Lesson 1 — Why build security in (SDLC + SDL basics)

1. What does SDLC stand for?
   A. Secure Design Life Cycle
   B. Software Design Life Cycle
   C. Software Development Life Cycle
   D. System Development Control Lifecycle

2. What does SDL stand for?
   A. Security Development Life Cycle
   B. Software Deployment Lifecycle
   C. System Design Logic
   D. Secure Data Layer

3. Software security entails:
   A. Adding security after deployment
   B. Building security into software through an SDL in an SDLC
   C. Only running vulnerability scans
   D. Only encrypting databases

4. Which are the three core elements of security?
   A. Authentication, Authorization, Auditing
   B. Confidentiality, Integrity, Availability
   C. Privacy, Safety, Reliability
   D. Risk, Threat, Vulnerability

5. Threat modeling and attack surface validation throughout the SDL primarily:
   A. Replace testing
   B. Eliminate the need for requirements
   C. Alleviate security vulnerabilities
   D. Increase feature delivery speed

6. Which SDLC phase creates a vision and next steps?
   A. Planning
   B. Design
   C. Testing
   D. Deployment

7. Which SDLC phase determines necessary software requirements?
   A. Maintenance
   B. Requirement
   C. Implementation

D. End of life

8. Which SDLC phase prepares requirements for the technical design?
   A. Design
   B. Deployment
   C. End of life
   D. Planning

9. Which SDLC phase determines resources involved in the application from a known resource?
   A. Implementation
   B. Testing
   C. Maintenance
   D. Requirements

10. Which SDLC phase verifies functions through a known environment?
   A. Design
   B. Testing
   C. Deployment
   D. End of life

11. Which SDLC phase pushes security out?
   A. Planning
   B. Deployment
   C. Maintenance
   D. Requirements

12. Which SDLC phase implements ongoing security monitoring?
   A. Maintenance
   B. Implementation
   C. Planning
   D. Testing

13. Which SDLC phase considers proper steps for removing software completely?
   A. Design
   B. Requirement
   C. End of life
   D. Deployment

14. Hardware refers to:
   A. Operating systems only
   B. Physical components of a computer system
   C. Code libraries

D. Threat models

15. Software refers to:
    A. Physical components
    B. Programs and operating systems
    C. Network cables
    D. Building layouts

16. Secure code is best described as:
    A. Code with no comments
    B. A principle design in coding referencing security best practices and safeguards
    C. Code that runs fast
    D. Code written only in C++

17. SDLC has how many major phases (as listed in Lesson 1)?
    A. 5
    B. 6
    C. 8
    D. 10

18. Which is NOT one of the listed SDLC phases?
    A. Planning
    B. Requirements
    C. Marketing
    D. Maintenance

19. Integrating and evaluating software and hardware used by an organization helps:
    A. Maximize organization's software and security
    B. Eliminate compliance needs
    C. Remove need for testing
    D. Guarantee zero vulnerabilities

20. Threat modeling is:
    A. A tool for encrypting data
    B. A structured process to protect against vulnerabilities
    C. A deployment script
    D. A maintenance schedule

Lesson 2 — SDL programs and maturity models (BSIMM, OWASP, NIST, CVE)

21. Implementing an SDL program ensures security is:
    A. Added only during maintenance
    B. Built into software design rather than an afterthought
    C. Only handled by legal
    D. Optional if agile is used

22. Which is a popular SDL model/resource listed?
    A. PCI DSS
    B. BSIMM
    C. ITIL
    D. COBIT

23. BSIMM primarily:
    A. Enforces coding standards automatically
    B. Studies real-world software security initiatives
    C. Replaces penetration testing
    D. Is a vulnerability scanner

24. BSIMM helps you determine:
    A. Only network topology
    B. Where software security stands and how to develop over time
    C. Only developer performance
    D. Only cloud costs

