between your organization and the cloud provider

Answer: A

NEW QUESTION 25
- (Exam Topic 1)
Egress monitoring solutions usually include a function that _____.
Response:

A. Uses biometrics to scan users
B. Inspects incoming packets
C. Resides on client machines
D. Uses stateful inspection

Answer: C

NEW QUESTION 29
- (Exam Topic 1)
When considering the option to migrate from an on-premises environment to a hosted cloud service, an organization should weigh the risks of allowing external entities to access the cloud data for collaborative purposes against _____.
Response:

A. Not securing the data in the legacy environment
B. Disclosing the data publicly
C. Inviting external personnel into the legacy workspace in order to enhance collaboration
D. Sending the data outside the legacy environment for collaborative purposes

Answer: D

NEW QUESTION 33
- (Exam Topic 1)
_____ is the legal concept whereby a cloud customer is held to a reasonable expectation for providing security of its users' and clients' privacy data in their control.
Response:

A. Due care
B. Due diligence
C. Liability
D. Reciprocity

Answer: B

NEW QUESTION 36
- (Exam Topic 1)
At which phase of the SDLC process should security begin participating?

A. Requirements gathering
B. Requirements analysis
C. Design
D. Testing

Answer: A

NEW QUESTION 41
- (Exam Topic 1)
Which of the following tools might be useful in data discovery efforts that are based on content analysis?

A. DLP
B. Digital Rights Management (DRM)
C. iSCSI
D. Fibre Channel over Ethernet (FCoE)

Answer: A

NEW QUESTION 42
- (Exam Topic 1)
Because PaaS implementations are so often used for software development, what is one of the vulnerabilities that should always be kept in mind?
Response:

A. Malware
B. Loss/theft of portable devices
C. Backdoors
D. DoS/DDoS

Answer: C

NEW QUESTION 46
- (Exam Topic 1)
The cloud deployment model that features joint ownership of assets among an affinity group is known as: Response:

A. Private
B. Public
C. Hybrid
D. Community

Answer: D

NEW QUESTION 51
- (Exam Topic 1)
Different types of cloud deployment models use different types of storage from traditional data centers, along with many new types of software platforms for deploying applications and configurations. Which of the following is NOT a storage type used within a cloud environment?

A. Docker
B. Object
C. Structured
D. Volume

Answer: A

NEW QUESTION 56
- (Exam Topic 1)
Which of the following types of organizations is most likely to make use of open source software technologies?

A. Government agencies
B. Corporations
C. Universities
D. Military

Answer: C

NEW QUESTION 59
- (Exam Topic 1)
Which Common Criteria Evaluation Assurance Level (EAL) is granted to those products that are formally verified in terms of design and tested by an independent third party?

A. 1
B. 3
C. 5

D. 7

Answer: D

NEW QUESTION 63
- (Exam Topic 1)
Which of the following data sanitation methods would be the MOST effective if you needed to securely remove data as quickly as possible in a cloud environment?
Response:

A. Zeroing
B. Cryptographic erasure
C. Overwriting
D. Degaussing

Answer: B

NEW QUESTION 66
- (Exam Topic 1)
A honeypot can be used for all the following purposes except _____.
Response:

A. Gathering threat intelligence
B. Luring attackers
C. Distracting attackers
D. Delaying attackers

Answer: B

NEW QUESTION 68
- (Exam Topic 1)
One of the security challenges of operating in the cloud is that additional controls must be placed on file storage systems because _____ .
Response:

A. File stores are always kept in plain text in the cloud
B. There is no way to sanitize file storage space in the cloud
C. Virtualization necessarily prevents the use of application-based security controls
D. Virtual machines are stored as snapshotted files when not in use

Answer: D

NEW QUESTION 71
- (Exam Topic 1)
Which type of report is considered for “general” use and does not contain any sensitive information? Response:

A. SOC 1
B. SAS-70
C. SOC 3
D. SOC 2

Answer: C

NEW QUESTION 73
- (Exam Topic 1)
Each of the following are dependencies that must be considered when reviewing the BIA after cloud migration except:
Response:

A. The cloud provider’s suppliers
B. The cloud provider’s vendors
C. The cloud provider’s utilities
D. The cloud provider’s resellers

Answer: D

NEW QUESTION 78
- (Exam Topic 1)
All of the following are terms used to described the practice of obscuring original raw data so that only a portion is displayed for operational purposes, except:
Response:

A. Tokenization
B. Data discovery
C. Obfuscation
D. Masking

Answer: B

NEW QUESTION 79

- (Exam Topic 1)
Which of the following top security threats involves attempting to send invalid commands to an application in an attempt to get the application to execute the code?
Response:

A. Cross-site scripting
B. Injection
C. Insecure direct object references
D. Cross-site request forgery

Answer: B

NEW QUESTION 80
- (Exam Topic 1)
The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes “sensitive data exposure.” Which of these is a technique to reduce the potential for a sensitive data exposure? Response:

