

Chapter 1

Domain 1.0: General Security Concepts

THE COMPTIA SECURITY+ EXAM SY0-701 TOPICS COVERED IN THIS CHAPTER INCLUDE THE FOLLOWING:

✓ **Domain 1.0: General Security Concepts**

- 1.1 Compare and contrast various types of security controls
 - Categories (Technical, Managerial, Operational, Physical)
 - Control types (Preventive, Deterrent, Detective, Corrective, Compensating, Directive)
- 1.2 Summarize fundamental security concepts
 - Confidentiality, Integrity, and Availability (CIA)
 - Non-repudiation
 - Authentication, Authorization, and Accounting (AAA) (Authenticating people, authenticating systems, authorization models)
 - Gap analysis
 - Zero trust (control plane, data plane)
 - Physical security (bollards, access control vestibule, fencing, video surveillance, security guard, access badge, lighting, sensors)
 - Deception and disruption technology (honeypot, honeynet, honeyfile, honeytokens)
- 1.3 Explain the importance of change management processes and the impact to security
 - Business processes impacting security operations (approval process, ownership, stakeholders, impact analysis, test results, backout plan, maintenance window, standard operating procedure)



- Technical implications (allow lists/deny lists, restricted activities, downtime, service restart, application restart, legacy applications, dependencies)
- Documentation (updating diagrams, updating policies/procedures)
- Version control
- 1.4 Explain the importance of using appropriate cryptographic solutions
 - Public key infrastructure (PKI) (Public key, private, key, key escrow)
 - Encryption (Level, transport/communication, asymmetric, symmetric, key exchange, algorithms, key length)
 - Tools (Trusted Platform Module [TPM], Hardware security module [HSM], key management systems, secure enclave)
 - Obfuscation (Steganography, tokenization, data masking)
 - Hashing
 - Salting
 - Digital Signatures
 - Key stretching
 - Blockchain
 - Open public ledger
 - Certificates (certificate authorities, certificate revocation lists [CRLs], Online Certificate Status Protocol [OCSP], self-signed, third-party, root of trust, certificate signing request [CSR] generation, wildcard)

1. Felicia wants to deploy an encryption solution that will protect files in motion as they are copied between file shares as well as at rest, and also needs it to support granular, per-user security. What type of solution should she select?
 - A. Partition encryption
 - B. File encryption
 - C. Full-disk encryption
 - D. Record-level encryption
2. Valerie wants to use a certificate to handle multiple subdomains for her website, including the `sales.example.com` and `support.example.com` subdomains. What type of certificate should she use?
 - A. A self-signed certificate
 - B. A root of trust certificate
 - C. A CRL certificate
 - D. A wildcard certificate
3. What information is analyzed during a gap analysis?
 - A. Control objectives and controls intended to meet the objectives
 - B. Physically separate networks and their potential connection points
 - C. Compensating controls and the controls they are replacing
 - D. Security procedures and the policies they are designed to support
4. Susan's team has recommended an application restart for a production, customer-facing application as part of an urgent patch due to a security update. What technical implication is the most common concern when conducting an application restart?
 - A. Application configuration changes caused by the restart
 - B. Whether the patch will properly apply
 - C. Lack of security controls during the restart
 - D. The downtime during the restart
5. Using a tool like `git` is most frequently associated with what critical change management process?
 - A. Having a backout plan
 - B. Stakeholder analysis
 - C. Version control
 - D. Standard operating procedures (SOPs)
6. Jacob is concerned that the password used for one of his organization's services is weak, and he wants to make it harder to crack by making it harder to test possible keys during a brute-force attack. What is this technique called?
 - A. Master keying
 - B. Key stretching
 - C. Key rotation
 - D. Passphrase armoring

7. Log monitoring is an example of what control category?
 - A. Technical
 - B. Managerial
 - C. Operational
 - D. Physical
8. Rick wants to make offline brute-force attacks against his password file very difficult for attackers. Which of the following is not a common technique to make passwords harder to crack?
 - A. Use of a salt
 - B. Use of a pepper
 - C. Use of a purpose-built password hashing algorithm
 - D. Encrypting password plain text using symmetric encryption
9. Diffie-Hellman and RSA are both examples of what important encryption-related solution?
 - A. Rekeying
 - B. Certificate revocation protocols
 - C. Key exchange algorithms
 - D. Key generation algorithms
10. Sally wants to ensure that her change management process includes a procedure for what to do if the change fails. What should she create to handle this possibility?
 - A. An impact analysis
 - B. A backout plan
 - C. A regression test
 - D. A maintenance window
11. Theresa is concerned that her scheduled maintenance window may extend beyond the allocated time due to an unexpected issue. What element from the CIA triad is she concerned about?
 - A. Criticality
 - B. Accessibility
 - C. Integrity
 - D. Availability
12. Alaina is concerned about vehicles that might impact her organization's backup generator. What should she install to prevent both inadvertent and purposeful vehicle impacts on a generator installed outside her building near a parking lot?
 - A. A speed bump
 - B. An access control vestibule
 - C. Bollards
 - D. A chain-link fence

