

ISC2

Exam Questions CCSP

Certified Cloud Security Professional



NEW QUESTION 1

- (Exam Topic 1)

DLP can be combined with what other security technology to enhance data controls? Response:

- A. DRM
- B. SIEM
- C. Kerberos
- D. Hypervisors

Answer: A

NEW QUESTION 2

- (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, what is one reason the threat of insecure interfaces and APIs is so prevalent in cloud computing? Response:

- A. Cloud customers and third parties are continually enhancing and modifying APIs.
- B. APIs can have automated settings.
- C. It is impossible to uninstall APIs.
- D. APIs are a form of malware.

Answer: A

NEW QUESTION 3

- (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 4

- (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 5

- (Exam Topic 1)

What is used with a single sign-on system for authentication after the identity provider has successfully authenticated a user?

Response:

- A. Token
- B. Key
- C. XML
- D. SAML

Answer: A

NEW QUESTION 6

- (Exam Topic 1)

When an organization implements an SIEM solution and begins aggregating event data, the configured event sources are only valid at the time it was configured. Application modifications, patching, and other upgrades will change the events generated and how they are represented over time. What process is necessary to ensure events are collected and processed with this in mind?

- A. Continual review
- B. Continuous optimization
- C. Aggregation updates
- D. Event elasticity

Answer: B

NEW QUESTION 7

- (Exam Topic 1)

Which of the following should occur at each stage of the SDLC?

- A. Added functionality
- B. Management review
- C. Verification and validation
- D. Repurposing of any newly developed components

Answer: C

NEW QUESTION 8

- (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 9

- (Exam Topic 1)

Which of the following is a file server that provides data access to multiple, heterogeneous machines/users on the network?

Response:

- A. Storage area network (SAN)
- B. Network-attached storage (NAS)
- C. Hardware security module (HSM)
- D. Content delivery network (CDN)

Answer: B

NEW QUESTION 10

- (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 10

- (Exam Topic 1)

Which of the following are contractual components that the CSP should review and understand fully when contracting with a cloud service provider? (Choose two.)

- A. Concurrently maintainable site infrastructure
- B. Use of subcontractors
- C. Redundant site infrastructure capacity components
- D. Scope of processing

Answer: BD

NEW QUESTION 11

- (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 15

- (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 17

- (Exam Topic 1)

Which of the following is the best and only completely secure method of data destruction? Response:

- A. Degaussing
- B. Crypto-shredding
- C. Physical destruction of resources that store the data
- D. Legal order issued by the prevailing jurisdiction where the data is geographically situated

Answer: C

NEW QUESTION 20

- (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 23

- (Exam Topic 1)

You are performing an audit of the security controls used in a cloud environment. Which of the following would best serve your purpose? Response:

- A. The business impact analysis (BIA)
- B. A copy of the VM baseline configuration
- C. The latest version of the company's financial records
- D. A SOC 3 report from another (external) auditor

Answer: B

NEW QUESTION 27

- (Exam Topic 1)

Which of the following is a method for apportioning resources that involves setting guaranteed minimums for all tenants/customers within the environment? Response:

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

Answer: A

NEW QUESTION 28

- (Exam Topic 1)

What sort of legal enforcement may the Payment Card Industry (PCI) Security Standards Council not bring to bear against organizations that fail to comply with the Payment Card Industry Data Security Standard (PCI DSS)?

Response:

- A. Fines
- B. Jail time
- C. Suspension of credit card processing privileges
- D. Subject to increased audit frequency and scope

Answer: B

NEW QUESTION 31

- (Exam Topic 1)

TLS uses _____ to authenticate a connection and create a shared secret for the duration of the session.

- A. SAML 2.0
- B. X.509 certificates
- C. 802.11X
- D. The Diffie-Hellman process

Answer: B

NEW QUESTION 32

- (Exam Topic 1)

Which of the following is a possible negative aspect of bit-splitting?

- A. Greater chance of physical theft of assets
- B. Loss of public image
- C. Some risk to availability, depending on the implementation
- D. A small fire hazard

Answer: C

NEW QUESTION 34

- (Exam Topic 1)

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 38

- (Exam Topic 1)

Why are PaaS environments at a higher likelihood of suffering backdoor vulnerabilities?

- A. They rely on virtualization.
- B. They are often used for software development.
- C. They have multitenancy.
- D. They are scalable.

Answer: B

NEW QUESTION 43

- (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 45

- (Exam Topic 1)

DAST checks software functionality in _____.

