

Chapter 1

Security Architecture

THE CASP+ EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE:

✓ Domain 1: Security Architecture

- 1.1 Given a scenario, analyze the security requirements and objectives to ensure an appropriate, secure network architecture for a new or existing network.
 - Services
 - Load balancer
 - Intrusion detection system (IDS)/network intrusion detection system (NIDS)/wireless intrusion detection system (WIDS)
 - Intrusion prevention system (IPS)/network intrusion prevention system (NIPS)/wireless intrusion prevention system (WIPS)
 - Web application firewall (WAF)
 - Network access control (NAC)
 - Virtual private network (VPN)
 - Domain Name System Security Extensions (DNSSEC)
 - Firewall/unified threat management (UTM)/next-generation firewall (NGFW)
 - Network address translation (NAT) gateway
 - Internet gateway
 - Forward/transparent proxy
 - Reverse proxy
 - Distributed denial-of-service (DDoS) protection
 - Routers
 - Mail security
 - Application programming interface (API) gateway/Extensible Markup Language (XML) gateway



- Traffic mirroring
- Switched port analyzer (SPAN) ports
- Port mirroring
- Virtual private cloud (VPC)
- Network tap
- Sensors
- Security information and event management (SIEM)
- File integrity monitoring (FIM)
- Simple Network Management Protocol (SNMP) traps
- NetFlow
- Data loss prevention (DLP)
- Antivirus
- Segmentation
 - Microsegmentation
 - Local area network (LAN)/virtual local area network (VLAN)
 - Jump box
 - Screened subnet
 - Data zones
 - Staging environments
 - Guest environments
 - VPC/virtual network (VNET)
 - Availability zone
 - NAC lists
 - Policies/security groups
 - Regions
 - Access control lists (ACLs)
 - Peer-to-peer
 - Air gap



- Deperimeterization/zero trust
 - Cloud
 - Remote work
 - Mobile
 - Outsourcing and contracting
 - Wireless/radio frequency (RF) networks
- Merging of networks from various organizations
 - Peering
 - Cloud to on premises
 - Data sensitivity levels
 - Mergers and acquisitions
 - Cross-domain
 - Federation
 - Directory services
- Software-defined networking (SDN)
 - Open SDN
 - Hybrid SDN
 - SDN overlay
- 1.2 Given a scenario, analyze the organizational requirements to determine the proper infrastructure security design.
 - Scalability
 - Vertically
 - Horizontally
 - Resiliency
 - High availability
 - Diversity/heterogeneity
 - Course of action orchestration
 - Distributed allocation
 - Redundancy
 - Replication
 - Clustering



- Automation
 - Autoscaling
 - Security Orchestration, Automation and Response (SOAR)
 - Bootstrapping
- Performance
- Containerization
- Virtualization
- Content delivery network
- Caching
- 1.3 Given a scenario, integrate software applications securely into an enterprise architecture.
 - Baseline and templates
 - Secure design patterns/types of web technologies
 - Storage design patterns
 - Container APIs
 - Secure coding standards
 - Application vetting processes
 - API management
 - Middleware
 - Software assurance
 - Sandboxing/development environment
 - Validating third-party libraries
 - Defined DevOps pipeline
 - Code signing
 - Interactive application security testing (IAST) vs. dynamic application security testing (DAST) vs. static application security testing (SAST)
 - Considerations of integrating enterprise applications
 - Customer relationship management (CRM)



- Enterprise resource planning (ERP)
- Configuration management database (CMDB)
- Content management system (CMS)
- Integration enablers
- Directory services
- Domain name system (DNS)
- Service-oriented architecture (SOA)
- Enterprise service bus (ESB)
- Integrating security into development life cycle
 - Formal methods
 - Requirements
 - Fielding
 - Insertions and upgrades
 - Disposal and reuse
 - Testing
 - Regression
 - Unit testing
 - Integration testing
 - Development approaches
 - SecDevOps
 - Agile
 - Waterfall
 - Spiral
 - Versioning
 - Continuous integration/continuous delivery (CI/CD) pipelines
 - Best practices
 - Open Web Application Security Project (OWASP)
 - Proper HypertextTransfer Protocol (HTTP) headers



- 1.4 Given a scenario, implement data security techniques for securing enterprise architecture.
 - Data loss prevention
 - Blocking use of external media
 - Print blocking
 - Remote Desktop Protocol (RDP) blocking
 - Clipboard privacy controls
 - Restricted virtual desktop infrastructure (VDI) implementation
 - Data classification blocking
 - Data loss detection
 - Watermarking
 - Digital rights management (DRM)
 - Network traffic decryption/deep packet inspection
 - Network traffic analysis
 - Data classification, labeling, and tagging
 - Metadata/attributes
 - Obfuscation
 - Tokenization
 - Scrubbing
 - Masking
 - Anonymization
 - Encrypted vs. unencrypted
 - Data life cycle
 - Create
 - Use
 - Share
 - Store
 - Archive
 - Destroy



- Data inventory and mapping
- Data integrity management
- Data storage, backup, and recovery
 - Redundant array of inexpensive disks (RAID)
- 1.5 Given a scenario, analyze the security requirements and objectives to provide the appropriate authentication and authorization controls.
 - Credential management
 - Password repository application
 - End-user password storage
 - On premises vs. cloud repository
 - Hardware key manager
 - Privileged access management
 - Password policies
 - Complexity
 - Length
 - Character classes
 - History
 - Maximum/minimum age
 - Auditing
 - Reversible encryption
 - Federation
 - Transitive trust
 - OpenID
 - Security Assertion Markup Language (SAML)
 - Shibboleth
 - Access control
 - Mandatory access control (MAC)
 - Discretionary access control (DAC)
 - Role-based access control



- Rule-based access control
- Attribute-based access control
- Protocols
 - Remote Authentication Dial-in User Server (RADIUS)
 - Terminal Access Controller Access Control System (TACACS)
 - Diameter
 - Lightweight Directory Access Protocol (LDAP)
 - Kerberos
 - OAuth
 - 802.1X
 - Extensible Authentication Protocol (EAP)
- Multifactor authentication (MFA)
 - Two-factor authentication (2FA)
 - 2-Step Verification
 - In-band
 - Out-of-band
- One-time password (OTP)
 - HMAC-based one-time password (HOTP)
 - Time-based one-time password (TOTP)
- Hardware root of trust
- Single sign-on (SSO)
- JavaScript Object Notation (JSON) web token (JWT)
- Attestation and identity proofing
- 1.6 Given a set of requirements, implement secure cloud and virtualization solutions.
 - Virtualization strategies
 - Type 1 vs. Type 2 hypervisors
 - Containers
 - Emulation



- Application virtualization
- VDI
- Provisioning and deprovisioning
- Middleware
- Metadata and tags
- Deployment models and considerations
 - Business directives
 - Cost
 - Scalability
 - Resources
 - Location
 - Data protection
 - Cloud deployment models
 - Private
 - Public
 - Hybrid
 - Community
- Hosting models
 - Multitenant
 - Single-tenant
- Service models
 - Software as a service (SaaS)
 - Platform as a service (PaaS)
 - Infrastructure as a service (IaaS)
- Cloud provider limitations
 - Internet Protocol (IP) address scheme
 - VPC peering
- Extending appropriate on-premises controls



- Storage models
 - Object storage/file-based storage
 - Database storage
 - Block storage
 - Blob storage
 - Key-value pairs
- 1.7 Explain how cryptography and public key infrastructure (PKI) support security objectives and requirements.
 - Privacy and confidentiality requirements
 - Integrity requirements
 - Non-repudiation
 - Compliance and policy requirements
 - Common cryptography use cases
 - Data at rest
 - Data in transit
 - Data in process/data in use
 - Protection of web services
 - Embedded systems
 - Key escrow/management
 - Mobile security
 - Secure authentication
 - Smart card
 - Common PKI use cases
 - Web services
 - Email
 - Code signing
 - Federation
 - Trust models
 - VPN
 - Enterprise and security automation/orchestration



- 1.8 Explain the impact of emerging technologies on enterprise security and privacy.
 - Artificial intelligence
 - Machine learning
 - Quantum computing
 - Blockchain
 - Homomorphic encryption
 - Private information retrieval
 - Secure function evaluation
 - Private function evaluation
 - Secure multiparty computation
 - Distributed consensus
 - Big Data
 - Virtual/augmented reality
 - 3D printing
 - Passwordless authentication
 - Nano technology
 - Deep learning
 - Natural language processing
 - Deep fakes
 - Biometric impersonation

12 Chapter 1 • Security Architecture

1. Your organization experienced a security event that led to the loss and disruption of services. You were chosen to investigate the disruption to prevent the risk of it happening again. What is this process called?
 - A. Incident management
 - B. Forensic tasks
 - C. Mandatory vacation
 - D. Job rotation
2. Brett is a new CISO, and he is evaluating different controls for availability. Which set of controls should he choose?
 - A. RAID 1, classification of data, and load balancing
 - B. Digital signatures, encryption, and hashes
 - C. Steganography, ACLs, and vulnerability management
 - D. Checksums, DOS attacks, and RAID 0
3. Charles has received final documentation from a compliance audit. The report suggested his organization should implement a complementary security tool to work with the firewall to detect any attempt at scanning. Which device does Charles choose?
 - A. RAS
 - B. PBX
 - C. IDS
 - D. DDT
4. Nicole is the security administrator for a large governmental agency. She has implemented port security, restricted network traffic, and installed NIDS, firewalls, and spam filters. She thinks the network is secure. Now she wants to focus on endpoint security. What is the most comprehensive plan for her to follow?
 - A. Antimalware/virus/spyware, host-based firewall, and MFA
 - B. Antivirus/spam, host-based IDS, and TFA
 - C. Antimalware/virus, host-based IDS, and biometrics
 - D. Antivirus/spam, host-based IDS, and SSO
5. Sally's CISO asked her to recommend an intrusion system to recognize intrusions traversing the network and send email alerts to the IT staff when one is detected. What type of intrusion system does the CISO want?
 - A. HIDS
 - B. NIDS
 - C. HIPS
 - D. NIPS