- 13.** Ben has deployed a data loss prevention (DLP) tool that inspects data and flags specific data types for review before emails containing it are sent outside the organization. What control type best describes this type of solution?
- A.** Managerial
 - B.** Detective
 - C.** Corrective
 - D.** Preventive
- 14.** What type of control is a policy or procedure?
- A.** Directive
 - B.** Corrective
 - C.** Detective
 - D.** Preventive
- 15.** Murali has deployed a file integrity monitoring tool and has configured alerts to notify him if files are modified. What control type best describes this solution?
- A.** Preventive
 - B.** Deterrent
 - C.** Directive
 - D.** Detective
- 16.** Charles wants to reduce the threat scope of compromised credentials. What type of the following security controls is best suited to meeting this need?
- A.** Single sign-on
 - B.** Federation
 - C.** Zero trust
 - D.** Multifactor authentication (MFA)
- 17.** Carol wants to obfuscate data that is contained in her database. She wants to be able to refer to the data elements without having the actual data exposed. What type of obfuscation option should she select?
- A.** Tokenization
 - B.** Encryption
 - C.** Data masking
 - D.** Data randomization
- 18.** What key is used to decrypt information sent by another individual between two people using public key encryption?
- A.** The recipient's private key
 - B.** The recipient's public key
 - C.** The sender's private key
 - D.** The sender's public key

19. Selah's organization has recently experienced a breach and the private keys for her organization's certificates were exposed. What should she immediately do?
- A. Reissue the certificates with changed hostnames and other details.
 - B. Replace the certificates with self-signed certificates until they can be replaced by the vendor.
 - C. Revoke the certificates and place them on a certificate revocation list.
 - D. Replace the certificates with wildcard certificates.
20. Which of the following is not a major concern related to downtime caused by patching and system updates?
- A. Attackers compromising the system or service while it is offline
 - B. Security systems or functions being offline during restart or shutdown processes
 - C. Unexpected extended downtime
 - D. Dependencies between systems or services related to downtime
21. Joanna wants to ensure that the most current version of each component in her application is deployed. What change management process will help the most with this requirement?
- A. Dependency mapping
 - B. Version control
 - C. Impact analysis
 - D. Allow and deny lists
22. Greg wants to implement a version control system to ensure that changes are made in ways that will not cause problems for his organization's critical software. Which of the following is not a common feature of version control systems designed for software source code?
- A. Atomic operations
 - B. File locking
 - C. Regression testing
 - D. Tagging and labeling
23. Christina wants to implement a physical security control that has the greatest flexibility in how it is applied because she knows that exceptions to security practices may be required at times. Which of the following solutions has the greatest flexibility?
- A. Video surveillance
 - B. Security guards
 - C. Access badges
 - D. Access control vestibules
24. Lisa wants to ensure that theft of a device will not lead to exposure of the data contained on the device if the device is locked or turned off. What type of encryption should she select to best ensure this?
- A. Volume-level encryption
 - B. Full-disk encryption
 - C. File-level encryption
 - D. Partition-level encryption

25. Mahmoud has been asked to implement an allow list for websites that users at his company can visit. What concern should he bring up to management due to this request?
- A. Allow lists cannot be used for websites.
 - B. Allow lists are overly permissive and are likely to allow unwanted sites to be visited.
 - C. Using an allow list for websites will take a lot of time to maintain.
 - D. Using an allow list for websites is easily bypassed.
26. Which of the following change management processes does not commonly directly involve stakeholders outside of the IT organization?
- A. Impact analysis
 - B. Building the backout plan
 - C. The change approval process
 - D. Determining the maintenance window
27. What hardware component is used to generate, store, and manage cryptographic keys?
- A. A CPU
 - B. A NSA
 - C. A TPM
 - D. A CCA
28. Chris wants to check to see if a certificate has been revoked. What protocol can he use to validate the current status of a certificate?
- A. TLS
 - B. OCRS
 - C. SSL
 - D. OCSP
29. Brian's organization uses a process where a secure module boots systems, then monitors them as each boot stage proceeds. It validates each signed boot stage and reports on whether the boot process was correct or not when complete. What is the secure module used to verify these stages called?
- A. A secure initiation manager
 - B. A root of trust
 - C. A boot hash
 - D. A cryptographic boot manager
30. A vulnerability scan shows that an embedded device that Alice is responsible for has a vulnerability. She knows the vendor is no longer in business and that there is no updated firmware or software update for the device. To resolve the issue, Alice places a firewall between the device and the rest of the network and creates rules that prevent the vulnerable service from being available to other devices. What type of control has Alice deployed?
- A. A directive control
 - B. A compensating control
 - C. A detective control
 - D. A procedural control

