[May-2018-NewCAS-003 VCE 270Q Instant Download in Braindump2go[23-33

2018 May New CompTIA CAS-003 Exam Dumps with PDF and VCE Just Updated Today! Following are some new CAS-003 Real Exam Questions:1.|2018 Latest CAS-003 Exam Dumps (PDF & VCE) 270Q Download:https://www.braindump2go.com/cas-003.html2.|2018 Latest CAS-003 Exam Questions & Answers Download:https://drive.google.com/drive/folders/11eVcvdRTGUBlESzBX9a6YlPUYiZ4xoHE?usp=sharing QUESTION 23A recent assessment identified that several users' mobile devices are running outdated versions of endpoint security software that do not meet the company's security policy. Which of the following should be performed to ensure the users can access the network and meet the company's security requirements?A. Vulnerability assessmentB. Risk assessmentC. Patch managementD. Device quarantineE. Incident managementAnswer: CQUESTION 24A software development team is conducting functional and user acceptance testing of internally developed web applications using a COTS solution. For automated testing, the solution uses valid user credentials from the enterprise directory to authenticate to each application. The solution stores the username in plain text and the corresponding password as an encoded string in a script within a file, located on a globally accessible network share. The account credentials used belong to the development team lead. To reduce the risks associated with this scenario while minimizing disruption to ongoing testing, which of the following are the BEST actions to take? (Choose two.)A. Restrict access to the network share by adding a group only for developers to the share's ACLB. Implement a new COTS solution that does not use hard-coded credentials and integrates with directory servicesC. Obfuscate the username within the script file with encoding to prevent easy identification and the account usedD. Provision a new user account within the enterprise directory and enable its use for authentication to the target applications. Share the username and password with all developers for use in their individual scriptsE. Redesign the web applications to accept single-use, local account credentials for authenticationAnswer: ABQUESTION 25The Chief Information Security Officer (CISO) for an organization wants to develop custom IDS rulesets faster, prior to new rules being released by IDS vendors. Which of the following BEST meets this objective?A. Identify a third-party source for IDS rules and change the configuration on the applicable IDSs to pull in the new rulesetsB. Encourage cybersecurity analysts to review open-source intelligence products and threat database to generate new IDS rules based on those sourcesC. Leverage the latest TCP- and UDP-related RFCs to arm sensors and IDSs with appropriate heuristics for anomaly detectionD. Use annual hacking conventions to document the latest attacks and threats, and then develop IDS rules to counter those threatsAnswer: BQUESTION 26 Management is reviewing the results of a recent risk assessment of the organization's policies and procedures. During the risk assessment it is determined that procedures associated with background checks have not been effectively implemented. In response to this risk, the organization elects to revise policies and procedures related to background checks and use a third-party to perform background checks on all new employees. Which of the following risk management strategies has the organization employed?A. TransferB. MitigateC. AcceptD. AvoidE. RejectAnswer: BQUESTION 27A penetration tester has been contracted to conduct a physical assessment of a site. Which of the following is the MOST plausible method of social engineering to be conducted during this engagement?A. Randomly calling customer employees and posing as a help desk technician requiring user password to resolve issuesB. Posing as a copier service technician and indicating the equipment had "phoned home" to alert the technician for a service callC. Simulating an illness while at a client location for a sales call and then recovering once listening devices are installedD. Obtaining fake government credentials and impersonating law enforcement to gain access to a company facilityAnswer: AQUESTION 28Drag and Drop QuestionDrag and drop the cloud deployment model to the associated use-case scenario. Options may be used only once or not at all. Answer: QUESTION 29A Chief Information Security Officer (CISO) is reviewing the results of a gap analysis with an outside cybersecurity consultant. The gap analysis reviewed all procedural and technical controls and found the following: High-impact controls implemented: 6 out of 10 Medium-impact controls implemented: 409 out of 472 Low-impact controls implemented: 97 out of 1000The report includes