25. How many best BSIMM practices are mentioned?
    A. 8
    B. 10
    C. 12
    D. 15

26. OWASP SAMM is best described as:
    A. A firewall standard
    B. A flexible and prescriptive framework for building security into dev orgs
    C. A bug bounty platform
    D. A logging format

27. NIST provides:
    A. Only incident response teams
    B. Research, info, and tools for gov and corporate information security
    C. Payment processing rules
    D. Only password managers

28. DHS has an established:
    A. Software Assurance Program

B. Browser Security Program
C. Hardware Certification Program
D. Encryption Export Program

29. CVE is:
A. A model to score severity
B. A list providing common names for publicly known vulnerabilities
C. A testing method
D. A secure coding language

30. Whatever SDL you use must be mapped to your:
A. Marketing plan
B. SDLC
C. HR policies
D. Sales funnel

31. Security metrics help corporations:
A. Avoid all audits
B. Decide on risk management requirements and security budgets
C. Remove need for governance
D. Disable testing

32. Security metrics can show customers:
A. Proof of security
B. Stock prices
C. Legal privileges
D. Source code

33. Application security is the process of:
A. Deleting old code
B. Developing, adding, and testing security features within applications
C. Printing audit reports
D. Buying new hardware

34. Application security aims to prevent:
A. Customer support tickets
B. Security vulnerabilities against threats
C. New feature releases
D. Backups

35. Static analysis is performed:
A. Only after deployment
B. Without executing programs
C. Only on virtual machines

D. Only by end users

36. Dynamic analysis is performed:
    A. Without code access
    B. When executing programs in real time
    C. Only on paper
    D. Only during planning

37. Fuzz testing uses:
    A. Valid expected data only
    B. Invalid/unexpected/random data
    C. Only encrypted data
    D. Only user interviews

38. A metric model allows an org to determine:
    A. Effectiveness of security controls
    B. Employee attendance
    C. Device battery life
    D. Marketing ROI

39. A measurement model is:
    A. A set of data security methods developers take to protect against vulnerabilities
    B. A penetration test plan
    C. A vulnerability name list
    D. A cloud contract

40. Which is NOT listed as a popular SDL model/resource?
    A. Cisco SDL
    B. Microsoft Trustworthy Computing SDL
    C. OWASP Code Review Guide
    D. ISO 9001

Lesson 3 — SDLC approaches (Waterfall, V-model, Agile, Scrum, XP)

41. Waterfall divides development into:
    A. Random phases
    B. Separate phases where one output feeds the next
    C. Only two phases

D. Only testing loops

42. A key advantage of Waterfall is:
    A. Unlimited revision time
    B. Splitting deliveries into stages for easier control
    C. No documentation needed
    D. No requirements needed

43. A key disadvantage of Waterfall is:
    A. Too much revision
    B. No time for reflection or design revision
    C. Too many daily meetings
    D. No testing phase

44. The V-model is:
    A. Fully linear without validation
    B. Waterfall variation that turns back upward after coding
    C. A cloud deployment model
    D. A security scoring model

45. Agile methodology:
    A. Forbids collaboration
    B. Mixes traditional and new practices
    C. Requires waterfall only
    D. Eliminates planning

46. Agile uses collaboration between:
    A. Single-role teams
    B. Self-organizing and cross-functional teams
    C. Only managers
    D. Only security teams

47. Agile has:
    A. 2 values and 4 principles
    B. 4 values and 12 principles
    C. 12 values and 4 principles
    D. 8 values and 8 principles

48. Agile allows customer satisfaction through:
    A. Delayed releases
    B. Rapid, continuous delivery of useful software
    C. No deployments
    D. Only annual upgrades

49. A disadvantage of Agile (per lesson) is difficulty:
   A. Writing code
   B. Assessing effort at the beginning of SDL
   C. Testing in production
   D. Hiring developers

50. Scrum framework allows a team to work:
   A. Rigidly and separately
   B. Flexibly and holistically toward a common goal
   C. Only by email
   D. Only in planning

