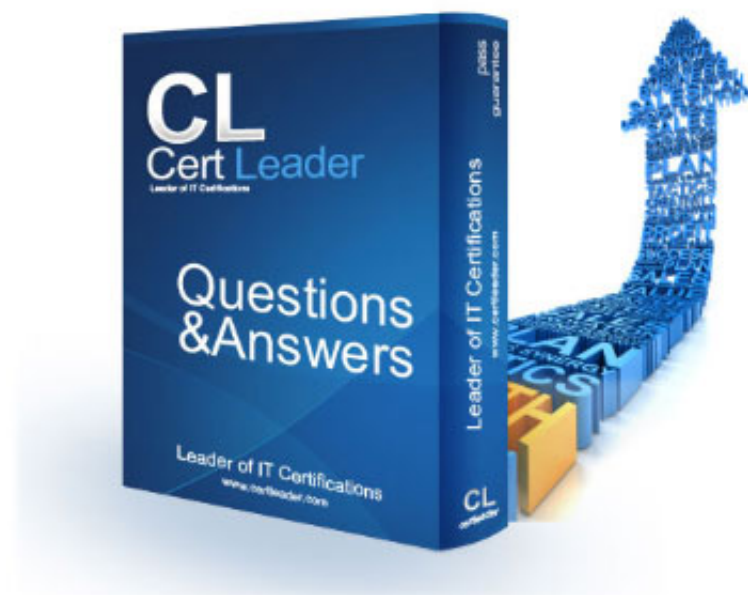


CCSP Dumps

Certified Cloud Security Professional

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



NEW QUESTION 1

- (Exam Topic 1)

Vulnerability scans are dependent on _____ in order to function. Response:

- A. Privileged access
- B. Vulnerability signatures
- C. Malware libraries
- D. Forensic analysis

Answer: B

NEW QUESTION 2

- (Exam Topic 1)

_____ can often be the result of inadvertent activity. Response:

- A. DDoS
- B. Phishing
- C. Sprawl
- D. Disasters

Answer: C

NEW QUESTION 3

- (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 4

- (Exam Topic 1) What can tokenization be used for? Response:

- A. Encryption
- B. Compliance with PCI DSS
- C. Enhancing the user experience
- D. Giving management oversight to e-commerce functions

Answer: B

NEW QUESTION 5

- (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 6

- (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 7

- (Exam Topic 1)

Which of the following is essential for getting full security value from your system baseline? Response:

- A. Capturing and storing an image of the baseline
- B. Keeping a copy of upcoming suggested modifications to the baseline
- C. Having the baseline vetted by an objective third party
- D. Using a baseline from another industry member so as not to engage in repetitious efforts

Answer: A

NEW QUESTION 8

- (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 “unvalidated redirects and forwards.”

Which of the following is a good way to protect against this problem? Response:

- A. Don't use redirects/forwards in your applications.
- B. Refrain from storing credentials long term.
- C. Implement security incident/event monitoring (security information and event management (SIEM)/security information management (SIM)/security event management (SEM)) solutions.
- D. Implement digital rights management (DRM) solutions.

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)

What is the federal agency that accepts applications for new patents?

- A. USDA
- B. USPTO
- C. OSHA
- D. SEC

Answer: B

NEW QUESTION 13

- (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 18

- (Exam Topic 1)

A typical DLP tool can enhance the organization's efforts at accomplishing what legal task? Response:

- A. Evidence collection
- B. Delivering testimony
- C. Criminal prosecution
- D. Enforcement of intellectual property rights

Answer: A

NEW QUESTION 23

- (Exam Topic 1)

The Transport Layer Security (TLS) protocol creates a secure communications channel over public media (such as the Internet). In a typical TLS session, who initiates the protocol?

Response:

- A. The server
- B. The client
- C. The certifying authority
- D. The ISP

Answer: B

NEW QUESTION 26

- (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 27

- (Exam Topic 1)

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.

If you don't use cross-certification, what other model can you implement for this purpose? Response:

- A. Third-party identity broker
- B. Cloud reseller
- C. Intractable nuanced variance
- D. Mandatory access control (MAC)

Answer: A

NEW QUESTION 28

- (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.

What should you not expect the tool to address? Response:

- A. Sensitive data sent inadvertently in user emails
- B. Sensitive data captured by screen shots
- C. Sensitive data moved to external devices
- D. Sensitive data in the contents of files sent via FTP

Answer: B

NEW QUESTION 30

- (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 32

- (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 36

- (Exam Topic 1)

Who is ultimately responsible for a data breach that includes personally identifiable information (PII), in the event of negligence on the part of the cloud provider?

