VCEplus.com

ISC.Premium.CISSP.by.VCEplus.100q - DEMO

Number: CISSP VCEplus
Passing Score: 800
Time Limit: 120 min

Exam Code: CISSP
Exam Name: Certified Information Systems Security Professional
Certification Provider: ISC
Corresponding Certification: CISSP
Website: https://vceplus.com - https://vceplus.co
Free Exam: https://vceplus.com/exam-cissp-2018/
Questions & Answers Exam Engine is rigorously checked before being put up for sale. We make sure there is nothing irrelevant in CISSP exam products and you get latest questions. We strive to deliver the best CISSP exam product for top grades in your first attempt.

VCEplus.com

Website: https://vceplus.com - https://vceplus.co
VCE to PDF Converter: https://vceplus.com/vce-to-pdf/
Facebook: https://www.facebook.com/VCE.For.All.VN/
Twitter : https://twitter.com/VCE_Plus

Sections
1. Security and Risk Management
2. Asset Security
3. Security Architecture and Engineering
4. Identity and Access Management (IAM)
5. Security Assessment and Testing
6. Security Operations
7. Software Development Security
8. Communication and Network Security

CEplus.com

9. Mixed questions

CEplus.com

VCEplus.com

Exam A

QUESTION 1
When dealing with compliance with the Payment Card Industry-Data Security Standard (PCI-DSS), an organization that shares card holder information with a service provider MUST do which of the following?

A. Perform a service provider PCI-DSS assessment on a yearly basis
B. Validate the service provider's PCI-DSS compliance status on a regular basis
C. Validate that the service providers security policies are in alignment with those of the organization
D. Ensure that the service provider updates and tests its Disaster Recovery Plan (DRP) on a yearly basis

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Section: Security Operations

QUESTION 2
During a Disaster Recovery (DR) assessment, additional coverage for assurance is required. What should an assessor do?

VCEplus.com

A. Increase the level of detail of the interview questions
B. Conduct a comprehensive examination of the Disaster Recovery Plan (DRP)
C. Increase the number and type of relevant staff to interview
D. Conduct a detailed review of the organization's DR policy

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Section: Security Operations

QUESTION 3
Which of the following is the MOST important reason for timely installation of software patches?

A. Patches are only available for a specific time
B. Attackers reverse engineer the exploit from the patch
C. Patches may not be compatible with proprietary software

CEplus.com

D. Attackers may be conducting network analysis

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Section: Security Operations

QUESTION 4
Which of the following initiates the systems recovery phase of a Disaster Recovery Plan (DRP)?

A. Evacuating the disaster site
B. Activating the organization's hot site
C. Issuing a formal disaster declaration
D. Assessing the extent of damage following the disaster

Correct Answer: B
Section: Security Operations
Explanation

CEplus.com

Explanation/Reference:
Section: Security Operations

QUESTION 5
In a change-controlled environment, which of the following is MOST likely to lead to unauthorized changes to production programs?

A. Developers checking out source code without approval
B. Developers using rapid application development (RAD) methodologies without approval
C. Promoting programs to production without approval
D. Modifying source code without approval

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Section: Security Operations

VCEplus.com

QUESTION 6
What is the GREATEST challenge of an agent-based patch management solution?

A. Time to gather vulnerability information about the computers in the program
B. Requires that software be installed, running, and managed on all participating computers
C. The significant amount of network bandwidth while scanning computers
D. The consistency of distributing patches to each participating computer

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Section: Security Operations

QUESTION 7
What should be used immediately after a Business Continuity Plan (BCP) has been invoked?

A. Emergency procedures describing the necessary actions to be taken following an incident which jeopardizes business operations
B. Fallback procedures describing what actions are to be taken to move essential business activities to alternative temporary locations
C. Maintenance schedule specifying how and when the plan will be tested and the process for maintaining the plan
D. Resumption procedures describing the actions to be taken to return to normal business operations

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Section: Security Operations

QUESTION 8
Which of the following actions MUST be performed when using Secure/Multipurpose Internet Mail Extensions (S/MIME) before sending an encrypted message to a recipient?