31. Jason knows that his Apple system uses a separate portion of its SoC (system on chip) to store keys and biometric information. What is this specialized component called?
- A. A TPM
 - B. A HSM
 - C. A secure enclave
 - D. A screened subnet
32. What change management term is used to describe the processes that an organization uses for each change that is made to ensure that a consistent process is used?
- A. Standard operating procedures
 - B. A change plan
 - C. Fixed operating procedures
 - D. A backout plan
33. Jack knows that there are three common types of database encryption. Which of the following is not a common type of database encryption?
- A. Sensitivity-based encryption
 - B. Transparent data encryption
 - C. Field-level encryption
 - D. Column-level encryption
34. Ujamaa wants to conduct a gap analysis as part of his security efforts. Which of the following best describes what he will analyze?
- A. Which services are not configured properly
 - B. Whether current patches are installed on all systems
 - C. The security program as implemented versus best practices
 - D. Legal requirements versus the security program
35. Brandon wants to deploy a detective control that will help him with physical security threats. Which of the following fits his needs?
- A. Fencing
 - B. Lighting
 - C. Video surveillance
 - D. Bollards
36. Jack has deployed a system that appears to attackers to be a vulnerable system. The system is specifically designed to capture information and data from attacks to allow for later analysis. What type of tool has Jack deployed?
- A. A tarpit
 - B. A honeypot
 - C. A beehive
 - D. An intrusion detection system

- 37.** Renee wants to ensure that her logs support nonrepudiation. What should she do to ensure this?
- A.** Encrypt, then hash the logs.
 - B.** Hash the logs and then digitally sign them.
 - C.** Digitally sign the log file, then encrypt it.
 - D.** Hash, then encrypt the logs.
- 38.** Isaac wants to deploy sensors to detect intruders in a facility, but he is concerned about the sensors being overly sensitive. What type of sensor is best suited to detecting intruders in an open office environment without significant expense or issues with sensitivity?
- A.** Infrared
 - B.** Pressure
 - C.** Microwave
 - D.** Ultrasonic
- 39.** Wayne wants to allow systems to claim identities as part of his AAA process. Which of the following is most commonly used to identify both individuals and systems?
- A.** Tokens
 - B.** Smartcards
 - C.** Certificates
 - D.** Usernames
- 40.** What are considerations like database and network connectivity, authentication system access, and network time availability considered in the context of change management processes?
- A.** Allowed services
 - B.** Standard operating procedures
 - C.** Denied services
 - D.** Dependencies
- 41.** What role does the policy engine play in a zero-trust environment?
- A.** It creates new administrative policies based on user behavior.
 - B.** It grants access based on policies created by administrators and based on security systems data.
 - C.** It enforces policies by monitoring connections between clients and servers.
 - D.** It suggests new administrative policies based on usage patterns for adoption by the organization.
- 42.** Which of the following is not a common post-change activity found in change management practices?
- A.** Updating diagrams
 - B.** Updating procedures
 - C.** Updating policies
 - D.** Updating contracts

43. Which of the following activities should Alaina not restrict as part of her preparation for a change window?
- A. Patching
 - B. Scaling clustered systems up or down
 - C. Changing hostnames
 - D. Modifying database configurations

44. What two key features define blockchain ledgers?
- A. They are immutable and nontransferable.
 - B. They are shared and can be modified by a vote among all participants.
 - C. They are unique to each participant and are atomic.
 - D. They are shared and immutable.

45. Damian issues the following command on his Linux server:

```
openssl req -new -newkey rsa:2048 -nodes -keyout exampleserver.  
key -out exampleserver.csr
```

What has he done?

- A. Created a certificate signing request
 - B. Created a certificate revocation request
 - C. Signed a certificate signing request
 - D. Updated the OCSP record for a certificate
46. Nick's organization sets aside Saturday nights from 2 a.m. to 4 a.m. for scheduled maintenance. What is this type of reserved time typically called?
- A. Allocated downtime
 - B. A maintenance window
 - C. An unscheduled outage
 - D. An allowed outage
47. Megan wants to assess the impact of a change as part of her change management process. Which of the following is most likely to help her assess impact?
- A. A backout plan
 - B. An estimate of the downtime expected
 - C. A list of stakeholders
 - D. A list of dependencies for impacted systems
48. Jared wants to estimate the downtime that will result as part of a planned change. Which of the following methods will most effectively help him estimate downtime?
- A. Average the downtime from other recent changes.
 - B. Contact the vendor for time estimates for the change.
 - C. Perform the change in a test environment.
 - D. Use a fixed maintenance window.

49. An encryption method in which all participants have the same key is known as which of the following types of encryption?
- A. Shared hashing
 - B. Asymmetric encryption
 - C. Symmetric encryption
 - D. Universal encryption
50. What important encryption challenge does asymmetric encryption help with by using public keys?
- A. Evil twins
 - B. Collision resistance
 - C. Key length
 - D. Key exchange
51. Rick's cloud provider offers a dedicated hardware security module. Which of the following capabilities is it unlikely to offer?
- A. Validating secure boot processes
 - B. Key generation
 - C. Encrypting and decrypting data
 - D. Creating digital signatures
52. Michelle believes that an image she has discovered in an attacker's directory of files contains additional information that has been hidden in it. What is this type of obfuscation called?
- A. Steganography
 - B. Image hashing
 - C. PNG warping
 - D. Image blocking
53. Which of the following is not a common transport encryption protocol?
- A. TLS
 - B. IPSec
 - C. SAML
 - D. SSH
54. What technology is record-level encryption most commonly associated with?
- A. Stored audio files
 - B. Databases
 - C. Physical disks
 - D. Removable storage

