1

Which of the following is the GREATEST security risk associated with the use of Identity as a Service (IDaaS) when an organization is developing its own software?

A. Incompatibility with Federated Identity Management (FIM)

B. Security Assertion Markup Language (SAML) integration

**C. Increased likelihood of confidentiality breach**

D. Denial of access due to reduced availability

2

Which of the following **MOST** applies to Session Imitation Protocol (SIP) security?

A. It requires a Public Key Infrastructure (PKI).

**B. It reuses security mechanisms derived from existing protocols.**

C. It leverages Hypertext Transfer Protocol (HTTP) over Transport Layer Security (TLS).

D. It supports end-to-end security natively.

3

When are security metrics **MOST** effective?

A. When they are considered as part of a larger and ongoing programmatic approach to security that views Information Technology (IT) security as a true business process and not simply an exercise in controls or technology

B. When they are considered to be accurate and tell the story of security to the board of directors so that business processes can be changed to reduce risk

C. When they are considered to be the means of justifying new people, processes, and/or technology for a business by showing the number of events that have been detected

D. When they are considered to be the means of developing policies and standard and dictating how business is done to ensure there are no security risks

4

Vulnerability scanners may allow for administrator to assign which of the following in order to assist in prioritizing remediation activities

A. Exploit code metrics

**B. Asset Value for networks**

C. Definitions for each exposure type

D. Vulnerability attack vectors

5

Which of the following is the FIRST step in data classification

A Perform a critically analysis

**B. Establish ownership**

C. Create a data dictionary

D. Define access rules

6

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 implementation

D. System initiation

7

What is the PRIMARY advantage of using automated application security testing tools?

**A. Large amounts of code can be tested using fewer resources.**

B. The application will fall less when tested using these tools.

C. Detailed testing of code functions can be performed.

D. The application can be protected in the production environment.

8

The information security staff is comparing the percentage of access control system login accounts that are explicitly linked to an employee in the organization's employee roster. Which of the following does this metric expose?

**A. The potential number of application access accounts that do not belong to current employees**

B. The number of access accounts that overlap organizational responsibility groups

C. The existence of secret application access accounts

D. The number of access accounts that have not been confirmed to have a continuing need

9

Which of the following could be a source of duress to an employee with access to corporate assets?

A. Shoulder surfing

B. Social engineering

C. Piggybacking

D. Harassment

10

Which of the following technologies are replacing manual user access reviews?

A. Log monitoring solution

B. Automated risk assessment

**C. Identity Access Management (LAM)**

D. Cloud Access Security Broker (CASB)

11

Which of the following criteria is MOST important to be used when classifying data?

A. Intellectual property listing

B. Storage location

C. Recording types of media used

**D. Meeting legal requirements**

12

Which of the following techniques should be used to analyze data packets in order to identify any malicious or harmful traffic flowing through virtual Machines (VM) to gamer ate alerts or take preventive action?

A. Port Scanning

B. Port Monitoring

C. Port Security

**D. Port Mirroring**

13

Which of the following will be the MOST effective in combatting an unknown variant of ransomware that is spreading through an organization?

A. Removal of unused accounts

B. Principle of least privilege

C. Antivirus software

**D. Application filtering firewall**

14

A provider is offering Software as a Service (SaaS) to their customers by hosting their application on a third-party cloud service. Who should determine the confidentiality, availability and integrity requirements of the application?

A. Network provider

B. Customers

C. Software service provider

**D. Cloud Service Provider (CSP)**

15

Which of the following techniques BEST mitigates introducing risk into Supply Chain Risk Management (SCRM)?

A. Address supply chain risk areas for internal and external vulnerabilities.

B. Analyze the likelihood of threat to the supply chain.

**C. Impose tight controls on access to the supply chain by approved vendors.**

D. Determine the degree of harm to the supply chain.

16

When considering the Open System Interconnect (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models, which of the following Is the MAIN difference between the two?

A. The TCP/IP model consists of four layers, while the OSI model consists of seven.

B. The TCP/IP model is an enhancement of the OSI model.

**C. The OSI model is used as a reference, while the TCP/IP model has been adopted as the de facto standard.**

D. Both models have been accepted as standards. but implementation varies from organization to organization

17

A security professional working in another country was offered a bribe, and is unsure how to respond. In reviewing the (ISC)2 Code of Ethics, which jurisdiction applies?