51. Extreme programming (XP) intends to improve:
   A. Hardware speed
   B. Software quality and responsiveness
   C. Legal compliance only
   D. Cloud costs only

52. XP is a type of:
   A. Waterfall
   B. Agile software development
   C. V-model only
   D. End-of-life planning

53. Waterfall methodology is best described as:
   A. Sequential, step-by-step process for requirements
   B. Randomized deployments
   C. Continuous delivery pipeline
   D. Threat modeling framework

54. The V-model creates a “V” shape because:
   A. Testing is removed
   B. Stage turns back upward after coding
   C. Requirements are skipped
   D. Maintenance precedes design

55. Agile emphasizes:
   A. Collaboration and adaptability
   B. No customer feedback
   C. Fixed scope always
   D. One-person teams

56. Scrum is primarily a:
   A. Security tool

B. Product development strategy/framework
C. Penetration test method
D. Compliance regulation

57. Which approach is explicitly said to be difficult for early SDL effort estimation?
A. Agile
B. Waterfall
C. V-model
D. End-of-life

58. Which is NOT listed as an SDLC approach in Lesson 3?
A. Scrum
B. XP
C. ITIL
D. Waterfall

59. Agile includes:
A. Four core values
B. Ten core values
C. Fourteen core values
D. No values

60. A waterfall outcome from one phase acts as:
A. Legal approval
B. Input for the next phase
C. Budget report
D. Threat source

Lesson 4 — SDL Phase A1: Security Assessment + Requirements

61. The first phase of the SDL is:
A. Architecture (A2)
B. Security Assessment (A1)
C. Ship (A5)
D. Post-Release Support

62. During A1, the team develops:
A. Final pen test report
B. Initial outline for security milestones integrated into schedule

C. Only marketing requirements
D. Only code review scripts

63. In A1, key stakeholders should:
A. Avoid discussing privacy
B. Have common understanding of security and privacy requirements
C. Skip security considerations
D. Only focus on UI design

64. Software security team should be included in SDLC kickoffs to ensure:
A. Security is built into the process
B. Testing is removed
C. Deployment is faster
D. Compliance is optional

65. A privacy impact assessment should include:
A. Only a logo
B. Summary of legislation and required steps
C. Only customer reviews
D. Only developer names

66. Creating success criteria for SDL phases helps:
A. Avoid documentation
B. Identify what worked/didn’t in postmortem
C. Remove metrics
D. Skip requirements

67. Creating key deliverables for each SDL phase ensures:
A. Tangible documented outcomes
B. No need to test
C. No need to plan
D. No need to trace requirements

68. In the SDL model, it is helpful to outline:
A. Vacation schedules
B. Metrics measured in every phase
C. Only marketing KPIs
D. Only sales targets

69. Three focus areas in secure software requirements are gathering requirements, data classification, and:
A. Network routing
B. Managing data protection requirements
C. Pricing strategy

D. Brand identity

70. Purpose of gathering requirements before kickoff is to:
A. Increase rework
B. Avoid common project failures by identifying requirements early
C. Delay delivery
D. Remove stakeholders

71. Functional requirements describe:
A. Constraints not affecting core purpose
B. What the system will do and its core purpose
C. Only legal standards
D. Only test scripts

72. Non-functional requirements describe:
A. Core purpose
B. Constraints/restrictions that do not impact core purpose
C. Only features
D. Only threat sources

73. Operational requirements refer to:
A. System function based on environment it will operate in
B. Only UI colors
C. Only database schema
D. Only encryption type

74. Compliance requirement areas are legal, financial, and:
A. Weather
B. Industry standards
C. Social media
D. Gamification

75. Product risk profile helps determine:
A. Actual cost of product from different perspectives
B. Only number of users
C. Only number of servers
D. Only code style

76. Requirement traceability matrix is:
A. A table listing all security requirements
B. A penetration test report
C. A DFD
D. A scanner output

77. Threat profile is:
    A. The attacker’s name
    B. The environment product operates in and threats in that environment
    C. A list of patches
    D. A deployment checklist

