1. What does the acronym CASP stand for?

A. Cybersecurity Assessment and Solutions Program
B. Certified Advanced Security Practitioner
C. Certified Advanced Security Project
D. CompTIA Advanced Security Practitioner

2. Which phase of the risk management process involves determining the likelihood and impact of a risk?

A. Risk identification
B. Risk assessment
C. Risk mitigation
D. Risk monitoring

3. Which of the following is a type of penetration testing where the tester has no prior knowledge of the target system?

A. White box testing
B. Black box testing
C. Gray box testing
D. Red team testing

4. What is the primary purpose of a Data Loss Prevention (DLP) solution?

A. Detect and prevent data breaches
B. Encrypt sensitive data
C. Monitor network traffic
D. Authenticate users

5. Which encryption method is considered to be a symmetric key algorithm?

A. RSA
B. AES
C. Diffie-Hellman
D. ECC

6. **Which of the following is NOT an access control model?**
   - **A. DAC**
   - **B. MAC**
   - **C. RBAC**
   - **D. ABC**

7. **Which security framework is focused primarily on improving an organization's cybersecurity posture?**
   - **A. ISO 27001**
   - **B. NIST Cybersecurity Framework**
   - **C. PCI DSS**
   - **D. GDPR**

8. **What is the primary purpose of a Security Information and Event Management (SIEM) system?**
   - **A. Real-time analysis of security alerts**
   - **B. User authentication**
   - **C. Data encryption**
   - **D. Intrusion prevention**

9. **Which of the following is a common method used for application hardening?**
   - **A. OSINT**
   - **B. Input validation**
   - **C. VPN**
   - **D. Firewall**

10. **Which cloud computing service model provides the most control over the underlying infrastructure?**
    - **A. IaaS**
    - **B. PaaS**
    - **C. SaaS**
    - **D. FaaS**

11. **Which type of attack involves intercepting and modifying communications between two parties without their knowledge?**
    - **A. Man-in-the-middle attack**
    - **B. Phishing**
    - **C. Brute force attack**
    - **D. DDoS**

12. Which of the following is a protocol that provides security for the transport layer of a network?

- **A. SSL**
- **B. TLS**
- **C. SSH**
- **D. IPSec**

13. What is a key difference between a false positive and a false negative in an intrusion detection system (IDS)?

- **A. False positives are missed attacks, while false negatives are incorrect alerts.**
- **B. False positives are incorrect alerts, while false negatives are missed attacks.**

14. What is the primary purpose of a honeypot?

- **A. Intrusion detection**
- **B. Vulnerability scanning**
- **C. Patch management**
- **D. Firewall configuration**

15. What type of firewall inspects packets at the application layer of the OSI model?

- **A. Packet-filtering firewall**
- **B. Stateful inspection firewall**
- **C. Application-level gateway (proxy) firewall**
- **D. Next-generation firewall**

16. Which of the following is NOT a type of intrusion detection system (IDS)?

- **A. Signature-based**
- **B. Anomaly-based**
- **C. Heuristic-based**
- **D. Rule-based**

17. What type of security testing involves simulating an attack by an external threat actor?

- **A. White box testing**
- **B. Black box testing**
- **C. Gray box testing**
- **D. Red team testing**

18. Which of the following is a vulnerability assessment tool?

- **A. Metasploit**
- **B. Wireshark**
- **C. Nessus**
- **D. Nmap**

19. What is the primary goal of a Business Continuity Plan (BCP)?

- **A. Ensuring the confidentiality of**
- **B. Maintaining ongoing operations during a disruption**
- **C. Recovering from a security breach**
- **D. Protecting the network from external threats**

20. What is the primary goal of a Disaster Recovery Plan (DRP)?

- **A. Ensuring the confidentiality of data**
- **B. Maintaining ongoing operations during a disruption**
- **C. Recovering IT systems and data after a disaster**
- **D. Protecting the network from external threats**

21. Which of the following is an example of a technical control?

- **A. Security policy**
- **B. User training**
- **C. Firewall**
- **D. Background checks**

22. What is the primary purpose of a Public Key Infrastructure (PKI)?

- **A. Encryption and decryption of data**
- **B. Authentication and non-repudiation**
- **C. Network traffic monitoring**
- **D. Intrusion detection**

