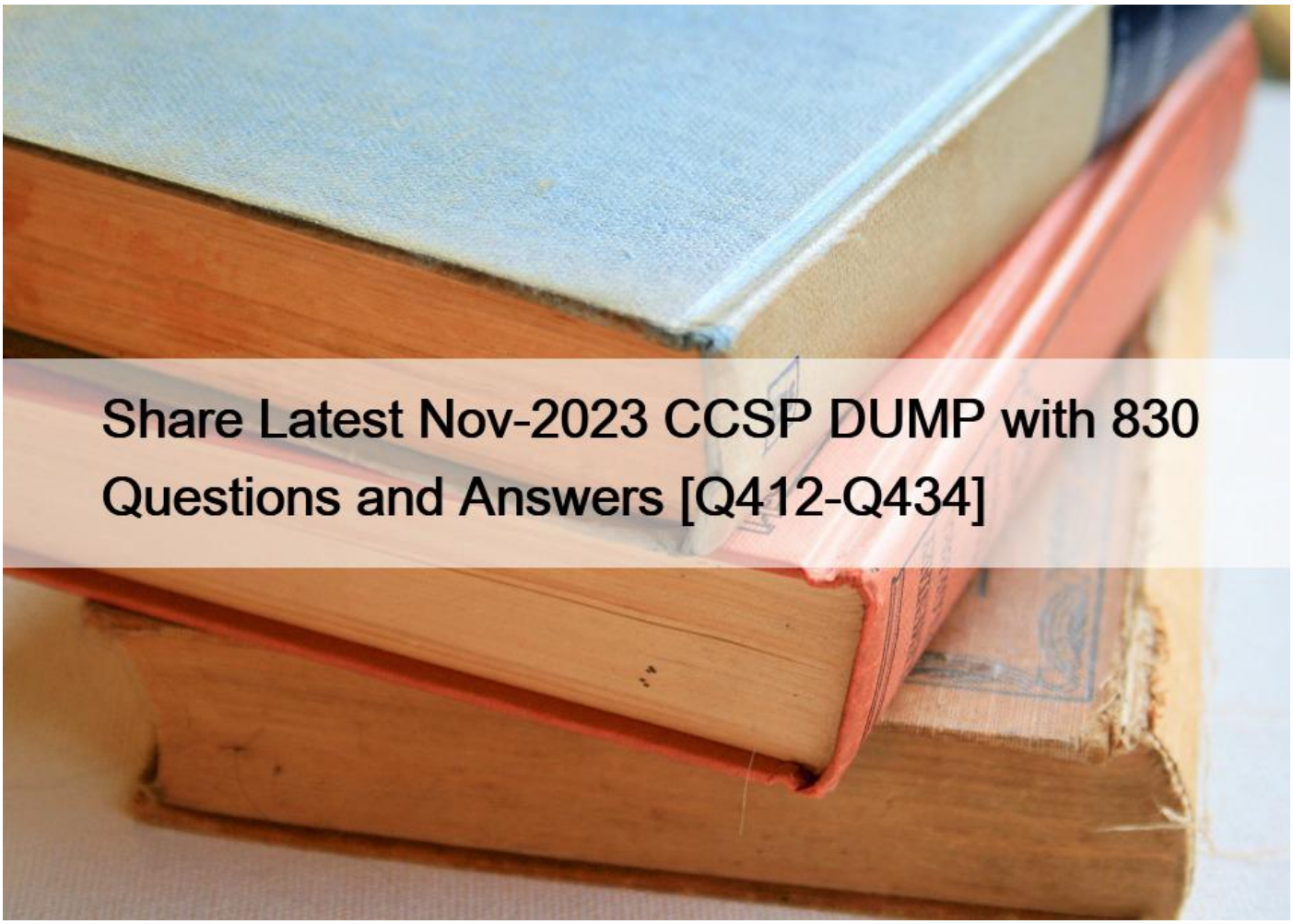
Share Latest Nov-2023 CCSP DUMP with 830 Questions and Answers [Q412-Q434



Share Latest Nov-2023 CCSP DUMP with 830 Questions and Answers
PDF Dumps 2023 Exam Questions with Practice Test

NEW QUESTION 412

All of the following are usually nonfunctional requirements except _____.

Response:
* Color
* Sound
* Security
* Function

NEW QUESTION 413

Which of the cloud cross-cutting aspects relates to the ability to easily move services and applications between different cloud providers?
* Reversibility
* Availability
* Portability
* Interoperability

Explanation

Portability is the ease with which a service or application can be moved between different cloud providers.