78. Privacy impact assessment evaluates:
    A. PII privacy issues and impact rating
    B. CPU performance only
    C. Marketing effectiveness
    D. UI layout

79. In A1, security milestones should be integrated into:
    A. HR handbook
    B. Development project schedule
    C. Customer support scripts
    D. Sales pipeline

80. Which is NOT a requirement type mentioned?
    A. Functional
    B. Non-functional
    C. Operational
    D. Artistic

Lesson 5 — SDL Phase A2: Architecture + Threat Modeling

81. The second SDL phase is focused on:
    A. End-of-life removal
    B. Bringing security considerations into the SDLC
    C. Only post-release response
    D. Only maintenance patches

82. Software security policy defines:
    A. Vacation rules
    B. What needs protection and how it will be protected
    C. Only coding language choice
    D. Only marketing scope

83. Threat modeling is a process to:
    A. Pinpoint threats and potential vulnerabilities to prioritize remediation
    B. Write UI requirements
    C. Remove testing
    D. Generate invoices

84. Threat modeling is proactive because it:
    A. Reacts only after attacks
    B. Prepares for threats before discovery
    C. Works only after deployment
    D. Eliminates risk

85. The 5 steps of threat modeling begin with:
    A. Identify security objectives
    B. Identify vulnerabilities
    C. Decompose it
    D. Identify threats

86. Which is the correct order?
    A. Survey → Decompose → Objectives → Threats → Vulnerabilities
    B. Objectives → Survey → Decompose → Threats → Vulnerabilities
    C. Decompose → Survey → Threats → Objectives → Vulnerabilities
    D. Objectives → Threats → Survey → Vulnerabilities → Decompose

87. Data flow diagrams provide:
    A. Legal proof
    B. Visual representation of a process flow
    C. Encryption keys
    D. Budget estimates

88. STRIDE includes:
    A. Spoofing
    B. Tampering
    C. Repudiation
    D. All of the above

89. Denial of service means:
    A. Denying access to valid users
    B. Changing stored data
    C. Reading files without permission
    D. Gaining admin access

90. Elevation of privilege means:
    A. Losing permissions

B. Gaining unauthorized privileged access
C. Writing documentation
D. Encrypting traffic

91. Spoofing means:
A. Legally logging in
B. Illegally accessing/using another user’s credentials
C. Destroying a database
D. Running scans

92. Tampering means:
A. Maliciously changing persistent data
B. Monitoring logs
C. Deleting backups
D. Creating DFDs

93. Repudiation means:
A. System can always trace actions
B. Illegal operations where system cannot trace them
C. System is offline
D. Strong authentication

94. Information disclosure means:
A. Sharing a press release
B. Reading a file you were not granted access to
C. Denying access
D. Elevating privileges

95. PASTA stands for:
A. Process for Attack Simulation and Threat Analysis
B. Password Analysis and Security Testing Approach
C. Program Assessment Standard for Technology Audits
D. Practical Agile Secure Threat Assessment

96. DREAD includes:
A. Damage potential
B. Reproducibility
C. Exploitability
D. All of the above

97. Threat source is:
A. Entity carrying out the attack
B. A patch
C. A compliance rule

D. A test script

98. Threat vector is:
A. Path attacker can take to exploit a vulnerability
B. A vulnerability database
C. A security policy
D. A code comment

99. Trike is a framework for:
A. Security auditing from risk management perspective
B. Cloud deployment
C. Network scanning
D. UI testing

100. Which is NOT listed as a threat modeling type?
A. Application-centric
B. Asset-centric
C. Ticket-centric
D. Both A and B are listed; C is not

Lesson 6 — SDL Phase A3: Design & Development testing foundations

101. A3 phase involves reviewing:
A. Only marketing policy
B. Policies outside SDL policy
C. Only code style rules
D. Only cloud contracts

102. Collaboration must occur between:
A. Software security group and centralized information security group
B. Sales and marketing only
C. Customers only
D. No one

