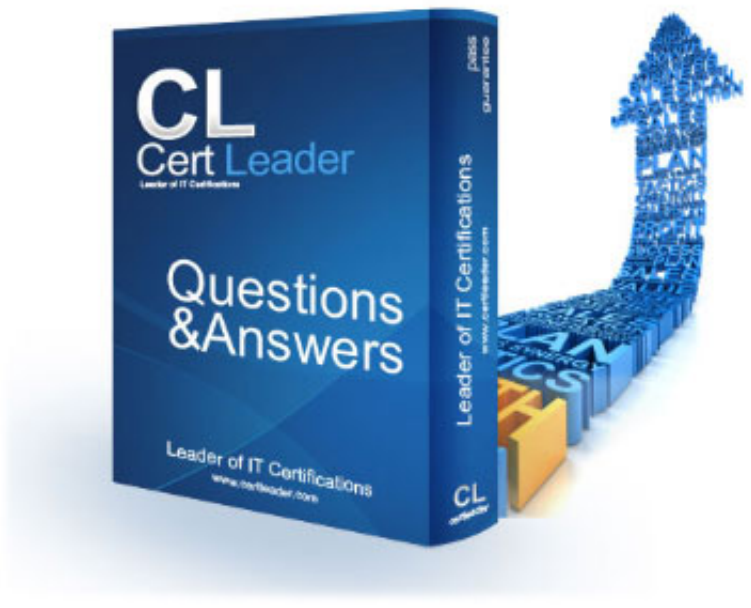
CISSP Dumps

Certified Information Systems Security Professional (CISSP)

https://www.certleader.com/CISSP-dumps.html



NEW QUESTION 1
- (Exam Topic 1)
An important principle of defense in depth is that achieving information security requires a balanced focus on which PRIMARY elements?

A. Development, testing, and deployment
B. Prevention, detection, and remediation
C. People, technology, and operations
D. Certification, accreditation, and monitoring

Answer: C

NEW QUESTION 2
- (Exam Topic 2)
In a data classification scheme, the data is owned by the

A. system security managers
B. business managers
C. Information Technology (IT) managers
D. end users

Answer: B

NEW QUESTION 3
- (Exam Topic 2)
Which of the following is an initial consideration when developing an information security management system?

A. Identify the contractual security obligations that apply to the organizations
B. Understand the value of the information assets
C. Identify the level of residual risk that is tolerable to management
D. Identify relevant legislative and regulatory compliance requirements

Answer: B

NEW QUESTION 4
- (Exam Topic 2)
Which of the following is MOST important when assigning ownership of an asset to a department?

A. The department should report to the business owner
B. Ownership of the asset should be periodically reviewed
C. Individual accountability should be ensured
D. All members should be trained on their responsibilities

Answer: B

NEW QUESTION 5
- (Exam Topic 2)
An organization has doubled in size due to a rapid market share increase. The size of the Information Technology (IT) staff has maintained pace with this growth. The organization hires several contractors whose onsite time is limited. The IT department has pushed its limits building servers and rolling out workstations and has a backlog of account management requests.
Which contract is BEST in offloading the task from the IT staff?

A. Platform as a Service (PaaS)
B. Identity as a Service (IDaaS)
C. Desktop as a Service (DaaS)
D. Software as a Service (SaaS)

Answer: B

NEW QUESTION 6
- (Exam Topic 3)
What is the second phase of Public Key Infrastructure (PKI) key/certificate life-cycle management?

A. Implementation Phase
B. Initialization Phase
C. Cancellation Phase
D. Issued Phase

Answer: D

NEW QUESTION 7
- (Exam Topic 4)
At what level of the Open System Interconnection (OSI) model is data at rest on a Storage Area Network (SAN) located?

A. Link layer
B. Physical layer

C. Session layer
D. Application layer

Answer: D

NEW QUESTION 8
- (Exam Topic 5)
A manufacturing organization wants to establish a Federated Identity Management (FIM) system with its 20 different supplier companies. Which of the following is the BEST solution for the manufacturing organization?

A. Trusted third-party certification
B. Lightweight Directory Access Protocol (LDAP)
C. Security Assertion Markup language (SAML)
D. Cross-certification

Answer: C

NEW QUESTION 9
- (Exam Topic 5)
Users require access rights that allow them to view the average salary of groups of employees. Which control would prevent the users from obtaining an individual employee's salary?

A. Limit access to predefined queries
B. Segregate the database into a small number of partitions each with a separate security level
C. Implement Role Based Access Control (RBAC)
D. Reduce the number of people who have access to the system for statistical purposes

Answer: C

NEW QUESTION 10
- (Exam Topic 5)
What is the BEST approach for controlling access to highly sensitive information when employees have the same level of security clearance?

A. Audit logs
B. Role-Based Access Control (RBAC)
C. Two-factor authentication
D. Application of least privilege

Answer: B

NEW QUESTION 10
- (Exam Topic 5)
Which of the following BEST describes an access control method utilizing cryptographic keys derived from a smart card private key that is embedded within mobile devices?

A. Derived credential
B. Temporary security credential
C. Mobile device credentialing service
D. Digest authentication

Answer: A

NEW QUESTION 11
- (Exam Topic 6)
Which of the following could cause a Denial of Service (DoS) against an authentication system?

A. Encryption of audit logs
B. No archiving of audit logs
C. Hashing of audit logs
D. Remote access audit logs

Answer: D

NEW QUESTION 12
- (Exam Topic 6)
Which of the following is of GREATEST assistance to auditors when reviewing system configurations?

A. Change management processes
B. User administration procedures
C. Operating System (OS) baselines
D. System backup documentation

Answer: A

NEW QUESTION 14

- (Exam Topic 6)
Which of the following is a PRIMARY benefit of using a formalized security testing report format and structure?

A. Executive audiences will understand the outcomes of testing and most appropriate next steps for corrective actions to be taken
B. Technical teams will understand the testing objectives, testing strategies applied, and business risk associated with each vulnerability
C. Management teams will understand the testing objectives and reputational risk to the organization
D. Technical and management teams will better understand the testing objectives, results of each test phase, and potential impact levels

Answer: D

NEW QUESTION 16
- (Exam Topic 7)
What would be the MOST cost effective solution for a Disaster Recovery (DR) site given that the organization's systems cannot be unavailable for more than 24 hours?

A. Warm site
B. Hot site
C. Mirror site
D. Cold site

Answer: A

NEW QUESTION 18
- (Exam Topic 7)
Which of the following is a PRIMARY advantage of using a third-party identity service?

A. Consolidation of multiple providers
B. Directory synchronization
C. Web based logon
D. Automated account management

Answer: D

NEW QUESTION 23
- (Exam Topic 7)
What is the PRIMARY reason for implementing change management?