23. What type of authentication factor is a fingerprint?

- **A. Something you know**
- **B. Something you have**
- **C. Something you are**
- **D. Somewhere you are**

24. Which type of malware typically spreads through email attachments?

A. Virus
B. Worm
C. Trojan
D. Ransomware

25. What is the primary purpose of a vulnerability scanner?

A. Detecting security weaknesses in a network
B. Exploiting vulnerabilities in systems
C. Analyzing network traffic
D. Authenticating users

26. Which of the following is a host-based intrusion detection system (HIDS)?

A. Snort
B. OSSEC
C. Bro
D. Suricata

27. What type of security control is a backup?

A. Preventive
B. Detective
C. Corrective
D. Deterrent

28. What is the primary goal of a risk assessment?

A. Identifying threats and vulnerabilities
B. Determining the likelihood and impact of risks
C. Implementing security controls
D. Monitoring the effectiveness of security controls

29. What does the acronym APT stand for?

A. Advanced Persistent Threat
B. Application Penetration Testing
C. Advanced Perimeter Technology
D. Adaptive Protocol Tunneling

30. Which type of social engineering attack involves impersonating a trusted authority to gain sensitive information?

A. Phishing
B. Pretexting
C. Baiting
D. Tailgating

31. What is the purpose of a network segmentation?

A. Improve network performance
B. Enhance network security
C. Expand network capacity
D. Simplify network management

32. Which of the following is a network-based intrusion detection system (NIDS)?

A. Snort
B. OSSEC
C. Bro
D. Suricata

33. What is the main purpose of security incident response?

A. Prevent security incidents
B. Manage and limit the impact of security incidents
C. Recover from security incidents
D. Detect security incidents

34. What type of attack involves overwhelming a system with an excessive amount of traffic?

A. Man-in-the-middle attack
B. Phishing
C. Brute force attack
D. DDoS

35. What is the primary purpose of a demilitarized zone (DMZ)?

A. Segment the internal network from the internet
B. Provide a secure area for sensitive data
C. Filter network traffic
D. Authenticate users

36. **What type of VPN is typically used to connect entire networks or sites?**
    A. **Remote access VPN**
    B. **Site-to-site VPN**
    C. **SSL VPN**
    D. **MPLS VPN**

37. **Which of the following is an example of a physical security control?**
    A. **Firewall**
    B. **Security policy**
    C. **Biometric scanner**
    D. **User training**

38. **What does the acronym TTP stand for in the context of cybersecurity?**
    A. **Techniques, Tactics, and Procedures**
    B. **Time to Patch**
    C. **Trusted Third Party**
    D. **Threat Tolerance Policy**

39. **What type of access control model is based on user roles and responsibilities?**
    A. **DAC**
    B. **MAC**
    C. **RBAC**
    D. **ABAC**

40. **What is the primary purpose of a secure coding standard?**
    A. **Ensure software performance**
    B. **Minimize software vulnerabilities**
    C. **Streamline software development**
    D. **Ensure software compatibility**

41. **Which of the following is a common method to securely erase data from a solid-state drive (SSD.?**
    A. **Degaussing**
    B. **Shredding**
    C. **Overwriting**
    D. **Crypto-shredding**

42. Which of the following is an example of a non-repudiation control?

- **A. Digital signatures**
- **B. Encryption**
- **C. Authentication**
- **D. Access control**

43. What type of attack involves exploiting a vulnerability in a system before the vulnerability is patched?

- **A. Zero-day attack**
- **B. Brute force attack**
- **C. Man-in-the-middle attack**
- **D. DDoS**

44. What is the primary purpose of a Security Operations Center (SOC. ?

- **A. Software development**
- **B. Network monitoring and incident response**
- **C. Policy enforcement**
- **D. Security training**

45. Which of the following is a type of endpoint protection solution?

- **A. Antivirus software**
- **B. Firewall**
- **C. Intrusion detection system**
- **D. Data loss prevention**

46. What type of attack involves sending a large number of SYN packets to a target system to consume resources and disrupt services?