Response:

- A. The production environment
- B. A runtime state
- C. The cloud
- D. An IaaS configuration

Answer: B

NEW QUESTION 46

- (Exam Topic 1)

A firewall can use all of the following techniques for controlling traffic except:

- A. Rule sets
- B. Behavior analysis
- C. Content filtering
- D. Randomization

Answer: D

NEW QUESTION 50

- (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. Management is interested in adopting an Agile development style.

This will be typified by which of the following traits? Response:

- A. Reliance on a concrete plan formulated during the Define phase
- B. Rigorous, repeated security testing

- C. Isolated programming experts for specific functional elements
- D. Short, iterative work periods

Answer: D

NEW QUESTION 53

- (Exam Topic 1)

Which security certification serves as a general framework that can be applied to any type of system or application?

- A. ISO/IEC 27001
- B. PCI DSS
- C. FIPS 140-2
- D. NIST SP 800-53

Answer: A

NEW QUESTION 56

- (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 60

- (Exam Topic 1)

All of the following are terms used to describe 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 65

- (Exam Topic 1)

Which of the following are considered to be the building blocks of cloud computing? Response:

- A. Data, access control, virtualization, and services
- B. Storage, networking, printing and virtualization
- C. CPU, RAM, storage and networking
- D. Data, CPU, RAM, and access control

Answer: C

NEW QUESTION 67

- (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 71

- (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 76

- (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 81

- (Exam Topic 1)

What is the amount of fuel that should be on hand to power generators for backup datacenter power, in all tiers, according to the Uptime Institute?

- A. 1
- B. 1,000 gallons
- C. 12 hours
- D. As much as needed to ensure all systems may be gracefully shut down and data securely stored

Answer: C

NEW QUESTION 84

- (Exam Topic 1)

Impact resulting from risk being realized is often measured in terms of _____.

- A. Amount of data lost
- B. Money
- C. Amount of property lost
- D. Number of people affected

Answer: B

NEW QUESTION 88

- (Exam Topic 1)

Application virtualization can typically be used for .

- A. Denying access to untrusted users
- B. Detecting and mitigating DDoS attacks
- C. Replacing encryption as a necessary control
- D. Running an application on an endpoint without installing it

Answer: D

NEW QUESTION 92

- (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 97

- (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 101

- (Exam Topic 1)

Which of the following is not a reason for conducting audits?

- A. Regulatory compliance
- B. User satisfaction
- C. Determination of service quality
- D. Security assurance

Answer: B

NEW QUESTION 103

- (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 104

- (Exam Topic 2)

Which of the following characteristics is associated with digital rights management (DRM) solutions (sometimes referred to as information rights management, or IRM)?

Response:

- A. Mapping to existing access control lists (ACLs)
- B. Delineating biometric catalogs
- C. Preventing multifactor authentication
- D. Prohibiting unauthorized transposition

Answer: A

NEW QUESTION 109

- (Exam Topic 2)

What could be the result of failure of the cloud provider to secure the hypervisor in such a way that one user on a virtual machine can see the resource calls of another user's virtual machine?

Response:

- A. Unauthorized data disclosure
- B. Inference attacks
- C. Social engineering
- D. Physical intrusion

Answer: B

NEW QUESTION 110

- (Exam Topic 2)

Which SSAE 16 audit report is simply an attestation of audit results? Response:

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

Answer: D

NEW QUESTION 111

- (Exam Topic 2)

Penetration testing is a(n) _____ form of security assessment.

Response:

- A. Active
- B. Comprehensive
- C. Total
- D. Inexpensive

Answer: A

NEW QUESTION 112

- (Exam Topic 2)

Which cloud service category is MOST likely to use a client-side key management system? Response:

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

Answer: B

NEW QUESTION 113

- (Exam Topic 2)

Which of the following methods is often used to obscure data from production systems for use in test or development environments?

Response:

- A. Tokenization
- B. Encryption
- C. Masking
- D. Classification

Answer: C

NEW QUESTION 114

- (Exam Topic 2)

The physical layout of a cloud data center campus should include redundancies of all the following except

_____.

Response:

- A. Physical perimeter security controls (fences, lights, walls, etc.)
- B. The administration/support staff building
- C. Electrical utility lines
- D. Communications connectivity lines

Answer: B

NEW QUESTION 116

- (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 120

- (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 121

- (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 126

- (Exam Topic 2)

All of the following entities are required to use FedRAMP-accredited Cloud Service Providers except

_____.

Response:

- A. The US post office
- B. The Department of Homeland Security
- C. Federal Express
- D. The CIA

Answer: C

NEW QUESTION 131

- (Exam Topic 2)

You are the IT security manager for a video game software development company. Which of the following is most likely to be your primary concern on a daily basis?