A. Country where (ISC)2 certification was earned

B. Country where employer resides

**C. Country where the security professional renders their services**

D. Country where security professional resides

18

Which of the following methods will BEST ensure the Operating System (OS), Including hibernation data, is encrypted?

A. Full Disk Encryption (FDE)

B. Identity-Based Encryption (IBE)

**C. Transparent Data Encryption (TDE)**

D. Triple Data Encryption Algorithm (3DES)

19

The security department wants to make sure that confidential data curtained on laptops about to be e-recycled is protected in the most cost-effective manner. Which of the following is the MOST appropriate sanitizing method to meet the defined requirements?

A. Destroy

**B. Purge**

C. Erase

D. Clear

20

A security professional works for an international company. The security professional has Identified, classified and organized the company's assets. Which of the following MUST be considered prior to implementing security controls?

A. Cost of controls

B. Support of controls

C. User acceptance

**D. Compliance requirements**

21

An organization is considering the virtualization of its environment and moving to a cloud-based hosting service. The security architect for the organization is concerned that moving to a cloud virtualization hosting service is high risk. What is MOST likely the concern of the security architect?

**A. Virtual Machines (VM) could be deployed onto the same physical machine as the organization's VMs and used to compromise the organization's VMs**

B. A Denial of Service (DOS) attack on the cloud-based hosting service could cause the organization's Virtual Machines (VM) to be inaccessible.

C. The cloud-based hosting service could cease operations, causing the organization to lose at hosted information.

D. The security architect has no visibility into the physical hardware that hosts the Virtual Machines (VM), and this hardware may not have sufficient capacity.

22

Which of the following statements is TRUE of Attribute Based Access Control (ABAC)?

**A. In ABAC, attribute values associated with users determine the association of users with privileges.**

B. ABAC pre-defines attributes that carry a specific set of privileges associated with these roles and to which subjects they are assigned.

C. In ABAC, authenticated attributes to objects outside of the subject's originating organization.

D. ABAC attributes assignments are based mostly upon more static organizational positions.

23

A software module creates test events against a website to era re that the website is behaving as expected. Which of the following type of transactions is this module performing?

A. Static transactions

B. Transparent transactions

C. Semantic transactions

**D. Synthetic transactions**

24

A users cell phone has been identified as potential evidence in a legal case. What is the recommended process to secure the device?

**A. Give it to the evidence custodian**

B. Store the device in a personal safe.

C. Lock it in an evidence file cabinet.

D. Give it to the asset manager to store the device.

25

A user is granted access to a new system. When should the user's current access be revoked?

**A. When access to the current system is no longer required**

B. As soon as access to the new system is granted

C. After the request for new access is approved

D. 24 hours after granting access to the new system

26

A data center organization based in the United Kingdom (UK) is looking to provide a Software as a Service (SaaS) portfolio to its customers. The market still does not consider it as a secure service provider. What MUST the organization do in order to demonstrate its security posture?

A. Comply with British Standard (BS) 25999 requirements.

**B. Undergo a Service Organization Control (SOC) 3 audit**

C. Achieve International Standardization Organization (ISO) 27002 certification.

D. Meet Evaluation Assurance Level (EAL) 4 from Common Criteria (CC).

27

Before employees are given access to information and Information Systems (IS), they must understand organizational expectations, policies, handling standards, and consequences of non-compliance. In what two agreements is this information usually codified?

A. Third party use agreement and secrecy agreement

B. Acceptable use agreement and secrecy agreement

C. Non-Disclosure Agreement (NDA) and internal use agreement

**D. Acceptable use agreement and confidentiality agreement**

28

As a generally agreed upon principle, how often should users be required to refresh security awareness training?

A. Every six months

B. Every month

C. Every two years

**D. Every year**

29

The (ISC)2 Code of Ethics is composed of several components. Which components are mandatory?

A. Signature and guidance

B. Preamble, canon, guidance and signature

**C. Preamble and canons**

D. Canons and guidance

30

What access recertification strategy should be used in the event an employee changes role or is terminated?

A. Rotational review

**B. Trigger-based review**

C. Risk review

D. Entitlement review

31

Which of the following is the BEST practice with regards to managing insider threats?

A. Al employees must sign a Non-Disclosure Agreement (NDA).

**B. All data requires the two person rule when viewing.**

C. Ensure all employees wear identification badges

D. Grant access to sensitive data to only those who need to know.

32

An organization has a requirement to continuously procure equipment that will be used to provides service to their customer. How would the organization BEST ensure that it will be able to obtain the equipment that would be needed to satisfy this requirement, as well as being ensured that the equipment will function as expected and required?

