Free Questions for CAS-004 by go4braindumps

Shared by Daugherty on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A web service provider has just taken on a very large contract that comes with requirements that are currently not being implemented in order to meet contractual requirements, the company must achieve the following thresholds

* 99 99% uptime

* Load time in 3 seconds

* Response time =

Starting with the computing environment, which of the following should a security engineer recommend to BEST meet the requirements? (Select THREE)

Options:

A- Installing a firewall at corporate headquarters

B- Deploying a content delivery network

C- Implementing server clusters

D- Employing bare-metal loading of applications

E- Lowering storage input/output

F- Implementing RAID on the backup servers

G- Utilizing redundant power for all developer workstations

H- Ensuring technological diversity on critical servers

Answer:

B, C, E

Explanation:

To meet the contractual requirements of the web service provider, a security engineer should recommend the following actions:

Deploying a content delivery network (CDN): A CDN is a distributed system of servers that delivers web content to users based on their geographic location, the origin of the content, and the performance of the network. A CDN can help improve the uptime, load time, and response time of web services by caching content closer to the users, reducing latency and bandwidth consumption.A CDN can also help mitigate distributed denial-of-service (DDoS) attacks by absorbing or filtering malicious traffic before it reaches the origin servers, reducing the impact on the web service availability12.

Implementing server clusters: A server cluster is a group of servers that work together to provide high availability, scalability, and load balancing for web services. A server cluster can help improve the uptime, load time, and response time of web services by distributing the workload across multiple servers, reducing the risk of single points of failure and performance bottlenecks.A server cluster can also help recover from failures by automatically switching to another server in case of a malfunction34.

Lowering storage input/output (I/O): Storage I/O is the amount of data that can be read from or written to a storage device in a given time. Storage I/O can affect the performance of web services by limiting the speed of data transfer between the servers and the storage devices. Lowering storage I/O can help improve the load time and response time of web services by reducing the latency and congestion of data access.Lowering storage I/O can be achieved by using faster storage devices, such as solid-state drives (SSDs), optimizing the storage layout and configuration, such as using RAID or striping, and caching frequently accessed data in memory5.

Installing a firewall at corporate headquarters is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. A firewall is a device or software that filters and blocks unwanted network traffic based on predefined rules. A firewall can help improve the security of web services by preventing unauthorized access and attacks, but it may also introduce additional latency and complexity to the network.

Employing bare-metal loading of applications is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. Bare-metal loading is a technique that allows applications to run directly on hardware without an operating system or a hypervisor. Bare-metal loading can help improve the performance and efficiency of applications by eliminating the overhead and interference of other software layers, but it may also increase the difficulty and cost of deployment and maintenance.

Implementing RAID on the backup servers is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. RAID (redundant array of independent disks) is a technique that combines multiple disks into a logical unit that provides improved performance, reliability, or both. RAID can help improve the availability and security of backup data by protecting it from disk failures or corruption, but it may also introduce additional complexity and overhead to the backup process.

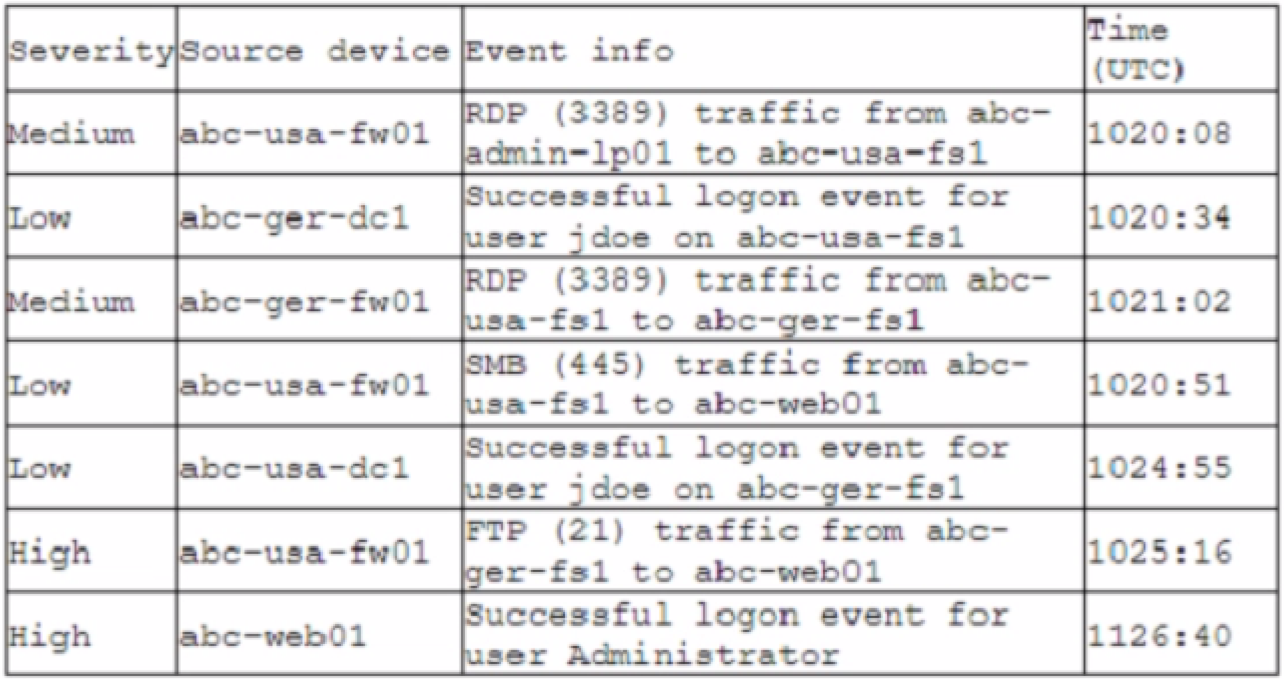
Utilizing redundant power for all developer workstations is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. Redundant power is a technique that provides multiple sources of power for an IT system in case one fails. Redundant power can help improve the availability and reliability of developer workstations by preventing them from losing power due to outages or surges, but it may also increase the cost and energy consumption of the system.