Response:

- A. Health and human safety
- B. Security flaws in your products
- C. Security flaws in your organization

D. Regulatory compliance

Answer: C

NEW QUESTION 136

- (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 140

- (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 142

- (Exam Topic 2)

Which of the following would NOT be included as input into the requirements gathering for an application or system?

Response:

- A. Users
- B. Management
- C. Regulators
- D. Auditors

Answer: D

NEW QUESTION 146

- (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 149

- (Exam Topic 2)

Which of the following would probably best aid an organization in deciding whether to migrate from a legacy environment to a particular cloud provider?

Response:

- A. Rate sheets comparing a cloud provider to other cloud providers
- B. Cloud provider offers to provide engineering assistance during the migration
- C. The cost/benefit measure of closing the organization's relocation site (hot site/warm site) and using the cloud for disaster recovery instead
- D. SLA satisfaction surveys from other (current and past) cloud customers

Answer: D

NEW QUESTION 150

- (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. Remove all nonessential programs from the baseline image
- B. Exclude the target system you intend to baseline from any scheduled updates/patching used in production systems
- C. Include the baseline image in the asset inventory/configuration management database
- D. Configure the host OS according to the baseline requirements

Answer: C

NEW QUESTION 151

- (Exam Topic 2)

Before deploying a specific brand of virtualization toolset, it is important to configure it according to _____.

Response:

- A. Industry standards
- B. Prevailing law of that jurisdiction
- C. Vendor guidance
- D. Expert opinion

Answer: C

NEW QUESTION 154

- (Exam Topic 2)

What is the most secure form of code testing and review? Response:

- A. Open source
- B. Proprietary/internal
- C. Neither open source nor proprietary
- D. Combination of open source and proprietary

Answer: D

NEW QUESTION 155

- (Exam Topic 2)

In application-level encryption, where does the encryption engine reside? Response:

- A. In the application accessing the database
- B. In the OS on which the application is run
- C. Within the database accessed by the application
- D. In the volume where the database resides

Answer: A

NEW QUESTION 159

- (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 160

- (Exam Topic 2)

You are the security manager for a company that is considering cloud migration to an IaaS environment. You are assisting your company's IT architects in constructing the environment. Which of the following options do you recommend?

Response:

- A. Unrestricted public access
- B. Use of a Type I hypervisor
- C. Use of a Type II hypervisor
- D. Enhanced productivity without encryption

Answer: B

NEW QUESTION 164

- (Exam Topic 2)

Tokenization requires at least _____ database(s).

Response:

- A. One
- B. Two
- C. Three
- D. Four

Answer: B

NEW QUESTION 165

- (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 170

- (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 171

- (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 172

- (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 177

- (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 182

- (Exam Topic 2)

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 "using components with known vulnerabilities."

Why would an organization ever use components with known vulnerabilities to create software? Response:

- A. The organization is insured.
- B. The particular vulnerabilities only exist in a context not being used by developers.
- C. Some vulnerabilities only exist in foreign countries.
- D. A component might have a hidden vulnerability.

Answer: B

NEW QUESTION 184

- (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 186

- (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 188

- (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 192

- (Exam Topic 2)

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 194

- (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 198

- (Exam Topic 2)

What aspect of data center planning occurs first? Response:

- A. Logical design
- B. Physical design
- C. Audit
- D. Policy revision

Answer: B

NEW QUESTION 199

- (Exam Topic 2)

TLS provides _____ and _____ for communications. Response:

- A. Privacy, security
- B. Security, optimization
- C. Privacy, integrity
- D. Enhancement, privacy

Answer: C

NEW QUESTION 202

- (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 205

- (Exam Topic 2)

Which of the following is a risk associated with manual patching especially in the cloud?

Response:

- A. No notice before the impact is realized
- B. Lack of applicability to the environment
- C. Patches may or may not address the vulnerability they were designed to fix.
- D. The possibility for human error

Answer: D

NEW QUESTION 210

- (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 211

- (Exam Topic 2)

Which of the following is a possible negative aspect of bit-splitting? Response:

- A. It may require trust in additional third parties beyond the primary cloud service provider.
- B. There may be cause for management concern that the technology will violate internal policy.
- C. Users will have far greater difficulty understanding the implementation.
- D. Limited vendors make acquisition and support challenging.

