



Question #:1

Which of the following would BEST identify and remediate a data-loss event in an enterprise using third-party, web-based services and file-sharing platforms?

- A. SIEM
- B. CASB
- C. UTM
- D. DLP

Answer: D

Question #:2

A network engineer needs to create a plan for upgrading the wireless infrastructure in a large office. Priority must be given to areas that are currently experiencing latency and connection issues. Which of the following would be the BEST resource for determining the order of priority?

- A. Nmap
- B. Heat maps
- C. Network diagrams
- D. Wireshark

Answer: B

Explanation

engineer needs to create a plan for upgrading the wireless infrastructure in a large office. Priority must be given to areas that are currently.

Site surveys and heat maps provide the following benefits: Identify trouble areas to help eliminate slow speeds and poor performance

Question #:3

Leveraging the information supplied below, complete the CSR for the server to set up TLS (HTTPS)

- Hostname: ws01
- Domain: comptia.org
- IPv4: 10.1.9.50

- IPV4: 10.2.10.50
- Root: home.aspx
- DNS CNAME:homesite.

Instructions:

Drag the various data points to the correct locations within the CSR. Extension criteria belong in the left hand column and values belong in the corresponding row in the right hand column.

Server

```

Hostname: ws01
Domain: comptia.org
IPv4: 10.1.9.50
IPv4: 10.2.10.50
Root: home.aspx
DNS CNAME: homesite
          
```

Certificate Signing Request

Extension	Value
?	?
?	?
?	?
?	?

Extensions

pki/identity

ocspNonCritical

subAltNames

extendedKeyUsage

Values

serverAuth

OCSP,URI=http://ocsp.pki.comptia.org

URL=http://homesite.comptia.org/home.aspx

ws01.comptia.org

DNS Name=*.comptia.org

identAuth

DNS Name=homesite.comptia.org

Answer:

Server Hostname: ws01
Domain: comptia.org
IPv4: 10.1.9.50
IPv4: 10.1.10.50
Root: home.aspx
DNS NAME: homesite

Certificate Signing Request

Extension	Value
commonName	ws01.comptia.org
extendedKeyUsage	OCSP_URI:http://ocsp.pki.comptia.org
policyIdentifier	URL=http://homesite.comptia.org/home.aspx
subjectName	DNS Name = *.comptia.org

serverAuth
OCSP_URI:http://ocsp.pki.comptia.org
URL=http://homesite.comptia.org/home.aspx
ws01.comptia.org
DNS Name = *.comptia.org
clientAuth
DNS Name=homesite.comptia.org



Explanation

Graphical user interface, application Description automatically generated

Certificate Signing Request

Extension	Value
commonName	ws01.comptia.org
extendedKeyUsage	OCSP_URI:http://ocsp.pki.comptia.org
policyIdentifier	URL=http://homesite.comptia.org/home.aspx
subjectName	DNS Name = *.comptia.org

Question #:4

A network engineer needs to build a solution that will allow guests at the company's headquarters to access the Internet via WiFi. This solution should not allow access to the internal corporate network, but it should require guests to sign off on the acceptable use policy before accessing the Internet. Which of the following should the engineer employ to meet these requirements?

- A. Implement open PSK on the APs
- B. Deploy a WAF
- C. Configure WIPS on the APs
- D. Install a captive portal

Answer: D

Question #:5

Which of the following scenarios BEST describes a risk reduction technique?

- A. A security control objective cannot be met through a technical change, so the company purchases insurance and is no longer concerned about losses from data breaches.
- B. A security control objective cannot be met through a technical change, so the company implements a policy to train users on a more secure method of operation.
- C. A security control objective cannot be met through a technical change, so the company changes as method of operation
- D. A security control objective cannot be met through a technical change, so the Chief Information Officer (CIO) decides to sign off on the risk.

Answer: B

Question #:6

Which of the following would be BEST for a technician to review to determine the total risk an organization can bear when assessing a "cloud-first" adoption strategy?

- A. Risk matrix
- B. Risk tolerance
- C. Risk register
- D. Risk appetite

Answer: B

Question #:7

A security analyst has received an alert about being sent via email. The analyst's Chief information Security Officer (CISO) has made it clear that PII must be handle with extreme care From which of the following did

the alert MOST likely originate?

- A. S/MIME
- B. DLP
- C. IMAP
- D. HIDS

Answer: B

Explanation

Network-based DLP monitors outgoing data looking for sensitive data. Network-based DLP systems monitor outgoing email to detect and block unauthorized data transfers and monitor data stored in the cloud.

Question #:8

A security engineer obtained the following output from a threat intelligence source that recently performed an attack on the company's server:

Which of the following BEST describes this kind of attack?

- A. Directory traversal
- B. SQL injection
- C. API
- D. Request forgery

Answer: D

Question #:9

Which of the following cryptographic concepts would a security engineer utilize while implementing non-repudiation? (Select TWO)

- A. Block cipher
- B. Hashing
- C. Private key

- D. Perfect forward secrecy
- E. Salting
- F. Symmetric keys

Answer: B C

Question #:10

A network technician is installing a guest wireless network at a coffee shop. When a customer purchases an item, the password for the wireless network is printed on the receipt so the customer can log in. Which of the following will the technician MOST likely configure to provide the highest level of security with the least amount of overhead?

- A. WPA-EAP
- B. WEP-TKIP
- C. WPA-PSK
- D. WPS-PIN

Answer: A