A. Use Software Conflagration Management (SCM) processes.

B. Use configuration management

C. Use a single approved vender.

**D. Use Supply Chain Risk Management (SCRM) processes.**

33

An organization contracts with a third-party to assess the effectiveness of its security awareness, education, and training program by comparing its overall security posture with those of its organizational peers. What term BEST describes this approach?

A. Security program benchmarking

B. Industry security risk survey

C. Security training needs assessment

**D. External security risk analysis**

34

Why is security awareness, education, and training required by MOST businesses?

A. Reduces leadership anxiety

**B. Compliance with laws and regulations**

C. Reduces corporate insurance

D. Compliance with corporate audit requirements

35

Which of the following is a defense against Structured Query Language (SQL) injection attacks?

A. Use of stored procedures

B. Use of Transport Layer Security (TLS)

C. Set Hyper Text Transfer Protocol (HTTP) only flag in response header.

**D. Implementation of input validation**

36

Security categorization of a system takes place during which phase of the System Development Life Cycle (SDLC)?

A. System requisition and development

B. System implementation

**C. System initiation**

D. System operators and maintenance

37

An option in the communications sector for long-haul signaling links is SS7 traffic over IP (SS7oIP)using what protocol as "glue"?

A. Encapsulating Security Payload (ESP) over Internet Protocol (IP) or Internet Protocol Security (IPSec)

**B. Reliable User Datagram Protocol (RUDP)**

C. Sequenced Packet Exchange (SPX)

D. Datagram Congestion Control Protocol (DCCP)

38

Which of the following penetration testing techniques can discover an active modem?

A. Eavesdropping

B. War driving

**C. War dialing**

D. Port scanning

39

Which of the following should be the FIRST response to the detection of a major security incident on a system?

A. Acquire a forensic image of the volatile memory.

**B. Immediately power off and take it to the lab.**

C. Acquire a forensic image of the disk storage.

D. Capture the details of open ports and running processes.

40

Which of the following is recommended to establish repeatable processes in a newly implemented network operations center (NOC)

A. Propriety knowledge

**B. Regulatory standards**

C. Related Experiences

D. Applicable framework

41

Asymmetric algorithms are used for which of the following when using Secure Sockets Layer/Transport Layer Security (SSUTLS) for implementing network security?

**A. Payload data encryption**

B. Peer authentication

C. Session encryption

D. Hashing digest

42

What testing method MOST efficiently identifies how code will handle input exceptions?

A. File dump analysis

**B. Fuzzing**

C. Logic validation

D. Code injection

43

Which of the following roles typically works with the Information Security officer (ISO) to ensure information protection, availability, and destruction requirements are met?

A. Information owner

B. Information compliance officer

C. Information user

**D. Information security analyst**

44

Which of the following statements about Multiprotocol Label Switching (MPLS) is correct?

A. Traffic on MPLS networks is not visible to service providers

**B. Provides simpler mechanisms for packet-oriented traffic engineering**

C. Site availability is of no concern for MPLS networks

D. Can replace an encrypted Virtual Private Network (VPN) solution

45

Which of the following is the MOST appropriate action when reusing media that contains sensitive data?

A. Encrypt

**B. Sanitize**

C. Erase

D. Degauss

46

What access control scheme uses fine-grained rules to specify the conditions under which access to each data ten or applications is granted?

**A. Attribute Based Access Control (ABAC)**

B. Mandatory Access Control (MAC)

C. Discretionary Access Control (DAC)

D. Role Based Access Control (RBAC)

47

Which of the following is an organization's BEST possible defense for avoiding penalties for negligence in protecting Personally Identifiable Information (PI)?

A. Perform a background check before hiring.

B. Ensure that the data is encrypted.

C. Observe due diligence procedures.

**D. Make security an integral part of the mission.**

48

Which of the following is TRUE regarding Mandatory Access Control (MAC)?

A. It only deals with authentication of the requester of information.

**B. Access control decisions are beyond the control of the individual owner of an object.**

C. It only deals with identification of the requester of information.

D. Access control decisions are made by the individual owner of the object.

49

Which of the following cryptographic attacks does a salted hashing function help thwart?

**A. Rainbow table attack**

B. Known password attack

C. Plain text attack

D. Known hash attack

50

Which of the following components of access control proves who the user is?