- **A. SYN flood**
- **B. Smurf attack**
- **C. Ping of death**
- **D. DDoS**

47. What is the primary purpose of a sandbox in cybersecurity?

- **A. Isolate and analyze suspicious files**
- **B. Store sensitive data securely**
- **C. Encrypt network traffic**
- **D. Authenticate users**

48. **Which of the following is an example of a Layer 2 network device?**
    - **E. Router**
    - **F. Switch**
    - **G. Firewall**
    - **H. Intrusion detection system**

49. **Which of the following is a key component of a defense-in-depth strategy?**
    - **A. Single point of failure**
    - **B. Layered security**
    - **C. Centralized management**
    - **D. Redundancy**

50. **What is the primary goal of change management in cybersecurity?**
    - **A. Ensure the security of new and updated systems**
    - **B. Minimize downtime during system changes**
    - **C. Track and document all changes to systems**
    - **D. Maintain a secure configuration baseline**

51. **What does the acronym SSO stand for in the context of authentication?**
    - **A. Secure System Operations**
    - **B. Single Sign-On**
    - **C. System Security Officer**
    - **D. Secure Socket Overlay**

52. **Which of the following is a type of incident response team?**
    - **A. Computer Emergency Response Team (CERT)**
    - **B. Incident Management Team (IMT)**
    - **C. Crisis Management Team (CMT)**
    - **D. Quality Assurance Team (QAT)**

53. **What type of malware typically encrypts files and demands payment for the decryption key?**
    - **A. Virus**
    - **B. Worm**
    - **C. Trojan**
    - **D. Ransomware**

54. Which of the following is a common method used for two-factor authentication 2FA?

- **A. Password and PIN**
- **B. Fingerprint and retina scan**
- **C. Username and password**
- **D. Password and one-time code**

55. What type of threat intelligence focuses on specific threat actors or campaigns?

- **A. Strategic threat intelligence**
- **B. Tactical threat intelligence**
- **C. Operational threat intelligence**
- **D. Technical threat intelligence**

56. Which of the following is a common method used to secure data at rest?

- **A. Data masking**
- **B. Encryption**
- **C. Tokenization**
- **D. Steganography**

57. Which of the following is a wireless security protocol that replaced WEP?

- **A. WPA**
- **B. WPA2**
- **C. WPA3**
- **D. WPS**

58. What is the primary purpose of an Intrusion Prevention System (IPS)?

- **A. Detect and block intrusions in real-time**
- **B. Analyze network traffic for anomalies**
- **C. Encrypt data in transit**
- **D. Authenticate users**

59. Which of the following is a common web application vulnerability?

- **A. Cross-site scripting (XSS)**
- **B. Buffer overflow**
- **C. Password spraying**
- **D. SYN flood**

60. What type of security control is a security awareness training program?

- **A. Technical control**
- **B. Administrative control**
- **C. Physical control**
- **D. Detective control**

61. Which of the following is a type of security event log?

- **A. Firewall logs**
- **B. User logs**
- **C. Training logs**
- **D. Policy logs**

62. What type of security testing involves validating security controls to ensure their effectiveness?

- **A. Vulnerability scanning**
- **B. Penetration testing**
- **C. Compliance auditing**
- **D. Security assessment**

63. Which of the following is a secure alternative to the Telnet protocol?

- **A. SSH**
- **B. SSL**
- **C. TLS**
- **D. IPSec**

64. What type of attack involves exploiting a vulnerability in the DNS system to redirect traffic to a malicious website?

- **A. DNS poisoning**
- **B. Phishing**
- **C. DDoS**
- **D. Man-in-the-middle attack**

65. **What is the primary purpose of a network access control (NAC. system?**
    A. **Monitor network traffic**
    B. **Authenticate and authorize devices on the network**
    C. **Encrypt network traffic**
    D. **Detect and block intrusions**

66. **Which of the following is an example of an indicator of compromise (IOC. ?**
    A. **Unusual login times**
    B. **Unauthorized software installation**
    C. **Suspicious network traffic**
    D. **All of the above**

67. **What does the acronym EDR stand for in the context of cybersecurity?**
    A. **Endpoint Detection and Response**
    B. **Event Data Recorder**
    C. **Electronic Data Repository**
    D. **Encryption and Decryption Resource**

68. **What type of analysis aims to identify patterns and trends in large datasets to predict future events or behaviors?**
    A. **Big data analysis**
    B. **Predictive analytics**
    C. **Data mining**
    D. **Machine learning**

69. **Which of the following is a secure method for managing and storing passwords?**
    A. **Sticky notes**
    B. **Spreadsheet**
    C. **Password manager**
    D. **Plain text file**