55. Yasmine submits the Windows BitLocker key to a central repository after she encrypts the machine. The central repository allows files to be uploaded, but not read, and is protected with access requiring special permissions. What type of solution is Yasmine's company using?
- A. A hardware security module
 - B. Perfect forward secrecy
 - C. Key escrow
 - D. Private keys
56. Valerie wants to authenticate her systems using her AAA system. Which of the following options is best suited to system authentication?
- A. Asymmetric authentication
 - B. Certificate-based authentication
 - C. Symmetric authentication
 - D. PIN-based authentication
57. Valentine wants to detect if an intruder has accessed a secured file server. Which of the following techniques will work best with a data loss prevention tool to identify data exfiltration?
- A. A honeypot
 - B. A honeynet
 - C. A honeyfile
 - D. A honeytokens
58. Jason has recommended that additional lighting be put in place on the exterior of his building as part of a security upgrade. What type of control is lighting?
- A. Operational
 - B. Deterrent
 - C. Corrective
 - D. Technical
59. Which of the following controls is typically the most expensive to implement?
- A. Bollards
 - B. Access control vestibules
 - C. Security guards
 - D. Access badges
60. Frankie wants to validate the integrity of a file by comparing it against an original copy. Which of the following solutions both fulfills this requirement and avoids known security issues?
- A. Hash the original file and the current file using MD5 and compare the hashes.
 - B. Hash the original file and the current file using SHA-1 and compare the hashes.
 - C. Hash the original file and the current file using SHA-256 and compare the hashes.
 - D. Hash the original file and the current file using AES and compare the hashes.

61. Joanna's organization has a policy that requires a user's password to be immediately reset to lock accounts if the account is determined to have been successfully phished. What type of control is this?
- A. A detective control
 - B. A directive control
 - C. A compensating control
 - D. A preventive control
62. Jackie wants to implement an AAA system for her network. What AAA protocol is commonly used for network devices?
- A. OpenID
 - B. SAML
 - C. RADIUS
 - D. TANGENT
63. Scott wants to automate policy creation in his zero-trust environment's policy engine. Which of the following is not a typical component for automated data and event-driven policy management?
- A. A SIEM
 - B. Threat feeds
 - C. Infrared sensor data
 - D. EDR tools
64. Valerie's organization has deployed a zero-trust solution, and Valerie receives an authentication prompt when she is attempting to access a file server. What component of the zero-trust architecture is she interacting with?
- A. A policy enforcement point
 - B. A policy administrator
 - C. The policy engine
 - D. The trust manager
65. Matt is assessing his organization's zero-trust model against the NIST Zero Trust Maturity Model. Which of the following is not a common element of zero-trust systems that would be assessed as part of the model?
- A. Identity
 - B. Business model
 - C. Networks
 - D. Devices
66. Quentin wants to deploy a single sign-on system to allow his users to log in to cloud services. Which of the following technologies is he most likely to deploy?
- A. OpenID
 - B. Kerberos
 - C. LDAP
 - D. TACACS+

67. Marty wants to deploy a corrective control to deal with a recently compromised system. Which of the following would be considered a corrective control?
- A. Patching the vulnerability that allowed the compromise to occur
 - B. Deploying full-disk encryption
 - C. Deploying an endpoint detection and response (EDR) tool
 - D. Enabling logging and sending logs to a SIEM
68. What important encryption feature is not supported by symmetric encryption?
- A. Confidentiality
 - B. Integrity
 - C. Nonrepudiation
 - D. Authentication
69. Theresa wants to use a cloud-hosted security solution that will allow her to safely store and manage secrets. What type of solution should she select?
- A. A TPM
 - B. A CA
 - C. A KMS
 - D. A CSR
70. Joanna is reviewing her account information on an e-commerce website and sees her credit card number displayed as XXXX-XXXX-XXXX-1234. What type of data obfuscation is in use?
- A. Hashing
 - B. Data masking
 - C. Field encryption
 - D. Tokenization
71. Amanda's organization wants to use a decentralized blockchain to store data. Which of the following is true about a decentralized blockchain?
- A. No individual or group controls the blockchain.
 - B. Only cryptocurrency-related data can be stored in a blockchain.
 - C. Blockchain data can be changed after being stored by the original submitter.
 - D. Blockchain ledgers are stored on central servers chosen by regular elections among blockchain participants.
72. What role does a subordinate CA have in a CA hierarchy?
- A. Subordinate CAs issue certificates based on subdomains.
 - B. Subordinate CAs provide control over certificate issuance while avoiding the cost of being a root CA.
 - C. Subordinate CAs validate root CA activities to ensure auditability.
 - D. Subordinate CAs review certificate signing requests before forwarding them to the root CA.