103. Purpose of testing activities is to:
A. Validate security before release
B. Replace requirements
C. Remove code review

D. Avoid environments

104. Building security in is less costly than:

A. Writing code
B. Fixing after deployment
C. Planning
D. Designing

105. Test environment should:

A. Be totally different than production
B. Mimic execution environment as closely as possible
C. Only be paper-based
D. Never use virtualization

106. Security testing techniques are categorized by:

A. Red/Blue/Purple
B. White/Gray/Black box
C. Gold/Silver/Bronze
D. Alpha/Beta/Gamma

107. White box testing is:

A. External with no knowledge
B. Internal with full knowledge
C. Only usability testing
D. Only in production

108. Black box testing is:

A. Internal testing with full knowledge
B. External perspective with no prior knowledge
C. Code review
D. Static analysis only

109. Gray box testing:

A. Has partial knowledge and analyzes source code to design test cases
B. Has no knowledge
C. Is only for performance testing
D. Is only for end-of-life

110. Alpha testing is done by:

A. External users
B. Developers themselves
C. Legal counsel
D. Customers only

111. Beta testing is done by:

A. Developers only
B. Those not familiar with the development
C. Only automated tools
D. Only management

112. Security test cases help determine:

A. Marketing goals
B. Security issues at the lowest level
C. Salary bands
D. UI color schemes

113. Scanning involves:

A. Writing requirements
B. Identifying deficiencies anywhere around the system
C. Creating DFDs
D. Creating policies

114. Security testing is:

A. Static and one-time
B. Ongoing
C. Only done after ship
D. Only done in planning

115. Applications should be tested:

A. Only in lab
B. Only in operational environment
C. In lab and true operational environment
D. Only on paper

116. System test means:

A. Test only one function
B. Test system and its interaction with other systems
C. Only test UI
D. Only test network

117. Scripts are:

A. Random notes
B. Detailed logical step instructions for person/tool
C. Legal contracts
D. User personas

118. Secure testing scripts are:

A. Created specifically for the application being tested

B. Only for marketing
C. Only for payroll
D. Only for end-of-life

119. External resources are:
A. Resources from company org
B. Temporarily hired to test/report findings
C. Always developers
D. Always customers

120. Internal resources are:
A. Always outside consultants
B. From the company’s organization
C. Only attackers
D. Only auditors

Lesson 7 — SDL Phase A4: Code review + AppSec tooling

121. A4 phase continues to focus on:
A. Removing software
B. Security testing processes and analysis necessities
C. Only marketing plans
D. Only HR onboarding

122. QA testing occurs:
A. Only during testing phase
B. Throughout the entire SDLC
C. Only after deployment
D. Only in end-of-life

123. Three test type categories are:
A. Unit, integration, system
B. Benchmarks, scheduled, exploratory
C. Static, dynamic, fuzz
D. Alpha, beta, gamma

124. Code review helps catch:
A. Bugs early to decrease fix cost
B. Only design issues

C. Only legal issues
D. Only performance metrics

125. Four basic techniques for code review include all EXCEPT:
A. Static analysis
B. Manual code review
C. Automated scanning
D. Waterfall planning

126. AppSec describes:
A. Finding, fixing, preventing vulnerabilities at application level
B. Hiring only security engineers
C. Marketing security
D. End-of-life removal

127. AppSec is difficult to scale for:
A. Small organizations
B. Large organizations
C. Individuals only
D. No one

128. Proxy scripts are used to:
A. Communicate a web security bug/control effectively
B. Replace encryption
C. Replace policies
D. Replace requirements

129. Passive scanner:
A. Modifies HTTPS inputs
B. Silently analyzes HTTP requests/responses passing through tool
C. Deletes logs
D. Only runs in planning

130. Active scanner:
A. Silently observes only
B. Modifies HTTPS inputs and analyzes responses
C. Writes code automatically
D. Creates DFDs