A. Certify and approve releases to the environment
B. Provide version rollbacks for system changes
C. Ensure that all applications are approved
D. Ensure accountability for changes to the environment

Answer: D

NEW QUESTION 28
- (Exam Topic 7)
When is a Business Continuity Plan (BCP) considered to be valid?

A. When it has been validated by the Business Continuity (BC) manager
B. When it has been validated by the board of directors
C. When it has been validated by all threat scenarios
D. When it has been validated by realistic exercises

Answer: D

NEW QUESTION 30
- (Exam Topic 8)
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

Answer: D

NEW QUESTION 35
- (Exam Topic 9)
What is the FIRST step in developing a security test and its evaluation?

A. Determine testing methods
B. Develop testing procedures
C. Identify all applicable security requirements
D. Identify people, processes, and products not in compliance

Answer: C

NEW QUESTION 39
- (Exam Topic 9)
Which of the following is the FIRST action that a system administrator should take when it is revealed during a penetration test that everyone in an organization has unauthorized access to a server holding sensitive data?

A. Immediately document the finding and report to senior management.
B. Use system privileges to alter the permissions to secure the server
C. Continue the testing to its completion and then inform IT management
D. Terminate the penetration test and pass the finding to the server management team

Answer: A

NEW QUESTION 40
- (Exam Topic 9)
To prevent inadvertent disclosure of restricted information, which of the following would be the LEAST effective process for eliminating data prior to the media being discarded?

A. Multiple-pass overwriting
B. Degaussing
C. High-level formatting
D. Physical destruction

Answer: C

NEW QUESTION 42
- (Exam Topic 9)
Contingency plan exercises are intended to do which of the following?

A. Train personnel in roles and responsibilities
B. Validate service level agreements
C. Train maintenance personnel
D. Validate operation metrics

Answer: A

NEW QUESTION 44
- (Exam Topic 9)
Why is a system's criticality classification important in large organizations?

A. It provides for proper prioritization and scheduling of security and maintenance tasks.
B. It reduces critical system support workload and reduces the time required to apply patches.
C. It allows for clear systems status communications to executive management.
D. It provides for easier determination of ownership, reducing confusion as to the status of the asset.

Answer: A

NEW QUESTION 46
- (Exam Topic 9)
Which security action should be taken FIRST when computer personnel are terminated from their jobs?

A. Remove their computer access
B. Require them to turn in their badge
C. Conduct an exit interview
D. Reduce their physical access level to the facility

Answer: A

NEW QUESTION 50
- (Exam Topic 9)
The type of authorized interactions a subject can have with an object is

A. control.
B. permission.
C. procedure.
D. protocol.

Answer: B

NEW QUESTION 53
- (Exam Topic 9)
Multi-threaded applications are more at risk than single-threaded applications to

A. race conditions.
B. virus infection.
C. packet sniffing.
D. database injection.

Answer: A

NEW QUESTION 54
- (Exam Topic 9)
An advantage of link encryption in a communications network is that it

A. makes key management and distribution easier.
B. protects data from start to finish through the entire network.
C. improves the efficiency of the transmission.
D. encrypts all information, including headers and routing information.

Answer: D

NEW QUESTION 57
- (Exam Topic 9)
In a financial institution, who has the responsibility for assigning the classification to a piece of information?

A. Chief Financial Officer (CFO)
B. Chief Information Security Officer (CISO)
C. Originator or nominated owner of the information
D. Department head responsible for ensuring the protection of the information

Answer: C

NEW QUESTION 62
- (Exam Topic 9)
What security management control is MOST often broken by collusion?

A. Job rotation
B. Separation of duties
C. Least privilege model
D. Increased monitoring

Answer: B

NEW QUESTION 65
- (Exam Topic 9)
Which of the following is a strategy of grouping requirements in developing a Security Test and Evaluation (ST&E)?

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

Answer: C

NEW QUESTION 70
- (Exam Topic 9)
The PRIMARY purpose of a security awareness program is to

A. ensure that everyone understands the organization's policies and procedures.
B. communicate that access to information will be granted on a need-to-know basis.
C. warn all users that access to all systems will be monitored on a daily basis.
D. comply with regulations related to data and information protection.

Answer: A

NEW QUESTION 71
- (Exam Topic 9)
Which of the following does the Encapsulating Security Payload (ESP) provide?

A. Authorization and integrity
B. Availability and integrity
C. Integrity and confidentiality
D. Authorization and confidentiality

Answer: C

NEW QUESTION 73
- (Exam Topic 9)
A practice that permits the owner of a data object to grant other users access to that object would usually provide

A. Mandatory Access Control (MAC).
B. owner-administered control.
C. owner-dependent access control.

D. Discretionary Access Control (DAC).

Answer: D

NEW QUESTION 74
- (Exam Topic 9)
Which of the following assessment metrics is BEST used to understand a system's vulnerability to potential exploits?

A. Determining the probability that the system functions safely during any time period
B. Quantifying the system's available services
C. Identifying the number of security flaws within the system
D. Measuring the system's integrity in the presence of failure

Answer: C

NEW QUESTION 76
- (Exam Topic 9)
An auditor carrying out a compliance audit requests passwords that are encrypted in the system to verify that the passwords are compliant with policy. Which of the following is the BEST response to the auditor?

A. Provide the encrypted passwords and analysis tools to the auditor for analysis.
B. Analyze the encrypted passwords for the auditor and show them the results.
C. Demonstrate that non-compliant passwords cannot be created in the system.
D. Demonstrate that non-compliant passwords cannot be encrypted in the system.

Answer: C

NEW QUESTION 77
- (Exam Topic 9)
Which of the following statements is TRUE for point-to-point microwave transmissions?

A. They are not subject to interception due to encryption.
B. Interception only depends on signal strength.
C. They are too highly multiplexed for meaningful interception.
D. They are subject to interception by an antenna within proximity.

Answer: D

NEW QUESTION 79
- (Exam Topic 9)
Which of the following is a security limitation of File Transfer Protocol (FTP)?

A. Passive FTP is not compatible with web browsers.
B. Anonymous access is allowed.
C. FTP uses Transmission Control Protocol (TCP) ports 20 and 21.
D. Authentication is not encrypted.

Answer: D

NEW QUESTION 82
- (Exam Topic 9)
Which one of the following effectively obscures network addresses from external exposure when implemented on a firewall or router?

A. Network Address Translation (NAT)
B. Application Proxy
C. Routing Information Protocol (RIP) Version 2
D. Address Masking

Answer: A

NEW QUESTION 84
- (Exam Topic 9)
In Business Continuity Planning (BCP), what is the importance of documenting business processes?

