CYBER SECURITY ASSESSMENT QUESTIONS WITH ANSWERS

1. According to the shared responsibility model, which cloud computing model places the most responsibility on the cloud service provider (CSP)?
   A. Hybrid Cloud
   B. Software as a Service (SaaS)
   C. Platform as a Service (PaaS)
   D. Infrastructure as a Service (IaaS)

2. Which option removes the risk of multitenancy in cloud computing?
   A. PaaS
   B. public cloud
   C. private cloud
   D. IaaS

3. Your organization recently implemented a unified messaging solution and VoIP phones on every desktop. You are responsible for researching the vulnerabilities of the VoIP system. Which type of attack are VoIP phones most vulnerable to experiencing?
   A. denial-of-service
   B. brute force attacks
   C. malware
   D. buffer overflow

4. Which security control cannot produce an active response to a security event?
   A. cloud access security broker (CASB)
   B. intrusion prevention system (IPS)
   C. intrusion detection system (IDS)
   D. next generation firewall

5. Packet sniffer is also called _____.
   A. SIEM
   B. UTM
   C. protocol analyzer
   D. data sink

6. Which option tests code while it is in operation?
   A. code review
   B. code analysis
   C. static analysis
   D. dynamic analysis

7. Which option describes testing that individual software developers can conduct on their own code?
   A. gray box testing
   B. integration testing
   C. white box testing

D. unit testing

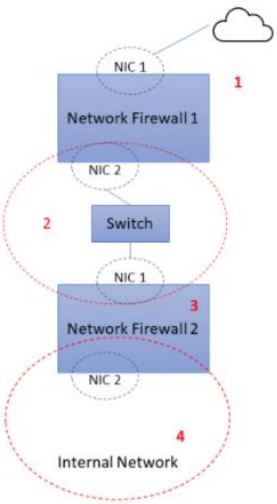
8. In black box penetration testing, what information is provided to the tester about the target environment?
   A. none
   B. limited details of server and network infrastructure
   C. all information
   D. limited details of server infrastructure

9. Which security control can best protect against shadow IT by identifying and preventing use of unsanctioned cloud apps and services?
   A. intrusion prevention system (IPS)
   B. next generation firewall
   C. cloud access security broker (CASB)
   D. intrusion detection system (IDS)

10. Which option describes the best defense against collusion?
    A. monitoring of normal employee system and data access patterns
    B. applying system and application updates regularly
    C. fault tolerant infrastructure and data redundancy
    D. separation of duties and job rotation

11. During a penetration test, you find a file containing hashed passwords for the system you are attempting to breach. Which type of attack is most likely to succeed in accessing the hashed passwords in a reasonable amount of time?
    A. rainbow table attack
    B. pass-the-hash attack
    C. password spray attack
    D. brute force attack

12. Which area is DMZ?



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

13. You configure an encrypted USB drive for a user who needs to deliver a sensitive file at an in-person meeting. What type of encryption is typically used to encrypt the file?
    A. file hash
    B. asymmetric encryption
    C. digital signature
    D. symmetric encryption

14. What is the difference between DRP and BCP
    A. DRP works to keep a business up and running despite a disaster. BCP works to restore the original business capabilities.
    B. BCP works to keep a business up and running despite a disaster. DRP works to restore the original business capabilities.
    C. BCP is part of DRP.
    D. DRP is part of BCP.

15. Which aspect of cybersecurity do Distributed Denial of Service (DDoS) attacks affect the most?
    A. non-repudiation
    B. integrity
    C. availability
    D. confidentiality

16. You need to recommend a solution to automatically assess your cloud hosted VMs against CIS benchmarks to identify deviations from security best practices. What type of solution should you recommend?
    A. Cloud Security Posture Management (CSPM)
    B. Intrusion Detection and Prevention System (IDPS)
    C. Cloud Workload Protection Platforms (CWPP)
    D. Cloud Access Security Brokers (CASBs)

17. _____ validates the integrity of data files.
    A. Compression
    B. Hashing
    C. Symmetric encryption
    D. Stenography