131. Spider does what?
A. Identifies inputs and supplies them to scanning components
B. Encrypts traffic
C. Scores CVSS

D. Writes policies

132. SonarQube is primarily for:
A. Network scanning
B. Static code analysis across many languages
C. Cloud billing
D. UX design

133. AST is:
A. A network cable
B. Basis for software metrics/issues generated later
C. A vulnerability database
D. A pen test phase

134. Control flow analysis is used to:
A. Trace data input to output
B. Step through logical conditions
C. Fuzz endpoints
D. Scan ports

135. Data flow analysis is used to:
A. Step through conditions only
B. Trace data from input points to output points
C. Run alpha tests
D. Manage HR

136. Scheduled tests are:
A. Optional
B. Mandatory requirements testing to validate security
C. Only exploratory
D. Only benchmarks

137. Exploratory tests are done by:
A. Development tester continually assessing quality
B. Only customers
C. Only legal
D. Only external attackers

138. Benchmarks are tests used to compare:
A. Estimates to actual results
B. Threat sources to vectors
C. UI colors to fonts
D. Laws to budgets

139. Pull request is:
A. Request to merge code into another branch
B. A pen test report
C. A scan type
D. A DFD

140. ZAP stands for:
A. Zero Attack Policy
B. Zed Attack Proxy
C. Zone Access Procedure
D. Zonal Analysis Platform

Lesson 8 — SDL Phase A5: Ship (final review + scanning + pen testing)

141. Ship (A5) phase occurs when:
A. Security team performs final analysis/security review
B. Requirements are written
C. DFDs are drawn
D. End-of-life begins

142. Policy compliance analysis verifies:
A. Product meets quality standards before release
B. Product is profitable
C. Developers are trained
D. Cloud is free

143. Vulnerability scanning tools attempt to identify:
A. Weakness in applications
B. UI alignment issues
C. Salary issues
D. Branding issues

144. Penetration testing simulates:
A. Customer usage
B. Hacker actions to identify vulnerabilities
C. Legal reviews
D. Documentation writing

145. Pen test phases listed are:

A. Plan, build, test, ship
B. Assess, identify, evaluate and plan, deploy
C. Scan, patch, re-scan, close
D. Discover, exploit, monetize, exit

146. Creating a networking laboratory helps you test:

A. Within controlled environment without written authorization/permissions
B. Only in production
C. Only on paper
D. Only with customer data

147. Nmap is used for:

A. Network scanning and security auditing
B. Code review
C. Password hashing
D. UI testing

148. Authenticated scans:

A. Require software to log onto system
B. Never use credentials
C. Only run externally
D. Only run at end-of-life

149. External scans target issues found:

A. Inside firewall only
B. Outside the firewall
C. Only in source code
D. Only in documentation

150. Internal scans identify issues that could be exploited:

A. From inside the network
B. Only outside network
C. Only by legal
D. Only by marketing

151. Intrusive target search means scans:

A. Never exploit
B. Exploit a vulnerability when identified
C. Only observe logs
D. Only list ports

152. A “range” is:

A. A budgeting spreadsheet

B. Networking lab to conduct vulnerability analysis testing
C. A code style guide
D. A cloud region only

153. Target machine is:
A. Virtual space to practice identifying attack surfaces
B. HR system
C. Legal database
D. Marketing site

154. Virtualization is:
A. Technology to create software services
B. Physical cabling method
C. Threat model type
D. Policy standard

155. Vulnerability scan means:
A. Explore apps/databases to identify weaknesses
B. Merge code branches
C. Train developers
D. Create compliance reports

156. Vulnerability sites provide:
A. Latest known vulnerabilities information
B. Only design templates
C. Only payroll forms
D. Only user stories

157. Open-source software license compliance refers to:
A. Regulations regarding licensing of in-house products
B. A scan type
C. A threat model
D. A pen test phase

158. Open-source software security is:
A. Identifying software security within in-house developed software
B. Only buying proprietary tools
C. Only marketing
D. Only end-of-life