A. Provides senior management with decision-making tools
B. Establishes and adopts ongoing testing and maintenance strategies
C. Defines who will perform which functions during a disaster or emergency
D. Provides an understanding of the organization's interdependencies

Answer: D

NEW QUESTION 86
- (Exam Topic 9)
What principle requires that changes to the plaintext affect many parts of the ciphertext?

A. Diffusion
B. Encapsulation
C. Obfuscation
D. Permutation

Answer: A

NEW QUESTION 87
- (Exam Topic 9)
Which one of the following is a fundamental objective in handling an incident?

A. To restore control of the affected systems
B. To confiscate the suspect's computers
C. To prosecute the attacker
D. To perform full backups of the system

Answer: A

NEW QUESTION 88
- (Exam Topic 9)
What maintenance activity is responsible for defining, implementing, and testing updates to application systems?

A. Program change control
B. Regression testing
C. Export exception control
D. User acceptance testing

Answer: A

NEW QUESTION 91
- (Exam Topic 9)
What is the MOST important purpose of testing the Disaster Recovery Plan (DRP)?

A. Evaluating the efficiency of the plan
B. Identifying the benchmark required for restoration
C. Validating the effectiveness of the plan
D. Determining the Recovery Time Objective (RTO)

Answer: C

NEW QUESTION 96
- (Exam Topic 9)
Passive Infrared Sensors (PIR) used in a non-climate controlled environment should

A. reduce the detected object temperature in relation to the background temperature.
B. increase the detected object temperature in relation to the background temperature.
C. automatically compensate for variance in background temperature.
D. detect objects of a specific temperature independent of the background temperature.

Answer: C

NEW QUESTION 99
- (Exam Topic 9)
When designing a vulnerability test, which one of the following is likely to give the BEST indication of what components currently operate on the network?

A. Topology diagrams
B. Mapping tools
C. Asset register
D. Ping testing

Answer: B

NEW QUESTION 104
- (Exam Topic 9)
Which of the following is the BEST mitigation from phishing attacks?

A. Network activity monitoring
B. Security awareness training
C. Corporate policy and procedures
D. Strong file and directory permissions

Answer: B

NEW QUESTION 105
- (Exam Topic 9)

Which one of the following affects the classification of data?

A. Passage of time
B. Assigned security label
C. Multilevel Security (MLS) architecture
D. Minimum query size

Answer: A

NEW QUESTION 109
- (Exam Topic 9)
Why must all users be positively identified prior to using multi-user computers?

A. To provide access to system privileges
B. To provide access to the operating system
C. To ensure that unauthorized persons cannot access the computers
D. To ensure that management knows what users are currently logged on

Answer: C

NEW QUESTION 114
- (Exam Topic 9)
Two companies wish to share electronic inventory and purchase orders in a supplier and client relationship. What is the BEST security solution for them?

A. Write a Service Level Agreement (SLA) for the two companies.
B. Set up a Virtual Private Network (VPN) between the two companies.
C. Configure a firewall at the perimeter of each of the two companies.
D. Establish a File Transfer Protocol (FTP) connection between the two companies.

Answer: B

NEW QUESTION 115
- (Exam Topic 10)
Which of the following is a process within a Systems Engineering Life Cycle (SELC) stage?

A. Requirements Analysis
B. Development and Deployment
C. Production Operations
D. Utilization Support

Answer: A

NEW QUESTION 118
- (Exam Topic 10)
Which of the following describes the concept of a Single Sign-On (SSO) system?

A. Users are authenticated to one system at a time.
B. Users are identified to multiple systems with several credentials.
C. Users are authenticated to multiple systems with one login.
D. Only one user is using the system at a time.

Answer: C

NEW QUESTION 120
- (Exam Topic 10)
Which of the following is the MOST difficult to enforce when using cloud computing?

A. Data access
B. Data backup
C. Data recovery
D. Data disposal

Answer: D

NEW QUESTION 125
- (Exam Topic 10)
Which of the following methods provides the MOST protection for user credentials?

A. Forms-based authentication
B. Digest authentication
C. Basic authentication
D. Self-registration

Answer: B

NEW QUESTION 126

- (Exam Topic 10)
Refer to the information below to answer the question.
A new employee is given a laptop computer with full administrator access. This employee does not have a personal computer at home and has a child that uses the computer to send and receive e-mail, search the web, and use instant messaging. The organization's Information Technology (IT) department discovers that a peer-to-peer program has been installed on the computer using the employee's access.
Which of the following documents explains the proper use of the organization's assets?

A. Human resources policy
B. Acceptable use policy
C. Code of ethics
D. Access control policy

Answer: B

NEW QUESTION 129
- (Exam Topic 10)
Which of the following is the BEST solution to provide redundancy for telecommunications links?

A. Provide multiple links from the same telecommunications vendor.
B. Ensure that the telecommunications links connect to the network in one location.
C. Ensure that the telecommunications links connect to the network in multiple locations.
D. Provide multiple links from multiple telecommunications vendors.

Answer: D

NEW QUESTION 130
- (Exam Topic 10)
Which of the following actions MUST be taken if a vulnerability is discovered during the maintenance stage in a System Development Life Cycle (SDLC)?

A. Make changes following principle and design guidelines.
B. Stop the application until the vulnerability is fixed.
C. Report the vulnerability to product owner.
D. Monitor the application and review code.

Answer: C

NEW QUESTION 132
- (Exam Topic 10)
During the procurement of a new information system, it was determined that some of the security requirements were not addressed in the system specification.
Which of the following is the MOST likely reason for this?

A. The procurement officer lacks technical knowledge.
B. The security requirements have changed during the procurement process.
C. There were no security professionals in the vendor's bidding team.
D. The description of the security requirements was insufficient.

Answer: D

NEW QUESTION 137
- (Exam Topic 10)
Which of the following problems is not addressed by using OAuth (Open Standard to Authorization) 2.0 to integrate a third-party identity provider for a service?

A. Resource Servers are required to use passwords to authenticate end users.
B. Revocation of access of some users of the third party instead of all the users from the third party.
C. Compromise of the third party means compromise of all the users in the service.
D. Guest users need to authenticate with the third party identity provider.

Answer: C

NEW QUESTION 139
- (Exam Topic 10)
Refer to the information below to answer the question.
A new employee is given a laptop computer with full administrator access. This employee does not have a personal computer at home and has a child that uses the computer to send and receive e-mail, search the web, and use instant messaging. The organization's Information Technology (IT) department discovers that a peer-to-peer program has been installed on the computer using the employee's access.
Which of the following could have MOST likely prevented the Peer-to-Peer (P2P) program from being installed on the computer?