Answer: A

NEW QUESTION 216

- (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 217

- (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 219

- (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 224

- (Exam Topic 2)

Which type of testing tends to produce the best and most comprehensive results for discovering system vulnerabilities?

Response:

- A. Static
- B. Dynamic
- C. Pen
- D. Vulnerability

Answer: A

NEW QUESTION 229

- (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 231

- (Exam Topic 2)

DLP solutions typically involve all of the following aspects except _____.

Response:

- A. Data discovery
- B. Tokenization
- C. Monitoring
- D. Enforcement

Answer: B

NEW QUESTION 234

- (Exam Topic 2)

Aside from the fact that the cloud customer probably cannot locate/reach the physical storage assets of the cloud provider, and that wiping an entire storage space would impact other customers, why would degaussing probably not be an effective means of secure sanitization in the cloud?

Response:

- A. All the data storage space in the cloud is already gaussed.
- B. Cloud data storage may not be affected by degaussing.
- C. Federal law prohibits it in the United States.
- D. The blast radius is too wide.

Answer: B

NEW QUESTION 238

- (Exam Topic 2)

Which of these characteristics of a virtualized network adds risks to the cloud environment? Response:

- A. Redundancy
- B. Scalability
- C. Pay-per-use
- D. Self-service

Answer: A

NEW QUESTION 239

- (Exam Topic 2)

Which of the following involves assigning an opaque value to sensitive data fields to protect confidentiality? Response:

- A. Obfuscation
- B. Masking
- C. Tokenization
- D. Anonymization

Answer: C

NEW QUESTION 244

- (Exam Topic 2)

Which of the following is not a way to manage risk? Response:

- A. Enveloping

- B. Mitigating
- C. Accepting
- D. Transferring

Answer: A

NEW QUESTION 245

- (Exam Topic 3)

Which of the following is NOT one of the security domains presented within the Cloud Controls Matrix? Response:

- A. Financial security
- B. Mobile security
- C. Data center security
- D. Interface security

Answer: A

NEW QUESTION 250

- (Exam Topic 3)

Federation allows _____ across organizations.

Response:

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

Answer: D

NEW QUESTION 253

- (Exam Topic 3)

Cloud vendors are held to contractual obligations with specified metrics by:

Response:

- A. SLAs
- B. Regulations
- C. Law
- D. Discipline

Answer: A

NEW QUESTION 256

- (Exam Topic 3)

Devices in the cloud datacenter should be secure against attack. All the following are means of hardening devices, except:

Response:

- A. Using a strong password policy
- B. Removing default passwords
- C. Strictly limiting physical access
- D. Removing all admin accounts

Answer: D

NEW QUESTION 261

- (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 262

- (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 263

- (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 265

- (Exam Topic 3)

Fiber-optic lines are considered part of layer _____ of the OSI model. Response:

- A. 1
- B. 3
- C. 5
- D. 7

Answer: A

NEW QUESTION 270

- (Exam Topic 3)

Digital rights management (DRM) tools can be combined with _____, to enhance security capabilities. Response:

- A. Roaming identity services (RIS)
- B. Egress monitoring solutions (DLP)
- C. Internal hardware settings (BIOS)
- D. Remote Authentication Dial-In User Service (RADIUS)

Answer: B

NEW QUESTION 275

- (Exam Topic 3)

Patches do all the following except _____.

Response:

- A. Address newly discovered vulnerabilities
- B. Solve cloud interoperability problems
- C. Add new features and capabilities to existing systems
- D. Address performance issues

Answer: B

NEW QUESTION 278

- (Exam Topic 3)

Which type of cloud-based storage is IRM typically associated with? Response:

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

Answer: D

NEW QUESTION 281

- (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 285

- (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 290

- (Exam Topic 3)

What type of redundancy can we expect to find in a datacenter of any tier?

Response:

- A. All operational components
- B. All infrastructure
- C. Emergency egress
- D. Full power capabilities

Answer: C

NEW QUESTION 292

- (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 297

- (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 301

- (Exam Topic 3)

FM-200 has all the following properties except _____.

