Free Questions for CAS-004 by certsinside

Shared by Williamson on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A healthcare system recently suffered from a ransomware incident As a result the board of directors decided to hire a security consultant to improve existing network security. The security consultant found that the healthcare network was completely flat, had no privileged access limits and had open RDP access to servers with personal health information. As the consultant builds the remediation plan, which of the following solutions would BEST solve these challenges? (Select THREE).

Options:

A- SD-WAN

B- PAM

C- Remote access VPN

D- MFA

E- Network segmentation

F- BGP

G- NAC

Answer:

A, C, E

Question 2

Question Type: MultipleChoice

An organization mat provides a SaaS solution recently experienced an incident involving customer data loss. The system has a level of sell-healing that includes monitoring performance and available resources. When me system detects an issue, the self-healing process is supposed to restart pans of me software.

During the incident, when me self-healing system attempted to restart the services, available disk space on the data drive to restart all the services was inadequate. The self-healing system did not detect that some services did not fully restart and declared me system as fully operational. Which of the following BEST describes me reason why the silent failure occurred?

Options:

A- The system logs rotated prematurely.

B- The disk utilization alarms are higher than what me service restarts require.

C- The number of nodes in me self-healing cluster was healthy,

D- Conditional checks prior to the service restart succeeded.

Answer:

D

Question 3

Question Type: MultipleChoice

The Chief Information Security Officer of a startup company has asked a security engineer to implement a software security program in an environment that previously had little oversight.

Which of the following testing methods would be BEST for the engineer to utilize in this situation?

Options:

A- Software composition analysis

B- Code obfuscation

C- Static analysis

D- Dynamic analysis

Answer:

C

Question 4

Question Type: MultipleChoice

A large number of emails have been reported, and a security analyst is reviewing the following information from the emails:

As part of the image process, which of the following is the FIRST step the analyst should take?

Options:

A- Block the email address carl b@comptia1 com, as it is sending spam to subject matter experts

B- Validate the final 'Received' header against the DNS entry of the domain.

C- Compare the 'Return-Path' and 'Received' fields.

D- Ignore the emails, as SPF validation is successful, and it is a false positive

Answer:

C

Question 5

Question Type: MultipleChoice

Company A acquired Company . During an audit, a security engineer found Company B's environment was inadequately patched. In response, Company A placed a firewall between the two environments until Company B's infrastructure could be integrated into Company A's security program.

Which of the following risk-handling techniques was used?

Options:

A- Accept

B- Avoid

C- Transfer

D- Mitigate

Answer:

D

Question 6

Question Type: MultipleChoice

An organization is prioritizing efforts to remediate or mitigate risks identified during the latest assessment. For one of the risks, a full remediation was not possible, but the organization was able to successfully apply mitigations to reduce the likelihood of impact.

Which of the following should the organization perform NEXT?

Options:

A- Assess the residual risk.

B- Update the organization's threat model.

C- Move to the next risk in the register.

D- Recalculate the magnitude of impact.

Answer:

D

Question 7

Question Type: MultipleChoice

A software house is developing a new application. The application has the following requirements:

Reduce the number of credential requests as much as possible

Integrate with social networks

Authenticate users

Which of the following is the BEST federation method to use for the application?

Options:

A- WS-Federation

B- OpenID

C- OAuth

D- SAML

Answer:

D

Question 8

Question Type: MultipleChoice

A company is looking for a solution to hide data stored in databases. The solution must meet the following requirements:

Be efficient at protecting the production environment

Not require any change to the application

Act at the presentation layer

Which of the following techniques should be used?

Options:

A- Masking

B- Tokenization

C- Algorithmic

D- Random substitution

Answer:

A

Question 9

Question Type: MultipleChoice

A forensic expert working on a fraud investigation for a US-based company collected a few disk images as evidence.

Which of the following offers an authoritative decision about whether the evidence was obtained legally?

Options:

A- Lawyers

B- Court

C- Upper management team

D- Police

Answer:

A

Question 10

Question Type: MultipleChoice

Technicians have determined that the current server hardware is outdated, so they have decided to throw it out.

Prior to disposal, which of the following is the BEST method to use to ensure no data remnants can be recovered?

Options:

A- Drive wiping

B- Degaussing

C- Purging

D- Physical destruction

Answer:

B

Question 11

Question Type: MultipleChoice

A Chief information Security Officer (CISO) has launched to create a rebuts BCP/DR plan for the entire company. As part of the initiative , the security team must gather data supporting s operational importance for the applications used by the business and determine the order in which the application must be back online. Which of the following be the FIRST step taken by the team?

Options:

A- Perform a review of all policies an procedures related to BGP a and DR and created an educated educational module that can be assigned to at employees to provide training on BCP/DR events.

B- Create an SLA for each application that states when the application will come back online and distribute this information to the business units.

C- Have each business unit conduct a BIA and categories the application according to the cumulative data gathered.

D- Implement replication of all servers and application data to back up detacenters that are geographically from the central datacenter and release an upload BPA to all clients.

Answer:

C

Question 12

Question Type: MultipleChoice

An engineering team is developing and deploying a fleet of mobile devices to be used for specialized inventory management purposes. These devices should:

* Be based on open-source Android for user familiarity and ease.

* Provide a single application for inventory management of physical assets.

* Permit use of the camera be only the inventory application for the purposes of scanning

* Disallow any and all configuration baseline modifications.

* Restrict all access to any device resource other than those requirement ?

Options:

A- Set an application wrapping policy, wrap the application, distributes the inventory APK via the MAM tool, and test the application restrictions.

B- Write a MAC sepolicy that defines domains with rules, label the inventory application, build the policy, and set to enforcing mode.

C- Swap out Android Linux kernel version for >2,4,0, but the internet build Android, remove unnecessary functions via MDL, configure to block network access, and perform integration testing

D- Build and install an Android middleware policy with requirements added, copy the file into/ user/init, and then built the inventory application.

Answer:

A