18. Which is an example of privacy regulation at the state government level in the U.S.?
    A. CCPA
    B. GDPR

C. NIST Privacy Framework
D. OSPF

19. What is the term for the policies and technologies implemented to protect, limit, monitor, audit, and govern identities with access to sensitive data and resources?
    A. identity and access management (IAM)
    B. privileged account management (PAM)
    C. authentication and authorization
    D. least privilege

20. You have configured audit settings in your organization's cloud services in the event of a security incident. What type of security control is an audit trail?
    A. preventive control
    B. detective control
    C. directive control
    D. corrective control

21. What is the name for a short-term interruption in electrical power supply?
    A. grayout
    B. blackout
    C. brownout
    D. whiteout

22. Your security team recommends adding a layer of defense against emerging persistent threats and zero-day exploits for all endpoints on your network. The solution should offer protection from external threats for network-connected devices, regardless of operating system. Which solution is best suited to meet this requirement?
    A. Security Information Event Management (SIEM)
    B. Extended Detection and Response (XDR)
    C. next generation firewall (NGFW)
    D. Cloud App Security Broker (CASB)

23. Which is not a threat modelling methodology?
    A. TRIKE
    B. TOGAF
    C. STRIDE
    D. MITRE ATT&CK

24. You organization is conducting a pilot deployment of a new e-commerce application being considered for purchase. You need to recommend a strategy to evaluate the security of the new software. Your organization does not have access to the application's source code.
    Which strategy should you choose?
    A. dynamic application security testing

B. unit testing
C. white box testing
D. static application security testing

25. You need to disable the camera on corporate devices to prevent screen capture and recording of sensitive documents, meetings, and conversations. Which solution would be suited to the task?
    A. Mobile Device Management (MDM)
    B. Data Loss Prevention (DLP)
    C. Intrusion Detection and Prevention System (IDPS)
    D. Cloud Access Security Broker (CASB)

26. How many keys would be necessary to accommodate 100 users in an asymmetric cryptography system?
    A. 200
    B. 400
    C. 100
    D. 300

27. Two competing online retailers process credit card transactions for customers in countries on every continent. One organization is based in the United States. The other is based in the Netherlands. With which regulation must both countries comply while ensuring the security of these transactions?
    A. Federal Information Security Management Act (FISMA)
    B. Payment Card Industry Data Security Standard (PCI-DSS) General Data Protection Regulation (GDPR)
    C. International Organization for Standardization and International Electrotechnical
    D. Commission (ISO/IEC 27018)

28. What provides a common language for describing security incidents in a structures and repeatable manner?
    A. Common event format
    B. common weakness enumeration
    C. common vulnerabilities and exposures
    D. common vulnerability scoring system

29. Which type of application can intercept sensitive information such as passwords on a network segment?
    A. log server
    B. network scanner
    C. firewall
    D. protocol analyzer

30. An attacker has discovered that they can deduce a sensitive piece of confidential information by analyzing multiple pieces of less sensitive public data. What type of security issue exists?
    A. aggregation
    B. inference
    C. SQL injection
    D. cross-origin resource sharing

31. What act grants an authenticated party permission to perform an action or access a resource?
    A. Zero Trust Security
    B. Role-Based Access Control (RBAC)
    C. authorization
    D. Single Sign-On

32. According to GDPR, a data _____ is the person about whom data is being collected.
    A. Processor
    B. object
    C. subject
    D. controller

33. Which is not a principle of zero trust security?
    A. use least privilege access
    B. verify explicitly
    C. trust but verify
    D. assume breach

34. Which attack exploits input validation vulnerabilities?
    A. ARP spoofing
    B. pharming attacks
    C. cross-site scripting (XSS)
    D. DNS poisoning

35. You are a security analyst, and you receive a text message alerting you of a possible attack. Which security control is the least likely to produce this type of alert?
    A. IDS
    B. SIEM
    C. packet sniffer
    D. IPS

36. SQL injection inserts a code fragment that makes a database statement universally true, like _____.
    A. SELECT * FROM users WHERE username = '' AND 1=1--'
    B. SELECT * FROM users WHERE username = '' AND 1!=1--'