Ensuring technological diversity on critical servers is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. Technological diversity is a technique that uses different types of hardware, software, or platforms in an IT environment. Technological diversity can help improve resilience by reducing single points of failure and increasing compatibility, but it may also introduce additional complexity and inconsistency to the environment.Reference:What Is CDN? How Does CDN Work? | Imperva,What Is Server Clustering? | IBM,What Is Server Clustering? | IBM,Server Clustering: What It Is & How It Works | Liquid Web,Storage I/O Performance - an overview | ScienceDirect Topics, [How to Improve Storage I/O Performance | StarWind Blog], [What Is Firewall Security? | Cisco], [What is Bare Metal? | IBM], [What is RAID? | Dell Technologies US], [What Is Redundant Power Supply? | Dell Technologies US], [Technological Diversity - an overview | ScienceDirect Topics]

Question 2

Question Type: MultipleChoice

A company recently deployed a SIEM and began importing logs from a firewall, a file server, a domain controller a web server, and a laptop. A security analyst receives a series of SIEM alerts and prepares to respond. The following is the alert information:



Severity	Source device	Event info	Time (UTC)
Medium	abc-usa-fw01	RDP (3389) traffic from abc-admin-lp01 to abc-usa-fs1	1020:08
Low	abc-ger-dc1	Successful logon event for user jdoe on abc-usa-fs1	1020:34
Medium	abc-ger-fw01	RDP (3389) traffic from abc-usa-fs1 to abc-ger-fs1	1021:02
Low	abc-usa-fw01	SMB (445) traffic from abc-usa-fs1 to abc-web01	1020:51
Low	abc-usa-dc1	Successful logon event for user jdoe on abc-ger-fs1	1024:55
High	abc-usa-fw01	FTP (21) traffic from abc-ger-fs1 to abc-web01	1025:16
High	abc-web01	Successful logon event for user Administrator	1126:40

Which of the following should the security analyst do FIRST?

Options:

A- Disable Administrator on abc-uaa-fsl, the local account is compromised

B- Shut down the abc-usa-fsl server, a plaintext credential is being used

C- Disable the jdoe account, it is likely compromised

D- Shut down abc-usa-fw01; the remote access VPN vulnerability is exploited

Answer:

C

Explanation:

Based on the SIEM alerts, the security analyst should first disable the jdoe account, as it is likely compromised by an attacker. The alerts show that the jdoe account successfully logged on to the abc-usa-fsl server, which is a file server, and then initiated SMB (445) traffic to the abc-web01 server, which is a web server. This indicates that the attacker may be trying to exfiltrate data from the file server to the web server. Disabling the jdoe account would help stop this unauthorized activity and prevent further damage.

Disabling Administrator on abc-usa-fsl, the local account is compromised, is not the first action to take, as it is not clear from the alerts if the local account is compromised or not. The alert shows that there was a successful logon event for Administrator on abc-usa-fsl, but it does not specify if it was a local or domain account, or if it was authorized or not. Moreover, disabling the local account would not stop the SMB traffic from jdoe to abc-web01.