A. Extensive user training on proper data handling techniques
B. Advanced firewalls inspecting all inbound traffic, to include content-based screening
C. Ensuring the use of utility backup power supplies
D. Roving security guards

Answer: A

NEW QUESTION 83
- (Exam Topic 1) What does nonrepudiation mean? Response:

A. Prohibiting certain parties from a private conversation
B. Ensuring that a transaction is completed before saving the results
C. Ensuring that someone cannot turn off auditing capabilities while performing a function
D. Preventing any party that participates in a transaction from claiming that it did not

Answer: D

NEW QUESTION 84
- (Exam Topic 1)
The physical layout of a cloud data center campus should include redundancies of all the following except _____ .
Response:

A. Generators
B. HVAC units
C. Generator fuel storage
D. Points of personnel ingress

Answer: D

NEW QUESTION 88
- (Exam Topic 1)
Log data should be protected _____.
Response:

A. One level below the sensitivity level of the systems from which it was collected
B. At least at the same sensitivity level as the systems from which it was collected
C. With encryption in transit, at rest, and in use
D. According to NIST guidelines

Answer: B

NEW QUESTION 90
- (Exam Topic 1)
Using one cloud provider for your operational environment and another for your BCDR backup will also give you the additional benefit of _____.
Response:

A. Allowing any custom VM builds you use to be instantly ported to another environment
B. Avoiding vendor lock-in/lockout
C. Increased performance
D. Lower cost

Answer: B

NEW QUESTION 92
- (Exam Topic 1)
The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. According to the CSA, an organization that suffers a data breach might suffer all of the following negative effects except _____.
Response:

A. Cost of compliance with notification laws
B. Loss of public perception/goodwill
C. Loss of market share
D. Cost of detection

Answer: D

NEW QUESTION 97
- (Exam Topic 1)
What are the phases of a software development lifecycle process model? Response:

A. Planning and requirements analysis, define, design, develop, testing, and maintenance
B. Define, planning and requirements analysis, design, develop, testing, and maintenance
C. Planning and requirements analysis, define, design, testing, develop, and maintenance
D. Planning and requirements analysis, design, define, develop, testing, and maintenance

Answer: A

NEW QUESTION 102
- (Exam Topic 1)
Data labels could include all the following, except: Response:

A. Source
B. Delivery vendor
C. Handling restrictions
D. Jurisdiction

Answer: B

NEW QUESTION 106
- (Exam Topic 1)
Which ISO standard refers to addressing security risks in a supply chain?

A. ISO 27001
B. ISO/IEC 28000:2007
C. ISO 18799
D. ISO 31000:2009

Answer: B

NEW QUESTION 109
- (Exam Topic 1)
During which stage of the SDLC process should security be consulted and begin its initial involvement?

A. Testing
B. Design
C. Development
D. Requirement gathering

Answer: D

NEW QUESTION 113
- (Exam Topic 1)
Static software security testing typically uses _____ as a measure of how thorough the testing was. Response:

A. Number of testers
B. Flaws detected
C. Code coverage
D. Malware hits

Answer: C

NEW QUESTION 115
- (Exam Topic 1)
You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting its testing environment. Previous releases have shipped with major flaws that were not detected in the testing phase; leadership wants to avoid repeating that problem. What tool/technique/technology might you suggest to aid in identifying programming errors?

A. Vulnerability scans
B. Open source review
C. SOC audits
D. Regulatory review

Answer: B

NEW QUESTION 119

- (Exam Topic 1)
Which cloud service category offers the most customization options and control to the cloud customer?
Response:

A. PaaS
B. IaaS
C. SaaS
D. DaaS

Answer: B

NEW QUESTION 120
- (Exam Topic 1)
Who should be the only entity allowed to declare that an organization can return to normal following contingency or BCDR operations?
Response:

A. Regulators
B. Law enforcement
C. The incident manager
D. Senior management

Answer: D

NEW QUESTION 124
- (Exam Topic 1)
Who will determine data classifications for the cloud customer?

A. The cloud provider
B. NIST
C. Regulators
D. The cloud customer

Answer: D

NEW QUESTION 125
- (Exam Topic 1)
Which of the following management risks can make an organization’s cloud environment unviable? Response:

A. Insider trading
B. VM sprawl
C. Hostile takeover
D. Improper personnel selection

Answer: B

NEW QUESTION 127
- (Exam Topic 1)
Which of the following best describes a cloud carrier?

A. A person or entity responsible for making a cloud service available to consumers
B. The intermediary who provides connectivity and transport of cloud services between cloud providers and cloud consumers
C. The person or entity responsible for keeping cloud services running for customers
D. The person or entity responsible for transporting data across the Internet

Answer: B

NEW QUESTION 131
- (Exam Topic 1)
You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment.
In order to increase the security value of the DLP, you should consider combining it with _____.
Response:

A. Digital rights management (DRM) and security event and incident management (SIEM) tools
B. An investment in upgraded project management software
C. Digital insurance policies
D. The Uptime Institute’s Tier certification

Answer: A

NEW QUESTION 132
- (Exam Topic 1)
The Cloud Security Alliance (CSA) publishes, the Notorious Nine, a list of common threats to organizations participating in cloud computing.
According to the CSA, all of the following activity can result in data loss except _____ .