6. Kenneth is the CISO of an engineering organization. He asked the security department to recommend a system to be placed on business-critical servers to detect and stop intrusions. Which of the following will meet the CISO's requirement?
 - A. HIPS
 - B. NIDS
 - C. HIDS
 - D. NIPS
7. Paul's company has discovered that some of his organization's employees are using personal devices, including cell phones, within highly secure areas. The CISO wants to know which employees are violating this policy. Which of the following devices can inform the CISO who is violating this policy?
 - A. DLP
 - B. WIDS
 - C. NIPS
 - D. Firewall
8. Suzette's company discovered that some of her organization's employees are copying corporate documents to Microsoft blob cloud drives outside the control of the company. She has been instructed to stop this practice from occurring. Which of the following can stop this practice from happening?
 - A. DLP
 - B. NIDS
 - C. NIPS
 - D. Firewall
9. Troy must decide about his organization's file integrity monitoring (FIM) monitoring. Stand-alone FIM generally means file analysis only. Another option is to integrate it with the host so that Troy can detect threats in other areas, such as system memory or an I/O. For the integration, which of the following does Troy need to use?
 - A. HIDS
 - B. ADVFIM
 - C. NIDS
 - D. Change management
10. Lisa is building a network intrusion detection system (NIDS). What can an NIDS do with encrypted network traffic?
 - A. Look for viruses
 - B. Examine contents of email
 - C. Bypass VPN
 - D. Nothing

11. What system is used to collect and analyze data logs from various network devices and to report detected security events?
 - A. Syslog server
 - B. NIPS
 - C. WIPS
 - D. SIEM system
12. The IT department decided to implement a security appliance in front of their web servers to inspect HTTP/HTTPS/SOAP traffic for malicious activity. Which of the following is the *best* solution to use?
 - A. Screened host firewall
 - B. Packet filter firewall
 - C. DMZ
 - D. WAF
13. A security audit was conducted for your organization. It found that a computer plugged into any Ethernet port in its shipping facility was able to access network resources without authentication. You are directed to fix this security issue. Which standard, if implemented, could resolve this issue?
 - A. 802.1x
 - B. 802.3
 - C. 802.1q
 - D. 802.11
14. Your CISO is concerned with unauthorized network access to the corporate wireless network. You want to set a mechanism in place that not only authenticates the wireless devices but also requires them to meet a predefined corporate policy before allowing them on the network. What technology *best* performs this function?
 - A. HIDS
 - B. NAC
 - C. Software agent
 - D. NIPS
15. David's security team is implementing NAC for authentication as well as corporate policy enforcement. The team wants to install software on the devices to perform these tasks. In the context of NAC, what is this software called?
 - A. Program
 - B. Process
 - C. Agent
 - D. Thread

16. Grace is investigating the encryption of data at rest and data in transit and trying to determine which algorithm is best in each situation. Which of the following does not contain data at rest?
- A. SAN
 - B. NAS
 - C. SSD
 - D. VPN
17. Your employees need internal access while traveling to remote locations. You need a service that enables them to securely connect back to a private corporate network from a public network to log into a centralized portal. You want the traffic to be encrypted. Which of the following is the *best* tool?
- A. Wi-Fi
 - B. VPN
 - C. RDP
 - D. NIC
18. Robert's employees complain that when they connect to the network through the VPN, they cannot view their social media posts and pictures. What mostly likely has been implemented?
- A. Split tunnels
 - B. DNS tunneling
 - C. ARP cache
 - D. Full tunnels
19. Robin's company is merging with another healthcare organization. The stakeholders are discussing the security aspects of combining digital communications. The main agreed-upon criterion for compliance and security is protecting the sharing of the business's domains. What is the best option for this organization?
- A. DNSSEC
 - B. TLS
 - C. SSL 2.0
 - D. Keeping both entities separate
20. You are a network security administrator for a SOHO. Your staff tends to work from coffee shops without understanding the need for a VPN. You must show them why this can be dangerous. What network traffic packets are commonly captured and used in a replay attack?
- A. Packet headers
 - B. Authentication
 - C. FTP
 - D. DNS

21. Sally needs to implement a network security device at the border of her corporate network and the Internet. This device filters network traffic based on source and destination IP addresses, source and destination port numbers, and protocols. Which network security device *best* suits her needs?
- A. Packet filter firewall
 - B. Proxy server
 - C. HSM
 - D. DMZ
22. The IT security department was tasked with recommending a single security device that can perform various security functions. The security functions include antivirus protection, anti-spyware, a firewall, and an IDP. What device should the IT security department recommend?
- A. Next-generation firewall
 - B. Unified threat management system
 - C. Quantum proxy
 - D. Next-generation IDP
23. One of your network administrators reports that they cannot connect to a device on the local network using its IP address. The device is up and running with an IP address of 10.0.0.5. Other hosts can communicate with the device. The default gateway is 10.0.0.1, and your local IP address is 10.0.0.3. What is the *best* type of scan to run to find the MAC of the offending machine?
- A. ARP
 - B. NAT gateway
 - C. IPConfig
 - D. IFConfig
24. Ronald has architected his network to hide the source of a network connection. What device has he most probably used?
- A. Proxy firewall
 - B. Internet gateway
 - C. Layer 3 switch
 - D. Bastion host
25. The IT group within your organization wants to filter requests between clients and their servers. They want to place a device in front of the servers that acts as a go-between for the clients and the servers. This device receives the request from the clients and forwards the request to the servers. The server will reply to the request by sending the reply to the device; then the device will forward the reply to the clients. What device best meets this description?
- A. Firewall
 - B. NIDS
 - C. Reverse proxy
 - D. Proxy

26. Many users within your organization clicked on emails that, while looking legitimate, are malicious. Malicious code executes once the email is opened, infecting the user's system with malware. What could be implemented on the email server to help prevent such emails from reaching the end user?
- A. Firewall
 - B. Spam filters
 - C. WAF
 - D. Forward proxy
27. Your network administrator, George, reaches out to you to investigate why your e-commerce site went down twice in the past three days. Everything looks good on your network, so you reach out to your ISP. You suspect an attacker set up botnets that flood your DNS server with invalid requests. You find this out by examining your external logging service. What is this type of attack called?
- A. DDoS
 - B. Spamming
 - C. IP spoofing
 - D. Containerization
28. Aaron's end users are having difficulty signing into the network. The investigation of the situation leads him to believe it is which type of attack?
- A. Port scanning
 - B. DDoS
 - C. Pass-the-hash
 - D. Trojan
29. A network engineer must configure a router on the network remotely. What protocol should be used to ensure a secure connection?
- A. Telnet
 - B. FTP
 - C. HTTP
 - D. SSH
30. Ian has joined a company that licenses a third party's software and email service that is delivered to end users through a browser. What type of organization does Ian work for?
- A. IaaS
 - B. SaaS
 - C. PaaS
 - D. BaaS

31. You are a security analyst with an enterprise global financial organization. The company just experienced an advanced persistent threat (APT) type of attack that was traced to ransomware delivered to end users via a phishing campaign. One of your IT analysts forwarded the email to the `phishing@mycompany.com` address. You want to rip open the ransomware to see what it does and what asset it touches. What do you build?
- A. Cloud sandbox
 - B. A container
 - C. SLA
 - D. A hypervisor
32. Cody configured the application programming interface (API) connection between your web application that manages retail transactions and your bank. This connection must be as secure as possible. Because the API connection will handle financial transactions, what is the *best* choice for securing the API if it is well designed?
- A. SOAP
 - B. HTTPS
 - C. REST
 - D. XML
33. Aniket is looking for a web server to process requests sent by XML. What is the *best* technology to use for this?
- A. REST
 - B. SOAP
 - C. Ajax
 - D. XSS
34. The Cisco switch port you are using for traffic analysis and troubleshooting has a dedicated SPAN port that is in an “error-disabled state”; what is the procedure to reenab le it after you enter privilege exec mode?
- A. Issue the `no shutdown` command on the error-disabled interface.
 - B. Issue the `shutdown` and then the `no shutdown` command on the error-disabled interface.
 - C. Issue the `no error` command on the error-disabled interface.
 - D. Issue the `no error-disable` command on the error-disabled interface.
35. You were asked to recommend a solution to intercept and mirror network traffic and analyze its content for malicious activity while not interacting with the host computer. Of the following, which is the *best* solution?
- A. System scanner
 - B. Application scanner
 - C. Active vulnerability scanner
 - D. Passive vulnerability scanner

- 36.** One of Robert's objectives and key results (OKRs) for the upcoming year is to modernize the IT strategy by adopting a virtual cloud and taking advantage of new features and storage. He understands that once intellectual property is in the cloud, he could have less visibility and control as a consumer. What else is a major security concern for important data stored in the public cloud versus a private cloud?
- A.** Cost effectiveness
 - B.** Elastic use
 - C.** Being on demand
 - D.** Data remnants
- 37.** Your news organization is dealing with a recent defacement of your website and secure web server. The server was compromised around a three-day holiday weekend while most of the IT staff was not at work. The network diagram, in the order from the outside in, consists of the Internet, firewall, IDS, SSL accelerator, web server farm, internal firewall, and internal network. You attempt a forensic analysis, but all the web server logs have been deleted, and the internal firewall logs show no activity. As the security administrator, what do you do?
- A.** Review sensor placement and examine the external firewall logs to find the attack.
 - B.** Review the IDS logs to determine the source of the attack.
 - C.** Correlate all the logs from all the devices to find where the organization was compromised.
 - D.** Reconfigure the network and put the IDS between the SSL accelerator and server farm to better determine the cause of future attacks.
- 38.** After merging with a newly acquired company, Gavin comes to work Monday morning to find a metamorphic worm from the newly acquired network spreading through the parent organization. The security administrator isolated the worm using a network traffic access point (TAP) mirroring all the new network traffic and found it spreading on TCP port 445. What does Gavin advise the administrator to do to immediately to minimize the attack?
- A.** Run Wireshark to watch for traffic on TCP port 445.
 - B.** Update antivirus software and scan the entire enterprise.
 - C.** Check the SIEM for alerts for any asset with TCP port 445 open.
 - D.** Deploy an ACL to all HIPS: DENY-TCP-ANY-ANY-445.
- 39.** Jonathan is a senior architect who has submitted budget requests to the CISO to upgrade their security landscape. One item to purchase in the new year is a security information and event management (SIEM) system. What is the primary function of a SIEM tool?
- A.** Blocking malicious users and traffic
 - B.** Monitoring the network
 - C.** Automating DNS servers
 - D.** Monitoring servers