A. Obtain the recipient's private key
B. Obtain the recipient's digital certificate
C. Digitally sign the message
D. Encrypt attachments

VCEplus.com

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Section: Security Operations

QUESTION 9
In order to support the least privilege security principle when a resource is transferring within the organization from a production support system administration role to a developer role, what changes should be made to that resource's access to the production Operating System (OS) directory structure?

A. From Read Only privileges to No Access privileges
B. From Author privileges to Administrative privileges
C. From Administrative privileges to No Access privileges
D. From No Access privileges to Author privileges

Correct Answer: A
Section: Security Operations
Explanation

VCEplus.com

Explanation/Reference:
Section: Security Operations

QUESTION 10
According to the Capability Maturity Model Integration (CMMI), which of the following levels is identified by a managed process that is tailored from the organization's set of standard processes according to the organization's tailoring guidelines?

A. Level 0: Incomplete
B. Level 1: Performed
C. Level 2: Managed
D. Level 3: Defined

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Section: Security Operations

CEplus.com

QUESTION 11
What is the BEST method if an investigator wishes to analyze a hard drive which may be used as evidence?

A. Leave the hard drive in place and use only verified and authenticated Operating Systems (OS) utilities to analyze the contents
B. Log into the system and immediately make a copy of all relevant files to a Write Once, Read Many (WORM) device
C. Remove the hard drive from the system and make a copy of the hard drive's contents using imaging hardware
D. Use a separate bootable device to make a copy of the hard drive before booting the system and analyzing the hard drive

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Section: Security Operations

QUESTION 12
Which of the following types of data would be MOST difficult to detect by a forensic examiner?

CEplus.com

A. Slack space data
B. Steganographic data
C. File system deleted data
D. Data stored with a different file type extension

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Section: Security Operations

QUESTION 13
Which of the following is the BEST approach for a forensic examiner to obtain the greatest amount of relevant information from malicious software?

A. Analyze the behavior of the program
B. Analyze the logs generated by the software
C. Review the code to identify its origin
D. Examine the file properties and permissions

CEplus.com

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Section: Security Operations

QUESTION 14
A Java program is being developed to read a file from computer A and write it to computer B, using a third computerC. The program is not working as expected. What is the MOST probable security feature of Java preventing the program from operating as intended?

A. Least privilege
B. Privilege escalation
C. Defense in depth
D. Privilege bracketing

Correct Answer: A
Section: Software Development Security
Explanation

CEplus.com

Explanation/Reference:
Section: Software Development Security

QUESTION 15
Which of the following is the PRIMARY risk with using open source software in a commercial software construction?

A. Lack of software documentation
B. License agreements requiring release of modified code
C. Expiration of the license agreement
D. Costs associated with support of the software

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

VCEplus.com

QUESTION 16
When in the Software Development Life Cycle (SDLC) MUST software security functional requirements be defined?

A. After the system preliminary design has been developed and the data security categorization has been performed
B. After the vulnerability analysis has been performed and before the system detailed design begins
C. After the system preliminary design has been developed and before the data security categorization begins
D. After the business functional analysis and the data security categorization have been performed

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 17
Which of the following is the BEST method to prevent malware from being introduced into a production environment?

A. Purchase software from a limited list of retailers
B. Verify the hash key or certificate key of all updates
C. Do not permit programs, patches, or updates from the Internet
D. Test all new software in a segregated environment

VCEplus.com

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 18
The configuration management and control task of the certification and accreditation process is incorporated in which phase of the System Development Life Cycle (SDLC)?

A. System acquisition and development
B. System operations and maintenance
C. System initiation
D. System implementation

CEplus.com

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 19
What is the BEST approach to addressing security issues in legacy web applications?

