CertsDeals

Free Questions for CAS-004 by certsdeals

Shared by Conway on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A software development company is building a new mobile application for its social media platform. The company wants to gain its users' trust by reducing the risk of on-path attacks between the mobile

client and its servers and by implementing stronger digital trust. To support users' trust, the company has released the following internal guidelines:

* Mobile clients should verify the identity of all social media servers locally.

* Social media servers should improve TLS performance of their certificate status

* Social media servers should inform the client to only use HTTPS.

Given the above requirements, which of the following should the company implement? (Select TWO).

Options:

A- Quick UDP internet connection

B- OCSP stapling

C- Private CA

D- DNSSEC

E- CRL

F- HSTS

G- Distributed object model

Answer:

B, F

Explanation:

The company should implement OCSP stapling and HSTS to improve TLS performance and enforce HTTPS. OCSP stapling is a technique that allows a server to provide a signed proof of the validity of its certificate along with the TLS handshake, instead of relying on the client to contact the certificate authority (CA) for verification. This can reduce the latency and bandwidth of the TLS handshake, as well as improve the privacy and security of the certificate status. HSTS stands for HTTP Strict Transport Security, which is a mechanism that instructs browsers to only use HTTPS when connecting to a website, and to reject any unencrypted or invalid connections. This can prevent downgrade attacks, man-in-the-middle attacks, and mixed content errors, as well as improve the performance of HTTPS connections by avoiding unnecessary redirects. Verified Reference:

https://www.techtarget.com/searchsecurity/definition/OCSP-stapling

https://www.techtarget.com/searchsecurity/definition/HTTP-Strict-Transport-Security

https://www.cloudflare.com/learning/ssl/what-is-hsts/

Question 2

Question Type: **MultipleChoice**

A systems administrator at a web-hosting provider has been tasked with renewing the public certificates of all customer sites. Which of the following would BEST support multiple domain names while minimizing the amount of certificates needed?

Options:

A- ocsp

B- CRL

C- SAN

D- CA

Answer:

C

Explanation:

The administrator should use SAN certificates to support multiple domain names while minimizing the amount of certificates needed. SAN stands for Subject Alternative Name, which is an extension of a certificate that allows it to include multiple fully-qualified domain names (FQDNs) within the same certificate. For example, a SAN certificate can secure www.example.com, www.example.net, and mail.example.org with one certificate. SAN certificates can reduce the cost and complexity of managing multiple certificates for different domains. SAN certificates can also support wildcard domains, such as *.example.com, which can cover any subdomain under that domain. Verified Reference:

https://www.techtarget.com/searchsecurity/definition/Subject-Alternative-Name

https://www.techtarget.com/searchsecurity/definition/wildcard-certificate

https://www.nexcess.net/help/what-is-a-multi-domain-ssl-certificate/

Question 3

Question Type: **MultipleChoice**

In comparison with traditional on-premises infrastructure configurations, defining ACLs in a CSP relies on:

Options:

A- cloud-native applications.

B- containerization.

C- serverless configurations.

D- software-defined netWorking.

E- secure access service edge.

Answer:

D

Explanation:

Defining ACLs in a CSP relies on software-defined networking. Software-defined networking (SDN) is a network architecture that decouples the control plane from the data plane, allowing for centralized and programmable network management. SDN can enable dynamic and flexible network configuration and optimization, as well as improved security and performance. In a CSP, SDN can be used to define ACLs that can apply to virtual networks, subnets, or interfaces, regardless of the physical infrastructure. SDN can also allow for granular and consistent ACL enforcement across different cloud services and regions. Verified Reference:

https://www.techtarget.com/searchsdn/definition/software-defined-networking-SDN

https://learn.microsoft.com/en-us/azure/architecture/guide/networking/network-security

https://www.techtarget.com/searchcloudcomputing/definition/cloud-networking

Question 4

Question Type: **MultipleChoice**

An organization is in frequent litigation and has a large number of legal holds. Which of the following types of functionality should the organization's new email system provide?

Options:

A- DLP

B- Encryption

C- E-discovery

D- Privacy-level agreements

Answer:

C

Explanation:

The organization's new email system should provide e-discovery functionality. E-discovery stands for electronic discovery, which is the process of identifying, preserving, collecting, processing, reviewing, analyzing, and producing electronically stored information (ESI) that is relevant to a legal matter. E-discovery can help the organization comply with legal holds, which are orders or notices to preserve relevant ESI when litigation is anticipated or ongoing. E-discovery can also help the organization reduce the costs and risks of litigation, as well as improve the efficiency and accuracy of the discovery process. Verified Reference:

https://www.techtarget.com/searchsecurity/definition/electronic-discovery

https://www.techtarget.com/searchsecurity/definition/legal-hold

https://www.ibm.com/topics/electronic-discovery

Question 5

Question Type: MultipleChoice

A third-party organization has implemented a system that allows it to analyze customers' data and deliver analysis results without being able to see the raw dat

a. Which of the following is the organization implementing?