40. Janet has critical files and intellectual property on several filesystems and needs to be alerted if these files are altered by either trusted insiders abusing their privilege or malware. What should she implement?
- A. FIM
 - B. PCI
 - C. DNS
 - D. TCP
41. You are configuring SNMP on a Windows server. You have found that you are currently running SNMPv2c. Why would you want to upgrade to SNMPv3?
- A. Cryptographic security system
 - B. Party-based security system
 - C. Easier to set up
 - D. Supports UDP
42. Victor is employed in a high-risk geographically diverse environment heavily using Cisco IOS. Which of these are not key service advantages of NetFlow?
- A. Peer-to-peer tunneling encryption
 - B. Network traffic accounting and usage-based billing
 - C. Network planning and security
 - D. DoS monitoring capabilities
43. One of your managers asked you to research data loss prevention techniques to protect data so that cyber attackers cannot monetize the stolen data. What DLP do you recommend?
- A. Encryption and tokenization
 - B. HIPAA and PCI
 - C. I&AM management
 - D. NIST frameworks
44. Eddie is looking for an antivirus detection tool that uses a rule or weight-based system to determine how much danger a program function could be. What type of antivirus does he need?
- A. Behavioral
 - B. Signature based
 - C. Heuristic
 - D. Automated

45. Simon's organization has endpoints that are considered low-priority systems. Even though they are considered low priority, they still must be protected from malicious code capable of destroying data and corrupting systems. Malicious code is capable of infecting files but generally needs help moving from one system to another. What type of security product protects systems from this type of malicious code only?
- A. Antimalware
 - B. Antispyware
 - C. Antivirus
 - D. Anti-adware
46. An employee downloads a video of someone stealing a package off their porch from their smart doorbell. How do you mitigate the risk of storing that type of data on your business network?
- A. Implementing a security policy and awareness
 - B. Performing audits
 - C. Monitoring networks for certain file types
 - D. Using third-party threat intelligence reports
47. You conduct a security assessment and find legacy systems with vital business processes using standard Telnet protocols. What should you do to mitigate the risk?
- A. Migrate from IPv4 to IPv6.
 - B. Install PuTTY.
 - C. Move the system to a secure VLAN.
 - D. Unplug the system until a replacement can be ordered.
48. Your hospital just merged with another hospital in another state that falls under a different legal jurisdiction. You are tasked with improving network security. Your CISO suggests data isolation by blocking communication between the two hospitals. How do you accomplish this?
- A. Implementing HIDS
 - B. Building gateway firewalls
 - C. Configuring ERP
 - D. Creating network microsegmentation
49. Your company grew to a point where a screened host firewall solution is no longer viable. IT wants to move to a screened subnet solution. Which of the following is considered a type of screened subnet?
- A. LAN
 - B. DMZ
 - C. Egress
 - D. WAN

50. Your CISO asked you to implement a solution on the jump servers in your DMZ that can detect and stop malicious activity. Which solution accomplishes this task?
- A. HIDS
 - B. NIDS
 - C. HIPS
 - D. NIPS
51. Matthew's company just learned that an attacker obtained highly classified information by querying the external DNS server. He is told to never let this happen again. Which of the following is the best option?
- A. Implement a split DNS. Create an internal and external zone to resolve all domain queries.
 - B. Implement a split DNS. Create an internal zone for an internal DNS for resolution and an external zone to be used by the Internet.
 - C. Create DNS parking for round-robin DNSBL.
 - D. Create DNS parking for cloud users.
52. Peyton is an IT administrator needing visibility into his staging network. He believes he has all the tools and controls in place, but he has no way to look for attackers who are currently exploiting the network. What tool can Peyton choose to help with seeing the dark spots in his environment?
- A. Fuzzer
 - B. HTTP interceptor
 - C. Port scanner
 - D. SIEM
53. You want to replace an access point's removable antenna with a better one based on the results gathered by a wireless site survey. You want to be able to focus more energy in one direction and less in another to better distinguish between networks. What type of antenna should you purchase?
- A. Directional
 - B. Omnidirectional
 - C. Parabolic dish
 - D. Radio
54. Which of the following is a protocol that provides a graphical interface to a Windows system over a network?
- A. RDP
 - B. VNC
 - C. VDI
 - D. DLP

55. An attacker scanned your network and discovered a host system running a vulnerable version of VNC. Which of the following can an attacker perform if they can access VNC on the host?
- A. Remotely access the BIOS of the host system.
 - B. Remotely view and control the desktop of the host system.
 - C. Remotely view critical failures, causing a stop error or the blue screen of death on the host system.
 - D. All of the above.
56. Levi's corporate public cloud network is configured such that all network devices reach each other without going through a routing device. The CISO wants the network reconfigured so that the network is segmented based on geography. In addition, the servers must be on their own subnetwork. What is a benefit of subdividing the network in this way?
- A. No benefit at all.
 - B. By subdividing the network, the port numbers can be better distributed among assets.
 - C. By subdividing the network, rules can be placed to control the flow of traffic from one subnetwork to another.
 - D. Ease of deployment.
57. Your security team implemented NAC lists for authentication as well as corporate policy enforcement. Originally, the team installed software on the devices to perform these tasks. However, the security team decided this method is no longer desirable. They want to implement a solution that performs the same function but doesn't require software be installed on the devices. In the context of NAC, what is this configuration called?
- A. Agent
 - B. Agentless
 - C. Volatile
 - D. Persistent
58. Jason's organization recently deployed some standard Linux systems in its network. The system admin for these Linux systems wants to secure these systems by using SELinux, which is required by their security policy. Which of the following is a benefit of using SELinux?
- A. Moves from a discretionary access control system to a system where the file creator controls the permissions of the file
 - B. Moves from a discretionary access control system to a mandatory access control system
 - C. Moves from a mandatory access control system to a system where the file creator controls the permissions of the file
 - D. Moves from a mandatory access control system to a discretionary access control system

59. Bobby is a security risk manager with a global organization. The organization recently evaluated the risk of flash floods on its operations in several regions and determined that the cost of responding is expensive. The organization chooses to take no action currently. What was the risk management strategy deployed?
 - A. Risk mitigation
 - B. Risk acceptance
 - C. Risk avoidance
 - D. Risk transference
60. Randolph is a newly hired CISO, and he is evaluating controls for the confidentiality portion of the CIA triad. Which set of controls should he choose to concentrate on for confidentiality?
 - A. RAID 1, classification of data, and load balancing
 - B. Digital signatures, encryption, and hashes
 - C. Steganography, ACL, and vulnerability management
 - D. Checksum, DOS attacks, and RAID 0
61. You are tasked with deploying a system so that it operates at a single classification level. All the users who access this system have the same clearance, classification, and need to know. What is this operating mode?
 - A. High mode
 - B. Dedicated
 - C. Peer to peer
 - D. Multilevel
62. You work as an independent security consultant for a small town in the Midwest that was just breached by a foreign country. When it came time for payment to a town vendor, someone changed the transfers of monies from a physical check to an electronic payment. In response, what is the first security practice suggestion you make to prevent this from recurring?
 - A. Incorporation
 - B. Investigation
 - C. Zero trust
 - D. Data diddling
63. A hospital database is hosting PHI data with high volatility. Data changes constantly and is used by doctors, nurses, and surgeons, as well as the finance department for billing. The database is located in a secure air-gapped network where there is limited access. What is the most likely threat?
 - A. Internal user fraud
 - B. Manipulated key-value pairs
 - C. Compliance
 - D. Inappropriate admin access

64. Jeremiah works for a global construction company and has found cloud computing meets 90 percent of his IT needs. Which of these is of least importance when considering cloud computing?
- A. Data classification
 - B. Encryption methodology
 - C. Incident response and disaster recovery
 - D. Physical location of data center
65. Your company hired a new IT manager who will be working remotely. Their first order of business is to perform a risk assessment on a new mobile device that is to be given to all employees. The device is commercially available and runs a popular operating system. What are the most important security factors that you should consider while conducting this risk assessment?
- A. Remote wipe and controls, encryption, and vendor track record
 - B. Encryption, IPV6, cost, and color
 - C. Remote wipe, maintenance, and inventory management
 - D. Remote monitoring, cost, SSD, and vendor track record
66. Your CEO purchased the latest and greatest mobile device (BYOD) and now wants you to connect it to the company's intranet. You have been told to research this process according to change management and security policy. What *best* security recommendation do you recommend making the biggest impact on risk?
- A. Making this a new corporate policy available for everyone
 - B. Adding a PIN to access the device
 - C. Encrypting nonvolatile memory
 - D. Auditing requirements
67. Brian's new insurance company is working with an ISP, and he wants to find out technical details, such as system numbers, port numbers, IP addressing, and the protocols used. What document will he find this information in?
- A. Memorandum of understanding
 - B. Disclosure of assets
 - C. Operation level agreement
 - D. Interconnection security agreement
68. Your IT staff is seeking a wireless solution to transmit data in a manufacturing area with lots of electrical motors. The technology must transmit approximately 1 Mbps of data approximately 1 meter using line of sight. No obstacles are between the devices using this technology. Because of the environment, using RF is not a viable solution. What technology is *best* suited for this situation?
- A. Wi-Fi
 - B. Bluetooth
 - C. IrDA
 - D. RF

69. Your company underwent a merger, and you are attempting to consolidate domains. What tool do you use to find out who the owner of a domain is, when it expires, and contract details?
- A. Netstat
 - B. Whois
 - C. SSH
 - D. TCPDump
70. Your department is looking for a new storage solution that enables a yet undetermined number of systems to connect using file-based protocols (such as NFS and SMB) for peer-ing. This solution will also be used for file-sharing services such as data storage, access, and management services to network clients. What is the *best* storage solution for your organization?
- A. SAN
 - B. NAS
 - C. DAG
 - D. DAS
71. Your CISO asks you to develop deployment solutions for internally developed software that offers the best customization as well as control over the product. Cost is not an issue. What is the *best* solution for you to choose?
- A. Hosted deployment solution with a lower up-front cost but that requires maintaining the hardware on which the software is residing
 - B. Cloud-based deployment solutions that require a monthly fee only
 - C. Elastic virtual hosting based on need
 - D. An on-premises traditional deployment solution
72. Fletcher is a security engineer for a government agency attempting to determine the control of highly classified customer information. Who should advise him on coordinating control of this sensitive data?
- A. Sales
 - B. HR
 - C. Board of directors
 - D. Legal counsel
73. Two CISOs brought their IT leadership together to discuss the BIA and DRP for a merger between two automobile manufacturers. Their first priority is to communicate securely using encryption. What is the *best* recommendation?
- A. DNSSEC on both domains
 - B. TLS on both domains
 - C. Use SMime in select email transmissions
 - D. Push all communication to the cloud