A. Debug the security issues
B. Migrate to newer, supported applications where possible
C. Conduct a security assessment
D. Protect the legacy application with a web application firewall

Correct Answer: D
Section: Software Development Security
Explanation

CEplus.com

Explanation/Reference:
Section: Software Development Security

QUESTION 20
Which of the following is a web application control that should be put into place to prevent exploitation of Operating System (OS) bugs?

A. Check arguments in function calls
B. Test for the security patch level of the environment
C. Include logging functions
D. Digitally sign each application module

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 21

VCEplus.com

An Intrusion Detection System (IDS) has recently been deployed in a Demilitarized Zone (DMZ). The IDS detects a flood of malformed packets. Which of the following BEST describes what has occurred?

A. Denial of Service (DoS) attack
B. Address Resolution Protocol (ARP) spoof
C. Buffer overflow
D. Ping flood attack

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 22
Which of the following command line tools can be used in the reconnaissance phase of a network vulnerability assessment?

VCEplus.com

A. dig
B. ipconfig
C. ifconfig
D. nbstat

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 23
In configuration management, what baseline configuration information MUST be maintained for each computer system?

A. Operating system and version, patch level, applications running, and versions.
B. List of system changes, test reports, and change approvals
C. Last vulnerability assessment report and initial risk assessment report
D. Date of last update, test report, and accreditation certificate

CEplus.com

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 24
Which Radio Frequency Interference (RFI) phenomenon associated with bundled cable runs can create information leakage?

A. Transference
B. Covert channel
C. Bleeding
D. Cross-talk

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

CEplus.com

QUESTION 25
An organization's information security strategic plan MUST be reviewed

A. whenever there are significant changes to a major application.
B. quarterly, when the organization's strategic plan is updated.
C. whenever there are major changes to the business.
D. every three years, when the organization's strategic plan is updated.

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 26
When building a data classification scheme, which of the following is the PRIMARY concern?

CEplus.com

A. Purpose
B. Cost effectiveness
C. Availability
D. Authenticity

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 27
Which technology is a prerequisite for populating the cloud-based directory in a federated identity solution?

A. Notification tool
B. Message queuing tool
C. Security token tool
D. Synchronization tool

CEplus.com

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 28
What is an advantage of Elliptic Curve Cryptography (ECC)?

A. Cryptographic approach that does not require a fixed-length key
B. Military-strength security that does not depend upon secrecy of the algorithm
C. Opportunity to use shorter keys for the same level of security
D. Ability to use much longer keys for greater security

Correct Answer: C
Section: Software Development Security

CEplus.com

Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 29
Backup information that is critical to the organization is identified through a

A. Vulnerability Assessment (VA).
B. Business Continuity Plan (BCP).
C. Business Impact Analysis (BIA).
D. data recovery analysis.

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

CEplus.com

QUESTION 30
When using Generic Routing Encapsulation (GRE) tunneling over Internet Protocol version 4 (IPv4), where is the GRE header inserted?

A. Into the options field
B. Between the delivery header and payload
C. Between the source and destination addresses
D. Into the destination address

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 31
An application developer is deciding on the amount of idle session time that the application allows before a timeout. The BEST reason for determining the session timeout requirement is

VCEplus.com

A. organization policy.
B. industry best practices.
C. industry laws and regulations.
D. management feedback.

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 32
Knowing the language in which an encrypted message was originally produced might help a cryptanalyst to perform a

A. clear-text attack.
B. known cipher attack.
C. frequency analysis.
D. stochastic assessment.

VCEplus.com

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 33
During the Security Assessment and Authorization process, what is the PRIMARY purpose for conducting a hardware and software inventory?

A. Calculate the value of assets being accredited.
B. Create a list to include in the Security Assessment and Authorization package.
C. Identify obsolete hardware and software.
D. Define the boundaries of the information system.

Correct Answer: A
Section: Software Development Security
Explanation

VCEplus.com

Explanation/Reference:
Section: Software Development Security

QUESTION 34
When evaluating third-party applications, which of the following is the GREATEST responsibility of Information Security?