73. Which of the following sensor types is commonly used to detect footsteps?
- A. Infrared
 - B. Pressure
 - C. Microwave
 - D. Ultrasonic
74. Which of the following is not a managerial control?
- A. Risk assessments
 - B. Including security in change management processes
 - C. Security planning exercises
 - D. Implementing firewalls
75. What purpose do third-party certificates serve for customers of cloud services?
- A. They reduce costs by using bring-your-own certificates.
 - B. They allow certificates for domains other than the service provider's domain.
 - C. They provide control over cryptographic security for the customer.
 - D. They allow more flexibility in TLS version selection.
76. Which of the following is not a common control focused on availability?
- A. Uninterruptible power systems
 - B. Redundant Internet connectivity
 - C. Disk encryption
 - D. Load balancers
77. What term describes a collection of honeypots on a network intended to capture information about cybersecurity threats?
- A. A honeyfarm
 - B. A honeynet
 - C. A honeycluster
 - D. A darknet
78. Skip wants to implement a deterrent control to prevent physical security issues for his organization. Which of the following controls should he select?
- A. A fence
 - B. A generator
 - C. Access badges
 - D. A camera system
79. What holds the position of the root of trust in a certificate chain?
- A. A hardened hardware device
 - B. A TPM
 - C. A root certificate
 - D. A wildcard certificate

- 80.** Jill needs to explain the concept of open public ledgers to her organization as management wants to adopt a blockchain-based system. What should she tell them about access to the ledger?
- A.** Members must be added by a vote of all current members.
 - B.** Anyone can join at any time.
 - C.** Members must be added by a vote of more than 51 percent of current members.
 - D.** Ledgers are public but membership is private and controlled by the creator of the ledger.
- 81.** Olivia wants to use a self-signed certificate in her test environment for her organization's services to save money on commercial certificates. What warning should her team give her about the use of self-signed certificates in a test environment?
- A.** Certificate root of trust validation attempts will fail if implemented.
 - B.** Self-signed certificates cannot be used for external users to support SSL.
 - C.** Self-signed certificates cannot be used for internal users to support SSL.
 - D.** Browsers will not allow self-signed certificates to be used when browsing sites.
- 82.** Amanda is concerned about issues with dependencies that may be found during her pending change. What practice should she implement to help ensure unexpected dependency issues are not encountered?
- A.** Update organizational policies and procedures before the change.
 - B.** Update functional diagrams before the change.
 - C.** Validate the change in a test environment.
 - D.** Document legacy applications that may create dependencies.
- 83.** Lucca has implemented an authentication scheme that relies on ticket-granting tickets as part of the authentication process. What common authentication service has he implemented?
- A.** TACACS+
 - B.** Kerberos
 - C.** MS-CHAP
 - D.** EAP
- 84.** Jocelyn wants to select a modern encryption algorithm for use in her organization. Which of the following is a currently recommended encryption algorithm?
- A.** AES-256
 - B.** SHA1
 - C.** DES
 - D.** Blowfish
- 85.** Elizabeth wants to classify the following controls by their category. What category best describes lighting, fences, bollards, and access control vestibules?
- A.** Technical
 - B.** Managerial
 - C.** Operational
 - D.** Physical

86. Jack wants to ensure the integrity of a file that he is sending to a third party via email. How can he provide the integrity of a file to an organization that he has not done business with before?
- A. Encrypt the file and send it to them.
 - B. Digitally sign the file.
 - C. Send a hash of the file in a separate email.
 - D. Email the file size and original name in a separate email.
87. Annie notices that her browser shows that the certificate for the site she is visiting is not valid. After performing some checks, she sees that the certificate is on the CA's certificate revocation list. Which of the following is not a reason for a certificate to be on a CRL?
- A. The CA is compromised.
 - B. The certificate's private key was compromised.
 - C. The certificate was signed with a stolen key.
 - D. The certificate expired.
88. Mohinder wants to use modern, secure hashing algorithms to validate files against known good originals. Which of the following hashing algorithms should he select?
- A. MD5
 - B. SHA-1
 - C. AES-256
 - D. SHA-256
89. Derrick wants to validate an encrypted and digitally signed message sent using asymmetric encryption. What does he need from the sender to validate the message?
- A. The sender's private key
 - B. Derrick's private key
 - C. The sender's public key
 - D. Derrick's public key
90. The major patch release that Susan's team installed has failed, resulting in a nonworking service. What should her team do according to change management best practices?
- A. Declare an outage.
 - B. Follow the documented backout plan.
 - C. Restore from backups to the previous version.
 - D. Uninstall the patch and validate service function.
91. The web server that Angela's organization manages was recently compromised and the SSL certificate's private key was accessed by attackers. Angela's team has completed remediation and has created a new CSR, including a new private key that they have secured. What type of control type best describes the creation of a new key and certificate in this circumstance?
- A. Corrective
 - B. Compensating
 - C. Deterrent
 - D. Detective