74. Your newly formed IT team is investigating cloud computing models. You would like to use a cloud computing model that is subscription based for common services and where the vendor oversees developing and managing as well as maintaining the pool of computer resources shared between multiple tenants across the network. Which of the following is the *best* choice for this situation?
- A. Public
 - B. Private
 - C. Agnostic
 - D. Hybrid
75. Alice and Bob are discussing federated identity and the differences between 2FA and MFA. Bob says it is the same thing, and Alice is explaining to him that it isn't. Which is the *best* statement that describes the difference?
- A. Multifactor authentication (MFA) requires users to verify their identity by providing multiple pieces of evidence that can include something they know, something they have, or something they are. Two-factor authentication (2FA) is a user providing two authentication methods like a password and a fingerprint.
 - B. 2FA and MFA have the same process with the caveat that 2FA must be two separate types of authentication methods. MFA could be two or more of the same methods.
 - C. 2FA is safer and easier for end users than MFA.
 - D. Multifactor authentication (MFA) requires users to verify their identity by providing at least two pieces of evidence that can include something they know, something they have, or something they are. Two-factor authentication (2FA) is a user providing two or more authentication methods like a password and a fingerprint.
76. For security reasons, Ted is moving from LDAP to LDAPS for standards-based specification for interacting with directory data. LDAPS provides for security by using which of the following?
- A. SSL
 - B. SSH
 - C. PGP
 - D. AES
77. The corporate network has grown to a point where the management of individual routers and switches is problematic. Your CISO wants to move to a solution where the control function of the routers and switches are centralized, leaving the routers and switches to perform the basic forwarding of traffic. Which technology *best* performs this function?
- A. CDC
 - B. NAS
 - C. SAN
 - D. SDN

78. A security engineer is concerned that logs may be lost on their hybrid SDN network if the devices should fail or become compromised by an attacker. What solution ensures that logs are not lost on these devices?
 - A. Configuring a firewall on the local machine
 - B. Archiving the logs on the local machine
 - C. Sending the logs to a syslog
 - D. Installing a NIPS
79. Your CISO watched the news about the latest supply chain breach and is genuinely concerned about this type of attacks affecting major organizations. He asks you, as a security analyst, to gather information about controls to put into place on your SDN network to stop these attacks from affecting your organization. How do you begin this process?
 - A. Get the latest IOCs from OSINT sources
 - B. Research best practices
 - C. Use AI and SIEM
 - D. Perform a sweep of your network using threat modeling
80. Cameron is a newly promoted network security administrator. His manager told him to start building his physical and SDN topology map with a concentration on finding out what ports are open on which assets across the entire enterprise. What tool will accomplish the task?
 - A. Netcat
 - B. Nmap
 - C. BurpSuite
 - D. IPConfig
81. Your organization has opted into a hybrid cloud solution for all your strategic organizations with multiple verticals with different IT requirements. Which one of these is an advantage?
 - A. Flexible, scalable, reliable, and improved security posture
 - B. Strong compatibility and integration requirements
 - C. Complexity as the organization evolves
 - D. Can be very expensive
82. While performing unit testing on software requested by your department, you found that privilege escalation is possible. Privilege escalation means that an attacker can elevate their privilege on a system from a lower level to an administrator level. What two performance unit testing techniques do you need to use?
 - A. Vertical and horizontal
 - B. Left and right
 - C. North to south
 - D. Ring 1 to 3

83. Phillip's financial company experienced a natural disaster, used a hot site for three months, and now is returning to the primary site. What processes should be restored first at the primary site?
- A. Finance department
 - B. External communication
 - C. Mission critical
 - D. Least business critical
84. You work in law enforcement supporting a network with HA. High availability is mandatory, as you also support emergency 911 services. Which of the following would hinder your HA ecosystem?
- A. Clustered servers
 - B. Primary firewall
 - C. Switched networks
 - D. Redundant communication links
85. Mark has been tasked with building a computer system that can scale well and that includes built-in logic for interfacing with many types of devices, including SATA, PCI, and USB, as well as GPU, network processors, and AV encoders/decoders. What type of system should he build?
- A. Matrix
 - B. Heterogeneous
 - C. LLC
 - D. Meshed network
86. Not having complete control over networks and servers is a real concern in your organization, and upper management asks you if the company's data is genuinely secure now that you have migrated to the cloud. They have asked you to present industry research at the next board of directors meeting to answer questions regarding cloud security and your company's cyber-resilience. What research would be of most interest to the board of directors?
- A. Processor power consumption
 - B. Encryption models
 - C. COCOA
 - D. CACAO
87. While investigating threats specific to your industry, you found information collected and analyzed by several companies with substantive expertise and access to source information. Which of these is the *least* beneficial item to your organization after subscribing to threat intelligence information?
- A. Determining acceptable business risks
 - B. Developing controls and budgets
 - C. Making equipment and staffing decisions
 - D. Creating a marketing plan for your product

- 88.** Andrew has evaluated several unified communications (UC) vendors. He has a need for one with their own data center facility hosting their own instance of the platform with built-in redundant power, remote backup, and secured entry as well as 24/7 staffing. Why would a UC vendor have minimal data center security?
- A.** Cost savings
 - B.** Compliance requirements
 - C.** Ease of setup and use
 - D.** Perfect forward secrecy
- 89.** Your organization slowly evolved from simply locking doors to RFID-enabled cards issued to employees to secure the physical environment. You want to protect these cards from cloning, because some parts of your organization host sensitive information. What should you implement?
- A.** Encryption
 - B.** IDR
 - C.** HIDS
 - D.** NIPS
- 90.** Damien is a security architect for a large enterprise bank that recently merged with a smaller local bank. The acquired bank has a legacy virtual cluster, and all these virtual machines use the same NIC to connect to the LAN. Some of the VMs are used for hosting databases for HR, and some are used to process mortgage applications. What is the biggest security risk?
- A.** Shared NICs negatively impacting the integrity of packets
 - B.** Bridging of networks impacting availability
 - C.** Availability between VMs impacting integrity
 - D.** Visibility between VMs impacting confidentiality
- 91.** One of the biggest issues your CISO has with migrating to more cloud environments is the process of acquiring and releasing resources. Technical as well as operational issues are associated with these processes. What type of procedure documentation should you create to help with this?
- A.** How to authenticate and authorize
 - B.** How to dynamically provision and deprovision
 - C.** How to use SaaS, IaaS, and PaaS
 - D.** How to build a Type 2 hypervisor
- 92.** You have received an RFQ response from a software company, which makes a tool that will allow you to record all changes in a single change management tool. This tool will track scheduling change, implementing change, the cost of change, and reporting. What type of software is this called?
- A.** Vulnerability management
 - B.** Change control
 - C.** Security information and event management
 - D.** Automation

93. You are investigating a new tool that helps identify, analyze, and report on threats in real time based mostly on logs. What is the *best* solution?
- A. SOAR
 - B. Antivirus
 - C. XSS
 - D. Port scanner
94. Steve is a software developer for a large retail organization. His CISO returned from a large conference and asked him to clarify exactly what the benefit of a container in software development is over virtual machines. Which of these is the *best* succinct answer?
- A. In a VM, hardware is virtualized to run multiple OS instances. Containers virtualize an OS to run multiple workloads on a single OS instance using a container engine.
 - B. In a container, hardware is virtualized to run a single OS, where a VM can run multiple applications across multiple assets with a single OS.
 - C. A VM is virtualized technology, but a container is not.
 - D. A container is the same thing as a virtual machine, just smaller in size.
95. As a leader in your organization in DevOps, you want to convince your CISO to move toward containerization. Which of these is not an advantage to using containers over VMs?
- A. Reduced and simplified security updates
 - B. Less code to transfer, migrate, and upload
 - C. Quicker spinning up applications
 - D. Large file size of snapshots
96. At the latest IT department meeting, a discussion on the best virtual methodology centered around using VMs versus containers. Which of these statements *best* aligns with those two models?
- A. VMs are better for lightweight native performance, whereas containers are better for heavyweight limited performance.
 - B. VMs are for running applications that need all the OS has to offer, whereas containers are better when maximizing number of applications on minimal resources.
 - C. VMs share the host OS, whereas containers run on their own OS.
 - D. Containers are fully isolated and more secure, whereas VMs use process-level isolation.
97. Ross is a security manager looking to improve security and performance of his unified communications (UC) server. Which of the following options might help with decreasing the attack surface?
- A. Adding more users
 - B. Adding more devices
 - C. Turning off unused services
 - D. Ease of setup

98. After analyzing traffic flows on the network, your department noticed that many internal users access the same resources on the Internet. This activity utilizes a lot of Internet bandwidth. Your department decides to implement a solution that can cache this type of traffic the first time it is requested and serve it to the internal users as requested, thereby reducing the Internet bandwidth used for accessing this traffic. Which solution *best* accomplishes this task?
- A. Proxy
 - B. Packet filter firewall
 - C. WAF
 - D. IPS
99. You were asked to recommend a technology that will lessen the impact of a DDoS attack on your CDN. Which of the following is the *best* technology?
- A. HIDS
 - B. Packet filter firewall
 - C. Proxy
 - D. Load balancing
100. Luke's company started upgrading the computers in your organization. As a security professional, you recommend creating a standard image for all computers with a set level of security configured. What is this process called?
- A. Configuration baselining
 - B. Imaging
 - C. Duplication
 - D. Ghosting
101. Lydia is a security administrator, and her hospital's security policy states that wearable technology and IoT devices are not allowed in secure areas where patient information is discussed. Wearable devices are designed to be worn by one individual, but some are quite powerful with artificial intelligence. Why is this a concern?
- A. Danger of eavesdropping and compliance violations
 - B. Insurance premiums going up
 - C. Malpractice and litigation
 - D. Chain of custody of evidence
102. Mark is evaluating cloud storage providers and gives each a product evaluation form. Which of these is not the best practice for a cloud service provider?
- A. Strict initial registration and validation
 - B. System event and network traffic monitoring
 - C. Utilization of weak encryption algorithms
 - D. Incident response processes that help BCP

- 103.** Containerization provides many benefits in flexibility and faster application development. Which of the following statements is false?
- A.** Containers share the host OS's kernel during runtime.
 - B.** Containers do not need to fully emulate an OS to work.
 - C.** One physical server running five containers needs only one OS.
 - D.** Containers are pure sandboxes just like VMs are.
- 104.** Hector has a team that replaced version 1.2 of software with 2.0. The newest version has a completely different interface in addition to updates. What is this called?
- A.** Versioning
 - B.** Coding integration
 - C.** Secure coding
 - D.** Vulnerability assessment
- 105.** Greg is a security researcher for a cybersecurity company. He is currently examining a third-party vendor and finds a way to use SQLi to deface their web server due to a missing patch in the company's web application. What is the threat of doing business with this organization?
- A.** Web defacement
 - B.** Unpatched applications
 - C.** Attackers
 - D.** Education awareness
- 106.** Your CISO decided to implement an overarching enterprise mobility management (EMM) strategy. She wants to ensure that sensitive corporate data is not compromised by the employees' apps on their mobile devices. Which of these will implement that *best*?
- A.** App config through IDC
 - B.** App wrapping through SDK
 - C.** Open source through API
 - D.** Platform DevOps
- 107.** You are a web developer who needs to secure API keys in a client-side JavaScript application created for your hospital. What is the *best* way to accomplish this task quickly and efficiently?
- A.** Disable API access and use a hash of the key.
 - B.** Set API access and a secret key pair.
 - C.** Curl a request with an `-H -o` option.
 - D.** Set a RESTful request with access pairs.