Shutting down the abc-usa-fsl server, a plaintext credential is being used, is not the first action to take, as it is not clear from the alerts if a plaintext credential is being used or not. The alert shows that there was RDP (3389) traffic from abc-admin1-logon to abc-usa-fsl, but it does not specify if the credential was encrypted or not. Moreover, shutting down the file server would disrupt its normal operations and affect other users.

Shutting down abc-usa-fw01; the remote access VPN vulnerability is exploited, is not the first action to take, as it is not clear from the alerts if the remote access VPN vulnerability is exploited or not. The alert shows that there was FTP (21) traffic from abc-usa-dcl to abc-web01, but it does not specify if it was related to the VPN or not. Moreover, shutting down the firewall would expose the network to other threats and affect other services.Reference:What is SIEM? | Microsoft Security, What is a SIEM Alert? | Cofense

Question 3

Question Type: MultipleChoice

A managed security provider (MSP) is engaging with a customer who was working through a complete digital transformation Part of this transformation involves a move to cloud servers to ensure a scalable, high-performance, online user experience The current architecture includes:

* Directory servers

* Web servers

* Database servers

* Load balancers

* Cloud-native VPN concentrator

* Remote access server

The MSP must secure this environment similarly to the infrastructure on premises Which of the following should the MSP put in place to BEST meet this objective? (Select THREE)

Options:

A- Content delivery network

B- Virtual next-generation firewall

C- Web application firewall

D- Software-defined WAN

E- External vulnerability scans

F- Containers

G- Microsegmentation

Answer:

B, C, G

Explanation:

A virtual next-generation firewall (vNGFW) is a software version of a NGFW that can be deployed on cloud servers to provide advanced network security features. A vNGFW can help secure the cloud environment similarly to the infrastructure on premises by providing functions such as URL filtering, SSL/TLS inspection, deep packet inspection, antivirus, IPS, application control, and sandboxing. A web application firewall (WAF) is a device or software that filters and blocks malicious web traffic from reaching an application. A WAF can help secure the web servers in the cloud environment by protecting them from common attacks such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). Microsegmentation is a technique that divides a network into smaller segments or zones based on criteria such as identity, role, or function. Microsegmentation can help secure the cloud environment by isolating different types of servers and applying granular security policies to each segment.

A content delivery network (CDN) is a distributed system of servers that delivers web content to users based on their geographic location, the origin of the content, and the performance of the network. A CDN can help improve the availability and performance of web applications by caching content closer to the users, reducing latency and bandwidth consumption. However, a CDN does not provide the same level of security as a vNGFW or a WAF. Software-defined WAN (SD-WAN) is a technology that uses software to manage the connectivity and routing of wide area network (WAN) traffic across multiple links or carriers. SD-WAN can help improve the reliability and efficiency of WAN connections by dynamically selecting the best path for each application based on factors such as bandwidth, latency, cost, and quality of service (QoS). However, SD-WAN does not provide the same level of security as a vNGFW or a WAF. External vulnerability scans are assessments that identify and report on the vulnerabilities and weaknesses of an IT system from an external perspective. External vulnerability scans can help improve the security posture of an IT system by providing visibility into its exposure to potential threats. However, external vulnerability scans do not provide the same level of protection as a vNGFW or a WAF. Containers are units of software that package an application and its dependencies into a standardized format that can run on any platform or environment. Containers can help improve the portability and scalability of applications by allowing them to run independently from the underlying infrastructure. However, containers do not provide the same level of security as microsegmentation.Reference: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.3: Implement solutions for the secure use of cloud services

Question 4

Question Type: MultipleChoice

A bank hired a security architect to improve its security measures against the latest threats The solution must meet the following requirements

* Recognize and block fake websites

* Decrypt and scan encrypted traffic on standard and non-standard ports

* Use multiple engines for detection and prevention

* Have central reporting

Which of the following is the BEST solution the security architect can propose?

Options:

A- CASB

B- Web filtering

C- NGFW

D- EDR

Answer:

C

Explanation:

A next-generation firewall (NGFW) is a device or software that provides advanced network security features beyond the traditional firewall functions. A NGFW can provide the following capabilities:

Recognize and block fake websites, using URL filtering and reputation-based analysis

Decrypt and scan encrypted traffic on standard and non-standard ports, using SSL/TLS inspection and deep packet inspection

Use multiple engines for detection and prevention, such as antivirus, intrusion prevention system (IPS), application control, and sandboxing