92. Mikayla's zero-trust system has received a request for access with an identity, and the basic criteria for access have been met. What should the system do next before providing access to the resource requested?
- A. Check the remote system's security status.
 - B. Require reauthentication using MFA.
 - C. Check the user's rights to ensure they can access the resource.
 - D. Determine its level of confidence in the request.
93. Charles sets up an RDP server on an isolated network segment and places a file on it called `passwords.xlsx`. He then configures his IPS and DLP systems to monitor for that file exiting the network segment. What type of tool has Charles deployed?
- A. A honeyfile
 - B. A SQL trap
 - C. A red flag
 - D. A trigger file
94. Lucca is using precomputed rainbow tables to attempt to crack hashed passwords from a data breach. He knows that two users have the same password, but the hashes do not match. What password hash security technique has Lucca most likely encountered?
- A. Password encryption
 - B. Salting
 - C. Hash rotation
 - D. Password mismatching
95. What operating system is commonly associated with secure enclaves?
- A. Windows
 - B. iOS
 - C. Linux
 - D. Android
96. Isaac is concerned that the passwords that his users are creating are too short and can be easily brute-forced if their hashes were compromised. Rather than make his users remember longer passwords, he would like to implement a technical solution to help make the hashes more resistant to cracking. What solution can he use to help with this?
- A. Implement pass-the-hash algorithms.
 - B. Use a collision-resistant hashing algorithm.
 - C. Implement key stretching techniques.
 - D. Encrypt passwords rather than hashing them.

97. Christina wants to implement access badges printed with picture IDs for her organization, but she wants to use a wireless reader. What access badge technology is commonly implemented in scenarios like this?
- A. Wi-Fi-enabled access badges
 - B. RFID access badges
 - C. Bluetooth-enabled access badges
 - D. NFC access badges
98. Kendra's vulnerability management team has discovered that Internet of Things (IoT) devices deployed a few years ago to monitor temperatures for critical refrigerated equipment are vulnerable to a new attack. After reviewing the issue, her team has discovered that the devices are no longer supported and that the manufacturer has gone out of business. They suggest moving the devices to an isolated network to help protect them. What type of control has Kendra's team suggested?
- A. A corrective control
 - B. A compensating control
 - C. A confidentiality control
 - D. A coordinated control
99. Which of the following is not a common factor in adaptive authentication for zero trust?
- A. Where the user is logging in from
 - B. Whether the user has logged in recently from another device
 - C. What device the user is logging in from
 - D. If the device is configured correctly
100. Juan's organization is designing their zero-trust model. Which of the following statements is true for network security zones?
- A. All communication is secured, regardless of the network security zone it occurs in.
 - B. Communication receives additional security in low-trust zones.
 - C. Communication receives less security in high-trust zones.
 - D. All zero-trust networks are considered secured zones.
101. What advantage do microwave sensors have over infrared sensors?
- A. They can detect heat signatures.
 - B. They are cheaper than infrared sensors.
 - C. They can penetrate some types of walls.
 - D. They do not interfere with sensitive equipment.

- 102.** Isaac is conducting a physical penetration test and wants to bypass an access control vestibule. What must he accomplish?
- A.** He needs to persuade an individual to allow him to follow them through a single door.
 - B.** He needs to acquire an individual's access card.
 - C.** He needs to persuade an individual to allow him to follow them through two doors in a row.
 - D.** He needs to acquire the individual's access PIN.
- 103.** Rachel wants to select an obfuscation method that will allow her customer service representatives to validate customer identities without providing full access to customer data. What should she select?
- A.** Tokenization
 - B.** Data masking
 - C.** Steganography
 - D.** Hashing
- 104.** Valerie's manager has informed her that version control must be implemented for her development team's work. Which of the following is not a common, security-related reason for version control?
- A.** To help with patching
 - B.** To track each contributor's workload
 - C.** To ensure the proper version is deployed
 - D.** To help with change management
- 105.** Jackie's change management process involves reporting functional validation test results to stakeholders. Which of the following is not a common stakeholder or stakeholder group for an application upgrade?
- A.** Application administrators
 - B.** Service owners
 - C.** System administrators
 - D.** Auditors
- 106.** How many keypairs are required for four individuals to communicate securely using asymmetric encryption?
- A.** 1
 - B.** 4
 - C.** 8
 - D.** 12

- 107.** Michelle wants to store secrets for her organization in a cloud service. She wants to ensure the greatest level of security for her organization, and she is willing to spend more money to provide that security. What solution should she look for?
- A.** A shared cloud TPM
 - B.** A shared cloud HSM
 - C.** A dedicated hardware cloud TPM
 - D.** A dedicated hardware cloud HSM
- 108.** Murali wants to digitally sign a file. What key does he need to sign it?
- A.** The recipient's private key
 - B.** His private key
 - C.** The recipient's public key
 - D.** His public key
- 109.** What information is necessary for a certificate to be identified properly in an OCSP request?
- A.** The domain name
 - B.** The original requestor's name
 - C.** The certificate's serial number
 - D.** The identifier for the open public ledger entry
- 110.** Rick checks the certificate for the site he is viewing and sees that it reads *.example.com. What type of certificate is this, and why is it in use?
- A.** It is a self-signed certificate, and it is used for testing purposes.
 - B.** It is a wildcard certificate and is used for testing purposes.
 - C.** It is a wildcard certificate and is used for multiple subdomains.
 - D.** It is a self-signed certificate and is used for multiple subdomains.
- 111.** John wants to write a procedure that addresses what to do if an employee inadvertently discloses their password due to a phishing attempt. What type of control is John considering?
- A.** A directive control
 - B.** A proactive control
 - C.** A deterrent control
 - D.** A preventive control
- 112.** Adam has been asked to implement an allow list for websites that his servers can visit. What concern should he raise about the implementation of allow lists?
- A.** Allow lists can be difficult to manage and cause failures if sites that are needed are not added.
 - B.** Allow lists do not prevent sites from being visited if they are not on the allow list.
 - C.** Allow lists cannot be configured to allow entire domains to be visited, creating significant overhead.
 - D.** Allow lists are prone to error, allowing unwanted sites to be added.