- 108.** Mitchell wants to enhance his overall security and compliance to protect his company more carefully. He engages his security team to examine enterprise application integration, data integration, message-oriented middleware (MOM), object request brokers (ORBs), and the enterprise service bus (ESB). He also wants to prioritize which web applications should be secured first and how they will be tested. What do you need to sit down with your IT security team and build?
- A.** Web application security plan
 - B.** Web application-level attack list
 - C.** Business logic justifications
 - D.** Container security
- 109.** Edwin's board of directors want to perform quarterly security testing. As CISO of a financial institution, he must form a plan specifically for the development of this test that includes software assurance. This test must have a low risk of impacting system stability because the company is in production. The suggestion was made to outsource this to a third party. The board of directors argue that a third party will not be as knowledgeable as the development team. What will satisfy the board of directors?
- A.** Gray-box testing by a major consulting firm
 - B.** Black-box testing by a major external consulting firm
 - C.** Gray-box testing by the development and security assurance teams
 - D.** White-box testing by the development and security assurance teams
- 110.** Trent is a security analyst for a financial organization and conducting a review of data management policies. After a complete review, he found settings disabled permitting developers to download supporting but trusted software. You submitted the recommendation that developers have a separate process to manually download software that should be vetted before its use. What process will support this recommendation?
- A.** NIPS
 - B.** Digitally signed applications
 - C.** Sandboxing
 - D.** PCI compliance
- 111.** Tiffany runs an organization that is blending its development team with the operations team because of the speed applications are being rolled out. Applications change with new services required in production, so she has undertaken the challenge of eliminating those silos of development and operations. What is this called?
- A.** Incremental
 - B.** DevOps
 - C.** Agile
 - D.** Waterfall

- 112.** Shelby is working for a software developer developing web applications for an international financial enterprise. She has also been tasked with building the rule set that governs the interaction between an end user and the web application linking authentication and access. What type of rule set is this?
- A.** Session management
 - B.** Secure cookies
 - C.** Java flags
 - D.** Stateless firewall
- 113.** Your software developer has a custom ROM for Android and wants to further customize it for mobile device use in your healthcare network. Android is an open source operating system, but your developer experiences difficulties uploading the new ROM to a test device even using validated third-party libraries for development. What does he need to unlock before uploading the new ROM?
- A.** Bootloader
 - B.** BIOS
 - C.** FIFO
 - D.** TPM
- 114.** Angel needs to provide software code for users to download. You want the users to be able to verify that the software has not changed or become corrupted. How might you provide this verification?
- A.** Code signing.
 - B.** Script signing.
 - C.** The user can attempt to install and run the program. If it installs and operates properly, it hasn't been altered.
 - D.** Have the user authenticate first. If the user is authenticated, the software they download must be genuine.
- 115.** You are creating a web application security plan and need to do white-box security testing on source code to find vulnerabilities earlier in the SDLC. If you can find vulnerabilities earlier in the process, they are cheaper to fix. What type of testing do you need to do?
- A.** SAST
 - B.** CAST
 - C.** DAST
 - D.** FAST
- 116.** You are creating a web application security plan and need to do black-box security testing on a running application. What type of testing do you need to do?
- A.** SAST
 - B.** CAST
 - C.** DAST
 - D.** IAST

117. You had your internal team do an analysis on compiled binaries to find errors in mobile and desktop applications. You would like an external agency to test them as well. Which of these tests *best* suits this need?
 - A. DAST
 - B. VAST
 - C. IAST
 - D. SAST
118. Craig's newly formed IT team is investigating cloud computing models. He wants to use a cloud computing model that is orchestrated as an integrated infrastructure environment. Apps and data can share resources based on business and technical policies. Which of the following is the *best* choice for this situation?
 - A. Public
 - B. Private
 - C. Agnostic
 - D. Hybrid
119. You have been newly hired as a CISO for a governmental contractor. One of your first conversations with the CEO is to review requirements for recovery time and recovery point objectives, and enterprise resource planning (ERP). Who should you bring to the round table to discuss metrics surrounding your RTO/RPO?
 - A. Board of directors
 - B. Chief financial officer
 - C. Data owners and custodians
 - D. Business unit managers and directors
120. Which of the following is a use case for configuration management software?
 - A. Incident remediation
 - B. Continuance
 - C. Asset management
 - D. Collaboration
121. You have been analyzing the backup schedule for a CMDB. Your CIO has said the company has an RPO of 48 hours. What is the minimum backup schedule for the CMDB?
 - A. 24 hours
 - B. 6 hours
 - C. 48 hours
 - D. 12 hours

- 122.** Your company is looking at a new CRM model to reach customers that includes social media. The marketing director, Tucker, would like to share news, updates, and promotions on all social websites. What are the major security risks?
- A.** Malware, phishing, and social engineering
 - B.** DDOS, brute force, and SQLi
 - C.** Mergers and data ownership
 - D.** Regulatory requirements and environmental changes
- 123.** In the last 5 years, your manufacturing group merged twice with competitors and acquired three startups, which led to more than 60 unique customer web applications. To reduce cost and improve workflows, you are put in charge of a project to implement centralized security. You need to ensure a model to enable integration and accurate identity information and authentication as well as repeatability. Which is the *best* solution?
- A.** Implementation of web access control and relay proxies
 - B.** Automated provisioning of identity management
 - C.** Self-service single sign-on using Kerberos
 - D.** Building an organizational wide granular access control model in a centralized location
- 124.** You are tasked with creating a single sign-on solution for your security organization. Which of these would you not deploy in an enterprise environment?
- A.** Directory services
 - B.** Kerberos
 - C.** SAML 2.0
 - D.** Workgroup
- 125.** The Domain Name System (DNS) maintains an index of every domain name and corresponding IP address. Before someone visits a website on your corporate network, DNS will resolve your domain name to its IP address. Which of the following is a weakness of DNS?
- A.** Spoofing
 - B.** Latency
 - C.** Authentication
 - D.** Inconsistency
- 126.** Your database team would like to use a service-oriented architecture (SOA). The CISO suggested you investigate the risk for adopting this type of architecture. What is the biggest security risk to adopting an SOA?
- A.** SOA is available only over the enterprise network.
 - B.** Lack of understanding from stakeholders.
 - C.** Risk of legacy networks and system vulnerabilities.
 - D.** Source code.

- 127.** A large enterprise social media organization underwent several mergers, divestitures, and acquisitions over the past three years. Because of this, the internal networks and software have extremely complex dependencies. Better integration is mandatory. Which of the following integration platforms is *best* for security and standards-based software architecture?
- A.** IDE
 - B.** DNS
 - C.** SOA
 - D.** ESB
- 128.** The retail division of your organization purchased touchscreen tablets and wireless mice and keyboards for all their representatives to increase productivity. You communicated the risk of nonstandard devices and wireless devices, but the deployment continued. What is the *best* method for evaluating and presenting potential threats to upper management?
- A.** Conducting a vulnerability assessment
 - B.** Developing a standard image for these assets
 - C.** Making new recommendations for security policies
 - D.** Working with the management team to understand the processes these devices will interface with, and to classify the risk connected with the hardware/software deployment life cycle
- 129.** You are selected to manage a software development and implementation project. Your manager suggests that you follow the phases in the SDLC. In which of these phases do you determine the controls needed to ensure that the system complies with standards?
- A.** Testing
 - B.** Initiation
 - C.** Accreditation
 - D.** Acceptance
- 130.** You were selected to manage a software development project. Your supervisor asked you to follow the proper phases in the systems development life cycle. Where does the SDLC begin?
- A.** Requirement analysis
 - B.** System design specifications
 - C.** Initiation
 - D.** Implementation
- 131.** You have turned a software project over to the fielding phase, delivering the working system to the customer. Which phase is this otherwise known as?
- A.** Deployment
 - B.** Licensing
 - C.** Development
 - D.** Evaluation

- 132.** Your vulnerability manager contacted you because of an operating system software issue. There are a few security-related issues due to patches and upgrades needed for an application on the systems in question. When is the *best* time to complete this task?
- A.** As quickly as possible after testing
 - B.** After experiencing the issue that the vulnerability manager described
 - C.** After other organizations have tested the patch or upgrade
 - D.** During the usual monthly maintenance
- 133.** Arnold has developed an application and want to prevent the reuse of information in memory when a user quits the program. Which of these is his *best* option to accomplish this task?
- A.** Garbage collection
 - B.** Data validation
 - C.** SDLC
 - D.** OOP
- 134.** Simon is a security engineer. While testing an application during a regular assessment to make sure it is configured securely, he sees a REQUEST containing method, resources, and headers, and a RESPONSE containing status code and headers. What technique did he most likely use to generate that type of output?
- A.** Fingerprinting
 - B.** Fuzzing
 - C.** Vulnerability scanning
 - D.** HTTP intercepting
- 135.** You have been asked to make a change to software code. What type of testing do you complete to make sure program inputs and outputs are correct and everything functions as it's supposed to?
- A.** White box
 - B.** Black hat
 - C.** Code review
 - D.** Regression
- 136.** You are conducting a unit test on a new piece of software. By looking at an individual program, how do you ensure that each module behaves as it should?
- A.** Input/output
 - B.** BIOS
 - C.** Processes running
 - D.** Services running

- 137.** Christopher is a software developer, and as part of the testing phase in the SDLC, he will need to ensure that an application is handling errors correctly. What is the *best* tool for him to use in this situation?
- A.** Fuzzer
 - B.** Compliance
 - C.** Access control
 - D.** Integration testing
- 138.** Your IT group is modernizing and adopting a DevSecOps approach, making everyone responsible for security. Traditionally, storage and security were separate disciplines inside IT as a whole. As a security analyst, what is your primary concern of data at rest?
- A.** Encryption
 - B.** Authentication
 - C.** Infrastructure
 - D.** Authorization
- 139.** As a software developer, Brian is extremely frustrated with a customer who keeps calling him on the phone and leaving messages to make changes to the software. What approach should Brian take with this customer to make the development process easier?
- A.** Change control
 - B.** Increase security
 - C.** Appraise senior management
 - D.** Provide detailed documentation
- 140.** Jackie is a software engineer and inherently prefers to use a flexible framework that enables software development to evolve with teamwork and feedback. What type of software development model would this be called?
- A.** Prototyping
 - B.** Ceremony
 - C.** Agile
 - D.** Radical
- 141.** You are working on a high-risk software development project that is large, the releases are to be frequent, and the requirements are complex. The waterfall and agile models are too simple. What software development model would you opt for?
- A.** Functional
 - B.** Cost estimation
 - C.** Continuous delivery
 - D.** Spiral