A. Accept the risk on behalf of the organization.
B. Report findings to the business to determine security gaps.
C. Quantify the risk to the business for product selection.
D. Approve the application that best meets security requirements.

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 35
An employee of a retail company has been granted an extended leave of absence by Human Resources (HR). This information has been formally communicated to the access provisioning team. Which of the following is the BEST action to take?

VCEplus.com

A. Revoke access temporarily.
B. Block user access and delete user account after six months.
C. Block access to the offices immediately.
D. Monitor account usage temporarily.

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 36
The goal of a Business Impact Analysis (BIA) is to determine which of the following?

A. Cost effectiveness of business recovery

CEplus.com

B. Cost effectiveness of installing software security patches
C. Resource priorities for recovery and Maximum Tolerable Downtime (MTD)
D. Which security measures should be implemented

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 37
An organization publishes and periodically updates its employee policies in a file on their intranet. Which of the following is a PRIMARY security concern?

A. Ownership
B. Confidentiality
C. Availability
D. Integrity

CEplus.com

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 38
What does the Maximum Tolerable Downtime (MTD) determine?

A. The estimated period of time a business critical database can remain down before customers are affected.
B. The fixed length of time a company can endure a disaster without any Disaster Recovery (DR) planning
C. The estimated period of time a business can remain interrupted beyond which it risks never recovering
D. The fixed length of time in a DR process before redundant systems are engaged

Correct Answer: C
Section: Software Development Security
Explanation

VCEplus.com

Explanation/Reference:
Section: Software Development Security

QUESTION 39
What is a characteristic of Secure Sockets Layer (SSL) and Transport Layer Security (TLS)?

A. SSL and TLS provide a generic channel security mechanism on top of Transmission Control Protocol (TCP).
B. SSL and TLS provide nonrepudiation by default.
C. SSL and TLS do not provide security for most routed protocols.
D. SSL and TLS provide header encapsulation over HyperText Transfer Protocol (HTTP).

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 40
How does a Host Based Intrusion Detection System (HIDS) identify a potential attack?

VCEplus.com

A. Examines log messages or other indications on the system.
B. Monitors alarms sent to the system administrator
C. Matches traffic patterns to virus signature files
D. Examines the Access Control List (ACL)

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 41
From a cryptographic perspective, the service of non-repudiation includes which of the following features?

A. Validity of digital certificates
B. Validity of the authorization rules
C. Proof of authenticity of the message

CEplus.com

D. Proof of integrity of the message

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 42
Which of the following BEST represents the concept of least privilege?

A. Access to an object is denied unless access is specifically allowed.
B. Access to an object is only available to the owner.
C. Access to an object is allowed unless it is protected by the information security policy.
D. Access to an object is only allowed to authenticated users via an Access Control List (ACL).

Correct Answer: A
Section: Software Development Security
Explanation

CEplus.com

Explanation/Reference:
Section: Software Development Security

QUESTION 43
Which of the following is an advantage of on-premise Credential Management Systems?

A. Lower infrastructure capital costs
B. Control over system configuration
C. Reduced administrative overhead
D. Improved credential interoperability

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

CEplus.com

QUESTION 44
Which of the following approaches is the MOST effective way to dispose of data on multiple hard drives?

A. Delete every file on each drive.
B. Destroy the partition table for each drive using the command line.
C. Degauss each drive individually.
D. Perform multiple passes on each drive using approved formatting methods.

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 45
Which of the following BEST describes Recovery Time Objective (RTO)?

CEplus.com

A. Time of application resumption after disaster
B. Time of application verification after disaster.
C. Time of data validation after disaster.
D. Time of data restoration from backup after disaster.

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 46
Which of the following is the PRIMARY benefit of a formalized information classification program?

A. It minimized system logging requirements.
B. It supports risk assessment.
C. It reduces asset vulnerabilities.
D. It drives audit processes.