A. Removing employee's full access to the computer
B. Supervising their child's use of the computer
C. Limiting computer's access to only the employee
D. Ensuring employee understands their business conduct guidelines

Answer: A

NEW QUESTION 141
- (Exam Topic 10)
Host-Based Intrusion Protection (HIPS) systems are often deployed in monitoring or learning mode during their initial implementation. What is the objective of

starting in this mode?

A. Automatically create exceptions for specific actions or files
B. Determine which files are unsafe to access and blacklist them
C. Automatically whitelist actions or files known to the system
D. Build a baseline of normal or safe system events for review

Answer: D

NEW QUESTION 146
- (Exam Topic 10)
The use of proximity card to gain access to a building is an example of what type of security control?

A. Legal
B. Logical
C. Physical
D. Procedural

Answer: C

NEW QUESTION 150
- (Exam Topic 10)
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.
In addition to authentication at the start of the user session, best practice would require re-authentication

A. periodically during a session.
B. for each business process.
C. at system sign-off.
D. after a period of inactivity.

Answer: D

NEW QUESTION 151
- (Exam Topic 10)
An organization decides to implement a partial Public Key Infrastructure (PKI) with only the servers having digital certificates. What is the security benefit of this implementation?

A. Clients can authenticate themselves to the servers.
B. Mutual authentication is available between the clients and servers.
C. Servers are able to issue digital certificates to the client.
D. Servers can authenticate themselves to the client.

Answer: D

NEW QUESTION 154
- (Exam Topic 10)
Which of the following secure startup mechanisms are PRIMARILY designed to thwart attacks?

A. Timing
B. Cold boot
C. Side channel
D. Acoustic cryptanalysis

Answer: B

NEW QUESTION 158
- (Exam Topic 10)
From a security perspective, which of the following is a best practice to configure a Domain Name Service (DNS) system?

A. Configure secondary servers to use the primary server as a zone forwarder.
B. Block all Transmission Control Protocol (TCP) connections.
C. Disable all recursive queries on the name servers.
D. Limit zone transfers to authorized devices.

Answer: D

NEW QUESTION 163
- (Exam Topic 10)
Without proper signal protection, embedded systems may be prone to which type of attack?

A. Brute force
B. Tampering
C. Information disclosure
D. Denial of Service (DoS)

Answer: C

NEW QUESTION 167
- (Exam Topic 10)
Which of the following is the BEST way to determine if a particular system is able to identify malicious software without executing it?

A. Testing with a Botnet
B. Testing with an EICAR file
C. Executing a binary shellcode
D. Run multiple antivirus programs

Answer: B

NEW QUESTION 169
- (Exam Topic 10)
Which of the following is the PRIMARY benefit of a formalized information classification program?

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

Answer: B

NEW QUESTION 171
- (Exam Topic 10)
Which of the following provides the MOST protection against data theft of sensitive information when a laptop is stolen?

A. Set up a BIOS and operating system password
B. Encrypt the virtual drive where confidential files can be stored
C. Implement a mandatory policy in which sensitive data cannot be stored on laptops, but only on the corporate network
D. Encrypt the entire disk and delete contents after a set number of failed access attempts

Answer: D

NEW QUESTION 172
- (Exam Topic 10)
What is the MOST important reason to configure unique user IDs?

A. Supporting accountability
B. Reducing authentication errors
C. Preventing password compromise
D. Supporting Single Sign On (SSO)

Answer: A

NEW QUESTION 173
- (Exam Topic 11)
Which of the following prevents improper aggregation of privileges in Role Based Access Control (RBAC)?

A. Hierarchical inheritance
B. Dynamic separation of duties
C. The Clark-Wilson security model
D. The Bell-LaPadula security model

Answer: B

NEW QUESTION 178
- (Exam Topic 11)
A health care provider is considering Internet access for their employees and patients. Which of the following is the organization's MOST secure solution for protection of data?

A. Public Key Infrastructure (PKI) and digital signatures
B. Trusted server certificates and passphrases
C. User ID and password
D. Asymmetric encryption and User ID

Answer: A

NEW QUESTION 181
- (Exam Topic 11)
What is the MOST effective method of testing custom application code?

A. Negative testing
B. White box testing

C. Penetration testing
D. Black box testing

Answer: B

NEW QUESTION 185
- (Exam Topic 11)
Which of the following BEST describes a Protection Profile (PP)?

A. A document that expresses an implementation independent set of security requirements for an IT product that meets specific consumer needs.
B. A document that is used to develop an IT security product from its security requirements definition.
C. A document that expresses an implementation dependent set of security requirements which contains only the security functional requirements.
D. A document that represents evaluated products where there is a one-to-one correspondence between a PP and a Security Target (ST).

Answer: A

NEW QUESTION 190
- (Exam Topic 11)
After a thorough analysis, it was discovered that a perpetrator compromised a network by gaining access to the network through a Secure Socket Layer (SSL) Virtual Private Network (VPN) gateway. The perpetrator guessed a username and brute forced the password to gain access. Which of the following BEST mitigates this issue?

A. Implement strong passwords authentication for VPN
B. Integrate the VPN with centralized credential stores
C. Implement an Internet Protocol Security (IPSec) client
D. Use two-factor authentication mechanisms

Answer: D

NEW QUESTION 192
- (Exam Topic 11)
Which of the following PRIMARILY contributes to security incidents in web-based applications?

A. Systems administration and operating systems
B. System incompatibility and patch management
C. Third-party applications and change controls
D. Improper stress testing and application interfaces

Answer: C

NEW QUESTION 193
- (Exam Topic 11)
Regarding asset security and appropriate retention, which of the following INITIAL top three areas are important to focus on?

A. Security control baselines, access controls, employee awareness and training
B. Human resources, asset management, production management
C. Supply chain lead time, inventory control, encryption
D. Polygraphs, crime statistics, forensics

Answer: A

NEW QUESTION 197
- (Exam Topic 11)
What is an important characteristic of Role Based Access Control (RBAC)?

A. Supports Mandatory Access Control (MAC)
B. Simplifies the management of access rights
C. Relies on rotation of duties
D. Requires two factor authentication

Answer: B

NEW QUESTION 200
- (Exam Topic 11)
Which of the following disaster recovery test plans will be MOST effective while providing minimal risk?

A. Read-through
B. Parallel
C. Full interruption
D. Simulation

Answer: B

NEW QUESTION 202
- (Exam Topic 11)

Which of the following standards/guidelines requires an Information Security Management System (ISMS) to be defined?

A. International Organization for Standardization (ISO) 27000 family
B. Information Technology Infrastructure Library (ITIL)
C. Payment Card Industry Data Security Standard (PCIDSS)
D. ISO/IEC 20000

Answer: A

NEW QUESTION 203
- (Exam Topic 11)
Which of the following roles has the obligation to ensure that a third party provider is capable of processing and handling data in a secure manner and meeting the standards set by the organization?