- 142.** You are a software engineer and need to use a software development process that follows an extremely strict predetermined path through a set of phases. What type of method is this called?
- A.** Agile
 - B.** Waterfall
 - C.** Adaptable
 - D.** Verifiable
- 143.** The SDLC phases are part of a bigger process known as the system life cycle (SLC). The SLC has two phases after the implementation phase of the SDLC that address postinstallation and future changes. What are they called?
- A.** Operations, maintenance, revisions, and replacement
 - B.** Replacement, crepitation, evaluation, and versioning
 - C.** Validation, verification, authentication, and monitoring
 - D.** Revisions, discovery, compliance, and functionality
- 144.** You are using continuous integration/continuous delivery methodology involving different members of your team while developing a new application. You meet every day after lunch to review, which can mean multiple integrations every day. What are the security implications of using CI/CD?
- A.** There are no security issues.
 - B.** Errors will not need to be fixed because the next integration will fix them.
 - C.** Encryption will be impossible because of timing.
 - D.** Errors can be handled as soon as possible.
- 145.** IT security is a rapidly evolving field. As a software engineer, you need to stay current on industry trends and potential impact on an enterprise. Many of these changes will lead to you adopting which of the following?
- A.** Best practices
 - B.** Digital threats
 - C.** Antivirus programs
 - D.** NIST
- 146.** You perform a security audit to find out whether any IoT devices on your network are publicly accessible. What website would you use to find this type of information?
- A.** Shodan
 - B.** OWASP
 - C.** VirusTotal
 - D.** Maltego

- 147.** During a web application security assessment, Kevin needs to grab the basic architecture to identify the framework used. He grabbed the HTTP header banner using Netcat, which gives you the application name, software version, and web server information. What activity did he just perform?
- A.** Fingerprinting
 - B.** Authentication
 - C.** Authorization
 - D.** Code review
- 148.** Many of your corporate users are using mobile laptop computers to perform their work remotely. Security is concerned that confidential data residing on these laptops may be disclosed and leaked to the public. What methodology *best* helps prevent the loss of such data?
- A.** DLP
 - B.** HIPS
 - C.** NIDS
 - D.** NIPS
- 149.** Your CISO, Karen, is concerned that all employees can use personal USB storage devices on the company's computers. She is concerned about malware introduction to the corporate environment and that data loss is possible if this practice continues. She wants to manage who can use USB storage devices on the company's computers. Which of the following actions should be used to implement this constraint?
- A.** Replacing all computers with those that do not have USB ports
 - B.** Placing glue in the computers' USB ports
 - C.** Cutting the computers' USB cables
 - D.** Configuring a Group Policy within Microsoft Active Directory to manage USB storage device use on those computers
- 150.** Many organizations prepare for highly technical attacks and forget about the simple low-tech means of gathering information. Dumpster diving can be useful in gaining access to unauthorized information. Which of these is the easiest to implement for reducing your company's dumpster-diving risk?
- A.** Data classification and printer restrictions of intellectual property.
 - B.** Purchase shredders for the copy rooms.
 - C.** Create policies and procedures for document shredding.
 - D.** Employ an intern to shred all printed documentation.
- 151.** Your organization decided to move away from dedicated computers on the desktop and move to a virtual desktop environment. The desktop image resides on a server within a virtual machine and is accessed via a desktop client over the network. Which of the following is being described?
- A.** VPN
 - B.** VDI
 - C.** VNC
 - D.** RDP

- 152.** Using Microsoft Network Monitor, you have captured traffic on TCP port 3389. Your security policy states that port 3389 is not to be used. What client-server protocol is probably running over this port?
- A.** SNMP
 - B.** RDP
 - C.** PuTTY
 - D.** FTP
- 153.** Your organization is pressured by both the company board and employees to allow personal devices on the network. They asked for email and calendar items to be synced between the company ecosystem and their BYOD. Which of the following *best* balances security and usability?
- A.** Allowing access for the management team only because they have a need for convenient access
 - B.** Not allowing any access between a BYOD device and the corporate network, only cloud applications
 - C.** Only allowing certain types of devices that can be centrally managed
 - D.** Reviewing security policy and performing a risk evaluation focused on central management, including the remote wipe and encryption of sensitive data and training users on privacy
- 154.** Nathan is tasked with writing the security viewpoint of a new program that his organization is starting. Which of the following techniques make this a repeatable process and can be used for creating the best security architecture?
- A.** Data classification, CIA triad, minimum security required, and risk analysis
 - B.** Historical documentation, continuous monitoring, and mitigation of high risks
 - C.** Implementation of proper controls, performance of qualitative analysis, and continuous monitoring
 - D.** Risk analysis; avoidance of critical risks, threats, and vulnerabilities; and the transference of medium risk
- 155.** You deployed more than half of your enterprise into the cloud, but you still have concerns about data loss, unauthorized access, and encryption. What continues to be the vulnerability in cloud infrastructure that leads to the most breaches?
- A.** Misconfiguration
 - B.** SIEM
 - C.** SaaS
 - D.** Machine learning

- 156.** Your company generates documents intended for public viewing. While your company wants to make these document public, it stills wants to prove the documents originated from the company. How can these documents be marked in such a way that information about their origin is maintained while not distorting the visual contents of the documents?
- A.** Blowfish
 - B.** Steganographic watermarking
 - C.** Digital signatures
 - D.** PKI
- 157.** Charlie works for a publisher and has been tasked with protecting the electronic media they produce. This will help ensure they receive the revenue for the product they produce. What is Charlie going to implement?
- A.** Single point-of-failure
 - B.** Digital rights management
 - C.** Separate of duties
 - D.** Mandatory vacations
- 158.** As a security analyst, Ben is searching for a method that can examine network traffic and filter its payload based on rules. What is this method called?
- A.** Network flow
 - B.** DLP
 - C.** Data flow enforcement
 - D.** Deep packet inspection
- 159.** You are a security administrator reviewing network logs. You notice a UDP trend where traffic increased more than 30 percent in the past 48 hours. You use Wireshark to capture the packets and see the following: UDP 192.168.1.1:123->46.110.10.5:123. What attack scenario is most likely occurring?
- A.** You are being attacked via the NTP client side and successfully exploited on 192.168.1.1.
 - B.** You are being attacked via the NTP server side and unsuccessfully exploited on 192.168.1.1.
 - C.** You are being attacked via the DNS client side and successfully exploited on 192.168.1.1.
 - D.** You are being attacked via the DNS server side and successfully exploited on 192.168.1.1.
- 160.** René is working with upper management to classify data to be shared in his collaboration tool, which will create extra security controls limiting the likelihood of a data breach. What principle of information security is he trying to enforce?
- A.** Confidentiality
 - B.** Integrity
 - C.** Accountability
 - D.** Availability

- 161.** A new objective for your department is to establish data provenance or historical data records. Moving forward, you must now document the data's source and all manipulations performed on it. Every data item will have detailed information about its origin and the ways it was influenced. Why is this crucial to the security of the data?
- A.** Unauthorized changes in metadata can lead you to the wrong datasets.
 - B.** Authorized changes to the data warehouse can lead you to the wrong datasets.
 - C.** Traceable data sources make it difficult to find security breaches.
 - D.** Traceable data sources make it difficult to find fake data generation.
- 162.** Your CTO believes in the adage "Security through obscurity." Which of the following types of obfuscation makes a program obscure to other computers?
- A.** Prevention
 - B.** Saturation
 - C.** Control flow
 - D.** Data
- 163.** Lynn uses a process that substitutes a sensitive data element with something that is not sensitive. She uses this process to map back to the sensitive data. What is this called?
- A.** Masking
 - B.** Encryption
 - C.** Tokenization
 - D.** Authorization
- 164.** Which of the following storage techniques should you deploy if you want the option to selectively provide availability to some hosts and to restrict availability to others by using a masking process?
- A.** NAS
 - B.** SAN
 - C.** iSCSI
 - D.** LUN
- 165.** Ashton's end users are using mobile devices to access confidential information on the corporate network. He needs to ensure that the information from all databases is kept secure as it is transmitted to these mobile devices. Encryption is a requirement. Of the following options, which one *best* describes a major concern with PII on mobile devices?
- A.** Mobile devices have more processing power than other computing devices.
 - B.** Mobile devices typically have less processing power than other computing devices.
 - C.** Mobile devices often have increased complexities.
 - D.** Mobile devices often have difficulties to obfuscate personal data.

- 166.** Bob needs your professional opinion on encryption capabilities. You explained to him that cryptography supports all the core principles of information security, with one exception. What is that exception?
- A.** Anonymity
 - B.** Integrity
 - C.** Confidentiality
 - D.** Availability
- 167.** Your app developers focus on the speed of app development more than security. Because of this, they use easy-to-implement encryption algorithms with known vulnerabilities. What is the result of using this type of encryption algorithm?
- A.** Malware infection
 - B.** Modification
 - C.** Attacker cracking the passwords
 - D.** Remote code execution
- 168.** After a meeting with the board of directors, your CEO is looking for a way to boost profits. He identified a need to implement cost savings on non-core-related business activities, and the suggestion was made to move the corporate email system to the cloud. You are the compliance officer tasked with making sure security and data issues are handled properly. What *best* describes your process?
- A.** End-to-end encryption, creation, and the destruction of mail accounts
 - B.** Vendor selection and RFP/RFQ
 - C.** Securing all virtual environments that handle email
 - D.** Data provisioning and processing while in transit and at rest
- 169.** Evan's cyber-company has officially grown out of its startup phase, and his team is tasked with creating a pre-disaster preparation plan that will sustain the business should a disaster, natural or human-made, occur. Which of the following is the most important?
- A.** Offsite backups
 - B.** Copies of the BDR
 - C.** Maintaining a warm site
 - D.** Chain of command
- 170.** Christopher is a web developer. He built a web form for customers to fill out and respond to the company via a web page. What is the first thing that a developer should do to prevent this page from becoming a security risk?
- A.** SQLi
 - B.** Input validation
 - C.** Cross-site request forgery
 - D.** Fuzzing