A. Misplaced crypto keys
B. Improper policy
C. Ineffectual backup procedures

D. Accidental overwrite

Answer: B

NEW QUESTION 134
- (Exam Topic 1)
Heating, ventilation, and air conditioning (HVAC) systems cool the data center by pushing warm air into _____.
Response:

A. The server inlets
B. Underfloor plenums
C. HVAC intakes
D. The outside world

Answer: D

NEW QUESTION 135
- (Exam Topic 1)
Which standards body depends heavily on contributions and input from its open membership base? Response:

A. NIST
B. ISO
C. ICANN
D. CSA

Answer: D

NEW QUESTION 139
- (Exam Topic 1)
Data labels could include all the following, except: Response:

A. Confidentiality level
B. Distribution limitations
C. Access restrictions
D. Multifactor authentication

Answer: D

NEW QUESTION 143
- (Exam Topic 2)
Which cloud service category brings with it the most expensive startup costs, but also the lowest costs for ongoing support and maintenance staff?
Response:

A. IaaS
B. SaaS
C. PaaS
D. DaaS

Answer: B

NEW QUESTION 147
- (Exam Topic 2)
Which of the following is the best example of a key component of regulated PII? Response:

A. Items that should be implemented
B. Mandatory breach reporting
C. Audit rights of subcontractors
D. PCI DSS

Answer: B

NEW QUESTION 152
- (Exam Topic 2)
Which of the following BCDR testing methodologies is least intrusive? Response:

A. Walk-through
B. Simulation
C. Tabletop
D. Full test

Answer: C

NEW QUESTION 155
- (Exam Topic 2)
In a Lightweight Directory Access Protocol (LDAP) environment, each entry in a directory server is identified by a _____.

Response:

A. Domain name (DN)
B. Distinguished name (DN)
C. Directory name (DN)
D. Default name (DN)

Answer: B

NEW QUESTION 160
- (Exam Topic 2)
You are the data manager for a retail company; you anticipate a much higher volume of sales activity in the final quarter of each calendar year than the other quarters.
In order to handle these increased transactions, and to accommodate the temporary sales personnel you will hire for only that time period, you consider augmenting your internal, on-premises production environment with a cloud capability for a specific duration, and will return to operating fully on-premises after the period of increased activity.
This is an example of _____.
Response:

A. Cloud framing
B. Cloud enhancement
C. Cloud fragility
D. Cloud bursting

Answer: D

NEW QUESTION 163
- (Exam Topic 2)
Which type of cloud service category would having a vendor-neutral encryption scheme for data at rest (DAR) be the MOST important?
Response:

A. Public
B. Hybrid
C. Private
D. Community

Answer: B

NEW QUESTION 166
- (Exam Topic 2)
The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing.
According to the CSA, what aspect of managed cloud services makes the threat of malicious insiders so alarming?
Response:

A. Scalability
B. Multitenancy
C. Metered service
D. Flexibility

Answer: B

NEW QUESTION 169
- (Exam Topic 2)
The destruction of a cloud customer's data can be required by all of the following except _____.
Response:

A. Statute
B. Regulation
C. The cloud provider's policy
D. Contract

Answer: C

NEW QUESTION 173
- (Exam Topic 2)
You are the security director for a chain of automotive repair centers across several states. Your company uses a cloud SaaS provider, for business functions that cross several of the locations of your facilities, such as: 1) ordering parts 2) logistics and inventory 3) billing, and 4) marketing.
The manager at one of your newest locations reports that there is a competing car repair company that has a logo that looks almost exactly like the one your company uses. What will most likely affect the determination of who has ownership of the logo?
Response:

A. Whoever first used the logo
B. The jurisdiction where both businesses are using the logo simultaneously
C. Whoever first applied for legal protection of the logo
D. Whichever entity has the most customers that recognize the logo

Answer: C

NEW QUESTION 175
- (Exam Topic 2)
The Cloud Security Alliance's (CSA's) Cloud Controls Matrix (CCM) addresses all the following security architecture elements except _____.
Response:

A. Physical security
B. IaaS
C. Application security
D. Business drivers

Answer: D

NEW QUESTION 177
- (Exam Topic 2)
Which type of threat is often used in conjunction with phishing attempts and is often viewed as greatly increasing the likeliness of success?
Response:

A. Unvalidated redirects and forwards
B. Cross-site request forgery
C. Cross-site scripting
D. Insecure direct object references

Answer: A

NEW QUESTION 179
- (Exam Topic 2)
Who should be involved in review and maintenance of user accounts/access? Response:

A. The user's manager
B. The security manager
C. The accounting department
D. The incident response team

Answer: A

NEW QUESTION 182
- (Exam Topic 2)
Which of the following is NOT a core component of an SIEM solution? Response:

A. Correlation
B. Aggregation
C. Compliance
D. Escalation

Answer: D

NEW QUESTION 187
- (Exam Topic 2)
Which of the following is a method for apportioning resources that involves setting maximum usage amounts for all tenants/customers within the environment?
Response:

A. Reservations
B. Shares
C. Cancellations
D. Limits

Answer: D

NEW QUESTION 190
- (Exam Topic 2)
Administrative penalties for violating the General Data Protection Regulation (GDPR) can range up to
_____ .
Response:

A. US$100,000
B. 500,000 euros
C. 20,000,000 euros
D. 1,000,000 euros

Answer: C

NEW QUESTION 194
- (Exam Topic 2)
An organization could have many reasons that are common throughout the industry to activate a BCDR situation. Which of the following is NOT a typical reason to activate a BCDR plan?
Response:

A. Natural disaster
B. Utility outage
C. Staff loss
D. Terrorist attack

Answer: C

NEW QUESTION 195
- (Exam Topic 2)
Although performing BCDR tests at regular intervals is a best practice to ensure processes and documentation are still relevant and efficient, which of the following represents a reason to conduct a BCDR review outside of the regular interval?
Response:

A. Staff changes
B. Application changes
C. Regulatory changes
D. Management changes

Answer: B

NEW QUESTION 199
- (Exam Topic 2)
Firewalls can detect attack traffic by using all these methods except _____.
Response:

A. Known past behavior in the environment
B. Identity of the malicious user
C. Point of origination
D. Signature matching

Answer: B

NEW QUESTION 203
- (Exam Topic 2)
Which kind of SSAE audit report is a cloud customer most likely to receive from a cloud provider? Response:

A. SOC 1 Type 1
B. SOC 2 Type 2
C. SOC 1 Type 2
D. SOC 3

Answer: D

NEW QUESTION 206
- (Exam Topic 2)
SOC 2 reports were intended to be _____.
Response:

A. Released to the public
B. Only technical assessments
C. Retained for internal use
D. Nonbinding

Answer: C

NEW QUESTION 208
- (Exam Topic 2)
There are two general types of smoke detectors. Which type uses a small portion of radioactive material? Response:

A. Photoelectric
B. Ionization
C. Electron pulse
D. Integral field

Answer: B

NEW QUESTION 213
- (Exam Topic 2)
Which of the following is not typically included in the list of critical assets specified for continuity during BCDR contingency operations?
Response:

A. Systems
B. Data
C. Cash
D. Personnel

Answer: C

NEW QUESTION 216
- (Exam Topic 2)
In the cloud motif, the data processor is usually: Response:

A. The party that assigns access rights
B. The cloud customer
C. The cloud provider
D. The cloud access security broker

Answer: C

NEW QUESTION 218
- (Exam Topic 2)
Single sign-on systems work by authenticating users from a centralized location or using a centralized method, and then allowing applications that trust the system to grant those users access. What would be passed between the authentication system and the applications to grant a user access?
Response:

A. Ticket
B. Certificate
C. Credential
D. Token

Answer: D

NEW QUESTION 219
- (Exam Topic 2)
What are the four cloud deployment models? Response:

A. Public, Internal, Hybrid, and Community
B. External, Private, Hybrid, and Community
C. Public, Private, Joint, and Community
D. Public, Private, Hybrid, and Community

Answer: D

NEW QUESTION 220
- (Exam Topic 2)
All of the following are activities that should be performed when capturing and maintaining an accurate, secure system baseline, except _____.
Response:

A. Audit the baseline to ensure that all configuration items have been included and applied correctly
B. Impose the baseline throughout the environment
C. Capture an image of the baseline system for future reference/versioning/rollback purposes
D. Document all baseline configuration elements and versioning data

Answer: B

NEW QUESTION 221
- (Exam Topic 2)
Which of the following is not a feature of SAST? Response:

A. Source code review
B. Team-building efforts
C. “White-box” testing
D. Highly skilled, often expensive outside consultants

Answer: B

NEW QUESTION 222
- (Exam Topic 2)
Your organization is considering a move to a cloud environment and is looking for certifications or audit reports from cloud providers to ensure adequate security controls and processes.
Which of the following is NOT a security certification or audit report that would be pertinent? Response:

A. FedRAMP
B. PCI DSS
C. FIPS 140-2
D. SOC Type 2

Answer: C

NEW QUESTION 223
- (Exam Topic 2)
Data transformation in a cloud environment should be of great concern to organizations considering cloud migration because _____ could affect data classification processes/implementations.
Response:

A. Multitenancy
B. Virtualization
C. Remote access
D. Physical distance

Answer: B

NEW QUESTION 226
- (Exam Topic 2)
What is a cloud storage architecture that manages the data in a hierarchy of files? Response:

A. Object-based storage
B. File-based storage
C. Database
D. CDN

Answer: B

NEW QUESTION 230
- (Exam Topic 2)
According to OWASP recommendations, active software security testing should include all of the following except _____ .
Response:

A. Session initiation testing
B. Input validation testing
C. Testing for error handling
D. Testing for weak cryptography

Answer: A

NEW QUESTION 233
- (Exam Topic 2)
Halon is now illegal to use for data center fire suppression. What is the reason it was outlawed? Response:

A. It poses a threat to health and human safety when deployed.
B. It can harm the environment.
C. It does not adequately suppress fires.
D. It causes undue damage to electronic systems.