**A. Authentication**

B. Identification

C. Authorization

D. Accounting

51

Which of the following represents the BEST example of Attribute Based Access Control (ABAC)

**A. A user is granted access to a resource only during business hours.**

B. A user is allowed to access a file based on their biometric profile.

C. A user is granted access based on the groups they are in.

D. A user in Human Resources (HR) is granted access to a file share.

52

An asset owner can BEST be identified by which of the following attributes?

A. The individual or unit that supplies the data used by the asset

**B. The individual or unit that is responsible for continued secure operation of the asset**

C. The individual or unit that procured or purchased the asset

D. The business or agency that is using the asset

53

Which data privacy principle specifies that gathering of personal data should be limited to the MINIMUM amount of data required for the purpose for which it is obtained?

A. Accountability

**B. Collection limitation**

C. Retention and destruction

D. Personally Identifiable Information (PO)

54

What is the FIRST step for a digital investigator to perform when using best practices to collect digital evidence from a potential crime scene?

A. Consult the lead investigator to learn the details of the case and required evidence.

B. Assure that grounding procedures have been followed to reduce the loss of digital data due to static electricity discharge.

C. Update the Basic Input Output System (BIOS) and Operating System (OS) of any tools used to assure evidence admissibility.

**D. Confirm that the appropriate warrants were issued to the subject of the investigation to eliminate illegal search claims.**

55

What should a Certified Information Systems Security Professional (CISSP) do when forced to choose between adhering to the (ISC)2 ethics or an employer's unethical request?

**A. Comply with the (ISC)2 Code of ethics.**

B. Temporally suspend membership in (ISC)2 while performing employer's request.

C. Follow the employer's directives and notify (Bo)2 of activity.

D. Provide diligent and competent service to principles.

56

An organization has a firewall layer at the perimeter of its network. It wants to decrease the spread of malicious software internally. Which of the following is the BEST initial way to accomplish this?

**A. Segment the network and deploy firewalls between the segments.**

B. Implement antivirus filtering on the existing firewalls.

C. Deploy Intrusion Prevention Systems (IPS) in key areas of the network.

D. Deploy Intrusion Detection Systems (IDS) and firewalls.

57

In a Security Operations Center (SOC), during which phase of the incident investigation would the following actions MOST likely be performed?

• Disconnecting a system from the network

• Moving an infected system to the quarantine network

• Stopping a service or a process

• Disabling an account

• Adding a firewall rule

A. Analysis

**B. Containment**

C. Closure

D. Resolution

58

When managing access, which of the following is the BEST way to promptly detect serious issues?

A. Require supervisors to review and approve access certifications.

**B. Automate the certification of all access privileges for appropriateness.**

C. Conduct routine reviews of user access privileges and compare any modifications to approved change request tickets.

D. Use event based certifications that are triggered by a change in a user's privileges which then requires review and approval.

59

Which of the following biometric systems typically provides the MOST accuracy?

**A. Iris patterns**

B. Fingerprint scanning

C. Voice recognition

D. Facial imaging

60

An organization decides to use a cloud provider to host their enterprise application. Which of the following roles should decide classification of information stored with the cloud provider?

A. Users of enterprise application

B. The Cloud Provider's External Auditor

C. System Administrator

**D. Information Owner**

61

An auditor recently discovered an organization is not in compliance with security policies and has generated an audit report. Which of the following items should be included in the audit reports final recommendation?

A. Findings, recommendations, estimated cost for remediation

B. Estimated cost for remediation, percentage of risk, management decision

**C. Findings, recommendations, follow-up activities**

D. Findings, control checks, suggested deadlines

62

Which of the following is MOST important to protect against disclosure within an environment using Hardware Security Modules (HSM)?

A. Key distribution

B. Key Encryption Key (KEK)

**C. Root key generation ceremony**

D. Initialization Vector (IV)

63

Procurement groups assist organizations in managing risk by ensuring contracting management processes include a Service Level Agreement (SA) and information security control provisions as part of supplier contract requirements. In addition to continuous monitoring for S.A compliance, what periodic process is required to validate contractual compliance with security obligations?

A. Documentation

**B. Assessment**

C. Research

D. Analysis

64

A security engineer has been tasked with researching various crypto processors for a new system design. The selected crypto processor must provide hardware authentication as well as cryptography. Which crypto processor should be selected?

A. Cyclic Curve

B. Elliptic Curve

C. Field-Programmable Gate Array (FPGA)

**D. Trusted Platform Module (TPM)**

65

Which of the following is the MOST likely benefit a Chief Information Security Officer (CISO) should consider when deciding on a Cloud Service Provider (CSP) to provide cloud asset management?

