[2018-June-NewFull Version CAS-002 Dumps PDF and VCE 900Q for Free Download[89-99

2018 June New CompTIA CAS-002 Exam Dumps with PDF and VCE Just Updated Today! Following are some new CAS-002 Real Exam Questions: 1.|2018 Latest CAS-002 Exam Dumps (PDF & VCE) 900Q&As Download:https://www.braindump2go.com/cas-002.html2.|2018 Latest CAS-002 Exam Questions & Answers Download:https://drive.google.com/drive/folders/0B75b5xYLjSSNQjRNekVOcFlaVm8?usp=sharingQUESTION 89A company decides to purchase COTS software. This can introduce new security risks to the network. Which of the following is the BEST description of why this is true?A. COTS software is typically well known and widely available. Information concerning vulnerabilities and viable attack patterns are never revealed by the developer to avoid a lawsuit.B. COTS software is not well known and is only available in limited quantities. Information concerning vulnerabilities is kept internal to the company that developed the software.C. COTS software is well known and widely available. Information concerning vulnerabilities and viable attack patterns is typically ignored within the IT community.D. COTS software is well known and widely available. Information concerning vulnerabilities and viable attack patterns is typically shared within the IT community.**Answer: D**QUESTION 90The increasing complexity of attacks on corporate networks is a direct result of more and more corporate employees connecting to corporate networks with mobile and personal devices. In most cases simply banning these connections and devices is not practical because they support necessary business needs. Which of the following are typical risks and mitigations associated with this new trend?A. Risks: Data leakage, lost data on destroyed mobile devices, smaller network attack surface, prohibitive telecommunications costsMitigations: Device Encryptions, lock screens, certificate based authentication, corporate telecom plansB. Risks: Confidentiality leaks through cell conversations, availability of remote corporate data, integrity of data stored on the devices Mitigations: Cellular privacy extensions, mobile VPN clients, over-the-air backups.C. Risks: Data exfiltration, loss of data via stolen mobile devices, increased data leakage at the network edgeMitigations: Remote data wipe capabilities, implementing corporate security on personally owned devicesD. Risks: Theft of mobile devices, unsanctioned applications, minimal device storage, call qualityMitigations: GPS tracking, centralized approved application deployment, over-the-air backups, QoS implementation**Answer: C**QUESTION 91When planning a complex system architecture, it is important to build in mechanisms to secure log information, facilitate audit log reduction, and event correlation. Besides synchronizing system time across all devices through NTP, which of the following is also a common design consideration for remote locations?A. Two factor authentication for all incident respondersB. A central SYSLOG server for collecting all logsC. A distributed SIEM with centralized sensorsD. A SIEM server with distributed sensors**Answer: D**QUESTION 92A financial institution has decided to purchase a very expensive resource management system and has selected the product and vendor. The vendor is experiencing some minor, but public, legal issues. Senior management has some concerns on maintaining this system should the vendor go out of business. Which of the following should the Chief Information Security Officer (CISO) recommend to BEST limit exposure?A. Include a source code escrow clause in the contract for this system.B. Require proof-of-insurance by the vendor in the RFP for this system.C. Include a penalty clause in the contract for this system.D. Require on-going maintenance as part of the SLA for this system.**Answer: A**QUESTION 93During a specific incident response and recovery process action, the response team determines that it must first speak to the person ultimately responsible for the data. With whom should the response team speak FIRST?A. Data UserB. Data OwnerC. Business OwnerD. Data Custodian**Answer: B**QUESTION 94After a recent outbreak of malware attacks, the Chief Information Officer (CIO) tasks the new security manager with determining how to keep these attacks from reoccurring. The company has a standard image for all laptops/workstations and uses a host-based firewall and anti-virus. Which of the following should the security manager suggest to INCREASE each system's security level?A. Upgrade all system's to use a HIPS and require daily anti-virus scans.B. Conduct a vulnerability assessment of the standard image and remediate findings.C. Upgrade the existing NIDS to NIPS and deploy the system across all network segments.D. Rebuild the standard image and require daily anti-virus scans of all PCs and laptops.**Answer: B**QUESTION 95To support a software security initiative business case, a project manager needs to provide a cost benefit analysis. The project manager has asked the security consultant to perform a return on investment study. It has been estimated that by spending $300,000 on the software security initiative, a 30% savings in cost will be realized for each project. Based on an average of 8 software projects at a current cost of $50,000 each, how many years will it take to see a positive ROI?A. Nearly four yearsB. Nearly six yearsC. Within the first yearD. Nearly three years**Answer: D**QUESTION 96A network security engineer would like to allow authorized groups to access network devices with a shell restricted to only show information while still authenticating the administrator's group to an unrestricted shell. Which of the following can be configured to authenticate and enforce these shell restrictions? (Select TWO).A. Single Sign OnB. Active DirectoryC.

KerberosD.   NIS+E.   RADIUSF.   TACACS+**Answer: EF**QUESTION 97SAML entities can operate in a variety of different roles. Valid SAML roles include which of the following?A.   Attribute authority and certificate authorityB.   Certificate authority and attribute requestorC.   Identity provider and service providerD.   Service provider and administrator**Answer: C**QUESTION 98 When authenticating over HTTP using SAML, which of the following is issued to the authenticating user?A.   A symmetric keyB.   A PKI ticketC.   An X.509 certificateD.   An assertion ticket**Answer: D**QUESTION 99An existing enterprise architecture included an enclave where sensitive research and development work was conducted. This network enclave also served as a storage location for proprietary corporate data and records. The initial security architect chose to protect the enclave by restricting access to a single physical port on a firewall. All downstream network devices were isolated from the rest of the network and communicated solely through the single 100mbps firewall port. Over time, researchers connected devices on the protected enclave directly to external resources and corporate data stores. Mobile and wireless devices were also added to the enclave to support high speed data research. Which of the following BEST describes the process which weakened the security posture of the enclave?A.   Emerging business requirements led to the de-perimiterization of the network.B.   Emerging security threats rendered the existing architecture obsolete. C.   The single firewall port was oversaturated with network packets.D.   The shrinking of an overall attack surface due to the additional access.**Answer: A**!!!RECOMMEND!!!1.|2018 Latest CAS-002 Exam Dumps (PDF & VCE) 900Q&As Download:https://www.braindump2go.com/cas-002.html2.|2018 Latest CAS-002 Study Guide Video: YouTube Video: YouTube.com/watch?v=k4FW5mVem0w