A. Data Custodian
B. Data Owner
C. Data Creator
D. Data User

Answer: B

NEW QUESTION 205
- (Exam Topic 11)
What is the MOST efficient way to secure a production program and its data?

A. Disable default accounts and implement access control lists (ACL)
B. Harden the application and encrypt the data
C. Disable unused services and implement tunneling
D. Harden the servers and backup the data

Answer: B

NEW QUESTION 207
- (Exam Topic 11)
Which of the following are Systems Engineering Life Cycle (SELC) Technical Processes?

A. Concept, Development, Production, Utilization, Support, Retirement
B. Stakeholder Requirements Definition, Architectural Design, Implementation, Verification, Operation
C. Acquisition, Measurement, Configuration Management, Production, Operation, Support
D. Concept, Requirements, Design, Implementation, Production, Maintenance, Support, Disposal

Answer: B

NEW QUESTION 210
- (Exam Topic 11)
An organization has hired a security services firm to conduct a penetration test. Which of the following will the organization provide to the tester?

A. Limits and scope of the testing.
B. Physical location of server room and wiring closet.
C. Logical location of filters and concentrators.
D. Employee directory and organizational chart.

Answer: A

NEW QUESTION 214
- (Exam Topic 11)
Which of the following BEST describes a rogue Access Point (AP)?

A. An AP that is not protected by a firewall
B. An AP not configured to use Wired Equivalent Privacy (WEP) with Triple Data Encryption Algorithm (3DES)
C. An AP connected to the wired infrastructure but not under the management of authorized network administrators
D. An AP infected by any kind of Trojan or Malware

Answer: C

NEW QUESTION 218
- (Exam Topic 11)
To protect auditable information, which of the following MUST be configured to only allow read access?

A. Logging configurations
B. Transaction log files
C. User account configurations
D. Access control lists (ACL)

Answer: B

NEW QUESTION 221
- (Exam Topic 11)
The BEST example of the concept of "something that a user has" when providing an authorized user access to a computing system is

A. the user's hand geometry.
B. a credential stored in a token.
C. a passphrase.
D. the user's face.

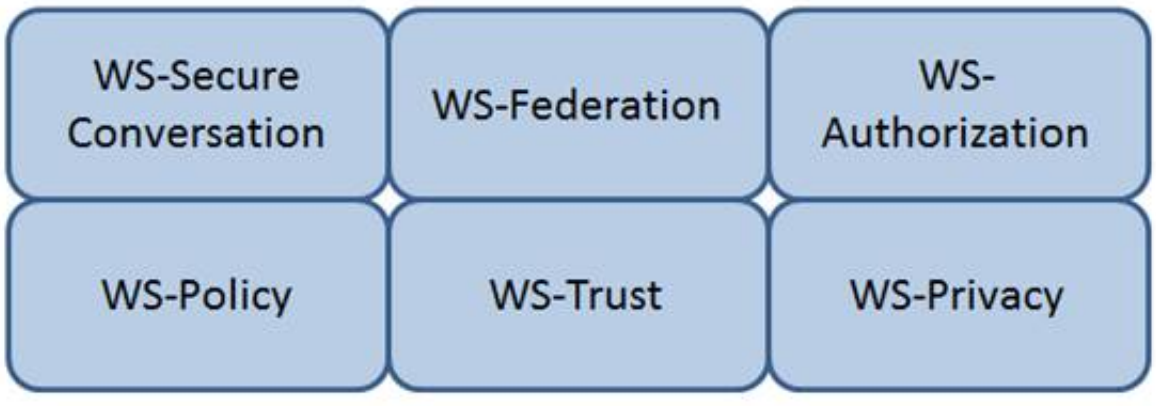
Answer: B

NEW QUESTION 222
- (Exam Topic 11)
What type of encryption is used to protect sensitive data in transit over a network?

A. Payload encryption and transport encryption
B. Authentication Headers (AH)
C. Keyed-Hashing for Message Authentication
D. Point-to-Point Encryption (P2PE)

Answer: A

NEW QUESTION 225
- (Exam Topic 11)
Which Web Services Security (WS-Security) specification maintains a single authenticated identity across multiple dissimilar environments? Click on the correct specification in the image below.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
WS-Federation
Reference: Java Web Services: Up and Running" By Martin Kalin page 228

NEW QUESTION 230
- (Exam Topic 11)
A security professional is asked to provide a solution that restricts a bank teller to only perform a savings deposit transaction but allows a supervisor to perform corrections after the transaction. Which of the following is the MOST effective solution?

A. Access is based on rules.
B. Access is determined by the system.
C. Access is based on user's role.
D. Access is based on data sensitivity.

Answer: C

NEW QUESTION 232
- (Exam Topic 11)
For privacy protected data, which of the following roles has the highest authority for establishing dissemination rules for the data?