**A. Replacing large capital expenditures with monthly expenses, and offloading the design of capacity to an Infrastructure as a Service (IaaS) provider**

B. Replacing large capital expenditures with monthly expenses, and offloading capacity planning to an Infrastructure as a Service (laas) provider

C. Computing performance needs before offloading to an Infrastructure as a Service (laaS) provider

D. Computing storage resource needs before offloading to an Infrastructure as a Service (IaaS) provider

66

An information security practitioner has been asked to advise on a Two Factor Authentication (2FA) access control solution focusing on the requirements of being secure and reliable. What solution would meet both of these requirements?

**A. Retinal scanning**

B. Physical token

C. Unique access word

D. Facial scanning

67

An organization is designing a new sales portal. To avoid a loss of revenue, the design requirements include resistance to Denial of Service (DoS) attacks and resilience to disasters or catastrophic system failures. Which of the following security principles is the organization addressing?

A. Confederately

B. Nonrepudiation

**C. Business Continuity (BC)**

D. Availability

68

What is the MAIN purpose for writing planned procedures in the design of Business Continuity Plans (BCP)?

**A. Eliminate unnecessary decision making.**

B. Minimize the risk of failure.

C. Accelerate the recovery process.

D. Establish lines of responsibility.

69

The security officer at an organization wants a security test of the new storage array before it is deployed into production. They have been given Internet Protocol (IP) addresses, Operating System (OS) version information and current protocols that are actively in use. Which of the following is the MOST appropriate initial test scenario?

**A. Gray box test**

B. Resiliency Assessment

C. Penetration Test

D. Vulnerability Assessment

70

A security analyst has been tasked with identifying unauthorized devices connected to the organization's internal network. What is the BEST technique to conduct this task?

A. Penetration testing

B. Vulnerability scanning

C. Log reviews

**D. Network discovery**

71

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. Encrypt attachments.

**B. Digitally sign the message.**

C. Obtain the recipient's private key.

D. Obtain the recipient's digital certificate.

72

An enterprise patch management program is MOST dependent upon which of the following?

**A. Software inventory**

B. Patch testing

C. Timing and prioritization

D. Operating Systems (OS)

73

Which of the following assessment method should used to establish the skill level needed to breach a system?

A. Functional testing

B. Vulnerability testing

C. Regression testing

**D. Penetration testing**

74

Which of the following reports describes the measures that have been implemented or planned to correct any deficiencies noted during the assessment of the security controls and reduce or eliminate known vulnerabilities in the Information System (IS)?

**A Plan of Action and Milestones (POA&M)**

B. Penetration Testing Discovery and Remediation Plan

C. System Assessment Report (SAR)

D. Systems Analysis and Design Flaws Report

75

In an embedded system, an onboard capacitor is rigged to burn out the data and logic circuit of the embedded chip if the chip is tampered with. What type of em bedded system attack would this countermeasure most effectively counter?

A. Timing attacks

B. Side channel attacks

**C. Invasive attacks**

D. Electromagnetic attacks

76

Which of the following is the BEST way to design and employ a security Information and event Management (SIEM) system when utilizing a Security Operations Center (SOC) for further analysis?

A. Limit the number of events collected and reported.

B. Design an elaborate audit reduction system and report all events.

C. Develop context-sensitive tasks for execution and reporting.

**D. Keep the functionality simple and report the most critical events.**

77

Which of the following BEST describes how access to a system is granted to federated user accounts?

**A. With the federation assurance level**

B. Based on defined criteria by the Relying party (RP)

C. Based on defined criteria by the Identity Provider (IdP)

D. With the identity assurance level

78

A company receives an email threat informing of an imminent Distributed Denial of Service (DDoS) attack targeting its web application, unless ransom is paid. Which of the following techniques BEST addresses that threat?

A. Coordinate with and utilize capabilities within Internet Service Provider (ISP)

B. Deploying load balancers to distribute inbound traffic across multiple data centers

C. Set up Web Application Firewalls (WAFs) to filter out malicious traffic

**D. Implementing reverse web-proxies to validate each new inbound connection**

79

Which of the following is mobile device remote fingerprinting?

A. Installing an application to retrieve common characteristics of the device

B. Retrieving the serial number of the mobile device

C. Identifying a device based on common characteristics shared by all devices of a certain type

**D. Storing information about a remote device in a cookie file**

80

What is the MOST common component of a vulnerability management framework?