- A. The user
- B. The subject
- C. The cloud provider
- D. The cloud customer

Answer: D

NEW QUESTION 40

- (Exam Topic 1)

Which of the following is not one of the defined security controls domains within the Cloud Controls Matrix, published by the Cloud Security Alliance?

Response:

- A. Financial
- B. Human resources
- C. Mobile security
- D. Identity and access management

Answer: A

NEW QUESTION 45

- (Exam Topic 1)

Which of the following is the recommended operating range for temperature and humidity in a data center?

Response:

- A. Between 62 °F - 81 °F and 40% and 65% relative humidity
- B. Between 64 °F - 81 °F and 40% and 60% relative humidity
- C. Between 64 °F - 84 °F and 30% and 60% relative humidity
- D. Between 60 °F - 85 °F and 40% and 60% relative humidity

Answer: B

NEW QUESTION 49

- (Exam Topic 1)

Which of the following practices can enhance both operational capabilities and configuration management efforts?

Response:

- A. Regular backups
- B. Constant uptime
- C. Multifactor authentication
- D. File hashes

Answer: D

NEW QUESTION 52

- (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 56

- (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 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 68

- (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 71

- (Exam Topic 1)

When a data center is configured such that the backs of the devices face each other and the ambient temperature in the work area is cool, it is called _____.

Response:

- A. Hot aisle containment
- B. Cold aisle containment
- C. Thermo-optimized
- D. HVAC modulated

Answer: A

NEW QUESTION 76

- (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 81

- (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 85

- (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 90

- (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 94

- (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. Most of the cloud customer's interaction with resources will be performed through APIs.
- B. APIs are inherently insecure.
- C. Attackers have already published vulnerabilities for all known APIs.
- D. APIs are known carcinogens.

Answer: A

NEW QUESTION 98

- (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 100

- (Exam Topic 1)

Which of the following is not typically included as a basic phase of the software development life cycle?

- A. Define
- B. Design
- C. Describe
- D. Develop

Answer: C

NEW QUESTION 102

- (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 105

- (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 110

- (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 115

- (Exam Topic 1)

When an organization considers cloud migrations, the organization's software developers will need to know which _____ and _____ which the organization will be using, in order to properly and securely create suitable applications.

- A. Geographic location, native language
- B. Legal restrictions, specific ISP
- C. Service model, deployment model
- D. Available bandwidth, telecommunications country code

Answer: C

NEW QUESTION 119

- (Exam Topic 1)

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 124

- (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 127

- (Exam Topic 1)

Which of the following is not an enforceable governmental request? Response:

- A. Warrant
- B. Subpoena
- C. Court order
- D. Affidavit

Answer: D

NEW QUESTION 130

- (Exam Topic 1)

DRM solutions should generally include all the following functions, except:

- A. Persistency
- B. Automatic self-destruct
- C. Automatic expiration
- D. Dynamic policy control

Answer: B

NEW QUESTION 132

- (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 135

- (Exam Topic 1)

SOX was enacted because of which of the following? Response:

- A. Poor BOD oversight
- B. Lack of independent audits
- C. Poor financial controls
- D. All of the above

Answer: D

NEW QUESTION 137

- (Exam Topic 1)

A honeypot should contain data_____.

Response:

- A. Raw
- B. Production
- C. Useless
- D. Sensitive

Answer: C

NEW QUESTION 141

- (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 145

- (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 148

- (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 152

- (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 154

- (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 157

- (Exam Topic 2)

What is the intellectual property protection for the logo of a new video game? Response:

- A. Copyright
- B. Patent
- C. Trademark
- D. Trade secret

Answer: C

NEW QUESTION 158

- (Exam Topic 2)

A process for _____ can aid in protecting against data disclosure due to lost devices. Response:

- A. User punishment
- B. Credential revocation
- C. Law enforcement notification
- D. Device tracking

Answer: B

NEW QUESTION 160

- (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 163

- (Exam Topic 2)

A federated identity system is composed of three main components. Which of the following is NOT one of the three main components?

Response:

- A. Identity provider
- B. User
- C. Relying party
- D. API

Answer: D

NEW QUESTION 165

- (Exam Topic 2)

A bare-metal hypervisor is Type _____.

Response:

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

Answer: A

NEW QUESTION 167

- (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 170

- (Exam Topic 2)

Your organization has made it a top priority that any cloud environment being considered to host production systems have guarantees that resources will always be available for allocation when needed.