70. **What type of malware is typically used for spying and collecting information without the user's knowledge?**
    A. **Spyware**
    B. **Adware**
    C. **Worm**
    D. **Ransomware**

71. Which of the following is a common method used to prevent SQL injection attacks?

- **A. Parameterized queries**
- **B. Input validation**
- **C. Encryption**
- **D. Secure coding**

72. What is the primary goal of a privacy impact assessment PIA?

- **A. Identify and address potential privacy risks**
- **B. Evaluate the security of data storage systems**
- **C. Assess compliance with data protection regulations**
- **D. Ensure the confidentiality of sensitive data**

73. What type of security control is an intrusion detection system (IDS)?

- **A. Preventive**
- **B. Detective**
- **C. Corrective**
- **D. Deterrent**

74. Which of the following is a secure protocol for transferring files over a network?

- **A. FTP**
- **B. TFTP**
- **C. SFTP**
- **D. SCP**

75. What type of attack involves sending malicious requests to a web server to exploit vulnerabilities in the server's software?

- **A. Web application attack**
- **B. Man-in-the-middle attack**
- **C. Phishing**
- **D. DDoSAnswers:**

76. Which of the following is a key component of a Business Continuity Plan (BCP)?

- **A. Risk assessment**
- **B. Incident response plan**
- **C. Disaster recovery plan**
- **D. Security policy**

77. What does the acronym DLP stand for in the context of cybersecurity?

- **E. Data Loss Prevention**
- **F. Digital Layer Protection**
- **G. Data Lifecycle Process**
- **H. Domain Lock Policy**

78. What type of encryption is used by the Advanced Encryption Standard (AES)?

- **A. Symmetric key encryption**
- **B. Asymmetric key encryption**
- **C. Hash function**
- **D. Stream cipher**

79. Which of the following is a common method for securely disposing of hard drives?

- **A. Overwriting**
- **B. Degaussing**
- **C. Shredding**
- **D. All of the above**

80. Which of the following is a secure method for transmitting sensitive information over an untrusted network?

- **A. VPN**
- **B. Telnet**
- **C. FTP**
- **D. HTTP**

81. What is the primary goal of a security audit?

- **A. Identify security vulnerabilities**
- **B. Assess compliance with security policies and regulations**
- **C. Monitor network traffic**
- **D. Ensure data confidentiality**

82. Which of the following is an example of an access control list (ACL)?

- **A. Firewall rules**
- **B. Password policy**
- **C. User training**
- **D. Intrusion detection system**

83. What type of attack involves exploiting weaknesses in the human element of security?

A. Social engineering
B. DDoS
C. Brute force
D. Buffer overflow

84. What is the primary purpose of a network firewall?

A. Detect intrusions
B. Monitor network traffic
C. Control network traffic based on predefined rules
D. Authenticate users

85. Which of the following is an example of a secure web protocol?

A. HTTP
B. HTTPS
C. FTP
D. Telnet

86. What type of security control is a security camera?

A. Technical control
B. Administrative control
C. Physical control
D. Detective control

87. Which of the following is a key principle of the CIA triad in information security?

A. Confidentiality
B. Integrity
C. Availability
D. All of the above

88. What is the primary purpose of a SIEM (Security Information and Event Management) system?

A. Encrypt network traffic
B. Authenticate users
C. Collect, analyze, and report on security-related events
D. Detect and block intrusions

89. Which of the following is a common method for detecting web application vulnerabilities?

A. Vulnerability scanning
B. Penetration testing
C. Static code analysis
D. All of the above

90. What is the primary goal of patch management in cybersecurity?

A. Minimize the risk associated with software vulnerabilities
B. Ensure software compatibility
C. Improve software performance
D. Monitor software usageAnswers:

91. What does the acronym BYOD stand for in the context of cybersecurity?

A. Bring Your Own Device
B. Build Your Own Defense
C. Backup Your Operating Data
D. Block Your Own Domains

92. Which of the following is a key component of an effective password policy?

A. Password length and complexity
B. Password storage location
C. Password sharing guidelines
D. All of the above

93. What type of malware typically self-replicates and spreads without user intervention?

A. Virus
B. Worm
C. Trojan
D. Ransomware

94. What is the primary purpose of a Public Key Infrastructure (PKI)?

A. Manage and distribute encryption keys
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

95. Which of the following is an example of a virtualization technology?

- **A. Docker**
- **B. Kubernetes**
- **C. VMware**
- **D. All of the above**

96. What type of security control is a password policy?

- **A. Technical control**
- **B. Administrative control**
- **C. Physical control**
- **D. Detective control**