C. SELECT * FROM users WHERE username = '' OR 1=1--'
D. SELECT * FROM users WHERE username = '' OR 1!=1--'

37. Which type of security assessment requires access to source code?
    A. static analysis
    B. black box testing
    C. dynamic analysis
    D. penetration testing

38. Which option is an open-source solution to scanning a network for active hosts and open ports?
    A. Autopsy
    B. Snort
    C. Nmap
    D. Wireshark

39. When implementing a data loss prevention (DLP) strategy, what is the first step in the process?
    A. Evaluate the features of available DLP products to determine which best meet your organization's needs.
    B. Examine the flow of sensitive data in your organization to better understand usage patterns.
    C. Conduct an inventory of all the data in your organization to establish classifications based on sensitivity.
    D. Conduct a risk assessment to determine the best data labelling strategy for your organization.

40. Which malware changes an operating system and conceals its tracks?
    A. virus
    B. worm
    C. rootkit
    D. Trojan horse

41. Virtual Private Networks (VPNs) use _ to create a secure connection between two networks.
    A. encryption
    B. a metropolitan area networks
    C. a virtual local area network
    D. a wide area networks

42. What is the process of challenging a user to prove their identity?
    A. authentication
    B. Single Sign-On
    C. authorization

D. Role-Based Access Control (RBAC)

43. Which cyberattack aims to exhaust an application's resources, making the application unavailable to legitimate users?
    A. SQL injection
    B. dictionary attack
    C. Distributed Denial of Service (DDoS)
    D. rainbow table attack

44. You are a recent cybersecurity hire, and your first assignment is to present on the possible threats to your organization. Which of the following best describes the task?
    A. risk mitigation
    B. threat assessment
    C. risk management
    D. enumeration

45. You are at a coffee shop and connect to a public wireless access point (WAP). What a type of cybersecurity attack are you most likely to experience?
    A. man-in-the-middle attack
    B. back door
    C. logic bomb
    D. virus

46. You have been tasked with recommending a solution to centrally manage mobile devices used throughout your organization. Which technology would best meet this need?
    A. Extended Detection and Response (XDR)
    B. Security Information Event Management (SIEM)
    C. Intrusion Detection and Prevention System (IDPS)
    D. Mobile Device Management (MDM)

47. Which type of vulnerability cannot be discovered in the course of a typical vulnerability assessment?
    A. file permissions
    B. buffer overflow
    C. zero-day vulnerability
    D. cross-site scripting

48. The DLP project team is about to classify your organization's data. What's is the primary purpose of classifying data?
    A. It identifies regulatory compliance requirements.
    B. It prioritizes IT budget expenditures.
    C. It quantifies the potential cost of a data breach.
    D. It establishes the value of data to the organization.

49. You are responsible for managing security of your organization's public cloud infrastructure. You need to implement security to protect the data and applications running in a variety of IaaS and PaaS services, including a new Kubernetes cluster. What type of solution is best suited to this requirement?
    A. Cloud Workload Protection Platforms (CWPP)
    B. Cloud Security Posture Management (CSPM)
    C. Cloud Access Security Brokers (CASBs)
    D. Intrusion Detection and Prevention System (IDPS)

50. Sharing account credentials violates the _____ aspect of access control.
    A. identification
    B. authorization
    C. accounting
    D. authentication

51. You have recovered a server that was compromised in a malware attack to its previous state. What is the final step in the incident response process?
    A. Eradication / Remediation
    B. Certification
    C. Reporting
    D. Lessons Learned

52. Which encryption type uses a public and private key pair for encrypting and decrypting data?
    A. asymmetric
    B. symmetric
    C. hashing
    D. all of these answers

53. You have just identified and mitigated an active malware attack on a user's computer, in which command and control was established. What is the next step in the process?
    A. Reporting
    B. Recovery
    C. Eradication / Remediation
    D. Lessons Learned

54. Which programming language is most susceptible to buffer overflow attacks?
    A. C
    B. Java
    C. Ruby
    D. Python