A. Backup management

**B. Patch management**

C. Risk analysis

D. Threat analysis

81

An audit requires that data must be deleted without remanence after a set period of time according to regulations. The data is stored using a Cloud Service Provider's (CSP) Infrastructure as a Service (laaS). How can it BEST be proven to the auditor that the data was destroyed?

A. Provide a copy of the contract with the CSP that references how data is routinely deleted

B. Request that the CSP ship the media containing the data for destruction on site

C. Obtain access to the cloud server where the database is stored using a web interface and delete the data.

D. Encrypt the data using Advanced Encryption Standard (AES) and destroy the encryption keys

82

Which concept might require users to use a second access token or to re-enter passwords to gain elevated access rights in the identity and access provisioning life cycle?

A. Enrollment

B. Access review

C. Time-based

**D. Least privilege**

83

During a vulnerability assessment, a Distributed Denial of Service (DDoS) vulnerability was identified on a server hosting static assets. What technology BEST mitigates this vulnerability?

A. Platform as a Service (PaaS)

**B. Content Delivery Network (CDN)**

C. Virtual Private Network (VPN)

D. Infrastructure as a Service (laaS)

84

The software development team of a company just finished developing a distributed application that will be used by Human Resources (HR) to track employees' entrance and exits times. During the use of the software, it appears to be a conflict with the Transmission Control Protocol (TCP) ports used by the application since there are another applications already running on the HR server. What would be the MOST likely range of TCP ports to be freely used that could avoid the conflict?

A. Ports 0 through 518

B. Ports 1024 though 49151

**C. Ports 49152 through 65535**

D. Ports 519 through 1023

85

An organization recently conducted a review of the security of its network applications. One of the vulnerabilities found was that the session key used in encrypting sensitive information to a third-party server had been hard-coded in the client and server applications. Which of the following would be **MOST** effective in mitigating this vulnerability?

A Diffie-Hellman (DH) algorithm

**B. Rivest-Shamir-Adleman (RSA) algorithm**

C. Elliptic Curve Cryptography (ECC) algorithm

D. Digital Signature algorithm (DSA)

86

Which of the following is the MOST important activity an organization performs to ensure that security is part of the overall organization culture?

A. Work with senior management to meet business goals.

**B. Ensure security policies are issued to all employees.**

C. Perform formal reviews of security incidents.

D. Manage a program of security audits.

87

As users switch roles within an organization, their accounts are given additional permissions to perform the duties of their new position. After a recent audit, it was discovered that many of these accounts maintained their old permissions as well. The obsolete permissions identified by the audit have been remediated and accounts have only the appropriate permissions to complete their jobs. Which of the following is the BEST way to prevent access privilege creep?

**A. Time-based review and certification**

B. Trigger-based review and certification

C. Implementing Identity Access Management (IAM) solution

D. Internal audit

88

What is the FIRST step an organization should take after It has had breaches of its Information System (IS) and has hired consultants to review its security program?

A. Provide a user training and awareness program.

B. Procure a security information management system.

C. Conduct certification and accreditation of the network.

**D. Implement a risk management process.**

89

Which is the RECOMMENDED configuration mode for sensors far an Intrusion Prevention System (IPS) if the prevention capabilities will be used?

A. Span

B. Inline

**C. Active**

D. Passive

90

Why is a ciphertext-only attack considered one of the most difficult decryption attacks?

A. Because it takes a long time to crack the encryption key

B. Because it requires greater processing power to derive the encryption key

C. Because the data is encrypted with a strong encryption algorithm

**D. Because the source data is unintelligible**

91

within the context of security engineering, what is the ultimate purpose of security risk treatment?

A. Establish security protocols for addressing system risk thorough Systems Engineering Life Cycle (SELC)

B. Eliminate high risk vulnerabilities within the architecture and design of the system

**C. Achieve residual risk that is within the specified risk tolerance of stakeholders**

D. Develop compensating technical controls that address stakeholder concerns

92

Why are mobile devices sometimes difficult to investigate in a forensic examination?

**A. They may have proprietary software installed to protect them.**

B. They have password-based security at logon.

C. There are no forensics tools available for examination.

D. They may contain cryptographic protection.

93

To prevent unauthorized remote access to an organization's public facing systems, which of the following should a security professional implement?

A. Biometric and smart card

B. Username and password

C. Radio Frequency Identification (RFID) and Personal Identification Number (PIN)

**D. Token and password**

94

Which of the following steps should be performed **FIRST** when purchasing Commercial Of-The-Shelf (COTS) software?