Have central reporting, using a unified management console and dashboard A cloud access security broker (CASB) is a device or software that acts as an intermediary between cloud service users and cloud service providers. A CASB can provide various security functions such as visibility, compliance, data security, and threat protection, but it does not provide all the capabilities of a NGFW. Web filtering is a technique that blocks or allows web access based on predefined criteria such as categories, keywords, or reputation. Web filtering can help recognize and block fake websites, but it does not provide all the capabilities of a NGFW. Endpoint detection and response (EDR) is a technology that monitors and analyzes the activity and behavior of endpoints such as computers or mobile devices. EDR can help detect and respond to advanced threats, but it does not provide all the capabilities of a NGFW.Reference: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.2: Select appropriate hardware and software solutions

Question 5

Question Type: MultipleChoice

A company wants to improve the security of its web applications that are running on in-house servers A risk assessment has been performed and the following capabilities are desired:

* Terminate SSL connections at a central location

* Manage both authentication and authorization for incoming and outgoing web service calls

* Advertise the web service API

* Implement DLP and anti-malware features

Which of the following technologies will be the BEST option?

Options:

A- WAF

B- XML gateway

C- ESB gateway

D- API gateway

Answer:

D

Explanation:

An API gateway is a device or software that acts as an intermediary between clients and servers that provide web services through application programming interfaces (APIs). An API gateway can provide various functions such as:

Terminating SSL connections at a central location, reducing the overhead on the backend servers and simplifying certificate management

Managing both authentication and authorization for incoming and outgoing web service calls, enforcing security policies and access control

Advertising the web service API, providing documentation and discovery features for developers and consumers

Implementing DLP and anti-malware features, preventing data leakage and malicious code injection A web application firewall (WAF) is a device or software that filters and blocks malicious web traffic from reaching an application. A WAF can provide some protection for web services, but it does not provide all the functions of an API gateway. An XML gateway is a device or software that validates, transforms, and routes XML messages between clients and servers that provide web services. An XML gateway can provide some functions of an API gateway, but it is limited to XML-based web services and does not support other formats such as JSON. An enterprise service bus (ESB) gateway is a device or software that integrates and orchestrates multiple web services into a single service or application. An ESB gateway can provide some functions of an API gateway, but it is more focused on business logic and workflow rather than security and performance.Reference: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.3: Implement solutions for the secure use of cloud services

Question 6

Question Type: MultipleChoice

A major broadcasting company that requires continuous availability to streaming content needs to be resilient against DDoS attacks Which of the following is the MOST important infrastructure security design element to prevent an outage7

Options:

A- Supporting heterogeneous architecture

B- Leveraging content delivery network across multiple regions

C- Ensuring cloud autoscaling is in place

D- Scaling horizontally to handle increases in traffic

Answer:

B

Explanation:

A content delivery network (CDN) is a distributed system of servers that delivers web content to users based on their geographic location, the origin of the content, and the performance of the network. A CDN can help improve the availability and performance of web applications by caching content closer to the users, reducing latency and bandwidth consumption. A CDN can also help mitigate distributed denial-of-service (DDoS) attacks by absorbing or filtering malicious traffic before it reaches the origin servers, reducing the impact on the application availability. Supporting heterogeneous architecture means using different types of hardware, software, or platforms in an IT environment. This can help improve resilience by reducing single points of failure and increasing compatibility, but it does not directly prevent DDoS attacks. Ensuring cloud autoscaling is in place means using cloud services that automatically adjust the amount of resources allocated to an application based on the demand or load. This can help improve scalability and performance by providing more resources when needed, but it does not directly prevent DDoS attacks. Scaling horizontally means adding more servers or nodes to an IT environment to increase its capacity or throughput. This can help improve scalability and performance by distributing the load across multiple servers, but it does not directly prevent DDoS attacks.Reference: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.4: Select controls based on systems security evaluation models

Question 7

Question Type: MultipleChoice

A security architect Is analyzing an old application that is not covered for maintenance anymore because the software company is no longer in business. Which of the following techniques should have been Implemented to prevent these types of risks?

Options:

A- Code reviews

B- Supply chain visibility

C- Software audits

D- Source code escrows

Answer:

D

Explanation:

A source code escrow is a legal agreement that involves a third party holding the source code of a software application on behalf of the software vendor and the software licensee. The source code escrow ensures that the licensee can access the source code in case the vendor goes out of business, fails to provide maintenance or support, or breaches the contract terms.

A source code escrow would have prevented the risk of having an old application that is not covered for maintenance anymore because the software company is no longer in business, because it would:

Allow the licensee to obtain the source code and continue to update, fix, or modify the application according to their needs.

Protect the vendor's intellectual property rights and prevent unauthorized disclosure or use of the source code.

Provide a legal framework and a trusted mediator for resolving any disputes or issues between the vendor and the licensee.