55. Which list correctly describes risk management techniques?
    A. risk acceptance, risk mitigation, risk containment, and risk qualification

B. risk avoidance, risk transference, risk containment, and risk quantification
C. risk avoidance, risk mitigation, risk containment, and risk acceptance
D. risk avoidance, risk transference, risk mitigation, and risk acceptance

56. To implement encryption in transit, such as with the HTTPS protocol for secure web browsing, which type(s) of encryption is/are used?
    A. asymmetric
    B. both symmetric and asymmetric
    C. neither symmetric or asymmetric
    D. symmetric

57. Which type of program uses Windows Hooks to capture keystrokes typed by the user, hides in the process list, and can compromise their system as well as their online access codes and password?
    A. trojan
    B. keystroke collector
    C. typethief
    D. keylogger

58. How does ransomware affect a victim's files?
    A. by destroying them
    B. by encrypting them
    C. by stealing them
    D. by selling them

59. Your computer has been infected and is sending out traffic to a targeted system upon receiving a command from a botmaster. What condition is your computer currently in?
    A. It has become a money mule.
    B. It has become a zombie.
    C. It has become a bastion host.
    D. It has become a botnet.

60. You choose a cybersecurity framework for your financial organization that implements an effective and auditable set of governance and management processes for IT. Which framework are you choosing?
    A. C2M2
    B. NIST SP 800-37
    C. ISO/IEC 27001
    D. COBIT

61. NIST issued a revision to SP 800-37 in December 2018. It provides a disciplined, structured, and flexible process for managing security and privacy risk. Which type of document is SP 800-37?
    A. a risk management framework

B. a guide to risk assessments
C. a guideline for vulnerability testing
D. a step-by-step guide for performing business impact analyses

62. The most notorious military-grade advanced persistent threat was deployed in 2010, and targeted centrifuges in Iran. What was this APT call?
A. duqu
B. agent BTZ
C. stuxnet
D. flame

63. Where would you record risks that have been identified and their details, such as their ID and name, classification of information, and the risk owner?
A. in the risk assessment documentation
B. in the risk register
C. in the business impact ledger
D. in the Orange Book

64. To prevent an incident from overwhelming resources, _____ is necessary.
A. disconnection from the network
B. early containment
C. continuation of monitoring for other incidents
D. eradication of the issues

65. FUD is expensive and often causes high drama over low risk. Which computer chip exploits were reported by CNN as needing to be completely replaced, but were later fixed with firmware updates?
A. fire and ice exploits
B. meltdown and spectre exploits
C. Intel and STMicro CPU exploits
D. super microboard and Apple iPhone exploits

66. The ASD Top Four are application whitelisting, patching of applications, patching of operating systems, and limiting administrative privileges. What percent of breaches do this account for?
A. 40 percent
B. 60 percent
C. 85 percent
D. 100 percent

67. You are working in the security operations center analyzing traffic on your network. You detect what you believe to be a port scan. What does this mean?
A. This could be a specific program being run by your accounting department.
B. This is an in-progress attack and should be reported immediately

C. This is normal operation for your business.
D. This could be a precursor to an attack.

68. How often is the ISF Standard of Good Practice updated?
    A. annual
    B. biannually
    C. bimonthly
    D. monthly

69. Your incident response team is unable to contain an incident because they lack authority to take action without management approval. Which critical step in the preparation phase did your team skip?
    A. From an incident response committee to oversee any incidents that may occur.
    B. Get preauthorized to take unilateral action and make or direct emergency changes.
    C. Bring management in as leadership on the incident response team.
    D. Assign a head of the emergency response team who has the correct authority

70. NIST SP 800-53 is one of two important control frameworks used in cybersecurity. What is the other one?
    A. ISO 27001
    B. NIST SP 800-54
    C. ISO 27002
    D. NIST SP 751-51

71. Which organization, established by NIST in 1990, runs workshops to foster coordination in incident prevention, stimulate rapid reaction to incidents, and allow experts to share information?
    A. Forum of Incident Response and Security Teams
    B. Crest UK Response Teams
    C. Community of Computer Incident Response Teams
    D. NIST Special Publication 800-61 Response Teams