a cost-benefit analysis for each control gap. The analysis yielded the following information: Average high-impact control implementation cost: $15,000; Probable ALE for each high-impact control gap: $95,000 Average medium-impact control implementation cost: $6,250; Probable ALE for each medium-impact control gap: $11,000Due to the technical construction and configuration of the corporate enterprise, slightly more than 50% of the medium-impact controls will take two years to fully implement. Which of the following conclusions could the CISO draw from the analysis?A. Too much emphasis has been placed on eliminating low-risk vulnerabilities in the pastB. The enterprise security team has focused exclusively on mitigating high-level risksC. Because of the significant ALE for each high-risk vulnerability, efforts should be focused on those controlsD. The cybersecurity team has balanced residual risk for both high and medium controlsAnswer: CQUESTION 30The Chief Information Security Officer (CISO) has asked the security team to determine whether the organization is susceptible to a zero-day exploit utilized in the banking industry and whether attribution is possible. The

CISO has asked what process would be utilized to gather the information, and then wants to apply signatureless controls to stop these kinds of attacks in the future. Which of the following are the MOST appropriate ordered steps to take to meet the CISO's request?A. 1. Perform the ongoing research of the best practices2. Determine current vulnerabilities and threats3. Apply Big Data techniques4. Use antivirus controlB. 1. Apply artificial intelligence algorithms for detection2. Inform the CERT team3. Research threat intelligence and potential adversaries4. Utilize threat intelligence to apply Big Data techniquesC. 1. Obtain the latest IOCs from the open source repositories2. Perform a sweep across the network to identify positive matches3. Sandbox any suspicious files 4. Notify the CERT team to apply a future proof threat modelD. 1. Analyze the current threat intelligence2. Utilize information sharing to obtain the latest industry IOCs3. Perform a sweep across the network to identify positive matches4. Apply machine learning algorithmsAnswer: CQUESTION 31A company wants to extend its help desk availability beyond business hours. The Chief Information Officer (CIO) decides to augment the help desk with a third-party service that will answer calls and provide Tier 1 problem resolution, such as password resets and remote assistance. The security administrator implements the following firewall change: The administrator provides the appropriate path and credentials to the third-party company. Which of the following technologies is MOST likely being used to provide access to the third company?A. LDAPB. WAYFC. OpenIDD. RADIUS E. SAMLAnswer: DQUESTION 32A financial consulting firm recently recovered from some damaging incidents that were associated with malware installed via rootkit. Post-incident analysis is ongoing, and the incident responders and systems administrators are working to determine a strategy to reduce the risk of recurrence. The firm's systems are running modern operating systems and feature UEFI and TPMs. Which of the following technical options would provide the MOST preventive value?A. Update and deploy GPOsB. Configure and use measured bootC. Strengthen the password complexity requirementsD. Update the antivirus software and definitionsAnswer: DQUESTION 33Two new technical SMB security settings have been enforced and have also become policies that increase secure communications. Network Client: Digitally sign communication Network Server: Digitally sign communicationA storage administrator in a remote location with a legacy storage array, which contains time-sensitive data, reports employees can no longer connect to their department shares. Which of the following mitigation strategies should an information security manager recommend to the data owner?A. Accept the risk, reverse the settings for the remote location, and have the remote location file a risk exception until the legacy storage device can be upgradedB. Accept the risk for the remote location, and reverse the settings indefinitely since the legacy storage device will not be upgradedC. Mitigate the risk for the remote location by suggesting a move to a cloud service provider. Have the remote location request an indefinite risk exception for the use of cloud storageD. Avoid the risk, leave the settings alone, and decommission the legacy storage deviceAnswer: A
!!!RECOMMEND!!!1.|2018 Latest CAS-003 Exam Dumps (PDF & VCE) 270Q Download:https://www.braindump2go.com/cas-003.html2.|2018 Latest CAS-003 Exam Questions & Answers Download: YouTube Video: YouTube.com/watch?v=wiypGN6OqiA