159. SQL injection is:
A. Code injection that might destroy software
B. A port scan technique
C. A DFD type

D. A compliance framework

160. Active and passive analysis techniques are useful during:
A. Vulnerability testing
B. Branding review
C. Sprint planning only
D. End-of-life only

Lesson 9 — Post-release support + PSIRT + CVSS + M&A

161. Having software security experts report to engineering enables:
A. Weaker relationship
B. Stronger relationship during secure development
C. No difference
D. Only legal alignment

162. Quality security is built:
A. Only in one SDLC phase
B. Throughout the entire engineering process
C. Only after release
D. Only in planning

163. Not every company can include all PRSAs, so you should:
A. Ignore security
B. Choose highest value and optimize available tools
C. Only do pen tests
D. Only do code reviews

164. CVSS is used to:
A. Assess severity of a vulnerability
B. Draw DFDs
C. Run port scans
D. Manage budgets

165. Post-release privacy issues may need additional:
A. Marketing
B. Development, QA, and/or security resources
C. Office space
D. Vacation time

166. Third-party reviews may be necessary when completing:
A. Post-release review
B. Planning
C. Requirements writing
D. End-of-life only

167. During M&A, software security may go under:
A. Architectural review
B. UI review only
C. Payroll review
D. Logo redesign

168. Requirements for post-release certifications should be included:
A. After deployment only
B. Before deployment in security/privacy requirements
C. Only in marketing
D. Only in HR policy

169. PSIRT is:
A. Team that receives/investigates/reports vulnerabilities
B. A scan tool
C. A threat model
D. A coding language

170. Post-Release Support phase is when orgs prepare for:
A. New hires
B. Vulnerabilities after product release
C. UI redesign
D. Budget cuts

171. Post-Release PSIRT Response involves:
A. Internal-only discoveries
B. External discovery of post-release vulnerabilities
C. Writing requirements
D. Decomposing apps

172. Legacy code is:
A. Old code no longer supported
B. New code in main branch
C. Code with tests
D. Code under active development

173. M&A means:
A. Metrics and Analysis

B. Merger and acquisition
C. Maintenance and Availability
D. Model and Architecture

174. Software Security Champion (SSC) is an expert on:
A. Promoting security awareness and best practices
B. Writing sales copy
C. Running payroll
D. Managing cloud bills

175. Software Security Evangelist (SSE) is an expert to promote:
A. Awareness of products to wider community
B. Only internal HR policies
C. Only compliance fines
D. Only backups

176. Strong security relationship is supported when security reports to:
A. Engineering organization
B. Customers
C. Vendors
D. Competitors

177. Security should be built:
A. Only at ship
B. Throughout engineering process
C. Only post-release
D. Only in design

178. Post-release privacy issues could require additional:
A. QA
B. Security
C. Development
D. All of the above

179. PSIRT deals with:
A. Marketing incidents
B. Software product security incidents and vulnerabilities
C. UI bugs only
D. Feature requests

180. Which term refers to consolidation of companies?
A. M&A
B. CVSS
C. CVE

D. STRIDE

Lesson 10 —Modern environments + OpenSAMM + BSIMM categories + STRIDE recap

181. Software is most likely deployed in:
A. Only Waterfall
B. Agile, DevOps, Digital Enterprise, or combinations
C. Only end-of-life
D. Only planning

182. Agile development is designed to:
A. Deliver value faster
B. Eliminate requirements
C. Stop deployments
D. Avoid collaboration

183. DevOps teams work together for:
A. Ongoing operations, enhancements, defect removal, optimization
B. Only marketing
C. Only requirements writing
D. Only end-of-life

184. Cloud technology has caused a rethinking of how apps are:
A. Built, deployed, and used
B. Sold only
C. Named only
D. Ignored

185. Moving to public cloud services has increased:
A. Security challenges
B. Printer usage
C. HR workload
D. Coffee sales

