Exam Questions CISMP-V9

BCS Foundation Certificate in Information Security Management Principles V9.0

https://www.2passeasy.com/dumps/CISMP-V9/

NEW QUESTION 1
One traditional use of a SIEM appliance is to monitor for exceptions received via syslog. What system from the following does NOT natively support syslog events?

A. Enterprise Wireless Access Point.
B. Windows Desktop Systems.
C. Linux Web Server Appliances.
D. Enterprise Stateful Firewall.

Answer: C

NEW QUESTION 2
How does the use of a "single sign-on" access control policy improve the security for an organisation implementing the policy?

A. Password is better encrypted for system authentication.
B. Access controllogs are centrally located.
C. Helps prevent the likelihood of users writing down passwords.
D. Decreases the complexity of passwords users have to remember.

Answer: B

NEW QUESTION 3
What physical security control would be used to broadcast false emanations to mask the presence of true electromagentic emanations fromgenuine computing equipment?

A. Faraday cage.
B. Unshielded cabling.
C. Copper infused windows.
D. White noise generation.

Answer: B

NEW QUESTION 4
Which of the following acronyms covers the real-time analysis of security alerts generated by applications and network hardware?

A. CERT
B. SIEM.
C. CISM.
D. DDoS.

Answer: B

Explanation:
https://en.wikipedia.org/wiki/Security_information_and_event_management

NEW QUESTION 5
What type of attack could directly affect the confidentiality of an unencrypted VoIP network?

A. Packet Sniffing.
B. Brute Force Attack.
C. Ransomware.
D. Vishing Attack

Answer: B

NEW QUESTION 6
When considering outsourcing the processing of data, which two legal "duty of care" considerations SHOULD the original data owner make?
* 1 Third party is competent to process the data securely.
* 2. Observes the same high standards as data owner.
* 3. Processes the data wherever the data can be transferred.
* 4. Archive the data for long term third party's own usage.

A. 2 and 3.
B. 3 and 4.
C. 1 and 4.
D. 1 and 2.

Answer: C

NEW QUESTION 7
Which of the following is often the final stage in the information management lifecycle?

A. Disposal.
B. Creation.
C. Use.

D. Publication.

Answer: A

Explanation:
https://timg.co.nz/blog-the-information-management-life-cycle/

NEW QUESTION 8
Why might the reporting of security incidents that involve personaldata differ from other types of security incident?

A. Personal data is not highly transient so its 1 investigation rarely involves the preservation of volatile memory and full forensic digitalinvestigation.
B. Personal data is normally handled on both IT and non-IT systems so such incidents need to be managed in two streams.
C. Data Protection legislation normally requires the reporting of incidents involving personal data to a Supervisory Authority.
D. Data Protection legislation is process-oriented and focuses on quality assurance of procedures and governance rather thandata-focused event investigation

Answer: D

NEW QUESTION 9
When handling and investigating digital evidence to be used in a criminal cybercrime investigation, which of the following principles isconsidered BEST practice?

A. Digital evidence must not be altered unless absolutely necessary.
B. Acquiring digital evidence cart only be carried on digital devices which have been turned off.
C. Digital evidence can only be handled by a member of law enforcement.
D. Digital devices must be forensically "clean" before investigation.

Answer: D

NEW QUESTION 10
Which types of organisations are likely to be the target of DDoS attacks?

A. Cloud service providers.
B. Any financial sector organisations.
C. Online retail based organisations.
D. Any organisation with an online presence.

Answer: D

NEW QUESTION 10
In order to maintain the currency of risk countermeasures, how often SHOULD an organisation review these risks?

A. Once defined, they do not need reviewing.
B. A maximum of once every other month.
C. When the next risk audit is due.
D. Risks remain under constant review.

Answer: D

NEW QUESTION 12
What Is the PRIMARY difference between DevOps and DevSecOps?

A. Within DevSecOps security is introduced at the end of development immediately prior to deployment.
B. DevSecOps focuses solely on iterative development cycles.
C. DevSecOps includes security on the same level as continuous integration and delivery.
D. DevOps mandates that security is integrated at the beginning of the development lifecycle.

Answer: C

Explanation:
https://www.viva64.com/en/b/0710/#:~:text=DevOps%20is%20a%20methodology%20aiming,in%20the%20sof

NEW QUESTION 16
Which of the following is NOT a valid statement to include in an organisation's security policy?

A. The policy has the support of Board and the Chief Executive.
B. The policy has been agreed and amended to suit all third party contractors.
C. How the organisation will manage information assurance.
D. The compliance with legal and regulatory obligations.

Answer: C

NEW QUESTION 21
What advantage does the delivery of online security training material have over the distribution of printed media?

A. Updating online material requires a single edi
B. Printed material needs to be distributed physically.

C. Online training material is intrinsically more accurate than printed material.
D. Printed material is a 'discoverable record' and could expose the organisation to litigation in the event of an incident.
E. Online material is protected by international digital copyright legislation across most territories.

Answer: B

NEW QUESTION 26
Which of the following uses are NOT usual ways that attackers have of leveraging botnets?

A. Generating and distributing spam messages.
B. Conducting DDOS attacks.
C. Scanning for system & application vulnerabilities.
D. Undertaking vishing attacks

Answer: D

NEW QUESTION 31
When securing a wireless network, which of the following is NOT best practice?