72. You have implemented controls to mitigate the threats, vulnerabilities, and impact to your business. Which type of risk is left over?
    A. inherent risk
    B. residual risk
    C. applied risk
    D. leftover risk

73. There are four possible treatments once an assessment has identified a risk. Which risk treatment implements controls to reduce risk?
    A. risk mitigation
    B. risk acceptance
    C. risk avoidance

D. risk transfer

74. Which security control scheme do vendors often submit their products to for evaluation, to provide an independent view of product assurance?
    A. Common Criteria
    B. risk management certification board
    C. OWASP security evaluation
    D. ISO 27000

75. Which organization has published the most comprehensive set of controls in its security guideline for the Internet of Things?
    A. IoT ISACA
    B. IoT Security Foundation
    C. OWASP
    D. GSMA

76. Which main reference coupled with the Cloud Security Alliance Guidance comprise the Security Guidance for Critical Areas of Focus in Cloud Computing?
    A. ISO 27001
    B. ISO 27017
    C. Cloud Security Guidelines
    D. Cloud Controls Matrix

77. What are the essential characteristics of the reference monitor?
    A. It is versatile, accurate, and operates at a very high speed.
    B. It is tamper-proof, can always be invoked, and must be small enough to test.
    C. It is restricted, confidential, and top secret

78. According to NIST, what is the first action required to take advantage of the cybersecurity framework?
    A. Identify the key business outcomes.
    B. Understand the threats and vulnerabilities.
    C. Conduct a risk assessment.
    D. Analyze and prioritize gaps to create the action plan.

79. You are implementing a cybersecurity program in your organization and want to use the "de facto standard" cybersecurity framework. Which option would you choose?
    A. the ISACA Cybersecurity Framework
    B. the COBIT Cybersecurity Framework
    C. the ISC2 Cybersecurity Framework
    D. the NIST Cybersecurity Framework

80. In 2014, 4,278 IP addresses of zombie computers were used to flood a business with over one million packets per minute for about one hour. What is this type of attack called?
    A. a salami attacks
    B. a DoS (Denial of Service) attack
    C. a DDoS (Distributed Denial of Service) attack
    D. a botnet attacks

81. The regulatory requirements for notifications of data breaches, particularly the European General Data Protection Regulations, have had what sort of effect on business?
    A. an increased business liability in the event of a data breach
    B. an increased consumer liability in the event of a data breach
    C. a decreased consumer liability in the event of a data breach
    D. a decreased business liability in the event of a data breach

82. Which compliance framework governs requirements for the U.S. healthcare industry?
    A. FedRAMP
    B. GDPR
    C. PCI-DSS
    D. HIPAA

83. What is the difference between DevOps and DevSecOps?
    A. DevSecOps requires the inclusion of cybersecurity engineers in the CI/CD process of DevOps.
    B. DevSecOps slows down the CI/CD process of DevOps.
    C. DevSecOps places security controls in the CI/CD process of DevOps.
    D. DevSecOps lets cybersecurity engineers dictate the CI/CD process of DevOps.

84. When does static application security testing require access to source code?
    A. always
    B. only when assessing regulatory compliance
    C. only if following the Agile model
    D. never

85. Your organization service customer orders with a custom ordering system developed in-hose. You are responsible for recommending a cloud model to meet the following requirements:

    Control of security required for regulatory compliance
    Legacy application and database support
    Scalability to meet seasonal increases in demand

    Which cloud model is the best option for these requirements?
    A. government cloud

B. public cloud
C. hybrid cloud
D. private cloud

86. You have just conducted a port scan of a network. There is no well-known port active. How do you find a webserver running on a host, which uses a random port number?
A. Give up on the current target network and move on to the next one.
B. Switch to another network scanning tool. Resort to more resource-intensive probing, like launching random attacks to all open ports.
C. Turn on the stealth mode in your network scanning tool. Check whether you missed any other active ports associated with web servers.
D. Turn on additional options in your network scanning tool to further investigate the details (type and version) of applications running on the rest of the active ports.