97. Which of the following is a common method for detecting anomalies in network traffic?

- **A. Signature-based detection**
- **B. Heuristic-based detection**
- **C. Behavior-based detection**
- **D. All of the above**

98. What is the primary purpose of a vulnerability scanner?

- **A. Detect and block intrusions**
- **B. Identify and assess vulnerabilities in systems**
- **C. Encrypt network traffic**
- **D. Authenticate users**

99. Which of the following is an example of a data leakage prevention (DLP) solution?

- **A. Network firewall**
- **B. Intrusion detection system**
- **C. Email filtering system**
- **D. Data encryption**

100. What type of security control is an intrusion prevention system (IPS)?

A. Preventive
B. Detective
C. Corrective
D. Deterrent

101. Which of the following is an example of a network security zone?

A. Demilitarized zone (DMZ)
B. Virtual private network (VPN)
C. Intrusion detection system (IDS)
D. Security Operations Center (SOC)

102. What is the primary goal of threat modeling in cybersecurity?

A. Identify potential threats and vulnerabilities in a system
B. Assess the likelihood and impact of threats
C. Implement security controls
D. Monitor the effectiveness of security controls

103. Which of the following is a secure alternative to the FTP protocol?

A. SFTP
B. SCP
C. HTTPS
D. All of the above

104. What type of malware is typically disguised as legitimate software?

A. Virus
B. Worm
C. Trojan
D. Ransomware

105. What is the primary purpose of a honeypot in cybersecurity?

A. Attract and analyze attacks
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

106. Which of the following is a common method for securely transmitting data over an untrusted network?

- **A. SSL/TLS**
- **B. VPN**
- **C. IPSec**
- **D. All of the above**

107. What is the primary purpose of an Information Security Management System (ISMS)?

- **A. Monitor network traffic**
- **B. Implement and manage a comprehensive security program**
- **C. Encrypt network traffic**
- **D. Authenticate users**

108. What type of security control is a user access review?

- **A. Technical control**
- **B. Administrative control**
- **C. Physical control**
- **D. Detective control**

109. What type of attack involves intercepting and modifying network traffic?

- **A. Man-in-the-middle attack**
- **B. DDoS**
- **C. Brute force**
- **D. Phishing**

110. What is the primary purpose of an application whitelist?

- **A. Control which applications are allowed to execute on a system**
- **B. Block malicious websites**
- **C. Encrypt network traffic**
- **D. Authenticate users**

111. Which of the following is a key principle of a Zero Trust security model?

- **A. Trust but verify**
- **B. Least privilege**
- **C. Separation of duties**
- **D. Defense-in-depth**

112. What type of security control is a biometric authentication system?

A. Technical control
B. Administrative control
C. Physical control
D. Detective control

113. What is the primary goal of a risk assessment in cybersecurity?

A. Identify and evaluate risks to information assets
B. Implement security controls
C. Monitor the effectiveness of security controls
D. Train users on security best practices

114. Which of the following is a common method for securely erasing data from solid-state drives (SSDs)?

A. Overwriting
B. Degaussing
C. Secure erase
D. Shredding

115. What type of attack involves exploiting a vulnerability in a system to gain unauthorized access?

A. Exploit attack
B. DDoS
C. Brute force
D. Phishing

116. What is the primary purpose of a Security Operations Center (SOC. ?

A. Monitor, detect, and respond to security incidents
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

117. What type of security control is an incident response plan?

A. Technical control
B. Administrative control
C. Physical control
D. Corrective control

118. **What type of malware typically displays unwanted advertisements to the user?**

A. **Adware**
B. **Spyware**
C. **Worm**
D. **Ransomware**

119. **What type of security testing involves attempting to compromise a system from an attacker's perspective?**

A. **Vulnerability scanning**
B. **Penetration testing**
C. **Compliance auditing**
D. **Security assessment**

120. **Which of the following is an example of a hardware security module (HSM)?**

A. **TPM**
B. **SIM card**
C. **Smart card**
D. **All of the above**

121. **What is the primary purpose of a digital certificate?**

A. **Encrypt network traffic**
B. **Authenticate users**
C. **Verify the identity of a person or organization**
D. **Store sensitive data**