- 171.** Marketing has put in a request for web-based meeting software with a third-party vendor. The software programs that you, a security analyst, have reviewed requires user registration and installation, and that user has to share their data as well as their desktop. To ensure that information is secure, which of the following controls is *best*?
- A.** Disallow the software; avoid the risk.
 - B.** Hire a third-party organization to perform the risk analysis, and based on outcomes, allow or disallow the software.
 - C.** Log and record every single web-based meeting.
 - D.** After evaluating several providers, ensure acceptable risk and that the read-write desktop mode can be prevented.
- 172.** With the rise of malware spread with removable media, your company wrote an amendment to include a ban of all flashcards and memory drives. They pose a threat due to all but which of the following?
- A.** Physical size
 - B.** Transportability
 - C.** Storage capacity
 - D.** Being cheap and easy to use
- 173.** A server holding sensitive financial records is running out of room. You are the information security manager and data storage falls under your purview. What is the *best* option?
- A.** Use first in, first out (FIFO).
 - B.** Compress and archive the oldest data.
 - C.** Move the data to the cloud.
 - D.** Add disk space in a RAID configuration.
- 174.** A situation that affects the CIA triad of an IT asset can include an internal and external risk source. A breach of physical security and theft of data can be instigated by_____.
- A.** untrusted insiders or trusted outsiders
 - B.** trusted insiders or untrusted outsiders
 - C.** hidden costs
 - D.** service deterioration
- 175.** During what phase of eDiscovery will you determine what digital data and documents should be collected for possible analysis and review?
- A.** Processing
 - B.** Identification
 - C.** Collection
 - D.** Curation

- 176.** You are a small company administrator hosting multiple virtualized client servers on a single host. You are told to add a new host to create a cluster. The new hardware and OS will be different, but the underlying technology will be compatible. Both hosts will be sharing the same storage. What goal are you trying to accomplish?
- A.** Increased availability
 - B.** Increased confidentiality
 - C.** Increased integrity
 - D.** Increased certification
- 177.** Good data management includes which of the following?
- A.** Data quality procedures, verification and validation, adherence to agreed-upon data management, and an ongoing data audit to monitor the use and integrity of existing data
 - B.** Cost, due care and due diligence, privacy, liability, and existing law
 - C.** Determining the impact the information has on the mission of the organization, understanding the cost of information, and determining who in the organization or outside of it has a need for the information
 - D.** Ensuring the longevity of data and their reuse for multiple purposes, facilitating the interoperability of datasets, and increasing data sharing
- 178.** Bob is implementing a new RAID configuration needed for redundancy in the event of disk failure. What security goal is Bob trying to accomplish?
- A.** Availability
 - B.** Integrity
 - C.** Confidentiality
 - D.** Disclosure
- 179.** You are monitoring your IT environment to detect techniques like credential dumping. Credential dumping is extracting usernames and passwords from a computer to then pass those credentials to other machines on a network. Where are the credentials stored on a Windows machine?
- A.** In the SAM
 - B.** In PSEXEC
 - C.** In Documents and Settings
 - D.** In WUTemp
- 180.** Jennie and her team are developing security policies, and they are currently working on a policy regarding password management. Which of these is not important?
- A.** Account lockout
 - B.** Training users to create complex easy-to-remember passwords and not use the same password over again
 - C.** Preventing users from using personal information in a password, such as their birthday or their spouse's name
 - D.** Storing passwords securely in a password manager application

- 181.** Keith's organization wants to move a vital company process to the cloud. He is tasked with conducting a risk analysis to minimize the risk of hosting email in the cloud. What is the best path forward?
- A.** All logins must be done over an encrypted channel and obtain an NDA and SLA from the cloud provider.
 - B.** Remind all users not to write down their passwords.
 - C.** Make sure that the OLA covers more than just operations.
 - D.** Require data classification.
- 182.** What is a major security concern associated with IoT?
- A.** Lack of encryption
 - B.** Use of hard-coded passwords
 - C.** Lack of firmware support
 - D.** All of the above
- 183.** Your company is recovering from a data breach. The breach was not deep but raised the security awareness profile of upper management. Realizing they have gaps in access control, upper management approved the purchase of password manager software for the organization. What else do you suggest they institute for end users?
- A.** 2FA
 - B.** Password isolation
 - C.** Disaster recovery
 - D.** IDR
- 184.** Which of the following access control principles should you implement to create a system of checks and balances on employees with heightened privileged access?
- A.** Rotation of duties
 - B.** Need to know
 - C.** Mandatory access control
 - D.** Separation of duties
- 185.** Your penetration testers' report shows that they obtained the credentials of specific user accounts through social engineering and phishing campaigns. Once on the organization's network, the penetration testers used these credentials to bypass access controls and to gain access to remote systems. In one case, they were able to switch from a user-level account to an administrator-level account. What is this type of attack called?
- A.** XSRF
 - B.** Password mitigation
 - C.** Token theft
 - D.** Privilege escalation

- 186.** You have an application that performs authentication, which makes checking for session management, brute forcing, and password complexity appropriate. What else might you check for?
- A.** SQLi
 - B.** Ransomware
 - C.** Privilege escalation
 - D.** Static analysis
- 187.** As the senior security architect, you create a security policy and standards that instruct employees to use strong passwords. You find that employees are still using weak passwords. Revising the procedures for creating strong passwords, which of these are you *least* likely to require for employees?
- A.** Change your password every 90 days.
 - B.** Use a combination of numbers, letters, uppercase and lowercase letters, and special characters.
 - C.** Use a minimum number of characters.
 - D.** Use a Merriam-Webster dictionary.
- 188.** You just accepted a CISO position for a small customer service business, and your first priority is to increase security and accessibility for current software-as-a-service (SaaS) applications. The applications are configured to use passwords. What do you implement first?
- A.** Deploy password managers for all employees.
 - B.** Deploy password managers for only the employees who use the SaaS tool.
 - C.** Create a VPN between your organization and the SaaS provider.
 - D.** Implement a system for time-based, one-time passwords.
- 189.** The collaboration tool that your company uses follows a username and password login model. If one of your employee's credentials are compromised, it could give attackers access to financial information, intellectual property, or client information. How would you mitigate this type of risk with a collaboration tool?
- A.** Strict password guidelines
 - B.** Only use HTTPS
 - C.** Restrict usage to VPN
 - D.** Disable SSO
- 190.** Wayne is a security manager for a small organization. He has evaluated several different types of access controls. Which of these are easiest for an attacker to bypass?
- A.** Fingerprint
 - B.** Password
 - C.** Iris scan
 - D.** CAC card

- 191.** What is FIM when it comes to obtaining access to networks?
- A.** Fighting insidious malware
 - B.** Federated identity management
 - C.** Forest integration modules
 - D.** Fact investigative modifications
- 192.** If Domain A trusts Domain B and Domain B trusts Domain C, what is it called when Domain A trusts Domain C because of the previously stated relationships?
- A.** Transitive tort
 - B.** Transitive trust
 - C.** Transitive trade
 - D.** Transitive theory
- 193.** You visit a website that requires credentials to log in. Besides providing the option of a username and password, you are also given the option to log in using your Facebook credentials. What type of authentication scheme is used?
- A.** SAML
 - B.** OAuth
 - C.** ClosedID
 - D.** OpenID
- 194.** You need to find a web-based language that is used to exchange security information with single sign-on (SSO). Which of the following is the *best* language to use?
- A.** SOAP
 - B.** Kerberos
 - C.** SAML/Shibboleth
 - D.** API
- 195.** Your IT manager wants to move from a centralized access control methodology to a decentralized access control methodology. You need a router that authenticates users from a locally stored database. This requires subjects to be added individually to the local database for access, which creates a security domain, or sphere of trust. What *best* describes this type of administration?
- A.** Decentralized access control requires more administrative work.
 - B.** Decentralized access control creates a bottleneck.
 - C.** Decentralized access control requires a single authorization server.
 - D.** Decentralized access control stores all the users in the same administrative location using RADIUS.

196. The CISO is researching ways to reduce risk associated with the separation of duties. In the case where one person is not available, another needs to be able to perform all the duties of their co-workers. What should the CISO implement to reduce risk?
 - A. Mandatory requirement of a shared account for administrative purposes
 - B. Audit of all ongoing administration activities
 - C. Separation of duties to ensure no single administrator has access
 - D. Role-based security on the primary role and provisional access to the secondary role on a case-by-case basis
197. You implement mandatory access control for your secure data storage system. You change default passwords and enforce the use of strong passwords. What else should you do to make this storage system even more secure?
 - A. Multifactor authentication
 - B. Multifactor authorization
 - C. Identification
 - D. Verification
198. Your data owner must assign classifications to information assets and ensure regulation compliance. Which of these other criteria is determined by a data owner?
 - A. Authorization
 - B. Authentication
 - C. Verification
 - D. Validation
199. As a security specialist for your organization, you are increasingly concerned about strong endpoint controls of developers' workstations as well as access control of servers running developer tools. Which of these is *not* a benefit of an attribute-based access control (ABAC) scheme?
 - A. Helping meet security goals and standards
 - B. Ensuring only authorized users have access to code repositories
 - C. Having runtime self-protection controls
 - D. Safeguarding system integrity
200. As a security administrator at a high-security governmental agency, you rely on some assets running high-end customized legacy software. What type of access control do you implement to protect your organization?
 - A. DAC
 - B. RBAC
 - C. MAC
 - D. ABAC

- 201.** Your organization needs an AAA server to support the users accessing the corporate network via a VPN. Which of the following will be used to provide AAA services?
- A.** RADIUS
 - B.** L2TP
 - C.** LDAP
 - D.** AD
- 202.** Your network administrator wants to use an authentication protocol to encrypt usernames and passwords on all Cisco devices. What is the *best* option for them to use?
- A.** RADIUS
 - B.** DIAMETER
 - C.** CHAP
 - D.** TACACS+
- 203.** Your company currently uses Kerberos authentication protocols and tickets to prove identity. You are looking for another means of authentication because Kerberos has several potential vulnerabilities, the biggest being which of the following?
- A.** Single point of failure
 - B.** Dynamic passwords
 - C.** Limited read/write cycles
 - D.** Consensus
- 204.** You need an authorization framework that gives a third-party application access to resources without providing the owners' credentials to the application. Which of these is your *best* option?
- A.** MAC
 - B.** EAP
 - C.** SAML
 - D.** OAuth
- 205.** You need develop a security logging process for your mission-critical servers to hold users accountable for their actions on a system after they log in. What is this called?
- A.** Authorization
 - B.** Authentication
 - C.** 2 -step verification
 - D.** Accountability

- 206.** Your credit card company identified that customers' top transaction on the web portal is resetting passwords. Many users forget their secret questions, so customers are calling to talk to tech support. You want to develop single-factor authentication to cut down on the overhead of the current solution. What solution do you suggest?
- A.** Push notification
 - B.** In-band certificate or token
 - C.** Login with third-party social media accounts
 - D.** SMS message to a customer's mobile number with an expiring OTP
- 207.** Your CISO wants to implement a solution within the organization where employees are required to authenticate once and then permitted to access the various computer systems they are authorized to access. The organization uses primarily Microsoft products. Which solution is *best* suited for this organization?
- A.** Kerberos
 - B.** SSL
 - C.** HOTP
 - D.** TOTP
- 208.** Your organization is upgrading computers. The new computers include a chipset on the motherboard that is used to store encryption keys. What is this chipset called?
- A.** EKC
 - B.** TPM
 - C.** ESM
 - D.** RSA
- 209.** You are logged into a website. While performing activities within the website, you access a third-party application. The application asks you if it can access your profile data as part of its process. What technology is this process describing?
- A.** Attestation
 - B.** OAuth
 - C.** JWT
 - D.** Cookies
- 210.** You are setting up a new virtual machine. What type of virtualization should you use to coordinate instructions directly to the CPU?
- A.** Type B.
 - B.** Type 1.
 - C.** Type 2.
 - D.** No VM directly sends instructions to the CPU.