Options:

A- Asynchronous keys

B- Homomorphic encryption

C- Data lake

D- Machine learning

Answer:

B

Explanation:

The organization is implementing homomorphic encryption. Homomorphic encryption is a type of encryption that allows computations to be performed on encrypted data without decrypting it first. This means that the organization can analyze the customers' data and deliver analysis results without being able to see the raw data, preserving the privacy and confidentiality of the customers. Homomorphic encryption can enable various applications, such as cloud computing, machine learning, and data analytics, that require processing sensitive data without compromising security. Verified Reference:

https://www.techtarget.com/searchsecurity/definition/homomorphic-encryption

https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-at-rest

https://www.ibm.com/topics/homomorphic-encryption

Question 6

Question Type: **MultipleChoice**

Which of the following should be established when configuring a mobile device to protect user internet privacy, to ensure the connection is encrypted, and to keep user activity hidden? (Select TWO).

Options:

A- proxy

B- Tunneling

C- VDI

D- MDM

E- RDP

F- MAC address randomization

Answer:

A, F

Explanation:

The methods that can be used to protect user internet privacy, to ensure the connection is encrypted, and to keep user activity hidden are proxy and MAC address randomization. A proxy is a server that acts as an intermediary between a user and the internet, hiding the user's IP address and location from websites and other online services. A proxy can also encrypt the connection between the user and the proxy server, preventing anyone from snooping on the user's traffic. MAC address randomization is a feature that changes the MAC address of a mobile device periodically or when connecting to different networks. A MAC address is a unique identifier of a network interface that can be used to track the device's location and activity. MAC address randomization can help protect the user's privacy by making it harder for third parties to link the device to a specific user or network. Verified Reference:

https://www.techtarget.com/searchsecurity/definition/proxy-server

https://www.techtarget.com/searchnetworking/definition/MAC-address-randomization

https://www.techtarget.com/searchsecurity/definition/MAC-address-Media-Access-Control-address

Question 7

Question Type: MultipleChoice

A security analyst has been tasked with providing key information in the risk register. Which of the following outputs or results would be used to BEST provide the information needed to determine the security posture for a risk decision? (Select TWO).

Options:

A- Password cracker

B- SCAP scanner

C- Network traffic analyzer

D- Vulnerability scanner

E- Port scanner

F- Protocol analyzer

Answer:

B, D

Explanation:

The tools that can be used to provide key information in the risk register are SCAP scanner and vulnerability scanner. SCAP stands for Security Content Automation Protocol, which is a set of standards and specifications for automating the management of security configuration, vulnerability assessment, and compliance evaluation. SCAP scanner is a tool that can scan systems and networks for security issues based on SCAP content. Vulnerability scanner is a tool that can scan systems and networks for known vulnerabilities and weaknesses. These tools can help the security analyst identify and prioritize the risks associated with the systems and networks, as well as provide possible remediation actions. Verified Reference:

https://www.techtarget.com/searchsecurity/definition/Security-Content-Automation-Protocol

https://learn.microsoft.com/en-us/azure/security/fundamentals/vulnerability-management

https://www.techtarget.com/searchsecurity/definition/vulnerability-scanner

Question 8

Question Type: MultipleChoice

Which of the following processes involves searching and collecting evidence during an investigation or lawsuit?

Options:

A- E-discovery

B- Review analysis

C- Information governance

D- Chain of custody

Answer:

A

Explanation:

The process that involves searching and collecting evidence during an investigation or lawsuit is e-discovery. E-discovery stands for electronic discovery, which is the process of identifying, preserving, collecting, processing, reviewing, analyzing, and producing electronically stored information (ESI) that is relevant to a legal matter. E-discovery can be used for civil litigation, criminal prosecution, regulatory compliance, internal investigations, and other purposes. E-discovery can help parties obtain evidence from various sources, such as emails, documents, databases, social media, cloud services, mobile devices, and others. Verified Reference:

https://www.techtarget.com/searchsecurity/definition/electronic-discovery

https://www.edrm.net/frameworks-and-standards/edrm-model/

https://www.law.cornell.edu/wex/electronic_discovery_(federal)