Answer: B

NEW QUESTION 234
- (Exam Topic 2)
What is a form of cloud storage where data is stored as objects, arranged in a hierarchal structure, like a file tree?
Response:

A. Volume storage
B. Databases
C. Content delivery network (CDN)
D. Object storage

Answer: D

NEW QUESTION 237
- (Exam Topic 2)
Each of the following is an element of the Identification phase of the identity and access management (IAM) process except _____.
Response:

A. Provisioning
B. Inversion
C. Management
D. Deprovisioning

Answer: B

NEW QUESTION 240
- (Exam Topic 2)
Which standards body depends heavily on contributions and input from its open membership base?
Response:

A. NIST
B. ISO
C. ICANN
D. CSA

Answer: D

NEW QUESTION 242
- (Exam Topic 2)
Which phase of the cloud data lifecycle also typically entails the process of data classification? Response:

A. Use
B. Store
C. Create
D. Archive

Answer: C

NEW QUESTION 243
- (Exam Topic 2)
All of the following might be used as data discovery characteristics in a content-analysis-based data discovery effort except _____.
Response:

A. Keywords
B. Pattern-matching
C. Frequency
D. Inheritance

Answer: D

NEW QUESTION 246
- (Exam Topic 2)
Federation should be _____ to the users.
Response:

A. Hostile
B. Proportional
C. Transparent
D. Expensive

Answer: C

NEW QUESTION 247
- (Exam Topic 2)
When designing a cloud data center, which of the following aspects is not necessary to ensure continuity of operations during contingency operations?
Response:

A. Access to clean water
B. Broadband data connection
C. Extended battery backup
D. Physical access to the data center

Answer: C

NEW QUESTION 252
- (Exam Topic 2)
Which SSAE 16 report is purposefully designed for public release (for instance, to be posted on a company's website)?
Response:

A. SOC 1
B. SOC 2, Type 1
C. SOC 2, Type 2
D. SOC 3

Answer: D

NEW QUESTION 253
- (Exam Topic 2)
Which type of report is considered for "general" use and does not contain any sensitive information? Response:

A. SOC 1
B. SAS-70
C. SOC 3
D. SOC 2

Answer: C

NEW QUESTION 257
- (Exam Topic 2)
You have been tasked by management to offload processing and validation of incoming encoded data from your application servers and their associated APIs.
Which of the following would be the most appropriate device or software to consider?
Response:

A. XML accelerator

B. XML firewall
C. Web application firewall
D. Firewall

Answer: A

NEW QUESTION 262
- (Exam Topic 2)
What is a cloud storage architecture that manages the data in caches of copied content close to locations of high demand?
Response:

A. Object-based storage
B. File-based storage
C. Database
D. CDN

Answer: D

NEW QUESTION 263
- (Exam Topic 2)
You are the security policy lead for your organization, which is considering migrating from your on-premises, legacy environment into the cloud. You are reviewing the Cloud Security Alliance Cloud Controls Matrix (CSA CCM) as a tool for your organization.
What is probably the best benefit offered by the CCM? Response:

A. The low cost of the tool
B. Allowing your organization to leverage existing controls across multiple frameworks so as not to duplicate effort
C. Simplicity of control selection from the list of approved choices
D. Ease of implementation by choosing controls from the list of qualified vendors

Answer: B

NEW QUESTION 266
- (Exam Topic 2)
Which of the following is a method for apportioning resources that involves prioritizing resource requests to resolve contention situations?
Response:

A. Reservations
B. Shares
C. Cancellations
D. Limits

Answer: B

NEW QUESTION 268
- (Exam Topic 2)
An audit against the _____ will demonstrate that an organization has ¬adequate security controls to meet its ISO 27001 requirements.
Response:

A. SAS 70 standard
B. SSAE 16 standard
C. ISO 27002 certification criteria
D. NIST SP 800-53

Answer: C

NEW QUESTION 269
- (Exam Topic 2)
What is the primary security mechanism used to protect SOAP and REST APIs? Response:

A. Firewalls
B. XML firewalls
C. Encryption
D. WAFs

Answer: C

NEW QUESTION 272
- (Exam Topic 2)
Which of the following is NOT a common component of a DLP implementation process? Response:

A. Discovery
B. Monitoring
C. Revision
D. Enforcement

Answer: C

NEW QUESTION 276
- (Exam Topic 2)
The tasks performed by the hypervisor in the virtual environment can most be likened to the tasks of the _____ in the legacy environment.
Response:

A. Central processing unit (CPU)
B. Security team
C. OS
D. PGP

Answer: A

NEW QUESTION 279
- (Exam Topic 2)
From a security perspective, automation of configuration aids in _____.
Response:

A. Enhancing performance
B. Reducing potential attack vectors
C. Increasing ease of use of the systems
D. Reducing need for administrative personnel

Answer: B

NEW QUESTION 280
- (Exam Topic 3)
Federation allows _____ across organizations.
Response:

A. Role replication
B. Encryption
C. Policy
D. Access

Answer: D

NEW QUESTION 283
- (Exam Topic 3)
You work for a company that operates a production environment in the cloud. Another company using the same cloud provider is under investigation by law enforcement for racketeering.
Your company should be concerned about this because of the cloud characteristic of . Response:

A. Virtualization
B. Pooled resources
C. Elasticity
D. Automated self-service

Answer: B

NEW QUESTION 287
- (Exam Topic 3)
The BCDR plan/process should be written and documented in such a way that it can be used by _____.
Response:

A. Users
B. Essential BCDR team members
C. Regulators
D. Someone with the requisite skills

Answer: D

NEW QUESTION 289
- (Exam Topic 3)
In attempting to provide a layered defense, the security practitioner should convince senior management to include security controls of which type?
Response:

A. Technological
B. Physical
C. Administrative
D. All of the above

Answer: D

NEW QUESTION 292
- (Exam Topic 3)
Which network protocol is essential for allowing automation and orchestration within a cloud environment? Response:

A. DNSSEC
B. DHCP
C. IPsec
D. VLANs

Answer: B

NEW QUESTION 295
- (Exam Topic 3)
Which of the following aspects of the BC/DR process poses a risk to the organization? Response:

A. Threat intelligence gathering
B. Preplacement of response assets
C. Budgeting for disaster
D. Full testing of the plan

Answer: D

NEW QUESTION 298
- (Exam Topic 3)
During the assessment phase of a risk evaluation, what are the two types of tests that are performed? Response:

A. Internal and external
B. Technical and managerial
C. Physical and logical
D. Qualitative and quantitative

Answer: D

NEW QUESTION 300
- (Exam Topic 3)
Access should be based on _____.
Response:

A. Regulatory mandates
B. Business needs and acceptable risk
C. User requirements and management requests
D. Optimum performance and security provision

Answer: B

NEW QUESTION 301
- (Exam Topic 3)
Digital rights management (DRM) solutions (sometimes referred to as information rights management, or IRM) often protect unauthorized distribution of what type of intellectual property?
Response:

A. Patents
B. Trademarks
C. Personally identifiable information (PII)
D. Copyright

Answer: D

NEW QUESTION 303
- (Exam Topic 3)
If bit-splitting is used to store data sets across multiple jurisdictions, how may this enhance security? Response:

A. By making seizure of data by law enforcement more difficult
B. By hiding it from attackers in a specific jurisdiction
C. By ensuring that users can only accidentally disclose data to one geographic area
D. By restricting privilege user access

Answer: A

NEW QUESTION 308
- (Exam Topic 3)
Although indirect identifiers cannot alone point to an individual, the more of them known can lead to a specific identity. Which strategy can be used to avoid such a connection being made?
Response:

A. Masking
B. Anonymization
C. Obfuscation
D. Encryption

Answer: B

NEW QUESTION 310
- (Exam Topic 3)
Typically, SSDs are _____.
Response:

A. More expensive than spinning platters
B. Larger than tape backup
C. Heavier than tape libraries
D. More subject to malware than legacy drives

Answer: A

NEW QUESTION 314
- (Exam Topic 3)
A cloud provider is looking to provide a higher level of assurance to current and potential cloud customers about the design and effectiveness of their security controls.
Which of the following audit reports would the cloud provider choose as the most appropriate to accomplish this goal?
Response:

A. SAS-70
B. SOC 1
C. SOC 2
D. SOC 3

Answer: D

NEW QUESTION 317
- (Exam Topic 3)
Which of the following is not a component of the of the STRIDE model? Response:

A. Spoofing
B. Repudiation
C. Information disclosure
D. External pen testing

Answer: D

NEW QUESTION 320
- (Exam Topic 3)
The ISO/IEC 27001:2013 security standard contains 14 different domains that cover virtually all areas of IT operations and procedures. Which of the following is NOT one of the domains listed in the standard?
Response:

A. Legal
B. Management
C. Assets
D. Supplier Relationships

Answer: A

NEW QUESTION 324
- (Exam Topic 3)
The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes “security misconfiguration.”
Which of these is a technique to reduce the potential for a security misconfiguration? Response:

A. Get regulatory approval for major configuration modifications.
B. Update the BCDR plan on a timely basis.
C. Train all users on proper security procedures.
D. Perform periodic scans and audits of the environment.