Maintaining portability gives an organization great flexibility between cloud providers and the ability to shop for better deals or offerings.

NEW QUESTION 414

Which of the following is the correct name for Tier II of the Uptime Institute Data Center Site Infrastructure Tier Standard Topology?

Response:
* Concurrently Maintainable Site Infrastructure
* Fault-Tolerant Site Infrastructure
* Basic Site Infrastructure
* Redundant Site Infrastructure Capacity Components

NEW QUESTION 415

The goals of SIEM solution implementation include all of the following, except:
* Dashboarding
* Performance enhancement
* Trend analysis
* Centralization of log streams

SIEM does not intend to provide any enhancement of performance; in fact, a SIEM solution may decrease performance because of additional overhead. All the rest are goals of SIEM implementations.

NEW QUESTION 416

At which phase of the SDLC process should security begin participating?

Response:
* Requirements gathering
* Requirements analysis
* Design
* Testing

NEW QUESTION 417

In the cloud motif, the data processor is usually:
* The party that assigns access rights
* The cloud customer
* The cloud provider

* The cloud access security broker

NEW QUESTION 418

What type of host is exposed to the public Internet for a specific reason and hardened to perform only that function for authorized users?
* Proxy
* Bastion
* Honeypot
* WAF
Explanation

A bastion host is a server that is fully exposed to the public Internet, but is extremely hardened to prevent attacks and is usually dedicated for a specific application or usage; it is not something that will serve multiple purposes. This singular focus allows for much more stringent security hardening and monitoring.

NEW QUESTION 419

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

Response:
* Token
* Key
* XML
* SAML

NEW QUESTION 420

Why does a Type 2 hypervisor typically offer less security control than a Type 1 hypervisor?
* A Type 2 hypervisor runs on top of another operating system and is dependent on the security of the OS for its own security.
* A Type 2 hypervisor allows users to directly perform some functions with their own access.
* A Type 2 hypervisor is open source, so attackers can more easily find exploitable vulnerabilities with that access.
* A Type 2 hypervisor is always exposed to the public Internet for federated identity access.
Explanation

A Type 2 hypervisor differs from a Type 1 hypervisor in that it runs on top of another operating system rather than directly tied into the underlying hardware of the virtual host servers. With this type of implementation, additional security and architecture concerns come into play because the interaction between the operating system and the hypervisor becomes a critical link. The hypervisor no longer has direct interaction and control over the underlying hardware, which means that some performance will be lost due to the operating system in the middle needing its own resources, patching requirements, and operational oversight.

NEW QUESTION 421

Which of the following threat types involves the sending of invalid and manipulated requests through a user’s client to execute commands on the application under their own credentials?
* Injection
* Cross-site request forgery
* Missing function-level access control
* Cross-site scripting
Explanation

A cross-site request forgery (CSRF) attack forces a client that a user has used to authenticate to an application to send forged requests under the user’s own credentials to execute commands and requests that the application thinks are coming from a trusted client and user. Although this type of attack cannot be used to steal data directly because the attacker has no way to see the results of the commands, it does open other ways to compromise an application. Missing function-level access control exists where an application only checks for authorization during the initial login process and does not further validate with each function call. An injection attack is where a malicious actor sends commands or other arbitrary data through input and data fields with the intent of having the application or system execute the code as part of its normal processing and queries.

Cross-site scripting occurs when an attacker is able to send untrusted data to a user’s browser without going through validation processes.

NEW QUESTION 422

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?
* Don’t use redirects/forwards in your applications.
* Refrain from storing credentials long term.
* Implement security incident/event monitoring (security information and event management (SIEM)/security information management (SIM)/security event management (SEM)) solutions.
* Implement digital rights management (DRM) solutions.

NEW QUESTION 423

Why does a Type 2 hypervisor typically offer less security control than a Type 1 hypervisor?
* A Type 2 hypervisor runs on top of another operating system and is dependent on the security of the OS for its own security.
* A Type 2 hypervisor allows users to directly perform some functions with their own access.
* A Type 2 hypervisor is open source, so attackers can more easily find exploitable vulnerabilities with that access.
* A Type 2 hypervisor is always exposed to the public Internet for federated identity access.