CEplus.com

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 47
Which of the following is the BEST method to reduce the effectiveness of phishing attacks?

A. User awareness
B. Two-factor authentication
C. Anti-phishing software
D. Periodic vulnerability scan

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

CEplus.com

QUESTION 48
The PRIMARY purpose of accreditation is to:

A. comply with applicable laws and regulations.
B. allow senior management to make an informed decision regarding whether to accept the risk of operating the system.
C. protect an organization's sensitive data.
D. verify that all security controls have been implemented properly and are operating in the correct manner.

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 49
Which of the following is a weakness of Wired Equivalent Privacy (WEP)?

CEplus.com

A. Length of Initialization Vector (IV)
B. Protection against message replay
C. Detection of message tampering
D. Built-in provision to rotate keys

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 50
When writing security assessment procedures, what is the MAIN purpose of the test outputs and reports?

A. To force the software to fail and document the process
B. To find areas of compromise in confidentiality and integrity
C. To allow for objective pass or fail decisions
D. To identify malware or hidden code within the test results

CEplus.com

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 51
Which of the following is the MAIN reason for using configuration management?

A. To provide centralized administration
B. To reduce the number of changes
C. To reduce errors during upgrades
D. To provide consistency in security controls

Correct Answer: D
Section: Software Development Security

VCEplus.com

Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 52
Which of the following is BEST suited for exchanging authentication and authorization messages in a multi-party decentralized environment?

A. Lightweight Directory Access Protocol (LDAP)
B. Security Assertion Markup Language (SAML)
C. Internet Mail Access Protocol
D. Transport Layer Security (TLS)

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

VCEplus.com

QUESTION 53
Which of the following is MOST important when deploying digital certificates?

A. Validate compliance with X.509 digital certificate standards
B. Establish a certificate life cycle management framework
C. Use a third-party Certificate Authority (CA)
D. Use no less than 256-bit strength encryption when creating a certificate

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 54
A user sends an e-mail request asking for read-only access to files that are not considered sensitive. A Discretionary Access Control (DAC) methodology is in place. Which is the MOST suitable approach that the administrator should take?

CEplus.com

A. Administrator should request data owner approval to the user access
B. Administrator should request manager approval for the user access
C. Administrator should directly grant the access to the non-sensitive files
D. Administrator should assess the user access need and either grant or deny the access

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 55
How should an organization determine the priority of its remediation efforts after a vulnerability assessment has been conducted?

A. Use an impact-based approach.
B. Use a risk-based approach.
C. Use a criticality-based approach.
D. Use a threat-based approach.

CEplus.com

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 56
Which of the following is the MOST important consideration when developing a Disaster Recovery Plan (DRP)?

A. The dynamic reconfiguration of systems
B. The cost of downtime
C. A recovery strategy for all business processes
D. A containment strategy

Correct Answer: B
Section: Software Development Security
Explanation

VCEplus.com

Explanation/Reference:
Section: Software Development Security

QUESTION 57
A proxy firewall operates at what layer of the Open System Interconnection (OSI) model?

A. Transport
B. Data link
C. Network
D. Application

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 58
Which of the following restricts the ability of an individual to carry out all the steps of a particular process?

A. Job rotation
B. Separation of duties
C. Least privilege
D. Mandatory vacations

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 59
Although code using a specific program language may not be susceptible to a buffer overflow attack,

A. most calls to plug-in programs are susceptible.
B. most supporting application code is susceptible.

CEplus.com

C. the graphical images used by the application could be susceptible.
D. the supporting virtual machine could be susceptible.

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 60
What is the BEST way to encrypt web application communications?

A. Secure Hash Algorithm 1 (SHA-1)
B. Secure Sockets Layer (SSL)
C. Cipher Block Chaining Message Authentication Code (CBC-MAC)
D. Transport Layer Security (TLS)

CEplus.com

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 61
Which of the following are effective countermeasures against passive network-layer attacks?