A. Information Systems Security Officer
B. Data Owner

C. System Security Architect
D. Security Requirements Analyst

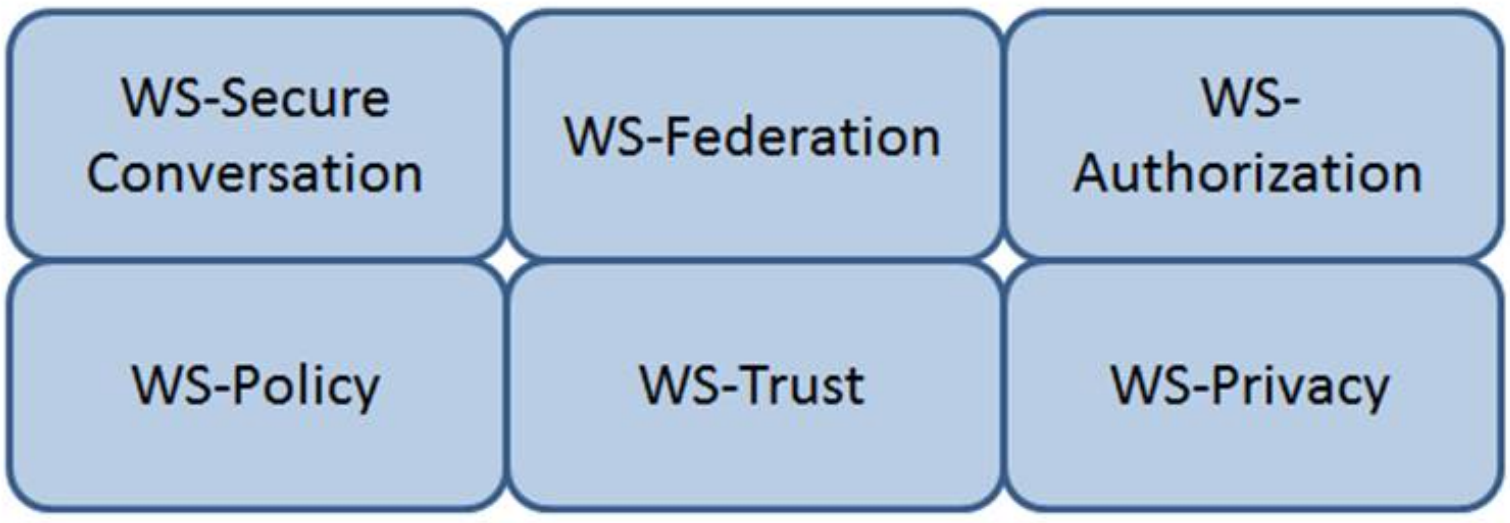
Answer: B

NEW QUESTION 235
- (Exam Topic 11)
Which of the following statements is TRUE regarding value boundary analysis as a functional software testing technique?

A. It is useful for testing communications protocols and graphical user interfaces.
B. It is characterized by the stateless behavior of a process implemented in a function.
C. Test inputs are obtained from the derived threshold of the given functional specifications.
D. An entire partition can be covered by considering only one representative value from that partition.

Answer: C

NEW QUESTION 240
- (Exam Topic 11)
Which Web Services Security (WS-Security) specification negotiates how security tokens will be issued, renewed and validated? Click on the correct specification in the image below.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
WS-Trust
The protocol used for issuing security tokens is based on WS-Trust. WS-Trust is a Web service specification that builds on WS-Security. It describes a protocol used for issuance, exchange, and validation of security tokens. WS-Trust provides a solution for interoperability by defining a protocol for issuing and exchanging security tokens, based on token format, namespace, or trust boundaries.
Reference: https://msdn.microsoft.com/en-us/library/ff650503.aspx

NEW QUESTION 242
- (Exam Topic 11)
Sensitive customer data is going to be added to a database. What is the MOST effective implementation for ensuring data privacy?

A. Discretionary Access Control (DAC) procedures
B. Mandatory Access Control (MAC) procedures
C. Data link encryption
D. Segregation of duties

Answer: B

NEW QUESTION 243
- (Exam Topic 11)

Data leakage of sensitive information is MOST often concealed by which of the following?

A. Secure Sockets Layer (SSL)
B. Secure Hash Algorithm (SHA)
C. Wired Equivalent Privacy (WEP)
D. Secure Post Office Protocol (POP)

Answer: A

NEW QUESTION 245
- (Exam Topic 11)
What does an organization FIRST review to assure compliance with privacy requirements?

A. Best practices
B. Business objectives
C. Legal and regulatory mandates
D. Employee's compliance to policies and standards

Answer: C

NEW QUESTION 249
- (Exam Topic 11)
An organization has decided to contract with a cloud-based service provider to leverage their identity as a service offering. They will use Open Authentication (OAuth) 2.0 to authenticate external users to the organization's services.
As part of the authentication process, which of the following must the end user provide?

A. An access token
B. A username and password
C. A username
D. A password

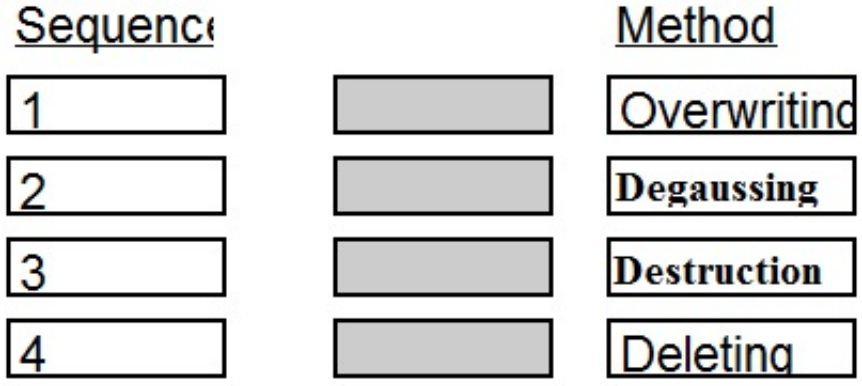
Answer: A

NEW QUESTION 253
- (Exam Topic 11)
Which one of the following is a common risk with network configuration management?

A. Patches on the network are difficult to keep current.
B. It is the responsibility of the systems administrator.
C. User ID and passwords are never set to expire.
D. Network diagrams are not up to date.

Answer: D

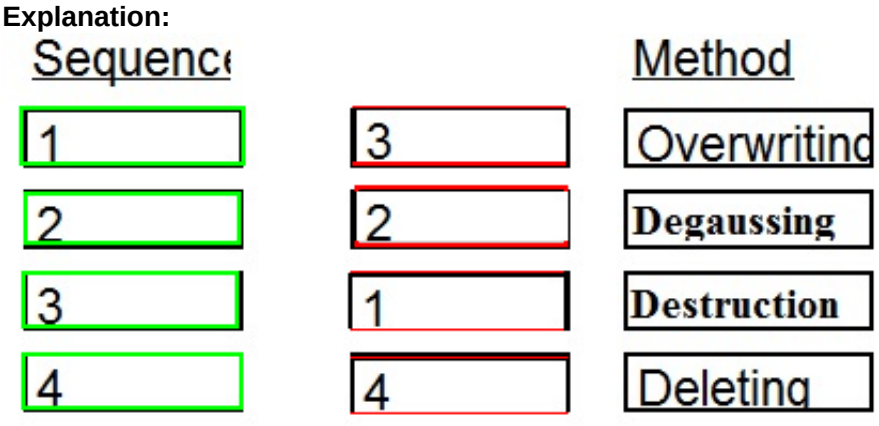
NEW QUESTION 254
- (Exam Topic 11)
Place in order, from BEST (1) to WORST (4), the following methods to reduce the risk of data remanence on magnetic mediA.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 256
- (Exam Topic 11)
The PRIMARY outcome of a certification process is that it provides documented

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

Answer: D

NEW QUESTION 260
- (Exam Topic 11)
What security risk does the role-based access approach mitigate MOST effectively?

A. Excessive access rights to systems and data
B. Segregation of duties conflicts within business applications
C. Lack of system administrator activity monitoring
D. Inappropriate access requests

Answer: A

NEW QUESTION 264
- (Exam Topic 11)
Which of the following is a recommended alternative to an integrated email encryption system?