A. Using WPA encryption on the wireless network.
B. Use MAC tittering on a SOHO network with a smart group of clients.
C. Dedicating an access point on a dedicated VLAN connected to a firewall.
D. Turning on SSID broadcasts to advertise security levels.

Answer: C

NEW QUESTION 34
Which of the following statements relating to digital signatures is TRUE?

A. Digital signatures are rarely legally enforceable even if the signers know they are signing a legal document.
B. Digital signatures are valid and enforceable in law in most countries in the world.
C. Digital signatures are legal unless there is a statutory requirement that predates the digital age.
D. A digital signature that uses a signer??s private key is illegal.

Answer: C

NEW QUESTION 36
What type of diagram used in application threat modeling includes malicious users as well as descriptions like mitigates and threatens?

A. Threat trees.
B. STRIDE charts.
C. Misuse case diagrams.
D. DREAD diagrams.

Answer: A

NEW QUESTION 41
What Is the first yet MOST simple and important action to take when setting up a new web server?

A. Change default system passwords.
B. Fully encrypt the hard disk.
C. Apply hardening to all applications.
D. Patch the OS to the latest version

Answer: C

NEW QUESTION 44
When an organisation decides to operate on the public cloud, what does it lose?

A. The right to audit and monitor access to its information.
B. Control over Intellectual Property Rights relating to its applications.
C. Physical access to the servers hosting its information.
D. The ability to determine in which geographies the information is stored.

Answer: A

NEW QUESTION 49
What Is the KEY purpose of appending security classification labels to information?

A. To provide guidance and instruction on implementing appropriate security controls to protect the information.
B. To comply with whatever mandatory security policy framework is in place within the geographical location in question.
C. To ensure that should the information be lost in transit, it can be returned to the originator using the correct protocols.
D. To make sure the correct colour-coding system is used when the information is ready for archive.

Answer: A

NEW QUESTION 54
How might the effectiveness of a security awareness program be effectively measured?
1)Employees are required to take an online multiple choice exam on security principles.
2)Employees are tested with social engineering techniques by an approved penetration tester. 3)Employees practice ethical hacking techniques on organisation systems.
4) No security vulnerabilities are reported during an audit.
5) Open source intelligence gathering is undertaken on staff social media profiles.

A. 3, 4 and 5.
B. 2, 4 and 5.
C. 1, 2 and 3.
D. 1, 2 and 5.

Answer: C

NEW QUESTION 58
By what means SHOULD a cloud service provider prevent one client accessing data belonging to another in a shared server environment?

A. By ensuring appropriate data isolation and logical storage segregation.
B. By using a hypervisor in all shared severs.
C. By increasing deterrent controls through warning messages.
D. By employing intrusion detection systems in a VMs.

Answer: D

NEW QUESTION 61
A security analyst has been asked to provide a triple A service (AAA) for both wireless and remote access network services in anorganizationand must avoid using proprietary solutions.
What technology SHOULD they adapt?

A. TACACS+
B. RADIUS.
C. Oauth.
D. MS Access Database.

Answer: C

NEW QUESTION 63
Which term describes a vulnerability that is unknown and therefore has no mitigating control which is immediately and generally available?

A. Advanced Persistent Threat.
B. Trojan.
C. Stealthware.
D. Zero-day.

Answer: D

Explanation:
https://en.wikipedia.org/wiki/Zero-day_(computing)

NEW QUESTION 66
You are undertaking a qualitative risk assessment of a likely security threat to an information system. What is the MAIN issue with this type of risk assessment?

A. These risk assessments are largely subjective and require agreement on rankings beforehand.
B. Dealing with statistical and other numeric data can often be hard to interpret.
C. There needs to be a large amount of previous data to "train" a qualitative risk methodology.
D. It requires the use of complex software tools to undertake this risk assessment.

Answer: D

NEW QUESTION 71
Which algorithm is a current specification for the encryption of electronic data established by NIST?

A. RSA.
B. AES.
C. DES.
D. PGP.

Answer: B

Explanation:
https://www.nist.gov/publications/advanced-encryption-standard-aes

NEW QUESTION 72
Which of the following compliance legal requirements are covered by the ISO/IEC 27000 series?

* 1. Intellectual Property Rights.
* 2. Protection of Organisational Records
* 3. Forensic recovery of data.
* 4. Data Deduplication.
* 5. Data Protection & Privacy.

A. 1, 2 and 3
B. 3, 4 and 5
C. 2, 3 and 4
D. 1, 2 and 5

Answer: D

NEW QUESTION 75
Which membership based organisation produces international standards, which cover good practice for information assurance?

A. BSI.
B. IETF.
C. OWASP.
D. ISF.

Answer: A

NEW QUESTION 78
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CISMP-V9 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CISMP-V9 Product From:

https://www.2passeasy.com/dumps/CISMP-V9/

Money Back Guarantee

CISMP-V9 Practice Exam Features:

* CISMP-V9 Questions and Answers Updated Frequently

* CISMP-V9 Practice Questions Verified by Expert Senior Certified Staff

* CISMP-V9 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CISMP-V9 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year