A. Federated security and authenticated access controls
B. Trusted software development and run time integrity controls
C. Encryption and security enabled applications
D. Enclave boundary protection and computing environment defense

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

VCEplus.com

QUESTION 62
What is the MOST important element when considering the effectiveness of a training program for Business Continuity (BC) and Disaster Recovery (DR)?

A. Management support
B. Consideration of organizational need
C. Technology used for delivery
D. Target audience

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 63
A database administrator is asked by a high-ranking member of management to perform specific changes to the accounting system database. The administrator is specifically instructed to not track or evidence the change in a ticket. Which of the following is the BEST course of action?

VCEplus.com

A. Ignore the request and do not perform the change.
B. Perform the change as requested, and rely on the next audit to detect and report the situation.
C. Perform the change, but create a change ticket regardless to ensure there is complete traceability.
D. Inform the audit committee or internal audit directly using the corporate whistleblower process.

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 64
Which of the following is the MOST important goal of information asset valuation?

A. Developing a consistent and uniform method of controlling access on information assets
B. Developing appropriate access control policies and guidelines
C. Assigning a financial value to an organization's information assets

CEplus.com

D. Determining the appropriate level of protection

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 65
Which of the following is a strategy of grouping requirements in developing a Security Test and Evaluation (ST&E)?

A. Tactical, strategic, and financial
B. Management, operational, and technical
C. Documentation, observation, and manual
D. Standards, policies, and procedures

Correct Answer: B
Section: Software Development Security
Explanation

CEplus.com

Explanation/Reference:
Section: Software Development Security

QUESTION 66
Which one of the following activities would present a significant security risk to organizations when employing a Virtual Private Network (VPN) solution?

A. VPN bandwidth
B. Simultaneous connection to other networks
C. Users with Internet Protocol (IP) addressing conflicts
D. Remote users with administrative rights

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

CEplus.com

QUESTION 67
Which of the following BEST describes a chosen plaintext attack?

A. The cryptanalyst can generate ciphertext from arbitrary text.
B. The cryptanalyst examines the communication being sent back and forth.
C. The cryptanalyst can choose the key and algorithm to mount the attack.
D. The cryptanalyst is presented with the ciphertext from which the original message is determined.

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 68
For network based evidence, which of the following contains traffic details of all network sessions in order to detect anomalies?

CEplus.com

A. Alert data
B. User data
C. Content data
D. Statistical data

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 69
Which of the following is the PRIMARY reason to perform regular vulnerability scanning of an organization network?

A. Provide vulnerability reports to management.
B. Validate vulnerability remediation activities.
C. Prevent attackers from discovering vulnerabilities.
D. Remediate known vulnerabilities.

VCEplus.com

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 70
Which of the following would BEST describe the role directly responsible for data within an organization?

A. Data custodian
B. Information owner
C. Database administrator
D. Quality control

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

VCEplus.com

QUESTION 71
The restoration priorities of a Disaster Recovery Plan (DRP) are based on which of the following documents?

A. Service Level Agreement (SLA)
B. Business Continuity Plan (BCP)
C. Business Impact Analysis (BIA)
D. Crisis management plan

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 72
The PRIMARY outcome of a certification process is that it provides documented

CEplus.com

A. interconnected systems and their implemented security controls.
B. standards for security assessment, testing, and process evaluation.
C. system weakness for remediation.
D. security analyses needed to make a risk-based decision.

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 73
A security architect plans to reference a Mandatory Access Control (MAC) model for implementation. This indicates that which of the following properties are being prioritized?

A. Confidentiality
B. Integrity
C. Availability
D. Accessibility

CEplus.com

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

Mandatory Access Control (MAC) is system-enforced access control based on a subject's clearance and an object's labels. Subjects and Objects have clearances and labels, respectively, such as confidential, secret, and top secret. A subject may access an object only if the subject's clearance is equal to or greater than the object's label. Subjects cannot share objects with other subjects who lack the proper clearance, or "write down" objects to a lower classification level (such as from top secret to secret). MAC systems are usually focused on preserving the confidentiality of data.
Reference: https://www.sciencedirect.com/topics/computer-science/mandatory-access-control

QUESTION 74
A vulnerability in which of the following components would be MOST difficult to detect?

