[December-2020CAS-003 CAS-003 726Q Exam Questions and CAS-003 Exam Dumps PDF Free Downloading - Braindump2go[Q606-Q626

December/2020 Latest Braindump2go CAS-003 Exam Dumps with PDF and VCE Free Updated Today! Following are some new CAS-003 Real Exam Questions!QUESTION 606A remote user reports the inability to authenticate to the VPN concentrator.During troubleshooting, a security administrate captures an attempted authentication and discovers the following being presented by the user's VPN client:

Which of the following BEST describes the reason the user is unable to connect to the VPN service?A. The user's certificate is not signed by the VPN service providerB. The user's certificate has been compromised and should be revoked.C. The user's certificate was not created for VPN useD. The user's certificate was created using insecure encryption algorithmsAnswer: BQUESTION 607A DevOps team wants to move production data into the QA environment for testing. This data contains credit card numbers and expiration dates that are not tied to any individuals.The security analyst wants to reduce risk.Which of the following will lower the risk before moving the data?A. Redacting all but the last four numbers of the cardsB. Hashing the card numbersC. Scrambling card and expiration dataD. Encrypting card and expiration numbersAnswer: BQUESTION 608Following the most recent patch deployment, a security engineer receives reports that the ERP application is no longer accessible. The security engineer reviews the situation and determines a critical security patch that was applied to the ERP server is the cause. The patch is subsequently backed out.Which of the following security controls would be BEST to implement to mitigate the threat caused by the missing patch?A. Anti-malwareB. Patch testingC. HIPSD. Vulnerability scannerAnswer: BQUESTION 609A Chief Information Security Officer (CISO) is running a test to evaluate the security of the corporate network and attached devices.Which of the following components should be executed by an outside vendor?A. Penetration testsB. Vulnerability assessmentC. Tabletop exercisesD. Blue-team operationsAnswer: AQUESTION 610A security manager is determining the best DLP solution for an enterprise.A list of requirements was created to use during the source selection.The security manager wants to confirm a solution exists for the requirements that have been defined.Which of the following should the security manager use?A. NDAB. RFPC. RFQD. MSAE. RFIAnswer: EQUESTION 611Designing a system in which only information that is essential for a particular job task is allowed to be viewed can be accomplished successfully by using:A. mandatory vacations.B. job rotationsC. role-based access controlD. discretionary accessE. separation of dutiesAnswer: CQUESTION 612The information security manager of an e-commerce company receives an alert over the weekend that all the servers in a datacenter have gone offline.Upon discussing this situation with the facilities manager, the information security manager learns there was planned electrical maintenance.The information security manager is upset at not being part of the maintenance planning, as this could have resulted in a loss of:A. data confidentiality.B. data security.C. PCI complianceD. business availability.Answer: DQUESTION 613A company contracts a security consultant to perform a remote white-box penetration test.The company wants the consultant to focus on Internet-facing services without negatively impacting production services.Which of the following is the consultant MOST likely to use to identify the company's attack surface? (Select TWO)A. Web crawlerB. WHOIS registryC. DNS recordsD. Company's firewall ACLE. Internal routing tablesF. Directory service queriesAnswer: BEQUESTION 614A company is concerned about disgruntled employees transferring its intellectual property data through covert channels.Which of the following tools would allow employees to write data into ICMP echo response packets?A. ThorB. Jack the RipperC. Burp SuiteD.

LokiAnswer: DQUESTION 615A security engineer is making certain URLs from an internal application available on the Internet. The development team requires the following- The URLs are accessible only from internal IP addresses- Certain countries are restricted- TLS is implemented.- System users transparently access internal application services in a round robin to maximize performanceWhich of the following should the security engineer deploy7A. DNS to direct traffic and a WAF with only the specific external URLs configuredB. A load balancer with GeolP restrictions and least-load-sensing traffic distributionC. An application-aware firewall with geofencing and certificate services using DNS for traffic directionD. A load balancer with IP ACL restrictions and a commercially available PKI certificateAnswer: BQUESTION 616A company enlists a trusted agent to implement a way to authenticate email senders positively. Which of the following is the BEST method for the company to prove Vie authenticity of the message?A. issue PlN-enabled hardware tokensB. Create a CA win all usersC. Configure the server to encrypt all messages in transitD. include a hash in the body of the messageAnswer: AQUESTION 617A company recently migrated to a SaaS-based email solution.The solution is configured as follows.- Passwords are synced to the cloud to allow for SSO- Cloud-based antivirus is enabled- Cloud-based anti-spam is enabled- Subscription-based blacklist is enabledAlthough the above controls are enabled, the company's security administrator is unable to detect an account compromise caused by phishing attacks in a timely fashion because email logs are not immediately available to review.Which of the following would allow the company to gam additional visibility and reduce additional costs? (Select TWO)A. Migrate the email antivirus and anti-spam on-premisesB. Implement a third-party CASB solution.C. Disable the current SSO model and enable federationD. Feed the attacker IPs from the company IDS into the email blacklistE. Install a virtual SIEM within the email cloud providerF. Add email servers to NOC monitoringAnswer: BEQUESTION 618The Chief Information Security Officer (CISO) of a company that has highly sensitive corporate locations wants its security engineers to find a solution to growing concerns regarding mobile devices.The CISO mandates the following requirements:- The devices must be owned by the company for legal purposes.- The device must be as fully functional as possible when off site.- Corporate email must be maintained separately from personal email- Employees must be able to install their own applications.Which of the following will BEST meet the CISO's mandate? (Select TWO).A. Disable the device's camera B. Allow only corporate resources in a container.C. Use an MDM to wipe the devices remotelyD. Block all sideloading of applications on devicesE. Use geofencmg on certain applicationsF. Deploy phones in a BYOD modelAnswer: BEQUESTION 619After analyzing code, two developers al a company bring these samples to the security operations manager.