Response:

- A. It's nontoxic at levels used for fire suppression
- B. It's gaseous at room temperature
- C. It may deplete the Earth's ozone layer
- D. It does not leave a film or coagulant after use

Answer: C

NEW QUESTION 304

- (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 307

- (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 311

- (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 "injection." In most cases, what is the method for reducing the risk of an injection attack? Response:

- A. User training
- B. Hardening the OS
- C. Input validation/bounds checking
- D. Physical locks

Answer: C

NEW QUESTION 316

- (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 317

- (Exam Topic 3)

It's important to maintain a current asset inventory list, including surveying your environment on a regular basis, in order to _____. Response:

- A. Prevent unknown, unpatched assets from being used as back doors to the environment
- B. Ensure that any lost devices are automatically entered into the acquisition system for repurchasing and replacement
- C. Maintain user morale by having their devices properly catalogued and annotated
- D. Ensure that billing for all devices is handled by the appropriate departments

Answer: A

NEW QUESTION 318

- (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 319

- (Exam Topic 3)

An audit against the _____ will demonstrate that an organization has a holistic, comprehensive security program. Response:

- A. SAS 70 standard
- B. SSAE 16 standard
- C. SOC 2, Type 2 report matrix
- D. ISO 27001 certification requirements

Answer: D

NEW QUESTION 322

- (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 324

- (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 326

- (Exam Topic 3)

You are the security manager for a small surgical center. Your organization is reviewing upgrade options for its current, on-premises data center. In order to best meet your needs, which one of the following options would you recommend to senior management?

Response:

- A. Building a completely new data center
- B. Leasing a data center that is currently owned by another firm
- C. Renting private cloud space in a Tier 2 data center
- D. Staying with the current data center

Answer: A

NEW QUESTION 331

- (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 332

- (Exam Topic 3)

Alice is the CEO for a software company; she is considering migrating the operation from the current on-premises legacy environment into the cloud.

In order to protect her company's intellectual property, Alice might want to consider implementing all these techniques/solutions except _____.

Response:

- A. Egress monitoring
- B. Encryption
- C. Turnstiles
- D. Digital watermarking

Answer: C

NEW QUESTION 336

- (Exam Topic 3)

In addition to BCDR, what other benefit can your data archive/backup provide? Response:

- A. Physical security enforcement
- B. Access control methodology
- C. Security control against data breach
- D. Identity management testing

Answer: D

NEW QUESTION 341

- (Exam Topic 3)

Which kind of SSAE audit reviews controls dealing with the organization's controls for assuring the confidentiality, integrity, and availability of data?

Response:

- A. SOC 1
- B. SOC 2
- C. SOC 3
- D. SOC 4

Answer: B

NEW QUESTION 343

- (Exam Topic 3)
_____ is perhaps the main external factor driving IAM efforts. Response:

- A. Regulation
- B. Business need
- C. The evolving threat landscape
- D. Monetary value

Answer: A

NEW QUESTION 345

- (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 348

- (Exam Topic 3)
Your application has been a continued target for SQL injection attempts. Which of the following technologies would be best used to combat the likeliness of a successful SQL injection exploit from occurring?
Response:

- A. XML accelerator
- B. WAF
- C. Sandbox
- D. Firewall

Answer: B

NEW QUESTION 353

- (Exam Topic 3)
What is one of the benefits of implementing an egress monitoring solution? Response:

- A. Preventing DDoS attacks
- B. Inventorying data assets
- C. Interviewing data owners
- D. Protecting against natural disasters

Answer: B

NEW QUESTION 358

- (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 359

- (Exam Topic 3)
It is important to include _____ in the design of underfloor plenums if they are also used for wiring. Response:

- A. Mantraps
- B. Sequestered channels
- C. Heat sinks
- D. Tight gaskets

Answer: D

NEW QUESTION 360

- (Exam Topic 3)
Bob is staging an attack against Alice's website. He is able to embed a link on her site that will execute malicious code on a visitor's machine, if the visitor clicks on the link. This is an example of which type of attack?
Response:

- A. Cross-site scripting
- B. Broken authentication/session management

- C. Security misconfiguration
- D. Insecure cryptographic storage

Answer: A

NEW QUESTION 365

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

CCSP Practice Exam Features:

- * CCSP Questions and Answers Updated Frequently
- * CCSP Practice Questions Verified by Expert Senior Certified Staff
- * CCSP Most Realistic Questions that Guarantee you a Pass on Your First Try
- * CCSP Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CCSP Practice Test Here](#)