87. Executives in your organization exchange emails with external business partners when negotiating valuable business contracts. To ensure that these communications are legally defensible, the security team has recommended that a digital signature be added to these messages.
What are the primary goals of the digital signature in this scenario? (Choose the best answer).
A. integrity and non-repudiation
B. privacy and non-repudiation
C. privacy and confidentiality
D. integrity and privacy

88. Which option is a mechanism to ensure non-repudiation?
A. MD5
B. Caesar cipher
C. symmetric-key encryption
D. asymmetric-key encryption

89. Which software development lifecycle approach is most compatible with DevSecOps?
A. Agile
B. Model-Driven Development
C. Waterfall
D. Model-Driven Architecture

90. Which information security principle states that organizations should defend systems against any particular attack using several independent methods?
A. separation of duties
B. privileged account management (PAM)
C. defense-in-depth
D. least privilege

91. Which option describes a core principle of DevSecOps?
    A. Testing and release should be 100% automated
    B. Role separation is the key to software security
    C. Final responsibility for security rests with the architect of the application
    D. Everyone in the process is responsible for security

92. You need to implement a solution to protect internet-facing applications from common attacks like XSSm CSRF, and SQL injection. Which option is best suited to the task?
    A. Security Information Event Management (SIEM)
    B. an Instruction Detection and Prevention System (IDPS) appliance
    C. a web application firewall (WAF)
    D. a stateful packet inspection firewall

93. Which phase of the incident response process happens immediately following identification?
    A. Eradication / Remediation
    B. Reporting
    C. Containment / Mitigation
    D. Recovery

94. How can a data retention policy reduce your organization's legal liability?
    A. by reducing DLP licensing costs
    B. by ensuring that data is not retained beyond its necessary retention date
    C. by destroying data that may implicate company executives in dishonest behavior
    D. by reducing cost associated with data storage and protection

95. You believe a recent service outage due to a denial-of-service attack from a disgruntled inside source. What is the name for the malicious act this employee has committed?
    A. espionage
    B. sabotage
    C. fraud
    D. confidentiality breach

96. Which option is a framework widely utilized by organizations in the development of security governance standards?
    A. Software Capability Maturity Model (SW-CMM)
    B. Control Objectives for Information and Related Technologies (COBIT)
    C. The Open Group Architecture Framework (TOGAF)
    D. Software Development Life Cycle (SDLC)

97. There are connection-oriented and connectionless protocols in networking. What do web browsers use to ensure the integrity of the data it sends and receives?
    A. UDP that is connection-oriented
    B. TCP that is connection-oriented

C. UDP that is connectionless
D. TCP that is connectionless

98. Which type of attack targets vulnerabilities associated with translating MAC addresses into IP addresses in computer networking?
A. DNS poisoning
B. CRL trapping
C. ARP spoofing
D. DDoS

99. You are part of an incident response team at your company. While sifting through log files collected by a SIEM, you discover some suspicious log entries that you want to investigate further. Which type of the following best refers to those recorded activities demanding additional scrutiny?
A. attack
B. information
C. threat
D. event

100. You are responsible for forensic investigations in your organization. You have been tasked with investigating a compromised virtual application server. Because a revenue generating application runs on the server, the server needs to be returned to service as quickly as possible.
What is the next step you should take to best fulfil your responsibilities and meet the needs of the business?
A. Restore the server from backup immediately.
B. Take the server offline until your investigation is complete.
C. Take a snapshot of the compromised virtual server for your investigation.
D. Restart the server. Remediate the issue after business hours.

101. Site-to-site VPN provides access from one network address space (192.168.0.0/24) to another network address space _ site-to-site VPN provides access from one network address space (192.168.0.0/24) to another network address space _____.
A. 192.168.0.1/24
B. 192.168.0.3/24
C. 10.10.0.0/24
D. 192.168.0.2/24

102. You are researching probable threats to your company's internet-facing web applications. Which organization should you reference as an authoritative source for information on web-based attack vectors?
A. EC-Council
B. ISACA
C. NIST

D. OWASP

103.Which action is most likely to simplify security staff training, improve integration between security components, and reduce risk to the business? (Choose the best answer.)