Which of the following concepts will you need to ensure is part of the contract and SLA? Response:

- A. Limits
- B. Shares

- C. Resource pooling
- D. Reservations

Answer: D

NEW QUESTION 172

- (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 176

- (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 181

- (Exam Topic 2)

Which one of the following is not one of the three common threat modeling techniques? Response:

- A. Focused on assets
- B. Focused on attackers
- C. Focused on software
- D. Focused on social engineering

Answer: D

NEW QUESTION 185

- (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 190

- (Exam Topic 2)

Which of the following is not one of the types of controls? Response:

- A. Transitional
- B. Administrative
- C. Technical
- D. Physical

Answer: A

NEW QUESTION 195

- (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 198

- (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 201

- (Exam Topic 2)

All of the following entitles 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 204

- (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 207

- (Exam Topic 2)

You are a consultant performing an external security review on a large manufacturing firm. You determine that its newest assembly plant, which cost \$24 million, could be completely destroyed by a fire but that a fire suppression system could effectively protect the plant.

The fire suppression system costs \$15 million. An insurance policy that would cover the full replacement cost of the plant costs \$1 million per month.

In order to establish the true annualized loss expectancy (ALE), you would need all of the following information except _____.

Response:

- A. The amount of revenue generated by the plant
- B. The rate at which the plant generates revenue
- C. The length of time it would take to rebuild the plant
- D. The amount of product the plant creates

Answer: D

NEW QUESTION 208

- (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 211

- (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 213

- (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 215

- (Exam Topic 2)
Which type of software is most likely to be reviewed by the most personnel, with the most varied perspectives?
Response:

- A. Database management software
- B. Open source software
- C. Secure software
- D. Proprietary software

Answer: B

NEW QUESTION 219

- (Exam Topic 2)
Tokenization requires at least _____ database(s).
Response:

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

Answer: B

NEW QUESTION 221

- (Exam Topic 2)
At which phase of the SDLC process should security begin participating? Response:

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

Answer: A

NEW QUESTION 223

- (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 227

- (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 230

- (Exam Topic 2)
What principle must always been included with an SOC 2 report? Response:

- A. Confidentiality
- B. Security
- C. Privacy
- D. Processing integrity

Answer: B

NEW QUESTION 231

- (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 233

- (Exam Topic 2)

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

Response:

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

Answer: A

NEW QUESTION 237

- (Exam Topic 2) What are SOCI/SOCII/SOCIII? Response:

- A. Risk management frameworks
- B. Access controls
- C. Audit reports
- D. Software development phases

Answer: C

NEW QUESTION 240

- (Exam Topic 2)

What type of software is often considered secured and validated via community knowledge?

Response:

- A. Proprietary
- B. Object-oriented
- C. Open source
- D. Scripting

Answer: C

NEW QUESTION 245

- (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 250

- (Exam Topic 2) What is a key component of GLBA? Response:

- A. The right to be forgotten
- B. EU Data Directives
- C. The information security program
- D. The right to audit

Answer: C

NEW QUESTION 254

- (Exam Topic 2)

You are the security subject matter expert (SME) for an organization considering a transition from the legacy environment into a hosted cloud provider's data center.

One of the challenges you're facing is whether the provider will have undue control over your data once it is within the provider's data center; will the provider be able to hold your organization hostage because they have your data?

This is a(n) _____ issue. Response:

- A. Interoperability
- B. Portability
- C. Availability
- D. Security

Answer: B

NEW QUESTION 259

- (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 261

- (Exam Topic 2)

Which of the following in a federated environment is responsible for consuming authentication tokens? Response:

- A. Relying party
- B. Identity provider
- C. Cloud services broker
- D. Authentication provider

Answer: A

NEW QUESTION 265

- (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 266

- (Exam Topic 2)

What is a data custodian responsible for? Response:

- A. The safe custody, transport, storage of the data, and implementation of business rules
- B. Data content, context, and associated business rules
- C. Logging and alerts for all data
- D. Customer access and alerts for all data

Answer: A

NEW QUESTION 270

- (Exam Topic 2)

A denial of service (DoS) attack can potentially impact all customers within a cloud environment with the continued allocation of additional resources. Which of the following can be useful for a customer to protect themselves from a DoS attack against another customer?