A Type 2 hypervisor differs from a Type 1 hypervisor in that it runs on top of another operating system rather than directly tied into the underlying hardware of the virtual host servers. With this type of implementation, additional security and architecture concerns come into play because the interaction between the operating system and the hypervisor becomes a critical link. The hypervisor no longer has direct interaction and control over the underlying hardware, which means that some performance will be lost due to the operating system in the middle needing its own resources, patching requirements, and operational oversight.

NEW QUESTION 424

When an API is being leveraged, it will encapsulate its data for transmission back to the requesting party or service.

What is the data encapsulation used with the SOAP protocol referred to as?
* Packet
* Payload
* Object
* Envelope

Explanation/Reference:

Explanation:

Simple Object Access Protocol (SOAP) encapsulates its information in what is known as a SOAP envelope. It then leverages common communications protocols for transmission. Object is a type of cloud storage, but also a commonly used term with certain types of programming languages. Packet and payload are terms that sound similar to envelope but are not correct in this case.

NEW QUESTION 425

Audits are either done based on the status of a system or application at a specific time or done as a study over a period of time that takes into account changes and processes.

Which of the following pairs matches an audit type that is done over time, along with the minimum span of time necessary for it?
* SOC Type 2, one year
* SOC Type 1, one year
* SOC Type 2, one month
* SOC Type 2, six months

SOC Type 2 audits are done over a period of time, with six months being the minimum duration.

SOC Type 1 audits are designed with a scope that’s a static point in time, and the other times provided for SOC Type 2 are incorrect.

NEW QUESTION 426

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:
* Scalability
* Multitenancy
* Metered service
* Flexibility

NEW QUESTION 427

With the rapid emergence of cloud computing, very few regulations were in place that pertained to it specifically, and organizations often had to resort to using a collection of regulations that were not specific to cloud in order to drive audits and policies.

Which standard from the ISO/IEC was designed specifically for cloud computing?
* ISO/IEC 27001
* ISO/IEC 19889
* ISO/IEC 27001:2015
* ISO/IEC 27018

Explanation/Reference:

Explanation:

ISO/IEC 27018 was implemented to address the protection of personal and sensitive information within a cloud environment. ISO/IEC 27001 and its later 27001:2015 revision are both general-purpose data security standards. ISO/IEC 19889 is an erroneous answer.

NEW QUESTION 428

You were recently hired as a project manager at a major university to implement cloud services for the academic and administrative systems. Because the load and demand for services at a university are very cyclical in nature, commensurate with the academic calendar, which of the following aspects of cloud computing would NOT be a primary benefit to you?
* Measured service
* Broad network access
* Resource pooling
* On-demand self-service

Broad network access to cloud services, although it is an integral aspect of cloud computing, would not being a specific benefit to an organization with cyclical business needs. The other options would allow for lower costs during periods of low usage as well as provide the ability to expand services quickly and easily when needed for peak periods. Measured service allows a cloud customer to only use the resources it needs at the time, and resource pooling allows a cloud customer to access resources as needed. On- demand self-service enables the cloud customer to change its provisioned resources on its own, without the need to interact with the staff from the cloud provider.

NEW QUESTION 429

What is a data custodian responsible for?
* The safe custody, transport, storage of the data, and implementation of business rules
* Data content, context, and associated business rules
* Logging and alerts for all data
* Customer access and alerts for all data

NEW QUESTION 430

Which standards body depends heavily on contributions and input from its open membership base?

Response:
* NIST
* ISO
* ICANN
* CSA

NEW QUESTION 431

With a federated identity system, what does the identity provider send information to after a successful authentication?
* Relying party
* Service originator
* Service relay
* Service relay

Explanation/Reference:

Explanation:

Upon successful authentication, the identity provider sends an assertion with appropriate attributes to the relying party to grant access and assign appropriate roles to the user. The other terms provided are similar sounding to the correct term but are not actual components of a federated system.

NEW QUESTION 432

Which of the following best describes SAML?
* A standard for developing secure application management logistics
* A standard for exchanging authentication and authorization data between security domains
* A standard for exchanging usernames and passwords across devices
* A standard used for directory synchronization

NEW QUESTION 433

SOC 2 reports were intended to be _____.

Response:
* Released to the public
* Only technical assessments
* Retained for internal use
* Nonbinding

NEW QUESTION 434

What type of storage structure does object storage employ to maintain files?
* Directory
* Hierarchical
* tree
* Flat

Object storage uses a flat file system to hold storage objects; it assigns files a key value that is then used to access them, rather than relying on directories or descriptive filenames. Typical storage layouts such as tree, directory, and hierarchical structures are used within volume storage, whereas object storage maintains a flat structure with key values.