Which of the following would BEST solve these coding problems?A. Use a privileged access management systemB. Prompt the administrator for the password .C. Use salted hashes with PBKDF2.D. Increase the complexity and length of the passwordAnswer: BQUESTION 620A security administrator receives reports that several workstations are unable to access resources within one network segment. A packet capture shows the segment is flooded with ICMPv6 traffic from the source fe80::21ae;4571:42ab:1fdd and for the destination ff02::1.Which of the following should the security administrator integrate into the network to help prevent this from occurring?A. Raise the dead peer detection interval to prevent the additional network chatterB. Deploy honeypots on the network segment to identify the sending machine.C. Ensure routers will use route advertisement guards. D. Deploy ARP spoofing prevention on routers and switches.Answer: DQUESTION 621Joe an application security engineer is performing an audit of an environmental control application.He has implemented a robust SDLC process and is reviewing API calls available to the application.During the review, Joe finds the following in a log file.

Which of the following would BEST mitigate the issue Joe has found?A. Ensure the API uses SNMPv1.B. Perform authentication via a secure channelC. Verify the API uses HTTP GET instead of POSTD. Deploy a WAF in front of the API and implement rate limitingAnswer: BQUESTION 622An organization implemented a secure boot on its most critical application servers which produce content and capability for other consuming servers A recent incident, however led the organization to implement a centralized attestation service for these critical servers.Which of the following MOST likely explains the nature of the incident that caused the organization to implement this remediation?A. An attacker masqueraded as an internal DNS serverB. An attacker leveraged a heap overflow vulnerability in the OSC. An attacker was able to overwrite an OS integrity measurement registerD. An attacker circumvented IEEE 802.1X network-level authentication requirements.Answer: CQUESTION 623A company's Internet connection is commonly saturated during business hours, affecting Internet availability. The company requires all Internet traffic to be business related.After analyzing the traffic over a period of a few hours, the security administrator observes

the following:

Protocol	Usage	%
TCP/SSL	324Gb	85%
UDP/HTTP	7Gb	0%
UDP/DNS	10Gb	3%
Other	8GB	2%

The majority of the IP addresses associated with the TCP/SSL traffic resolve to CDNs.Which of the following should the administrator recommend for the CDN traffic to meet the corporate security requirements?A. Block outbound SSL traffic to prevent data exfiltration.B. Confirm the use of the CDN by monitoring NetFlow dataC. Further investigate the traffic using a sanctioned MITM proxy.D. Implement an IPS to drop packets associated with the CDN.Answer: AQUESTION 624An attacker has been compromising banking institution targets across a regional area. The Chief Information Security Officer (CISO) at a local bank wants to detect and prevent an attack before the bank becomes a victim.Which of the following actions should the CISO take?A. Utilize cloud-based threat analytics to identify anomalous behavior in the company's B2B and vendor trafficB. Purchase a CASB solution to identify and control access to cloud-based applications and services and integrate them with on-premises legacy security monitoringC. Instruct a security engineer to configure the IDS to consume threat intelligence feeds from an information-sharing association in the banking sectorD. Attend and present at the regional banking association lobbying group meetings each month and facilitate a discussion on the topic.Answer: CQUESTION 625Users have reported that an internally developed web application is acting erratically, and the response output is inconsistent. The issue began after a web application dependency patch was applied to improve security.Which of the following would be the MOST appropriate tool to help identify the issue?A. FuzzerB. SCAP scannerC. Vulnerability scannerD. HTTP interceptorAnswer: AQUESTION 626A company makes consumer health devices and needs to maintain strict confidentiality of unreleased product designs.Recently unauthorized photos of products still in development have been for sale on the dark web. The Chief Information Security Officer (CISO) suspects an insider threat, but the team that uses the secret outdoor testing area has been vetted many times and nothing suspicious has been found. Which of the following is the MOST likely cause of the unauthorized photos?A. The location of the testing facility was discovered by analyzing fitness device information the test engineers posted on a websiteB. One of the test engineers is working for a competitor and covertly installed a RAT on the marketing department's serversC. The company failed to implement least privilege on network devices, and a hacktivist published stolen public relations photosD. Pre-release marketing materials for a single device were accidentally left in a public locationAnswer: DResources From:1.2020 Latest Braindump2go CAS-003 Exam Dumps (PDF & VCE) Free Share:https://www.braindump2go.com/cas-003.html2.2020 Latest Braindump2go CAS-003 PDF and VCE Dumps Free Share:https://drive.google.com/drive/folders/11eVcvdRTGUBlESzBX9a6YlPUYiZ4xoHE?usp=sharing3.2020 Free Braindump2go CAS-003 PDF Download:https://www.braindump2go.com/free-online-pdf/CAS-003-Dumps(646-660).pdf
https://www.braindump2go.com/free-online-pdf/CAS-003-Dumps(677-692).pdf
https://www.braindump2go.com/free-online-pdf/CAS-003-PDF(661-676).pdf
https://www.braindump2go.com/free-online-pdf/CAS-003-PDF(693-704).pdf
https://www.braindump2go.com/free-online-pdf/CAS-003-PDF-Dumps(606-617).pdf
https://www.braindump2go.com/free-online-pdf/CAS-003-VCE(618-629).pdf
https://www.braindump2go.com/free-online-pdf/CAS-003-VCE(630-645).pdf
https://www.braindump2go.com/free-online-pdf/CAS-003-VCE-Dumps(705-716).pdfFree Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!