CEplus.com

A. Kernel
B. Shared libraries
C. Hardware
D. System application

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 75
During which of the following processes is least privilege implemented for a user account?

A. Provision
B. Approve
C. Request
D. Review

CEplus.com

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 76
Which of the following is a document that identifies each item seized in an investigation, including date and time seized, full name and signature or initials of the person who seized the item, and a detailed description of the item?

A. Property book
B. Chain of custody form
C. Search warrant return
D. Evidence tag

Correct Answer: B
Section: Software Development Security

CEplus.com

Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 77
Which of the following is needed to securely distribute symmetric cryptographic keys?

A. Officially approved Public-Key Infrastructure (PKI) Class 3 or Class 4 certificates
B. Officially approved and compliant key management technology and processes
C. An organizationally approved communication protection policy and key management plan
D. Hardware tokens that protect the user's private key.

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

CEplus.com

QUESTION 78
Reciprocal backup site agreements are considered to be

A. a better alternative than the use of warm sites.
B. difficult to test for complex systems.
C. easy to implement for similar types of organizations.
D. easy to test and implement for complex systems.

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 79
In which identity management process is the subject's identity established?

A. Trust

CEplus.com

B. Provisioning
C. Authorization
D. Enrollment

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 80
In order to assure authenticity, which of the following are required?

A. Confidentiality and authentication
B. Confidentiality and integrity
C. Authentication and non-repudiation
D. Integrity and non-repudiation

CEplus.com

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 81
At which layer of the Open Systems Interconnect (OSI) model are the source and destination address for a datagram handled?

A. Transport Layer
B. Data-Link Layer
C. Network Layer
D. Application Layer

Correct Answer: C
Section: Software Development Security
Explanation

VCEplus.com

Explanation/Reference:
Section: Software Development Security

QUESTION 82
An organization regularly conducts its own penetration tests. Which of the following scenarios MUST be covered for the test to be effective?

A. Third-party vendor with access to the system
B. System administrator access compromised
C. Internal attacker with access to the system
D. Internal user accidentally accessing data

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 83
A company was ranked as high in the following National Institute of Standards and Technology (NIST) functions: Protect, Detect, Respond and Recover. However, a low maturity grade was attributed to the Identify function. In which of the following the controls categories does this company need to improve when analyzing its processes individually?

A. Asset Management, Business Environment, Governance and Risk Assessment
B. Access Control, Awareness and Training, Data Security and Maintenance
C. Anomalies and Events, Security Continuous Monitoring and Detection Processes
D. Recovery Planning, Improvements and Communications

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 84
What is the difference between media marking and media labeling?

A. Media marking refers to the use of human-readable security attributes, while media labeling refers to the use of security attributes in internal data structures.

CEplus.com

B. Media labeling refers to the use of human-readable security attributes, while media marking refers to the use of security attributes in internal data structures.
C. Media labeling refers to security attributes required by public policy/law, while media marking refers to security required by internal organizational policy.
D. Media marking refers to security attributes required by public policy/law, while media labeling refers to security attributes required by internal organizational policy.

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 85
What balance MUST be considered when web application developers determine how informative application error messages should be constructed?

A. Risk versus benefit
B. Availability versus auditability
C. Confidentiality versus integrity
D. Performance versus user satisfaction

CEplus.com

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 86
What operations role is responsible for protecting the enterprise from corrupt or contaminated media?

A. Information security practitioner
B. Information librarian
C. Computer operator
D. Network administrator

Correct Answer: B
Section: Software Development Security
Explanation

VCEplus.com

Explanation/Reference:
Section: Software Development Security

QUESTION 87
Which of the following is a characteristic of the initialization vector when using Data Encryption Standard (DES)?