- 113.** Jim wants to implement an authentication framework for his wireless network. Which of the following is most commonly used for wireless network authentication?
- A.** EAP
 - B.** MS-CHAP
 - C.** Kerberos
 - D.** LDAP
- 114.** Gary is preparing change management documentation for an application restart after patching. What step should immediately follow the application restart?
- A.** Validation testing
 - B.** Documenting the change occurred
 - C.** Updating version control
 - D.** Vulnerability scanning
- 115.** Anna has been told that her organization has deployed microwave sensors in the organization's warehouses. What are microwave sensors most frequently used to detect?
- A.** Motion
 - B.** Glass break
 - C.** Heat signatures
 - D.** Pressure
- 116.** When is data on a drive that uses full-disk encryption at the greatest risk?
- A.** During the system boot process
 - B.** When the system is off
 - C.** When the system is logged in and in use
 - D.** When the system is being shut down
- 117.** Alex has configured full-disk encryption for laptops that his organization issues to employees. What cybersecurity objective does this primarily support?
- A.** Confidentiality
 - B.** Availability
 - C.** Authenticity
 - D.** Integrity
- 118.** What process reviews control objectives for an organization, system, or service to determine if controls do not meet the control objectives?
- A.** A penetration test
 - B.** A gap analysis
 - C.** A Boolean analysis
 - D.** A risk analysis

- 119.** Frank configures an access control list to ensure that only specific IP addresses are able to connect to a service. What type of control has he deployed?
- A.** Managerial
 - B.** Physical
 - C.** Technical
 - D.** Operational
- 120.** Annie has recently implemented a video surveillance system for her organization. What is the largest driver for new ongoing costs for an unmonitored video surveillance system?
- A.** Camera maintenance
 - B.** The ongoing cost of storage
 - C.** Security guards
 - D.** Licensing
- 121.** Henry's organization has recently experienced a ransomware attack and is restoring backups from a secure backup system. What type of security control is Henry using?
- A.** A preventive control
 - B.** A directive control
 - C.** A compensating control
 - D.** A corrective control
- 122.** What data obfuscation technique relies on a lookup table that allows you to match the data you want to secure to a randomly generated value to ensure that the actual value is not easily accessible?
- A.** Hashing
 - B.** Tokenization
 - C.** Randomization
 - D.** Masking
- 123.** What challenge drives the need for key exchange mechanisms?
- A.** The number of keys required for symmetric encryption
 - B.** The need to determine if a key is public
 - C.** The need to exchange keys in a way that prevents others from obtaining a copy
 - D.** The need to securely return keys to their owner after they are traded
- 124.** Jackie is performing an impact analysis prior to a large-scale change her team is preparing to implement. Which of the following groups is not typically part of the impact analysis?
- A.** Stakeholders
 - B.** System administrators
 - C.** Service owners
 - D.** Legal counsel

- 125.** Ilya wants to create a certificate signing request. Which of the following is not a typical part of a CSR?
- A.** The common name of the server
 - B.** The organization's legal name
 - C.** A contact email address
 - D.** The organization's phone number
- 126.** Before Tony stores a password hash, he appends a string of characters that is unique to each password generated using an algorithm he created. What technique is Tony using to help protect his password hashes?
- A.** Tokenization
 - B.** Steganography
 - C.** Salting
 - D.** Key stretching
- 127.** Which of the following is not a step taken when a transaction is entered in a blockchain?
- A.** The value of the block is determined.
 - B.** The transaction is sent to a peer-to-peer network of computers.
 - C.** The transaction is validated using equations.
 - D.** A transaction history is maintained as part of the blockchain.
- 128.** Kent wants to encrypt network traffic in transit. What cryptographic protocol is most frequently used to add encryption to existing protocols?
- A.** S/MIME
 - B.** TLS
 - C.** MPLS
 - D.** SSH
- 129.** Which of the following is not a common concern in change management processes related to legacy applications?
- A.** Lack of vendor support
 - B.** Lack of patches and updates
 - C.** Ongoing licensing costs
 - D.** Availability of third-party or consultant expertise
- 130.** Elaine wants to document the technical concerns that dependencies create as part of her change management process. Which of the following concerns is the most common when dependencies are encountered as part of change management?
- A.** Documenting the dependencies to ensure they are addressed
 - B.** Removing the dependencies as part of the change
 - C.** Patching the dependencies in addition to the main application
 - D.** Updating diagrams related to the dependencies