Response:

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

Answer: B

NEW QUESTION 273

- (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 277

- (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 278

- (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 281

- (Exam Topic 2)

_____ can often be the result of inadvertent activity. Response:

- A. DDoS
- B. Phishing
- C. Sprawl
- D. Disasters

Answer: C

NEW QUESTION 286

- (Exam Topic 2)

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 288

- (Exam Topic 2)

Your organization is developing software for wide use by the public. You have decided to test it in a cloud environment, in a PaaS model. Which of the following should be of particular concern to your organization for this situation?

Response:

- A. Vendor lock-in
- B. Backdoors
- C. Regulatory compliance
- D. High-speed network connectivity

Answer: B

NEW QUESTION 293

- (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 296

- (Exam Topic 2)

Which of the following data protection methodologies maintains the ability to connect back values to the original values?

Response:

- A. Tokenization
- B. Anonymization
- C. Obfuscation
- D. Dynamic mapping

Answer: A

NEW QUESTION 297

- (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 299

- (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 304

- (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 305

- (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 307

- (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 311

- (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 316

- (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 319

- (Exam Topic 3)

Which of the following threats from the OWASP Top Ten is the most difficult for an organization to protect against?

Response:

- A. Advanced persistent threats
- B. Account hijacking
- C. Malicious insiders
- D. Denial of service

Answer: C

NEW QUESTION 324

- (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 327

- (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 331

- (Exam Topic 3)

When a customer performs a penetration test in the cloud, why isn't the test an optimum simulation of attack conditions?

Response:

- A. Attackers don't use remote access for cloud activity
- B. Advanced notice removes the element of surprise
- C. When cloud customers use malware, it's not the same as when attackers use malware
- D. Regulator involvement changes the attack surface

Answer: B

NEW QUESTION 333

- (Exam Topic 3)

Which of the following is not a component of the STRIDE model? Response:

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

Answer: D

NEW QUESTION 334

- (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 336

- (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 339

- (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 342

- (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 343

- (Exam Topic 3)

The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. A cloud customer that does not perform sufficient due diligence can suffer harm if the cloud provider they've selected goes out of business.

What do we call this problem? Response:

- A. Vendor lock-in
- B. Vendor lock-out
- C. Vendor incapacity
- D. Unscaled

Answer: B

NEW QUESTION 346

- (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 350

- (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 353

- (Exam Topic 3)

With data in transit, which of the following will be the MOST major concern in order for a DLP solution to properly work?

Response:

- A. Scalability
- B. Encryption
- C. Redundancy
- D. Integrity

Answer: B

NEW QUESTION 354

- (Exam Topic 3)

DLP solutions can aid in deterring loss due to which of the following?

Response:

- A. Randomization
- B. Inadvertent disclosure
- C. Natural disaster
- D. Device failure

Answer: B

NEW QUESTION 358

- (Exam Topic 3)

What is the cloud service model in which the customer is responsible for administration of the OS? Response:

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

Answer: A

NEW QUESTION 360

- (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 362

- (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 364

- (Exam Topic 3)

Your company maintains an on-premises data center for daily production activities but wants to use a cloud service to augment this capability during times of increased demand (cloud bursting).

Which deployment model would probably best suit the company's needs? Response:

- A. Public
- B. Private

- C. Community
- D. Hybrid

Answer: D

NEW QUESTION 366

- (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 369

- (Exam Topic 3)

All of these are reasons an organization may want to consider cloud migration except: Response:

- A. Reduced personnel costs
- B. Elimination of risks
- C. Reduced operational expenses
- D. Increased efficiency

Answer: B

NEW QUESTION 371

- (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 374

- (Exam Topic 3)

What type of identity system allows trust and verifications between the authentication systems of multiple organizations?

Response:

- A. Federated
- B. Collaborative
- C. Integrated
- D. Bidirectional

Answer: A

NEW QUESTION 379

- (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 383

- (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 387

- (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 390

- (Exam Topic 3)

Tokenization requires two distinct _____.
Response:

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

Answer: B

NEW QUESTION 394

- (Exam Topic 3)

Which ISO/IEC standards set documents the cloud definitions for staffing and official roles? Response:

- A. ISO/IEC 27001
- B. ISO/IEC 17788
- C. ISO/IEC 17789
- D. ISO/IEC 27040

Answer: B

NEW QUESTION 397

- (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 399

- (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 404

- (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 408

- (Exam Topic 3)

In which of the following situations does the data owner have to administer the OS? Response:

- A. IaaS
- B. PaaS
- C. Offsite archive
- D. SaaS

Answer: A

NEW QUESTION 409

- (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 413

- (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 415

- (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 419

- (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 420

.....

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>