A. adopting a "best-in-suite" approach to security
B. adopting a "trust but verify" approach to security
C. adopting a "best-of-breed" approach to security
D. adopting a "defense-in-depth" approach to security

104._____ attacks can execute the code injected by attackers as part of user inputs.

A. Ping of death
B. Buffer overflow
C. Distributed Denial of Service
D. Denial of Service

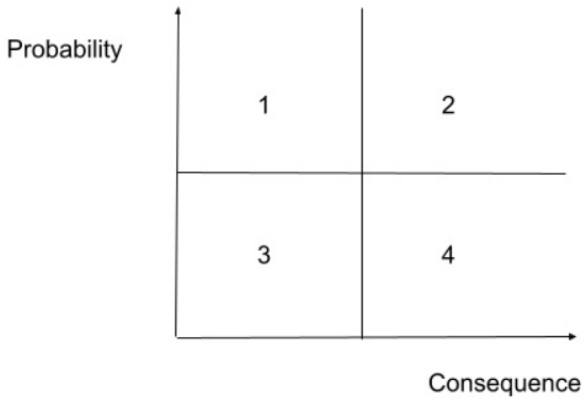
105.Which activity is not part of risk assessment?

A. identifying and valuing assets
B. analyzing risks by criticality and cost
C. discontinuing activities that introduce risk
D. identifying threats and analyzing vulnerabilities

106.In response to an alert regarding a possible security incident, you are analyzing the logs for a web application. In the process, you see the following string: ./../../../var/secrets What type of attack was most likely attempted against the application?

A. brute force
B. session hijacking
C. cross-site scripting
D. directory traversal

107.Which quadrant should be the focus of risk management?



A. 2

B. 1
C. 3
D. 4

108.Which option will not actively identify a security incident?
A. Extended Detection and Response (XDR)
B. Cloud Security Posture Management (CSPM)
C. Security Information Event Management (SEIM)
D. Endpoint Detection and Response (EDR)

109.A website is asking for a password and also sending an authentication code to your phone. What factors are used in this multi-factor authentication scenario?
A. what you have and what you do
B. what you know and what you are
C. what you have and what you know
D. what you do and what you know

110.Which option is a list of publicly disclosed information security defects?
A. DBIR
B. CVE
C. CWE
D. CERT

111.What is cryptovirology?
A. Plain cryptography
B. Antivirus
C. Design powerful malicious software
D. Asymmetric backdoor

112.What does a metamorphic virus do?
A. Static analyser
B. Antivirus
C. Generates a whole variable code using a variable encryptor
D. Mutation function

113.What is the most common cause of cyber incidents in organisations?
A. Vulnerabilities in softwares
B. Social Engineering
C. Ransomware
D. Phishing

114.Which of the following terms is used to describe a collection of unrelated patches?
A. Hotfix
B. Update

C. Security Fix
D. Service Pack

115.How often should security teams conduct a review of the privileged access that a user has to sensitive systems?
A. On a periodic basis
B. When a User leaves the organisation
C. When a user changes roles
D. On a daily basis

116.What Term is used to describe the default set of privileges assigned to a user when a new account is created?
A. Aggregation
B. Transitivity
C. Baseline
D. Entitlement

117.Who is the father of computer security??
A. August Kerckhoffs
B. Bob Thomas
C. Charles Thomas
D. Robert Kerckhoffs

118.Which type of attack uses formal emails to entice specific individuals into signing in and changing their passwords?
A. vishing
B. spear phishing
C. brute force attack
D. password spray attack

119.A data asset register should contain which of the following?
A. the location of the data.
B. The value of the asset.
C. The owner of the asset.
D. All of these options.