A. It must be known to both sender and receiver.
B. It can be transmitted in the clear as a random number.
C. It must be retained until the last block is transmitted.
D. It can be used to encrypt and decrypt information.

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 88
In general, servers that are facing the Internet should be placed in a demilitarized zone (DMZ). What is MAIN purpose of the DMZ?

VCEplus.com

A. Reduced risk to internal systems.
B. Prepare the server for potential attacks.
C. Mitigate the risk associated with the exposed server.
D. Bypass the need for a firewall.

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 89
Network-based logging has which advantage over host-based logging when reviewing malicious activity about a victim machine?

A. Addresses and protocols of network-based logs are analyzed.
B. Host-based system logging has files stored in multiple locations.

CEplus.com

C. Properly handled network-based logs may be more reliable and valid.
D. Network-based systems cannot capture users logging into the console.

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 90
Which of the following is the PRIMARY reason for employing physical security personnel at entry points in facilities where card access is in operation?

A. To verify that only employees have access to the facility.
B. To identify present hazards requiring remediation.
C. To monitor staff movement throughout the facility.
D. To provide a safe environment for employees.

CEplus.com

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 91
Between which pair of Open System Interconnection (OSI) Reference Model layers are routers used as a communications device?

A. Transport and Session
B. Data-Link and Transport
C. Network and Session
D. Physical and Data-Link

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

VCEplus.com

QUESTION 92
Which type of security testing is being performed when an ethical hacker has no knowledge about the target system but the testing target is notified before the test?

A. Reversal
B. Gray box
C. Blind
D. White box

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 93
Which of the following countermeasures is the MOST effective in defending against a social engineering attack?

VCEplus.com

A. Mandating security policy acceptance
B. Changing individual behavior
C. Evaluating security awareness training
D. Filtering malicious e-mail content

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 94
Which of the following information MUST be provided for user account provisioning?

A. Full name
B. Unique identifier
C. Security question

VCEplus.com

D. Date of birth

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 95
Which of the following adds end-to-end security inside a Layer 2 Tunneling Protocol (L2TP) Internet Protocol Security (IPSec) connection?

A. Temporal Key Integrity Protocol (TKIP)
B. Secure Hash Algorithm (SHA)
C. Secure Shell (SSH)
D. Transport Layer Security (TLS)

Correct Answer: B
Section: Software Development Security
Explanation

VCEplus.com

Explanation/Reference:
Section: Software Development Security

QUESTION 96
A company has decided that they need to begin maintaining assets deployed in the enterprise. What approach should be followed to determine and maintain ownership information to bring the company into compliance?

A. Enterprise asset management framework
B. Asset baseline using commercial off the shelf software
C. Asset ownership database using domain login records
D. A script to report active user logins on assets

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

CEplus.com

QUESTION 97
In the Software Development Life Cycle (SDLC), maintaining accurate hardware and software inventories is a critical part of

A. systems integration.
B. risk management.
C. quality assurance.
D. change management.

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 98
As a best practice, the Security Assessment Report (SAR) should include which of the following sections?

CEplus.com

A. Data classification policy
B. Software and hardware inventory
C. Remediation recommendations
D. Names of participants

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 99
The application of a security patch to a product previously validate at Common Criteria (CC) Evaluation Assurance Level (EAL) 4 would

A. require an update of the Protection Profile (PP).
B. require recertification.
C. retain its current EAL rating.
D. reduce the product to EAL 3.

VCEplus.com

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Section: Software Development Security

QUESTION 100
Which of the following media sanitization techniques is MOST likely to be effective for an organization using public cloud services?

A. Low-level formatting
B. Secure-grade overwrite erasure
C. Cryptographic erasure
D. Drive degaussing

Correct Answer: B
Section: Software Development Security
Explanation

VCEplus.com

Explanation/Reference:
Section: Software Development Security