122. **Which of the following is a key component of a secure software development life cycle (SDLC. ?**

A. **Security training for developers**
B. **Regular security testing**
C. **Secure coding practices**
D. **All of the above**

123. **What type of security control is a network segmentation?**

A. **Preventive**
B. **Detective**
C. **Corrective**
D. **Deterrent**

124. Which of the following is a common method for mitigating Distributed Denial of Service (DDoS) attacks?

A. Network traffic filtering
B. Rate limiting
C. Content delivery networks (CDNs)
D. All of the above

125. What is the primary goal of a data classification policy?

A. Ensure data confidentiality, integrity, and availability
B. Identify and label sensitive data based on its value and sensitivity
C. Monitor and control access to data
D. Encrypt sensitive data

126. Which of the following is a type of multi-factor authentication (MFA)?

A. Something you know
B. Something you have
C. Something you are
D. All of the above

127. What type of malware is typically designed to encrypt a user's data and demand a ransom for its release?

A. Adware
B. Spyware
C. Worm
D. Ransomware

128. What is the primary purpose of a Web Application Firewall (WAF)?

A. Detect and block web application attacks
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

129. Which of the following is a key component of a secure password hashing algorithm?

A. Salt
B. Key length
C. Initialization vector
D. Encryption mode

130. What type of security control is a security awareness training program?

A. Technical control
B. Administrative control
C. Physical control
D. Detective control

131. Which of the following is a key component of an effective incident response plan?

A. Roles and responsibilities
B. Communication and coordination
C. Containment and eradication
D. All of the above

132. What is the primary purpose of a digital signature?

A. Encrypt network traffic
B. Authenticate users
C. Verify the integrity and authenticity of a message or document
D. Store sensitive data

133. Which of the following is a common method for protecting data at rest?

A. Data encryption
B. Data masking
C. Data tokenization
D. All of the above

134. What is the primary purpose of a network intrusion detection system (NIDS)?

A. Monitor network traffic and detect potential intrusions
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

135. Which of the following is an example of a secure email protocol?

A. SMTP
B. IMAP
C. POP3
D. S/MIME

136. What type of security control is a backup and recovery plan?

A. Technical control
B. Administrative control
C. Physical control
D. Corrective control

137. What is the primary goal of a change management process in cybersecurity?

A. Minimize the risk associated with changes to systems and applications
B. Ensure software compatibility
C. Improve software performance
D. Monitor software usage

138. Which of the following is a key component of a data loss prevention (DLP) strategy?

A. Data classification
B. Data encryption
C. Data monitoring and control
D. All of the above

139. What type of security control is an air-gapped computer?

A. Technical control
B. Administrative control
C. Physical control
D. Preventive control

140. What is the primary purpose of a log management system in cybersecurity?

A. Encrypt network traffic
B. Authenticate users
C. Collect, analyze, and store log data
D. Detect and block intrusions

141. Which of the following is a key component of a defense-in-depth security strategy?

A. Layered security
B. Risk assessment
C. Incident response
D. Security training

142. What type of attack involves sending a large number of requests to a target system to overwhelm its resources and make it unavailable?

A. Denial of Service (DoS) attack
B. Man-in-the-middle attack
C. Brute force
D. Phishing

143. What is the primary purpose of a network access control (NAC. solution?

A. Monitor network traffic
B. Control access to a network based on predefined rules and policies
C. Encrypt network traffic
D. Authenticate users

