Braindump2go Guarantee All Exams 100% Pass One Time!

➢ Vendor: CompTIA

➢ Exam Code: CAS-003

➢ Exam Name: CompTIA Advanced Security Practitioner (CASP)

➢ New Updated Questions from Braindump2go (Updated in Dec./2020)

Visit Braindump2go and Download Full Version CAS-003 Exam Dumps

QUESTION 705
The security administrator of a small firm wants to stay current on the latest security vulnerabilities and attack vectors being used by crime syndicates and nation-states.
The information must be actionable and reliable.
Which of the following would BEST meet the needs of the security administrator?

A. Software vendor threat reports
B. White papers
C. Security blogs
D. Threat data subscription

Answer: D

QUESTION 706
An organization is moving internal core data-processing functions related to customer data to a global public cloud provider that uses aggregated services from other partner organizations.
Which of the following compliance issues will MOST likely be introduced as a result of the migration?

A. Internal data integrity standards and outsourcing contracts and partnerships
B. Data ownership, internal data classification, and risk profiling of outsourcers
C. Company audit functions, cross-boarding jurisdictional challenges, and export controls
D. Data privacy regulations, data sovereignty, and third-party providers

Answer: D

QUESTION 707
A global company has decided to implement a cross-platform baseline of security settings for all company laptops.
A security engineer is planning and executing the project.
Which of the following should the security engineer recommend?

A. Replace each laptop in the company's environment with a standardized laptop that is preconfigured to match the baseline settings
B. Create batch script files that will enable the baseline security settings and distribute them to global employees for execution
C. Send each laptop to a regional IT office to be reimaged with the new baseline security settings enabled and then redeployed
D. Establish GPO configurations for each baseline setting, test that each works as expected, and have each setting deployed to the laptops.
E. Leverage an MDM solution to apply the baseline settings and deploy continuous monitoring of security configurations.

CAS-003 Exam Dumps CAS-003 Exam Questions CAS-003 PDF Dumps CAS-003 VCE Dumps

https://www.braindump2go.com/cas-003.html

Answer: B

QUESTION 708
A security administrator is investigating an incident involving suspicious word processing documents on an employee's computer, which was found powered off in the employee's office.
Which of the following tools is BEST suited for extracting full or partial word processing documents from unallocated disk space?

A. memdump
B. forenoat
C. dd
D. nc

Answer: B

QUESTION 709
The email administrator must reduce the number of phishing emails by utilizing more appropriate security controls.
The following configurations already are in place
- Keyword Mocking based on word lists
- URL rewriting and protection
- Stopping executable files from messages
Which of the following is the BEST configuration change for the administrator to make?

A. Configure more robust word lists for blocking suspicious emails
B. Configure appropriate regular expression rules per suspicious email received
C. Configure Bayesian filtering to block suspicious inbound email
D. Configure the mail gateway to strip any attachments

Answer: B

QUESTION 710
Within the past six months, a company has experienced a series of attacks directed at various collaboration tools. Additionally, sensitive information was compromised during a recent security breach of a remote access session from an unsecure site.
As a result, the company is requiring all collaboration tools to comply with the following:
- Secure messaging between internal users using digital signatures
- Secure sites for video-conferencing sessions
- Presence information for all office employees
- Restriction of certain types of messages to be allowed into the network.
Which of the following applications must be configured to meet the new requirements? (Select TWO.)

A. Remote desktop
B. VoIP
C. Remote assistance
D. Email
E. Instant messaging
F. Social media websites

Answer: BE

QUESTION 711
A government entity is developing requirements for an RFP to acquire a biometric authentication system.
When developing these requirements, which of the following considerations is MOST critical to the verification and validation of the SRTM?

A. Local and national laws and regulations

B. Secure software development requirements
C. Environmental constraint requirements
D. Testability of requirements

Answer: A

QUESTION 712
A SaaS provider decides to offer data storage as a service. For simplicity, the company wants to make the service available over industry standard APIs, routable over the public Internet.
Which of the following controls offers the MOST protection to the company and its customers' information?

A. Detailed application logging
B. Use of non-standard ports
C. Web application firewall
D. Multifactor authentication

Answer: D

QUESTION 713
A security administrator wants to stand up a NIPS that is multilayered and can incorporate many security technologies into a single platform.
The product should have diverse capabilities, such as antivirus, VPN, and firewall services, and be able to be updated in a timely manner to meet evolving threats.
Which of the following network prevention system types can be used to satisfy the requirements?

A. Application firewall
B. Unified threat management
C. Enterprise firewall
D. Content-based IPS

Answer: A

QUESTION 714
The Chief Financial Officer (CFO) of an organization wants the IT department to add the CFO's account to the domain administrator group.
The IT department thinks this is nsky and wants support from the security manager before proceeding.
Which of the following BEST supports the argument against providing the CFO with domain administrator access?

A. Discretionary access control
B. Separation of duties
C. Data classification
D. Mandatory access control

Answer: B

QUESTION 715
A company is trying to resolve the following issues related to its web servers and Internet presence:
- The company's security rating declined on multiple occasions when it failed to renew a TLS certificate on one or more infrequently used web servers
- The company is running out of public IPs assigned by its ISP
- The company is implementing a WAF and the WAF vendor charges by back-end hosts to which the WAF routes
Which of the following solutions will help the company mitigate these issues? (Select TWO).

A. Use a DMZ architecture
B. Implement reverse proxy servers
C. Use an automated CA service API for certificate renewal

D. Work with the company's ISP to configure BGP
E. Deploy IPv6 for external-facing servers
F. Implement self-signed certificates and disable trust verification.

Answer: AE

QUESTION 716
A manufacturing company employs SCADA systems to drive assembly lines across geographically dispersed sites. Therefore, the company must use the Internet to transport control messages and responses.
Which of the following architectural changes when integrated will BEST reduce the manufacturing control system's attack surface? (Select TWO)

A. Design a patch management capability for control systems.
B. Implement supply chain security.
C. Integrate message authentication
D. Add sensors and collectors at the Internet boundary.
E. Isolate control systems from enterprise systems.
F. Implement a site-to-site VPN across sites

Answer: AE