120.Once you have confirmed that Burpsuite is intercepting website requests, where can you check to see if you have credentials in cleartext to access the target webpage?
A. Select Go on the Repeater tab
B. See the loopback address and port are on in the Options tab
C. Check the Raw section in the Intercept tab
D. Check for a login.php line in the Proxy tab

121.Threat actors will attempt to find an attack vector on their target by mapping the attack _____.

A. surface
B. infrastructure
C. threat
D. door

122.How would an organisation ensure software product support in the event a supplier goes out of business or is sold to a competitor?

A. They could employ the software developers once the supplier organisation has gone out of business.
B. They could ensure support by acquiring the supplier organisation.
C. They could ensure support through an escrow agreement.
D. They could reverse engineer the product so that it could be supported in-house.

123.Which of the following is the security standard that applies to the certification of security controls within products?

A. ISO/IEC 27001.
B. ISO/IEC 9000.
C. ISO/IEC 15408.
D. ISO/IEC 13335.

124.What is the main role of the board member known as the information security manager?

A. To ensure appropriate security controls are implemented across the organisation.
B. To provide day-to-day management of the information assurance function.
C. To have a detailed understanding of the organisation's vulnerabilities.
D. To have a detailed understanding of threats faced by the organisation.

125.What are the two main approaches used to determine the likelihood of a threat occurring?

A. Qualitative and statistical
B. Statistical and quantitative
C. Statistical and assumptive
D. Qualitative and quantitative

126.Which type of hackers are often organized and funded by a nation's military intelligence or security services, and attempt to gain access to a foreign adversary's state secrets or military intelligence?

A. hacktivists
B. competitors
C. black hat hackers
D. state-sponsored hackers

127.Which of the following methods combines two binary streams to create one new stream that contains hidden information that cannot be retrieved without the other stream that was used to create it?

A. substitution cipher
B. weaponization
C. transposition cipher
D. XOR encryption

128.What is Drupalgeddon?

A. A web app proxy tool
B. A DDoS bot
C. A network packet capturing device
D. a SQL injection flaw\

129.The algorithm used by an encryption technique to hide information is known as the _____.

A. cipher
B. XOR
C. encoding
D. cyber kill chain

130.Which of these is not an issue that could arise as a result of outsourcing software development?

A. The accidental or deliberate introduction of malicious code.
B. The loss of intellectual property or trade secrets.
C. Legal disputes could develop between the customer and the supplier.
D. The laws on the protection of data do not apply to information sent to a third party.

131.A _____ hat is a hacker who may not operate according to ethical testing standards but does not have malicious intent.

A. gray
B. blue
C. red
D. purple

132.Understanding that multifactor authentication (MFA) is a best practice, which option should be avoided as a secondary authentication factor in MFA whenever possible?

A. biometric authentication
B. OAUTH Token
C. authenticator apps
D. SMS message

ANSWERS

1.B
2.C
3.A
4.C
5.C
6.D
7.D
8.A
9.C
10.D
11.A
12.C
13.D
14.A
15.C
16.A
17.B
18.A
19.A
20.D
21.B
22.C
23.B
24.A
25.A
26.A
27.B
28.C
29.D
30.B
31.C
32.C
33.C
34.C
35.C
36.C
37.A
38.C
39.A
40.C
41.A
42.A

43.C
44.C
45.A
46.D
47.C
48.C
49.A
50.B
51.D
52.A
53.C
54.A
55.D
56.B
57.D
58.B
59.B
60.B
61.A
62.C
63.B
64.B
65.B
66.C
67.D
68.A
69.B
70.C
71.A
72.B
73.A
74.A
75.B
76.D
77.B
78.A
79.D
80.C
81.A
82.D
83.A
84.A
85.C
86.D

87.A
88.D
89.A
90.C
91.A
92.C
93.B
94.B
95.B
96.B
97.B
98.C
99.D
100.C
101.A
102.D
103.B
104.B
105.C
106.D
107.A
108.B
109.A
110.C
111.D
112.C
113.B
114.A
115.D
116.D
117.A
118.B
119.D
120.D
121.A
122.C
123.C
124.A
125.D
126.D
127.D
128.-
129.-
130.-

131.-

132.-