186. Digital enterprises use technology to:
A. Enable and improve business activities
B. Avoid business activities
C. Remove all risk

D. Ban software

187. OpenSAMM business functions include governance, construction, verification, and:
A. Marketing
B. Deployment
C. Payroll
D. Recruiting

188. BSIMM is a study of:
A. Only CVEs
B. Existing software security initiatives in larger development
C. Only networks
D. Only regulations

189. The four BSIMM category types are governance, intelligence, SSDL touchpoints, and:
A. Sales
B. Deployment
C. Finance
D. Branding

190. Threats can be classified using STRIDE. Which is included?
A. Spoofing
B. Tampering
C. Elevation of privilege
D. All of the above

191. In OpenSAMM, “verification” is centered around:
A. Managing overall activities
B. Checking and testing artifacts produced through development
C. Releasing software
D. Capturing security info only

192. In OpenSAMM, “governance” is centered around:
A. How org manages overall software development activities
B. How org releases software
C. Only code review
D. Only environment hardening

193. “Construction” in OpenSAMM is centered around:
A. How org defines goals and creates software within projects
B. Only incident response
C. Only vulnerability disclosure

D. Only HR

194. “Deployment” in OpenSAMM is centered around:

A. How org releases software
B. Only threat modeling
C. Only coding
D. Only design review

195. Code review (CR) is a practice of:

A. Verification
B. Deployment
C. Governance
D. Construction

196. Design review (DR) is a practice of:

A. Verification
B. Construction
C. Governance
D. Deployment

197. Education and guidance (EG) is a practice of:

A. Governance
B. Verification
C. Deployment
D. Construction

198. Environment hardening (EH) is a practice of:

A. Deployment
B. Governance
C. Verification
D. Construction

199. Vulnerability management (VM) is a practice of:

A. Deployment
B. Construction
C. Verification
D. Governance

200. Threat assessment (TA) is a practice of:

A. Construction
B. Governance
C. Verification
D. Deployment

Answer Key

1 C
2 A
3 B
4 B
5 C
6 A
7 B
8 A
9 A
10 B
11 B
12 A
13 C
14 B
15 B
16 B
17 C
18 C
19 A
20 B

21 B
22 B
23 B
24 B
25 C
26 B
27 B
28 A
29 B
30 B
31 B
32 A
33 B
34 B
35 B
36 B
37 B
38 A
39 A
40 D

41 B
42 B
43 B
44 B
45 B
46 B
47 B
48 B
49 B
50 B
51 B
52 B
53 A
54 B
55 A
56 B
57 A
58 C
59 A
60 B

61 B
62 B
63 B
64 A
65 B
66 B
67 A
68 B
69 B
70 B
71 B
72 B
73 A
74 B
75 A
76 A
77 B
78 A
79 B
80 D

81 B
82 B
83 A

84 B
85 A
86 B
87 B
88 D
89 A
90 B
91 B
92 A
93 B
94 B
95 A
96 D
97 A
98 A
99 A
100 C

101 B
102 A
103 A
104 B
105 B
106 B
107 B
108 B
109 A
110 B
111 B
112 B
113 B
114 B
115 C
116 B
117 B
118 A
119 B
120 B

121 B
122 B
123 B
124 A
125 D
126 A

127 B
128 A
129 B
130 B
131 A
132 B
133 B
134 B
135 B
136 B
137 A
138 A
139 A
140 B

141 A
142 A
143 A
144 B
145 B
146 A
147 A
148 A
149 B
150 A
151 B
152 B
153 A
154 A
155 A
156 A
157 A
158 A
159 A
160 A

161 B
162 B
163 B
164 A
165 B
166 A
167 A
168 B
169 A

170	B
171	B
172	A
173	B
174	A
175	A
176	A
177	B
178	D
179	B
180	A
181	B
182	A
183	A
184	A
185	A
186	A
187	B
188	B
189	B
190	D
191	B
192	A
193	A
194	A
195	A
196	A
197	A
198	A
199	A
200	A