A. Harden the hosting server, and perform hosting and application vulnerability scans.

B. Establish policies and procedures on system and services acquisition.

C. Establish a risk management strategy.

**D. Undergo a security assessment as part of authorization process.**

95

A security compliance manager of a large enterprise wants to reduce the time it takes to perform network, system, and application security compliance audits while increasing quality and effectiveness of the results. What should be implemented to **BEST** achieve the desired results?

A. Configuration Management Database (CMDB)

B. Source code repository

C. Configuration Management Plan (CMP)

**D. System performance monitoring application**

96

What is the PRIMARY objective for establishing information asset handling requirements?

A. Dispose of information assets quickly and efficiently to minimize storage costs.

B. Prevent widespread distribution of information assets within an organization.

**C. Protect information assets from unauthorized disclosure, modification, removal or destruction.**

D. Restrict the use of physical media for storing critical information assets.

97

Alternate encoding such as hexadecimal representations is **MOST** often observed in which of the following forms of attack?

A. Cross site scripting (XSS)

B. Denial of Service (DoS)

C. Rootkit exploit

**D. Smurf**

98

Which of the following **BEST** describes a Protection Profile (PP)?

A. A document that expresses an implementation dependent set of security requirements which contains only the security functional requirements.

**B. A document that expresses an implementation independent set of security requirements for an IT product that meets specific consumer needs.**

C. A document that is used to develop an IT security product from its security requirements definition. 0

D. A document that represents evaluated products where there is a one-to-one correspondence between a PP and a Security Target (ST).

99

Which of the below strategies would MOST comprehensively address the risk of malicious insiders leaking sensitive information?

A. Least privilege access, Data Loss Protection (DLP), physical access controls

B. Data Loss Protection (DLP), firewalls, data classification

**C. Staff vetting, least privilege access, Data Loss Protection (DLP)**

D. Background checks, data encryption, web proxies

100

What is the purpose of gathering evidence during the assessment process of a system?

A. Build credibility of the control assessor

B. Compile information to be included in the audit report

C. Create trustworthiness of the assessment results

**D. Provide data for operational status reporting**

101

An organization is considering moving its data center to a virtualized platform. For which of the following technologies would a security practitioner need to create security best practices?

**A. The hypervisor**

B. Network interfaces

C. Application console

D. Virtual ports

102

While developing the asset and information ownership policy for an organization, the security administrator tells the Information Owners (10) they are responsible for their designated information assets. Which of the following are the key responsibilities placed on the IOs?

A. Identify who is responsible for the information, ensure the data is accessible to appropriate users, and archive the data

**B. Determine the impact, identify the Information value, and know when the information should be destroyed**

C. Determine who has need for the data, verify quality of newly added data, and identify who is responsible for the data

D. Identify the information value, ensure the data is accessible to appropriate users, and archive the data

103

Users at an organization's headquarters and regional offices must access the various business units' technology environments. However, each business unit must implement different access controls in order to meet local compliance requirements. Which Identity and Access Management (MI) deployment model would BEST fit the organization?

**A. Confederated**

B. Federated

C. Decentralized

D. Centralized

104

The security management of an organization has recommended a set of security policies and standards that have been approved by senior management. Which of the following MUST be true regarding the policies and standards?

A. Contains a standalone section to address non-employees

**B. Available to all external stakeholders**

C. Applicable to anyone who has access to the corporate network

D. Reviewed by the senior Human Resources (HR) executive

105

Which of the following application security testing and examination techniques is PRIMARILY used to assess the security of individual high-risk compiled components and associated interactions between components?

A. Command injection attacks

B. Distributed Denial of Service (DDoS) attacks

**C. Black box testing**

D. Static testing

106

Which one of the following access controls implements the concept of compartmentalization?

A. Least privilege

B. Discretionary

C. Context-dependent

**D. Mandatory**

107

A security team member was selected as a member of a Change Control Board (CCB) for an organization. Which of the following s one of their responsibilities?

A. Logging the change

**B. Approving or disapproving the change**

C. Carrying out the requested change

D. Determining the impact of the change

108

Which data management role has the primary responsibility to ensure that important datasets are accessible within defined specifications?

A. Administrator

B. Manager

**C. Custodian**

D. Owner

109

A security engineer is tasked with implementing a new identity solution. The client doesn't want to install maintain the infrastructure. Which of the following would qualify as the BEST solution?