- 131.** Gary has implemented record-level encryption for his database. How many keys will he use in a typical implementation of record-level encryption?
- A.** One key per record
 - B.** One key per column
 - C.** One key per table
 - D.** One key per database
- 132.** Justin's laptop is part of his organization's zero-trust architecture. What term is used to refer to a device like a laptop, desktop, or mobile device in a zero-trust design?
- A.** A subject
 - B.** A policy engine
 - C.** A service provider
 - D.** A policy application point
- 133.** Susan's organization has deployed a zero-trust architecture. Which of the following zero-trust control plane components uses rules to determine who can access a service based on the security status of their system, threat data, and similar information?
- A.** Adaptive authorization
 - B.** Threat scope reduction
 - C.** Policy-driven access control
 - D.** Secured zones
- 134.** Scott wants to implement OCSP as part of an application he is creating. What will he implement?
- A.** A corrective control security process
 - B.** Certificate status checking
 - C.** Transport encryption
 - D.** Full-disk encryption
- 135.** Which of the following is not a common reason to implement key escrow?
- A.** Regulatory compliance
 - B.** Providing access to encrypted data for administrative reasons
 - C.** Providing access to encrypted data in emergencies
 - D.** Preventing the need for key rotation after a user leaves
- 136.** Yariv discovers that he has exposed his private key to other users in his organization by sending it via email instead of his public key. What should he do?
- A.** Ask the other users to delete any copies of his private key that they may have.
 - B.** Immediately add his key to a CRL and reissue the key.
 - C.** Create a new keypair and notify others that he has replaced his keypair.
 - D.** Continue to operate as normal as long as the private key was not used maliciously.

- 137.** What happens if a mistake is made and an incorrect transaction is entered into the open public ledger in a blockchain?
- A.** The transaction is reversed once it is discovered, and the original transaction is removed from the record.
 - B.** A new transaction must be processed, and both transactions remain in the record.
 - C.** The original transaction is updated and becomes the new record.
 - D.** An error block must be mined and labeled with the transaction number and error details.
- 138.** Which of the following activities will not typically result in a need to update policies and procedures?
- A.** Deploying a new application
 - B.** Installing patches for an existing application
 - C.** Conducting a lessons learned exercise after an incident
 - D.** Changes in regulations
- 139.** Hrant's organization wants to ensure that staff members use both something they know and something they have as part of their physical access control scheme. Which of the following solutions meets that requirement?
- A.** Security guards and access badges
 - B.** Keys and access control vestibules
 - C.** Access badges and PINs
 - D.** Security guards and access control vestibules
- 140.** Julia wants to detect if an intruder enters a space using a sensor system. Which of the following is not typically used to detect intruders?
- A.** Infrared sensors
 - B.** Pressure sensors
 - C.** Microwave sensors
 - D.** Ultrasonic sensors
- 141.** Which of the following is not true for a secure cryptographic hash system?
- A.** Hashes are a one-way function.
 - B.** Hashes generate a fixed length output.
 - C.** Hashes may generate the same output for multiple inputs.
 - D.** Hashes are commonly used to verify the integrity of files.
- 142.** Casey wants to prevent tailgating attacks on her datacenter. What type of physical security solution should she put in place?
- A.** Video surveillance
 - B.** Bollards
 - C.** An access control vestibule
 - D.** Access badges

- 143.** As Casey continues to work to secure her datacenter, she decides to deploy access badges. What technique will provide the greatest assurance that a stolen or cloned access badge will not allow an attacker access?
- A.** Use barcode-based badges.
 - B.** Require a PIN along with the badge.
 - C.** Use RFID-based badges.
 - D.** Include a picture of the user on the badge.
- 144.** What term describes the function of digital signatures related to proving that the signature was provided by the owner of a given private key?
- A.** Ledger-based validation
 - B.** Nonrepudiation
 - C.** Key stretching
 - D.** Authentication
- 145.** John wants to send his public key to another user. What steps are necessary to do so?
- A.** The key must be sent using Diffie–Hellman.
 - B.** The key can simply be sent via email or other means.
 - C.** The key must be sent using RSA.
 - D.** The key must be signed, then sent via email or other means.
- 146.** Tracy wants to use the most secure salting solution she can. Which of the following options will provide the most secure salt?
- A.** Set a salt value and store it in a database.
 - B.** Set a salt value and store it in the program code.
 - C.** Generate a unique salt for each hashed entry.
 - D.** Generate a unique salt value every time a value is used.
- 147.** Bob conducts a periodic risk assessment of his organization. What category of security control is this?
- A.** Technical
 - B.** Managerial
 - C.** Operational
 - D.** Physical
- 148.** After a breach, Jackie removes malicious software from a server that she is responsible for. What control type should she classify this as?
- A.** Preventive
 - B.** Corrective
 - C.** Compensating
 - D.** Deterrent

- 149.** What can a root SSL (TLS) certificate do?
- A.** Remove a certificate from a CRL
 - B.** Generate a signing key and use it to sign a new certificate
 - C.** Authorize new CA users
 - D.** Allow key stretching
- 150.** Christina wants to authenticate individuals as part of her AAA implementation. What will she need to do to authenticate users?
- A.** Match users to roles and ensure that rights are assigned.
 - B.** Conduct biometric enrollments for every user.
 - C.** Use identity proofing for each user she creates.
 - D.** Ensure that users provide an identity and one or more authentication factors.