A. Sign emails containing sensitive data
B. Send sensitive data in separate emails
C. Encrypt sensitive data separately in attachments
D. Store sensitive information to be sent in encrypted drives

Answer: C

NEW QUESTION 267
- (Exam Topic 11)
Which of the following protocols would allow an organization to maintain a centralized list of users that can read a protected webpage?

A. Lightweight Directory Access Control (LDAP)
B. Security Assertion Markup Language (SAML)
C. Hypertext Transfer Protocol (HTTP)
D. Kerberos

Answer: A

NEW QUESTION 271
- (Exam Topic 11)
Which of the following is the PRIMARY issue when collecting detailed log information?

A. Logs may be unavailable when required
B. Timely review of the data is potentially difficult
C. Most systems and applications do not support logging
D. Logs do not provide sufficient details of system and individual activities

Answer: B

NEW QUESTION 272
- (Exam Topic 11)
By carefully aligning the pins in the lock, which of the following defines the opening of a mechanical lock without the proper key?

A. Lock pinging
B. Lock picking
C. Lock bumping
D. Lock bricking

Answer: B

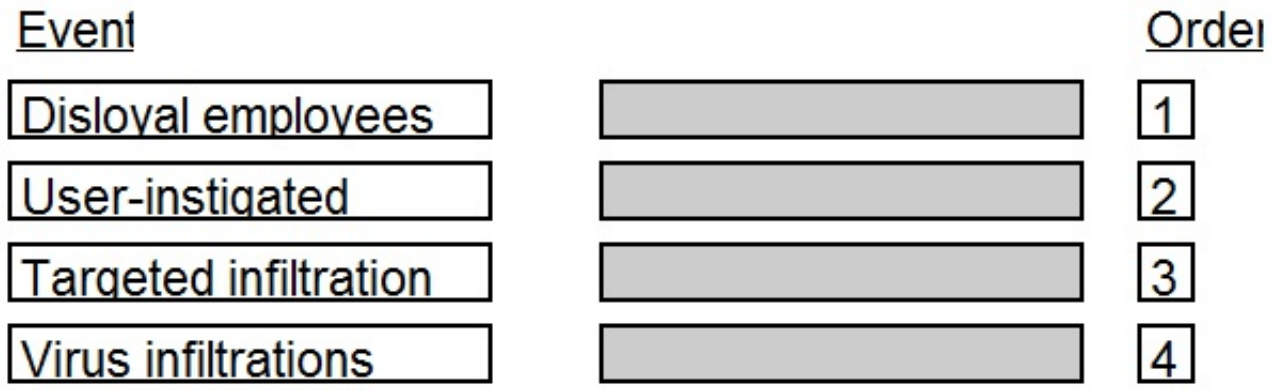
NEW QUESTION 276
- (Exam Topic 11)
Which of the following could elicit a Denial of Service (DoS) attack against a credential management system?

A. Delayed revocation or destruction of credentials
B. Modification of Certificate Revocation List
C. Unauthorized renewal or re-issuance
D. Token use after decommissioning

Answer:

B

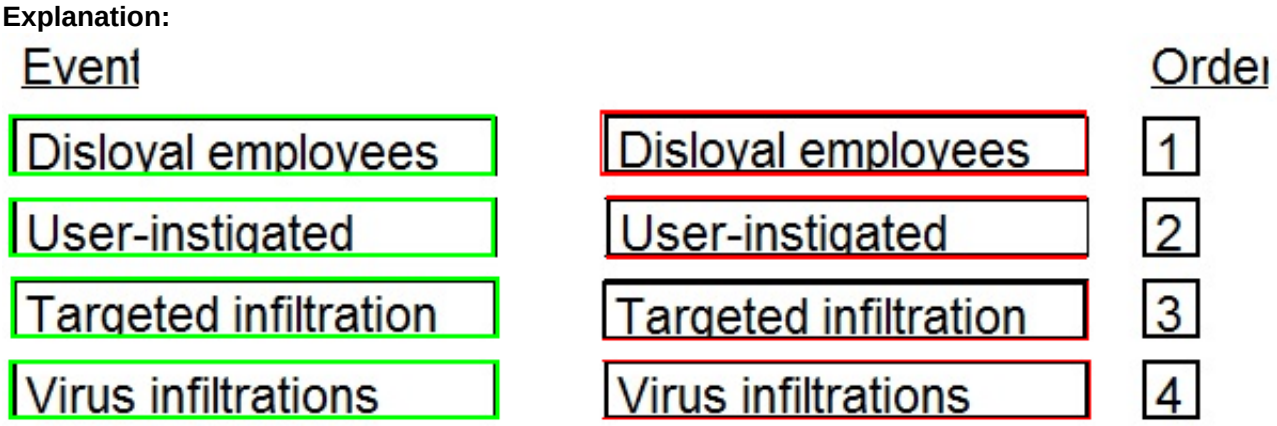
NEW QUESTION 280
- (Exam Topic 11)
In which order, from MOST to LEAST impacted, does user awareness training reduce the occurrence of the events below?



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 282
- (Exam Topic 12)
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.

Answer: B

NEW QUESTION 285
- (Exam Topic 12)
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

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

Answer: A

NEW QUESTION 288
- (Exam Topic 12)
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

Answer: B

NEW QUESTION 291
- (Exam Topic 12)
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

Answer: B

NEW QUESTION 295
- (Exam Topic 12)
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

Answer: B

NEW QUESTION 300
- (Exam Topic 12)
Determining outage costs caused by a disaster can BEST be measured by the

A. cost of redundant systems and backups.
B. cost to recover from an outage.
C. overall long-term impact of the outage.
D. revenue lost during the outage.

Answer: C

NEW QUESTION 302
- (Exam Topic 12)
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.
C. the graphical images used by the application could be susceptible.
D. the supporting virtual machine could be susceptible.

Answer: C

NEW QUESTION 306
- (Exam Topic 12)
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.

Answer: D

NEW QUESTION 308
- (Exam Topic 12)
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

Answer: C

NEW QUESTION 309
- (Exam Topic 12)
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

Answer: C

NEW QUESTION 314
- (Exam Topic 12)

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
D. Proof of integrity of the message

Answer: C

NEW QUESTION 317
- (Exam Topic 12)
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.

Answer: C

NEW QUESTION 320
- (Exam Topic 12)
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.

Answer: B

NEW QUESTION 325
- (Exam Topic 12)
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.

Answer: B

NEW QUESTION 328
- (Exam Topic 12)
What is a characteristic of Secure Socket 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).

Answer: A

NEW QUESTION 329
- (Exam Topic 13)
Which of the following is the MOST effective method to mitigate Cross-Site Scripting (XSS) attacks?