A. Active Directory (AD)

**B. Azure Active Directory (AD)**

C. Microsoft Identity Manager (MIM)

D. Active Directory Federation Services (ADFS)

110

If an intrusion causes the system processes to hang, which of the following has been affected?

A. System integrity

B. System confidentiality

**C. System availability**

D. System auditability

111

There is a need to validate and encrypt the entirety of every Internet Protocol (IP) packet used in a Virtual Private Network (VPN) connection. Which of the following would need to be implemented?

A. Layer 3 Tunneling Protocol (L3TP)

B. Encapsulating Security Payload (ESP) in transport mode

**C. Encapsulating Security Payload (ESP) in tunnel mode**

D. Layer 2 Tunneling Protocol (L2TP)

112

Which of the following is the FIRST thing to consider when reviewing Information Technology (IT) internal controls?

A. The cost of the control

B. The impact of the control

C. The nature of the risk

**D. The risk culture of the organization**

113

What is the BEST solution for providing Single Sign-On (SSO) for both cloud and on-premises applications?

**A. Federated Identity Management (FIM)**

B. Directory synchronization

C. Open Authentication (OAuth) 2

D. Cloud-based identity management

114

Which of the following is a security control commonly implemented across Infrastructure as a Service (laaS), Platform as a Service (PaaS) and Software as a Service (SaaS) cloud services?

A. Physical system separation

B. Strict source Internet Protocol (IP) address routing

C. Data encryption

**D. Data Rights Management (DRM)**

115

A development team is starting to design a new product and the group engaged the organization's security architect to review the design. The architect mapped out the application to determine the key areas where data flows in and out of the application and determined the associated risk for each area. What threat model methodology did the architect use?

**A. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)**

B. Representational State Transfer (REST) assessment

C. Penetration testing

D. Attack surface analysis

116

Which of the following Business Continuity (BC) testing strategies will help create the most realistic BC test?

A. Begin the exercise with vague information of the disaster scenario

**B. Begin the exercise with complete details of the disaster scenario**

C. Use very dramatic scenarios to encourage creative solutions

D. Only test outages one system at a time

117

Which of the following is a function of the Trusted Platform Module (TPM)?

**A. Verification of Operating System (OS)**

B. Network verification

C. Tamper evidence

D. Tamper response

118

What principle requires that changes to the plaintext affect many parts of the ciphertext?

**A. Diffusion**

B. Obfuscation

C. Encapsulation

D. Permutation

119

Which of the following is the primary advantage of segmenting Virtual Machines (VM) using physical networks?

A. Removes the need for dedicated virtual security controls

B. Simplicity of network configuration and network redundancy

C. Removes the need for decentralized management solutions

**D. Simplicity of network configuration and network monitoring**

120

The Chief Information Security Officer (CISO) of a successful startup is looking into the organization's cyber crisis management practices. Which of the following would be the BEST approach to the topic?

**A. Address cyber-related crisis at the organization-wide level, involving key stakeholders while defining individual roles and areas of responsibility.**

B. Ensure that Disaster Recovery Plans (DRP) are in place and are regularly crisis tested through table-top exercises.

C. Establish and operate a resilient infrastructure, with capacity and redundancy to survive crisis incidents.

D. Manage cyber incidents at the operational level since they will most likely be handled through technology.

121

Which Systems and Organization Controls (SOC) report(s) provides an assessment of an organization's security, availability, processing integrity, confidentiality, or privacy?

**A. SOC 2 and 3 only**

B. SOC 1 only

C. SOC 3 only

D. SOC 1 and 2 only

122

Ensuring that all available information is provided to management when discussing technological alternatives is a component of which of the following concepts?

A. Security education and training

B. Organizational code of ethics

**C. Cyber threat modelling**

D. Legal and regulatory compliance

123

Which of the following is the BEST practice prior to conducting an internal audit?

A. Brief senior management on process and format.

**B. Confirm that stakeholder expectations for the audit are understood.**

C. Advise the compliance team of incidents that possibly could be found during the audit.

D. Seek authorization for collecting evidence from the technical team.

124

Which of the following are required components for implementing software configuration management systems?

**A. Audit control and signoff**

B. Rollback and recovery processes

C. User training and acceptance

D. Regression testing and evaluation

125

An organization currently has an automated process which allows users to request. approve. and grant access to applications. Which of the following is the BEST control to add to their provisioning process? O

A. Authorization

B. Account security

C. Authentication

D. System security