Answer: D

NEW QUESTION 327
- (Exam Topic 3)
You are developing a new process for data discovery for your organization and are charged with ensuring that all applicable data is included. Which of the following is NOT one of the three methods of data discovery?
Response:

A. Metadata
B. Content analysis
C. Labels
D. Classification

Answer: D

NEW QUESTION 328
- (Exam Topic 3)
Which of the following aids in the ability to demonstrate due diligence efforts?
Response:

A. Redundant power lines
B. HVAC placement
C. Security training documentation
D. Bollards

Answer: C

NEW QUESTION 329
- (Exam Topic 3)
A truly airgapped machine selector will _____.
Response:

A. Terminate a connection before creating a new connection
B. Be made of composites and not metal
C. Have total Faraday properties
D. Not be portable

Answer: A

NEW QUESTION 331
- (Exam Topic 3)
Which of the following would NOT be used to determine the classification of data?
Response:

A. Metadata
B. PII
C. Creator
D. Future use

Answer: D

NEW QUESTION 334
- (Exam Topic 3)
When using an Infrastructure as a Service (IaaS) solution, what is the capability provided to the customer? Response:

A. To provision processing, storage, networks, and other fundamental computing resources when the consumer is not able to deploy and run arbitrary software, which can include operating systems and applications.
B. To provision processing, storage, networks, and other fundamental computing resources when the provider is able to deploy and run arbitrary software, which can include operating systems and applications.
C. To provision processing, storage, networks, and other fundamental computing resources when the auditor is able to deploy and run arbitrary software, which can include operating systems and applications.
D. To provision processing, storage, networks, and other fundamental computing resources when the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

Answer: D

NEW QUESTION 337
- (Exam Topic 3)
You are the security manager for a small retail business involved mainly in direct e-commerce transactions with individual customers (members of the public). The bulk of your market is in Asia, but you do fulfill orders globally.
Your company has its own data center located within its headquarters building in Hong Kong, but it also uses a public cloud environment for contingency backup and archiving purposes. Your company has decided to expand its business to include selling and monitoring life-support equipment for medical providers.
What characteristic do you need to ensure is offered by your cloud provider? Response:

A. Full automation of security controls within the cloud data center
B. Tier 4 of the Uptime Institute certifications
C. Global remote access
D. Prevention of ransomware infections

Answer: B

NEW QUESTION 339
- (Exam Topic 3)
What is the major difference between authentication/authorization? Response:

A. Code verification/code implementation
B. Identity validation/access permission
C. Inverse incantation/obverse instantiation
D. User access/privileged access

Answer: B

NEW QUESTION 341
- (Exam Topic 3)
Which of the following might make crypto-shredding difficult or useless? Response:

A. Cloud provider also managing the organization's keys
B. Lack of physical access to the environment
C. External attackers
D. Lack of user training and awareness

Answer: A

NEW QUESTION 345
- (Exam Topic 3)
What aspect of a Type 2 hypervisor involves additional security concerns that are not relevant with a Type 1 hypervisor?
Response:

A. Reliance on a host operating system
B. Auditing
C. Proprietary software
D. Programming languages

Answer: A

NEW QUESTION 347
- (Exam Topic 3)
Virtual machine (VM) configuration management (CM) tools should probably include _____.
Response:

A. Biometric recognition
B. Anti-tampering mechanisms
C. Log file generation
D. Hackback capabilities

Answer: C

NEW QUESTION 352
- (Exam Topic 3)
When a user accesses a system, what process determines the roles and privileges that user is granted within the application?
Response:

A. Authorization
B. Authentication
C. Provisioning
D. Privilege

Answer: A

NEW QUESTION 356
- (Exam Topic 3)
Which type of web application monitoring most closely measures actual activity? Response:

A. Synthetic performance monitoring
B. Real-user monitoring (RUM)
C. Security information and event management (SIEM)
D. Database application monitor (DAM)

Answer: B

NEW QUESTION 358
- (Exam Topic 3)
Web application firewalls (WAFs) are designed primarily to protect applications from common attacks like: Response:

A. Syn floods
B. Ransomware
C. XSS and SQL injection
D. Password cracking

Answer: C

NEW QUESTION 361
- (Exam Topic 3)
There are two reasons to conduct a test of the organization's recovery from backup in an environment other than the primary production environment. Which of the following is one of them? Response:

A. It is good to invest in more than one community.
B. You want to approximate contingency conditions, which includes not operating in the primary location.
C. It is good for your personnel to see other places occasionally.