144. Which of the following is an example of a security information and event management (SIEM) solution?

A. Splunk
B. Snort
C. Wireshark
D. Nessus

145. What type of security control is an encryption algorithm?

A. Technical control
B. Administrative control
C. Physical control
D. Preventive control

146. Which of the following is a key component of a mobile device management (MDM) solution?

A. Device inventory and configuration
B. Application whitelisting
C. Data encryption
D. All of the above

147. What type of security control is an intrusion detection system (IDS)?

A. Preventive
B. Detective
C. Corrective
D. Deterrent

148. What is the primary purpose of a secure coding standard?

A. Define best practices for developing secure software
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

149. Which of the following is a common method for protecting data in transit?

A. SSL/TLS
B. Data masking
C. Data tokenization
D. Data encryption

150. What type of security control is a two-factor authentication (2FA. system?

A. Technical control
B. Administrative control
C. Physical control
D. Detective control

151. What is the primary goal of a security policy in an organization?

A. Define the organization's security objectives and requirements
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

152. What type of security testing involves analyzing source code for potential vulnerabilities?

A. Static code analysis
B. Dynamic code analysis
C. Penetration testing
D. Vulnerability scanning

153. Which of the following is a key component of a secure network architecture?

A. Network segmentation
B. Network access control
C. Intrusion detection and prevention
D. All of the above

154. What type of security control is a firewall rule that blocks all incoming traffic?

A. Preventive
B. Detective
C. Corrective
D. Deterrent

155. What is the primary purpose of a remote access policy?

A. Define the rules and requirements for remote access to an organization's network
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

156. What type of security control is a biometric lock on a server room door?

A. Technical control
B. Administrative control
C. Physical control
D. Preventive control

157. What is the primary purpose of a network intrusion prevention system (NIPS)?

A. Monitor network traffic and block potential intrusions
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

158. Which of the following is a common method for securely storing passwords in a database?

A. Plaintext
B. Hashing with salt
C. Reversible encryption
D. Base64 encoding

159. What type of security control is a security incident response plan?

A. Technical control
B. Administrative control
C. Physical control
D. Corrective control

160. What is the primary purpose of an asset management system in cybersecurity?

A. Track and manage hardware and software assets
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

161. What type of security control is a digital certificate?

A. Technical control
B. Administrative control
C. Physical control
D. Preventive control

162. What is the primary purpose of a patch management process?

A. Update and maintain software to address vulnerabilities and improve security
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

163. What type of security control is an IP-based access control list (ACL)?

A. Preventive
B. Detective
C. Corrective
D. Deterrent

164. What is the primary purpose of a business continuity plan (BCP)?

A. Ensure the organization can continue operating during and after a disruptive event
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

165. Which of the following is a common method for securely disposing of electronic media?

A. Shredding
B. Degaussing
C. Wiping
D. All of the above

166. What type of security control is a video surveillance system?

A. Technical control
B. Administrative control
C. Physical control
D. Detective control

167. What is the primary purpose of a security audit?

A. Assess compliance with security policies and standards
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

168. Which of the following is a key component of an effective vulnerability management program?

A. Regular vulnerability scanning
B. Timely patching and remediation
C. Risk-based prioritization
D. All of the above

169. What type of security control is an application sandbox?

A. Preventive
B. Detective
C. Corrective
D. Deterrent

170. What is the primary purpose of a disaster recovery plan (DRP)?

A. Restore critical systems and data following a disaster
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

171. Which of the following is a common method for detecting web application vulnerabilities?

A. Static code analysis
B. Dynamic code analysis
C. Penetration testing
D. All of the above

172. What type of security control is a user account lockout policy?

A. Preventive
B. Detective
C. Corrective
D. Deterrent

173. What is the primary purpose of a configuration management database (CMDB. ?

A. Track and manage configuration items and their relationships
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

174. What type of security control is a user authentication system?

A. Technical control
B. Administrative control
C. Physical control
D. Preventive control

175. What is the primary purpose of a data retention policy?

A. Define the rules and requirements for retaining and disposing of data
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

176. Which of the following is a key component of an effective security awareness training program?

A. Regular training sessions
B. Engaging content
C. Testing and assessment
D. All of the above

177. What type of security control is a virtual private network (VPN)?

A. Technical control
B. Administrative control
C. Physical control
D. Preventive control

178. What is the primary purpose of a data leak prevention (DLP) solution?

A. Prevent unauthorized disclosure of sensitive data
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

179. Which of the following is a common method for detecting network vulnerabilities?

A. Static code analysis
B. Dynamic code analysis
C. Penetration testing
D. Vulnerability scanning

180. What type of security control is a network firewall?

A. Preventive
B. Detective
C. Corrective
D. Deterrent

181. What is the primary purpose of a data backup and recovery plan?

A. Ensure data can be restored following a disaster or data loss event
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