- 211.** Your organization must perform vast amounts of computations of big data overnight. To minimize TCO, you rely on elastic cloud services. The virtual machines and containers are created and destroyed nightly. What is the biggest risk to confidentiality?
- A.** Data center distribution
 - B.** Encryption
 - C.** Physical loss of control of assets
 - D.** Data scraping
- 212.** Your DevOps team decided to use containers because they allow running applications on any hardware. What is the first thing your team should do to have a secure container environment?
- A.** Install IPS.
 - B.** Lock down Kubernetes and monitor registries.
 - C.** Configure antimalware and traffic filtering.
 - D.** Disable services that are not required and install monitoring tools.
- 213.** You work in information security for a stock trading organization. You have been tasked with reducing cost and managing employee workstations. One of the biggest concerns is how to prevent employees from copying data to any external storage. Which of the following *best* manages this situation?
- A.** Move all operations to the cloud and disable VPN.
 - B.** Implement server virtualization and move critical applications to the server.
 - C.** Use VDI and disable hardware and storage mapping from a thin client.
 - D.** Encrypt all sensitive data at rest and in transit.
- 214.** You are exploring the best option for your team to read data that was written onto storage material by a device you do not have access to, and the backup device has been broken. Which of the following is the *best* option for this?
- A.** Type 1 hypervisor
 - B.** Type 2 hypervisor
 - C.** Emulation
 - D.** PaaS
- 215.** You are a security architect building out a new hardware-based VM. Which of the following would *least* likely threaten your new virtualized environment?
- A.** Patching and maintenance
 - B.** VM sprawl
 - C.** Oversight and responsibility
 - D.** Faster provisioning and disaster recovery

- 216.** GPS is built into cell phones and cameras, enabling coordinated longitude and latitude to be embedded in a machine-readable format as part of a picture or in apps and games. Besides physical coordinates of longitude and latitude, which of these will not be embedded in the metadata of a photo taken with a cell phone?
- A.** Names of businesses that are near your location
 - B.** Elevation
 - C.** Bearing
 - D.** Phone number
- 217.** Your CISO asked you to help review data protection, system configurations, and hardening guides that were developed for cloud deployment. He would like you to make a list of goals for security improvement based on your current deployment. What is the *best* source of information to help you build this list?
- A.** Pentesting reports
 - B.** CVE database
 - C.** Implementation guides
 - D.** Security assessment reports
- 218.** Management of your hosted application environment requires end-to-end visibility and a high-end performance connection while monitoring for security issues. What should you consider for the most control and visibility?
- A.** You should consider a provider with connections from your location directly into the applications cloud resources.
 - B.** You should have a private T1 line installed for this access.
 - C.** You should secure a VPN concentrator for this task.
 - D.** You should use HTTPS.
- 219.** As the IT director of a nonprofit agency, you have been challenged at a local conference to provide technical cloud infrastructure that will be shared between several organizations like yours. Which is the *best* cloud partnership to form?
- A.** Private cloud
 - B.** Public cloud
 - C.** Hybrid cloud
 - D.** Community cloud
- 220.** Your objectives and key results (OKRs) being measured for this quarter include realizing the benefits of a single-tenancy cloud architecture. Which one of these results is a benefit of a single-tenancy cloud service?
- A.** Security and cost
 - B.** Reliability and scaling
 - C.** Ease of restoration
 - D.** Maintenance

- 221.** With 80 percent of your enterprise in a VPC model, which of the following is *not* a key enabling technology?
- A.** Fast WAN and automatic IP addressing
 - B.** High-performance hardware
 - C.** Inexpensive servers
 - D.** Complete control over process
- 222.** You have a new security policy that requires backing up critical data offsite. This data must be backed up hourly. Cost is important. What method are you most likely to deploy?
- A.** File storage
 - B.** Electronic vaulting
 - C.** Block storage
 - D.** Object storage
- 223.** Your current data storage solution has too many vulnerabilities that are proprietary to the manufacturer who created your storage devices. This, combined with a lack of encryption, is leading you to choose cloud storage for your database over on-premises storage. By choosing cloud storage, you will gain encryption of the data, but you will also bring in which attribute to your architecture?
- A.** Identity
 - B.** Infrastructure
 - C.** Complexity
 - D.** Confidentiality
- 224.** You want to implement a technology that will verify an email originated from a particular user and that the contents of the email were not altered. Of the answers provided, which technology provides such a function?
- A.** Digital signature
 - B.** Symmetric encryption
 - C.** Asymmetric encryption
 - D.** Nonrepudiation
- 225.** Which of the following protocols could be used for exchanging information while implementing a variety of web services in your organization?
- A.** SOAP
 - B.** HTTP
 - C.** SNMP
 - D.** ASP

- 226.** Your CISO is concerned with the secure management of cryptographic keys used within the organization. She wants to use a system where the keys are broken into parts, and each part is encrypted and stored separately by contracted third parties. What is this process called?
- A.** Key objectives
 - B.** Key revenue
 - C.** Key escrow
 - D.** Key isolation
- 227.** Your VPN needs the strongest authentication possible. Your network consists of Microsoft servers. Which of the following protocols provide the most secure authentication?
- A.** EAP-TLS with smart cards
 - B.** SPAP
 - C.** CHAP
 - D.** LEAP
- 228.** You own a small training business with two classrooms. Your network consists of a firewall, an enterprise-class router, a 48-port switch, 1 printer, and 18 laptops in each classroom. The laptops are reimaged once a month with a golden patched image with up-to-date antivirus and antimalware. User authentication is two-factor with passwords and smart cards. The network is configured to use IPv4. You also have a wireless hotspot for students to connect their personal mobile devices. What could you improve on for a more resilient technical security posture?
- A.** Enhanced TLS controls
 - B.** Stronger user authentication
 - C.** Sufficient physical controls
 - D.** IPv6
- 229.** You are a network defender and are finding it difficult to keep up with the volume of network attacks. What can you leverage to help with early detection and response to these threats, especially new ones?
- A.** Machine learning
 - B.** SIEM
 - C.** DevSecOps
 - D.** Security as Code
- 230.** You need an encryption algorithm that offers easier key exchange and key management than symmetric offers. Which of the following is your *best* option?
- A.** Asymmetric
 - B.** Quantum
 - C.** Hashing
 - D.** Scytale

- 231.** Your company wants to begin using biometrics for authentication. Which of the following are not biometrics that can be verified by a system to give an individual access?
- A.** Facial recognition
 - B.** Iris recognition
 - C.** Retina recognition
 - D.** PIN recognition
- 232.** Laura is a proponent of using a distributed ledger to secure transactions. She wants to make it difficult to tamper with a single record because an attacker would need to change the block containing that record as well as those linked to it to avoid detection. Participants will have a private key assigned to their transactions that acts as a personal digital signature. What type of cryptographic system does Laura need to implement?
- A.** Homomorphic encryption
 - B.** Secure multiparty computation
 - C.** Blockchain
 - D.** Distributed consensus
- 233.** Felipe wants to use a protocol that allows a client to retrieve an element of a database without the owner of that database knowing which element was selected. If implemented securely, the client will only learn about the element they are querying for and nothing else preserving privacy. Which of the following provides the *best* solution?
- A.** Strong private information retrieval
 - B.** Secure function evaluation
 - C.** Private function evaluation
 - D.** Big data
- 234.** Augmented reality (AR) advances are exciting, and cybersecurity is now dealing with a vast amount of complexity. The adoption of AR brings an expanding landscape of new cybersecurity vulnerabilities. Consumers and businesses are grappling with big data breaches, and implementing effective cybersecurity measures is a necessity for modern businesses. Which of these is not an urgent or relevant cybersecurity issue involving AR?
- A.** Cloud structure
 - B.** Innovation outpacing secure development
 - C.** Wearable exposure
 - D.** Micro/nano technology
- 235.** Three-dimensional printers include computers and run software that could be vulnerable to security issues that bad actors can take advantage of. To mitigate this issue, 3D printing vendors need to make secure coding and design a core part of their development process. Printer owners should also consider doing which of these first?
- A.** Securely downloading plans for 3D printers
 - B.** Hardening their devices when possible and considering the security of the 3D production
 - C.** Encrypting SD cards used to hold all printing plans
 - D.** Cleaning the laser that melts the powdered material into objects layer by layer

- 236.** Naomi wants to use passwordless authentication in her corporate network. Which of the following statements is not true?
- A.** Linux supports passwordless SSH logins.
 - B.** Microsoft supports passwordless sign-in on Windows products and networks running Microsoft Active Directory.
 - C.** Passwordless authentication can be used only on mobile devices.
 - D.** Microsoft LDAP supports passwordless authentication through FIDO2 keys.
- 237.** You want your organization to benefit from artificial intelligence, but some in the application development department are confused about what AI actually is. Which statement is true?
- A.** Artificial intelligence and machine learning are the same.
 - B.** Machine learning and deep learning are the same.
 - C.** Machine learning leads to deep learning, which leads to artificial intelligence.
 - D.** Artificial intelligence parses big data to make decisions.
- 238.** Terry is heading a project to implement a chatbot on the homepage of your insurance company to move away from live agents. What technology will he most likely employ?
- A.** Natural language processing
 - B.** Biometrics
 - C.** Virtual reality
 - D.** Deep fake