D. Your regulators won't follow you offsite, so you'll be unobserved during your test.

Answer: B

NEW QUESTION 363
- (Exam Topic 3)
Which of the following methods of addressing risk is most associated with insurance? Response:

A. Transference
B. Avoidance
C. Acceptance
D. Mitigation

Answer: A

NEW QUESTION 367
- (Exam Topic 3)
Tokenization requires two distinct _____.
Response:

A. Authentication factors
B. Databases
C. Encryption keys
D. Personnel

Answer: B

NEW QUESTION 371
- (Exam Topic 3)
Which characteristic of automated patching makes it attractive? Response:

A. Cost
B. Speed
C. Noise reduction
D. Capability to recognize problems quickly

Answer: B

NEW QUESTION 372
- (Exam Topic 3)
Your company operates in a highly competitive market, with extremely high-value data assets. Senior management wants to migrate to a cloud environment but is concerned that providers will not meet the company's security needs.
Which deployment model would probably best suit the company's needs? Response:

A. Public
B. Private
C. Community
D. Hybrid

Answer: B

NEW QUESTION 374
- (Exam Topic 3)
What are the objectives of change management? (Choose all that apply.)
Response:

A. Respond to a customer's changing business requirements while maximizing value and reducing incidents, disruption, and rework
B. Ensure that changes are recorded and evaluated
C. Respond to business and IT requests for change that will disassociate services with business needs
D. Ensure that all changes are prioritized, planned, tested, implemented, documented, and reviewed in a controlled manner

Answer: AB

NEW QUESTION 375
- (Exam Topic 3)
Which of the following is not a security concern related to archiving data for long-term storage? Response:

A. Long-term storage of the related cryptographic keys
B. Format of the data
C. Media the data resides on
D. Underground depth of the storage facility

Answer: D

NEW QUESTION 376

- (Exam Topic 3)
A web application firewall (WAF) can understand and act on _____ traffic.
Response:

A. Malicious
B. SMTP
C. ICMP
D. HTTP

Answer: D

NEW QUESTION 377
- (Exam Topic 3) Who operates the management plane? Response:

A. Regulators
B. End consumers
C. Privileged users
D. Privacy data subjects

Answer: C

NEW QUESTION 380
- (Exam Topic 3)
In a data retention policy, what is perhaps the most crucial element? Response:

A. Location of the data archive
B. Frequency of backups
C. Security controls in long-term storage
D. Data recovery procedures

Answer: D

NEW QUESTION 384
- (Exam Topic 3)
Your company has just been served with an eDiscovery order to collect event data and other pertinent information from your application during a specific period of time, to be used as potential evidence for a court proceeding.
Which of the following, apart from ensuring that you collect all pertinent data, would be the MOST important consideration?
Response:

A. Encryption
B. Chain of custody
C. Compression
D. Confidentiality

Answer: B

NEW QUESTION 387
- (Exam Topic 3)
Security best practices in a virtualized network environment would include which of the following? Response:

A. Using distinct ports and port groups for various VLANs on a virtual switch rather than running them through the same port
B. Running iSCSI traffic unencrypted in order to have it observed and monitored by NIDS
C. Adding HIDS to all virtual guests
D. Hardening all outward-facing firewalls in order to make them resistant to attack

Answer: A

NEW QUESTION 389
- (Exam Topic 3)
You work for a government research facility. Your organization often shares data with other government research organizations.
You would like to create a single sign-on experience across the organizations, where users at each organization can sign in with the user ID/authentication issued by that organization, then access research data in all the other organizations.
Instead of replicating the data stores of each organization at every other organization (which is one way of accomplishing this goal), you instead want every user to have access to each organization's specific storage resources.
In order to pass the user IDs and authenticating credentials of each user among the organizations, what
protocol/language/motif will you most likely utilize? Response:

A. Representational State Transfer (REST)
B. Security Assertion Markup Language (SAML)
C. Simple Object Access Protocol (SOAP)
D. Hypertext Markup Language (HTML)

Answer: B

NEW QUESTION 390
- (Exam Topic 3)
With cloud computing crossing many jurisdictional boundaries, it is a virtual certainty that conflicts will arise between differing regulations. What is the major

impediment to resolving conflicts between multiple jurisdictions to form an overall policy?
Response:

A. Language differences
B. Technologies used
C. Licensing issues
D. Lack of international authority

Answer: D

NEW QUESTION 394
- (Exam Topic 3)
Managed cloud services exist because the service is less expensive for each customer than creating the same services for themselves in a legacy environment. Using a managed service allows the customer to realize significant cost savings through the reduction of
_____.
Response:

A. Risk
B. Security controls
C. Personnel
D. Data

Answer: C

NEW QUESTION 395
- (Exam Topic 3)
What is the term used to describe loss of access to data because the cloud provider has ceased operation? Response:

A. Closing
B. Vendor lock-out
C. Vendor lock-in
D. Masking

Answer: B

NEW QUESTION 398
- (Exam Topic 3)
Software-defined networking (SDN) is intended to separate different network capabilities and allow for the granting of granular configurations, permissions, and features to non-network staff or customers. Which network capability is separated from forwarding of traffic?
Response:

A. Routing
B. Firewalling
C. Filtering
D. IPS

Answer: C

NEW QUESTION 399
- (Exam Topic 3)
Setting thermostat controls by measuring the temperature will result in the _____ highest energy costs. Response:

A. Server inlet
B. Return air
C. Under-floor
D. External ambient

Answer: B

NEW QUESTION 402
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CCSP Exam with Our Prep Materials Via below:

https://www.certleader.com/CCSP-dumps.html