182. What type of security control is a network intrusion detection system (NIDS)?

A. Technical control
B. Administrative control
C. Physical control
D. Detective control

183. What is the primary purpose of a security risk assessment?

A. Identify, evaluate, and prioritize risks to information assets
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

184. Which of the following is a key component of a secure cloud computing environment?

A. Data encryption
B. Access control
C. Monitoring and auditing
D. All of the above

185. What type of security control is an application whitelist?

A. Preventive
B. Detective
C. Corrective
D. Deterrent

186. What is the primary purpose of a security incident response team (SIRT)?

A. Investigate and respond to security incidents
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

187. Which of the following is a common method for detecting advanced persistent threats (APTs)?

A. Heuristic analysis
B. Behavioral analysis
C. Signature-based detection
D. All of the above

188. What type of security control is a network access control (NAC. system?

A. Technical control
B. Administrative control
C. Physical control
D. Preventive control

189. What is the primary purpose of a data classification policy?

A. Define the rules and requirements for handling and protecting sensitive data
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

190. Which of the following is a key component of a secure software development life cycle (SDLC. ?

A. Threat modeling
B. Secure coding practices
C. Regular security testing
D. All of the above

191. What type of security control is a server room access control system?

A. Technical control
B. Administrative control
C. Physical control
D. Preventive control

192. What is the primary purpose of a vendor risk management program?

A. Evaluate and manage the security risks associated with third-party vendors
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

193. Which of the following is a common method for securely transmitting data over a public network?

A. VPN
B. SSH
C. SSL/TLS
D. All of the above

194. What type of security control is a security policy?

A. Technical control
B. Administrative control
C. Physical control
D. Preventive control

195. What is the primary purpose of a secure network design?

A. Minimize the attack surface and reduce the likelihood of successful attacks
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

196. What type of security control is a host-based intrusion detection system (HIDS)?

A. Technical control
B. Administrative control
C. Physical control
D. Detective control

197. What is the primary purpose of a data loss prevention (DLP) policy?

A. Define the rules and requirements for preventing unauthorized disclosure of sensitive data
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

198. Which of the following is a common method for managing the risks associated with a bring-your-own-device (BYOD. policy?

A. Mobile device management (MDM)
B. Data encryption
C. Network segmentation
D. All of the above

199. What type of security control is an email filtering system?

A. Preventive
B. Detective
C. Corrective
D. Deterrent

200. What is the primary purpose of a security information and event management (SIEM) system?

A. Collect, analyze, and respond to security events and incidents
B. Authenticate users
C. Encrypt network traffic
D. Store sensitive data

1. D	51. B	101.A	151.A
2. B	52. A	102.A	152.A
3. B	53. D	103.D	153.D
4. A	54. D	104.C	154.A
5. B	55. C	105.A	155.A
6. D	56. B	106.D	156.C
7. B	57. A	107.B	157.A
8. A	58. A	108.B	158.B
9. B	59. A	109.A	159.D
10. A	60. B	110.A	160.A
11. A	61. A	111.B	161.D
12. B	62. D	112.A	162.A
13. B	63. A	113.A	163.A
14. A	64. A	114.C	164.A
15. C	65. B	115.A	165.D
16. C	66. D	116.A	166.C
17. D	67. A	117.D	167.A
18. C	68. B	118.A	168.D
19. B	69. C	119.B	169.A
20. C	70. A	120.D	170.A
21. C	71. A	121.C	171.D
22. B	72. A	122.D	172.A
23. C	73. B	123.A	173.A
24. A	74. C	124.D	174.A
25. A	75. A	125.B	175.A
26. D	76. C	126.D	176.D
27. B	77. A	127.D	177.A
28. B	78. A	128.A	178.A
29. A	79. D	129.A	179.D
30. B	80. A	130.B	180.A
31. D	81. B	131.D	181.A
32. B	82. A	132.C	182.D
33. A	83. A	133.D	183.A
34. B	84. C	134.A	184.D
35. A	85. B	135.D	185.A
36. A	86. C	136.D	186.A
37. B	87. D	137.A	187.D
38. B	88. C	138.D	188.D
39. A	89. D	139.C	189.A
40. C	90. A	140.C	190.D
41. C	91. A	141.A	191.C
42. D	92. D	142.A	192.A
43. C	93. B	143.B	193.D
44. B	94. A	144.A	194.B
45. C	95. D	145.D	195.A
46. C	96. B	146.D	196.D
47. B	97. D	147.B	197.A
48. C	98. B	148.A	198.D
49. A	99. C	149.A	199.A
50. A	100. A	150.A	200.A