A. Use Software as a Service (SaaS)
B. Whitelist input validation
C. Require client certificates
D. Validate data output

Answer: B

NEW QUESTION 332
- (Exam Topic 13)
Who is responsible for the protection of information when it is shared with or provided to other organizations?

A. Systems owner
B. Authorizing Official (AO)
C. Information owner
D. Security officer

Answer: C

Explanation:

Section: Security Operations

NEW QUESTION 334
- (Exam Topic 13)
What protocol is often used between gateway hosts on the Internet?

A. Exterior Gateway Protocol (EGP)
B. Border Gateway Protocol (BGP)
C. Open Shortest Path First (OSPF)
D. Internet Control Message Protocol (ICMP)

Answer: B

NEW QUESTION 339
- (Exam Topic 13)
What is the PRIMARY role of a scrum master in agile development?

A. To choose the primary development language
B. To choose the integrated development environment
C. To match the software requirements to the delivery plan
D. To project manage the software delivery

Answer: D

NEW QUESTION 343
- (Exam Topic 13)
Drag the following Security Engineering terms on the left to the BEST definition on the right.

Security Engineering Term		Definition
Risk		A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of
Security Risk Treatment		The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.
Protection Needs Assessment		The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
Threat Assessment		The method used to identify feasible security risk mitigation options and plans.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Risk - A measure of the extent to which an entity is threatened by a potential circumstance of event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence.
Protection Needs Assessment - The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should be asset be lost, modified, degraded, disrupted, compromised, or become unavailable.
Threat assessment - The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
Security Risk Treatment - The method used to identify feasible security risk mitigation options and plans.

NEW QUESTION 348
- (Exam Topic 13)
An organization has outsourced its financial transaction processing to a Cloud Service Provider (CSP) who will provide them with Software as a Service (SaaS). If there was a data breach who is responsible for monetary losses?

A. The Data Protection Authority (DPA)

B. The Cloud Service Provider (CSP)
C. The application developers
D. The data owner

Answer: B

NEW QUESTION 352
- (Exam Topic 13)
Mandatory Access Controls (MAC) are based on:

A. security classification and security clearance
B. data segmentation and data classification
C. data labels and user access permissions
D. user roles and data encryption

Answer: A

NEW QUESTION 356
- (Exam Topic 13)
What does electronic vaulting accomplish?

A. It protects critical files.
B. It ensures the fault tolerance of Redundant Array of Independent Disks (RAID) systems
C. It stripes all database records
D. It automates the Disaster Recovery Process (DRP)

Answer: A

Explanation:
Section: Security Operations

NEW QUESTION 359
- (Exam Topic 13)
What is the second step in the identity and access provisioning lifecycle?

A. Provisioning
B. Review
C. Approval
D. Revocation

Answer: B

NEW QUESTION 364
- (Exam Topic 13)
Transport Layer Security (TLS) provides which of the following capabilities for a remote access server?

A. Transport layer handshake compression
B. Application layer negotiation
C. Peer identity authentication
D. Digital certificate revocation

Answer: C

NEW QUESTION 365
- (Exam Topic 13)
Which of the following would MINIMIZE the ability of an attacker to exploit a buffer overflow?

A. Memory review
B. Code review
C. Message division
D. Buffer division

Answer: B

NEW QUESTION 368
- (Exam Topic 13)
A vulnerability assessment report has been submitted to a client. The client indicates that one third of the hosts that were in scope are missing from the report.
In which phase of the assessment was this error MOST likely made?

A. Enumeration
B. Reporting
C. Detection
D. Discovery

Answer: A

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 369
- (Exam Topic 13)
After following the processes defined within the change management plan, a super user has upgraded a device within an Information system.
What step would be taken to ensure that the upgrade did NOT affect the network security posture?

A. Conduct an Assessment and Authorization (A&A)
B. Conduct a security impact analysis
C. Review the results of the most recent vulnerability scan
D. Conduct a gap analysis with the baseline configuration

Answer: B

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 371
- (Exam Topic 13)
Which of the following mandates the amount and complexity of security controls applied to a security risk?

A. Security vulnerabilities
B. Risk tolerance
C. Risk mitigation
D. Security staff

Answer: C

NEW QUESTION 376
- (Exam Topic 13)
Digital certificates used in Transport Layer Security (TLS) support which of the following?

A. Information input validation
B. Non-repudiation controls and data encryption
C. Multi-Factor Authentication (MFA)
D. Server identity and data confidentially

Answer: D

NEW QUESTION 377
- (Exam Topic 13)
What does a Synchronous (SYN) flood attack do?

A. Forces Transmission Control Protocol /Internet Protocol (TCP/IP) connections into a reset state
B. Establishes many new Transmission Control Protocol / Internet Protocol (TCP/IP) connections
C. Empties the queue of pending Transmission Control Protocol /Internet Protocol (TCP/IP) requests
D. Exceeds the limits for new Transmission Control Protocol /Internet Protocol (TCP/IP) connections

Answer: B

NEW QUESTION 382
- (Exam Topic 13)
A minimal implementation of endpoint security includes which of the following?

A. Trusted platforms
B. Host-based firewalls
C. Token-based authentication
D. Wireless Access Points (AP)

Answer: A

NEW QUESTION 387
- (Exam Topic 13)
Which of the following alarm systems is recommended to detect intrusions through windows in a high-noise, occupied environment?

A. Acoustic sensor
B. Motion sensor
C. Shock sensor
D. Photoelectric sensor

Answer: C

NEW QUESTION 390
- (Exam Topic 13)

In a High Availability (HA) environment, what is the PRIMARY goal of working with a virtual router address as the gateway to a network?

A. The second of two routers can periodically check in to make sure that the first router is operational.
B. The second of two routers can better absorb a Denial of Service (DoS) attack knowing the first router is present.
C. The first of two routers fails and is reinstalled, while the second handles the traffic flawlessly.
D. The first of two routers can better handle specific traffic, while the second handles the rest of the traffic seamlessly.

Answer: C

NEW QUESTION 392
- (Exam Topic 13)
Who would be the BEST person to approve an organizations information security policy?

A. Chief Information Officer (CIO)
B. Chief Information Security Officer (CISO)
C. Chief internal auditor
D. Chief Executive Officer (CEO)

Answer: B

Explanation:
Section: Security Operations

NEW QUESTION 393
- (Exam Topic 13)
Which of the following is the BEST metric to obtain when gaining support for an Identify and Access Management (IAM) solution?

A. Application connection successes resulting in data leakage
B. Administrative costs for restoring systems after connection failure
C. Employee system timeouts from implementing wrong limits
D. Help desk costs required to support password reset requests

Answer: D

NEW QUESTION 398
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CISSP Exam with Our Prep Materials Via below:

https://www.certleader.com/CISSP-dumps.html